10-1-2010

Nonlocal quantum information in bipartite quantum error correction

Mark M. Wilde
Université McGill

David Fattal
Hewlett Packard Laboratories

Recommended Citation

Nonlocal quantum information in bipartite quantum error correction

Mark M. Wilde · David Fattal

Abstract We show how to convert an arbitrary stabilizer code into a bipartite quantum code. A bipartite quantum code is one that involves two senders and one receiver. The two senders exploit both nonlocal and local quantum resources to encode quantum information with local encoding circuits. They transmit their encoded quantum data to a single receiver who then decodes the transmitted quantum information. The nonlocal resources in a bipartite code are ebits and nonlocal information qubits and the local resources are ancillas and local information qubits. The technique of bipartite quantum error correction is useful in both the quantum communication scenario described above and in fault-tolerant quantum computation. It has application in fault-tolerant quantum computation because we can prepare nonlocal resources offline and exploit local encoding circuits. In particular, we derive an encoding circuit for a bipartite version of the Steane code that is local and additionally requires only nearest-neighbor interactions. We have simulated this encoding in the CNOT extended rectangle with a publicly available fault-tolerant simulation software. The result is that there is an improvement in the "pseudothreshold" with respect to the baseline Steane code, under the assumption that quantum memory errors occur less frequently than quantum gate errors.

PACS 03.67.-a · 03.67.Pp

1 Introduction

Quantum error correction is the theory upon which future quantum computation and quantum communication devices will depend for reliable operation [43, 24, 8, 23]. This theory is the formal "quantization" of the classical error correction theory [37] and borrows several fundamental concepts from the classical theory, such as digitization, redundancy, and measurement of errors. Though, the way in which these concepts manifest in quantum error correction is different from the way that they manifest in classical error correction.

The exploitation of several different forms of "quantum redundancy" [9] has been a crucial component of progress [43, 35, 4, 2, 41, 7, 6, 34, 52] in the theory of quantum error correction. First, Shor realized that we can obtain the quantum redundancy necessary for a quantum error-correcting code by entangling information qubits with extra "ancilla" qubits [43]. Here, the ancilla qubits play the role of the resource for quantum redundancy. Ten years later, Kribs *et al.* realized that a noisy qubit, a so-called *gauge* qubit, is useful for quantum redundancy and formulated the theory of operator quantum error correction (also known as subsystem quantum error correction) [35]. Other researchers then showed that quantum codes with gauge qubits improve the noise threshold for reliable fault-tolerant quantum computation [4, 2, 41]. Shortly after the Kribs *et al.* result, Brun *et al.* realized that an *ebit*, a bipartite maximally entangled Bell state shared between a sender and receiver, is useful for quantum redundancy, and they formulated the

theory of entanglement-assisted quantum error correction [7,6]. Kremsky *et al.* followed by showing how ancillas and ebits are useful for the simultaneous transmission of classical and quantum information and formulated the classically-enhanced theory of quantum error correction [34,52]. These latter two theories of quantum error correction emerged from advances in quantum Shannon theory, in particular, from the father protocol [16,15] and the classically-enhanced quantum communication protocol [17], respectively.

In this paper, we develop a version of the stabilizer formalism for quantum error correction that we name the *bipartite stabilizer formalism.*[1] A bipartite quantum error-correcting code is useful in a quantum communication scenario in which two senders encode quantum information by exploiting nonlocal resources that they share. They both then transmit this encoded quantum information to a single receiver who decodes the transmitted information.

We also introduce a new form of quantum redundancy to the theory of quantum error correction: a *nonlocal information qubit.* The standard form of a nonlocal information qubit is as follows:

$$|\varphi\rangle^{AB} \equiv \alpha |00\rangle^{AB} + \beta |11\rangle^{AB},$$

where the coefficients α and β are arbitrary complex coefficients such that $|\alpha|^2 + |\beta|^2 = 1$ and the superscripts indicate that one party, Alice, possesses the first qubit and another party, Bob, possesses the second qubit. We discuss this resource in more detail later, but suffice it for now to say that its power stands somewhere in between an information qubit (or logical qubit) and an ebit. In this sense, it is perhaps most similar to a coherent bit channel [28,54,53]. Nonlocal information qubits may arise naturally in the setting of quantum network protocols [36,33] or distributed quantum computation [27, 10,21,20,39]. In the sections of this paper on quantum communication, we simply assume that two senders have such a resource available, perhaps distributed to them from some "source" party, and the senders would like to exploit it for quantum communication purposes.

We also show how an example of a bipartite quantum code, a variant of the Steane code, can lead to increased performance in fault-tolerant quantum computation (under certain assumptions) [44,3,23]. The increased performance occurs for this code because its encoding circuit is localized and has fewer error locations than the encoding circuit for the baseline Steane code. Additionally, the code retains the error-correcting properties of the stabilizer code from which it is derived, ensuring the ability to correct errors on all qubits (similar to the example in Ref. [42]). In particular, we present a version of the Steane code [40] that requires only nearest neighbor interactions among four qubits for its encoding, assuming that the seven-qubit quantum register is initialized with three ebits and one information qubit. Simulations then demonstrate that this version of the Steane code outperforms the baseline Steane code, under the assumption that quantum memory errors occur less frequently than quantum gate errors.

The present work represents an extension of the entanglement-assisted stabilizer formalism. We exploit recent ideas from the structure of entanglement-assisted quantum codes [50,48] and entanglement measures of stabilizer states [22] to construct our bipartite quantum codes. We motivate new ideas for research pursuits in network quantum Shannon theory [57], specifically related to the multiple access quantum channel [57,56,1,32,59,31].

The next section of this paper develops the resource of a nonlocal information qubit. Section 3 shows how to construct a two-sender one-receiver quantum code from any stabilizer code, under the assumption that the two senders possess ebits and nonlocal information qubits. That section also includes an example of this type of code. We then present our fault-tolerant quantum computation simulation results for the performance of the CNOT extended rectangle [3] using a bipartite variation of the Steane code [40]. We finally conclude with some open questions for investigation.

2 Nonlocal Quantum Information

2.1 Nonlocal Information Qubits

A nonlocal information qubit is the following state of two spatially separated qubits:

$$|\varphi\rangle^{AB} \equiv \alpha |00\rangle^{AB} + \beta |11\rangle^{AB}, \tag{1}$$

---

[1] Information theorists would typically denote such a scenario as a "multiple access coding" scenario [11]. This name is typically reserved for more exotic coding structures such as those used in code division multiple access [47] or superposition coding [60]. We choose the name "bipartite quantum error correction" to distinguish the coding structure presented here because it is not as exotic as either of the former methods (it simply cuts a stabilizer code into two parts).

where one party, Alice, possesses the first qubit and another party, Bob, possesses the second qubit. We take the standard form of the nonlocal information qubit to be as above. It is always possible to manipulate the nonlocal information qubit to be in the above standard form by means of local operations. Neither Alice nor Bob alone can do anything much with the nonlocal information qubit, but a third party Claire can decode it if both Alice and Bob each send her their respective qubit. Claire decodes simply by applying a CNOT from the first qubit to the second qubit once she receives both of them.

The nonlocal information qubit admits mathematical manipulation through the use of the stabilizer formalism [24]. The Pauli operator $Z^A Z^B$ stabilizes the nonlocal qubit because the state in (1) is in the $+1$-eigenspace of the operator $Z^A Z^B$. Local errors of the form X^A or X^B anticommute with the operator $Z^A Z^B$. Claire can detect these errors by measuring the operator $Z^A Z^B$ if she possesses both qubits after Alice and Bob transmit them to her. It is also possible to manipulate the quantum information in the nonlocal information qubit through the use of logical operators. The X logical operator of the nonlocal information qubit is $X^A X^B$ and the Z logical operator is either Z^A or Z^B. The logical Hamadard operation is a nonlocal operation that transforms $|00\rangle^{AB}$ to $(|00\rangle^{AB} + |11\rangle^{AB})/\sqrt{2}$ and $|11\rangle^{AB}$ to $(|00\rangle^{AB} - |11\rangle^{AB})/\sqrt{2}$. One cannot fully manipulate the quantum information in the nonlocal information qubit unless one possesses both qubits or unless, in some cases, we allow for classical communication between both senders so that, e.g., they can apply a coordinated X rotation to implement the logical X operator.

We can represent the stabilizer operator ZZ of a nonlocal information qubit as the following binary vector by exploiting the Pauli-to-binary isomorphism (See Ref. [24]):

$$H \equiv \begin{bmatrix} 1\ 1 \,|\, 0\ 0 \end{bmatrix}$$
$$\equiv \begin{bmatrix} H_Z^A\ H_Z^B \,|\, H_X^A\ H_X^B \end{bmatrix},$$

where the matrix to the left of the vertical bar captures the "Z" part of the operator and the matrix to the right of the vertical bar captures the "X" part of the operator. We can represent the logical operators XX and ZI with the following two respective row vectors:

$$L \equiv \begin{bmatrix} 0\ 0 & 1\ 1 \\ 1\ 0 & 0\ 0 \end{bmatrix}$$
$$\equiv \begin{bmatrix} L_Z^A\ L_Z^B \,|\, L_X^A\ L_X^B \end{bmatrix}.$$

Let H^A denote the following matrix:

$$H^A \equiv \begin{bmatrix} H_Z^A \,|\, H_X^A \end{bmatrix}, \tag{2}$$

and let H^B, L^A, and L^B denote similarly defined matrices. Let G denote the following matrix:

$$G \equiv \begin{bmatrix} H \\ L \end{bmatrix},$$

and we can define G^A and G^B similarly to the definitions of H^A, H^B, L^A, and L^B. For any given matrix of the form $F \equiv [F_Z | F_X]$, we can define a corresponding symplectic product matrix Ω_F where

$$\Omega_F \equiv F_Z F_X^T + F_X F_Z^T, \tag{3}$$

and addition is binary. It is straightforward to check that the following relations hold for the nonlocal information qubit:

$$\frac{1}{2}\text{rank}\,(\Omega_L) = \frac{1}{2}\text{rank}\,(\Omega_{L^A}) = \frac{1}{2}\text{rank}\,(\Omega_{L^B})$$
$$= \frac{1}{2}\text{rank}\,(\Omega_G)$$
$$= \frac{1}{2}\text{rank}\,(\Omega_{G^A}) = \frac{1}{2}\text{rank}\,(\Omega_{G^B})$$
$$= 1.$$

These types of calculations become important later in this paper because they allow us to calculate the number of nonlocal information qubits in a given set of generators.

2.2 Ebits

An *ebit* is a special case of a nonlocal information qubit where $\alpha = \beta = 1/\sqrt{2}$. Let $|\Phi\rangle^{AB}$ denote the state of an ebit where

$$|\Phi\rangle^{AB} \equiv \frac{|00\rangle^{AB} + |11\rangle^{AB}}{\sqrt{2}}.$$

The stabilizer operators of an ebit are $Z^A Z^B$ and $X^A X^B$ and, thus, it has error correction capability only. It can detect local errors of the form X^A, Z^A, X^B, and Z^B.

The binary representation of the stabilizer operators of an ebit are as follows:

$$H \equiv \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix},$$
$$\equiv \begin{bmatrix} H_Z^A & H_Z^B & | & H_X^A & H_X^B \end{bmatrix}.$$

Defining H^A, H^B, Ω_{H^A}, and Ω_{H^B} similar to the way we did in (2) and (3), it is straightforward to show that

$$\frac{1}{2}\text{rank}\left(\Omega_{H^A}\right) = \frac{1}{2}\text{rank}\left(\Omega_{H^B}\right) = 1.$$

This result is expected because an ebit contains exactly one ebit of entanglement and the above matrix rank calculation is equivalent to the bipartite entanglement measure of Fattal *et al.* [22]. This entanglement measure, in turn, coincides with the von Neumann entropy of entanglement measure.

2.3 Nonlocal Information Qubits versus Ebits

The nonlocal information qubit is a hybrid resource for nonlocal quantum redundancy in a quantum error-correcting code. It mixes the abilities of an ebit and an information qubit, because it possesses both error detection capability and information coding ability. That is, it can encode exactly one qubit into the nonlocal subspace spanned by the states $\{|00\rangle^{AB}, |11\rangle^{AB}\}$, while at the same time detecting local errors of the form X^A and X^B. In contrast, an ebit is only useful as an error correction resource because it cannot encode arbitrary quantum information.

The power of a nonlocal information qubit as used in a quantum error-correcting code lies in-between that of an information qubit and that of an ebit (as discussed above). Thus, *there is a qualitative sense in which it is similar to a coherent bit channel* [28,54,53], because a coherent bit channel is a resource with communication power in-between a noiseless qubit channel and a shared, noiseless ebit. Consider that the resource of a noiseless information qubit is qualitatively similar to a noiseless qubit channel because it arises from the ability to simulate a noiseless qubit channel. That is, there is some means by which a source S can distribute an information qubit to Alice with the noiseless qubit channel

$$|x\rangle^S \rightarrow |x\rangle^A,$$

where $x \in \{0,1\}$, if she possesses the noiseless information qubit $|\psi\rangle^A = \alpha|0\rangle^A + \beta|1\rangle^A$. Similarly, the resource of a nonlocal information qubit is qualitatively similar to a noiseless coherent bit channel because it arises from the ability to simulate a noiseless coherent bit channel, where we define a coherent bit channel as the following isometric map:

$$|x\rangle^S \rightarrow |x\rangle^A |x\rangle^B,$$

where $x \in \{0,1\}$. The input system to the coherent bit channel is a source system S, and the output systems are those of Alice and Bob. In particular, the map maintains coherent superpositions, from which it gains its name as the coherent bit channel. We leave it open as to who possesses the source system because it could be Alice (as originally defined in Ref. [28]) or Bob, or some other system. So, we assume that there is some means by which a noiseless coherent bit channel is simulated if Alice and Bob possess a nonlocal information qubit, i.e., there is some means by which the following map occurs:

$$\alpha|0\rangle^S + \beta|1\rangle^S \rightarrow |\varphi\rangle^{AB},$$
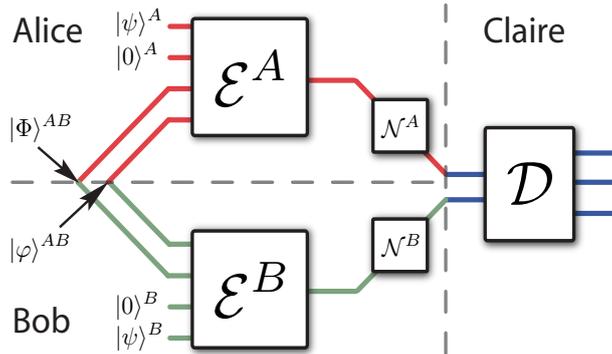
Fig. 1 (Color online) The operation of an $[[8, 1, 1, 1; 1]]$ two-sender one-receiver quantum error-correcting code. Alice would like to send the information qubit $|\psi\rangle^A$, Bob would like to send the information qubit $|\psi\rangle^B$, and both Alice and Bob would like to send the nonlocal information qubit $|\varphi\rangle^{AB}$. For quantum redundancy, Alice uses an ancilla $|0\rangle^A$, Bob uses an ancilla $|0\rangle^B$, and they both exploit an ebit in the state $|\Phi\rangle^{AB}$. They both transmit their encoded state over respective noisy quantum channels $\mathcal{N}^A$ and $\mathcal{N}^B$ connecting them to Claire, and she then decodes the three information qubits.

where $|\varphi\rangle^{AB}$ is defined in (1). Here, we do not concern ourselves with how they happen to come upon nonlocal information qubits, but we merely assume that they have a supply and would like to transmit them to the receiver Claire.

In further analogy of the nonlocal information qubit with the coherent bit channel, an ebit arises when we send a qubit in the state $(|0\rangle + |1\rangle)/\sqrt{2}$ through the coherent bit channel.

3 Bipartite Stabilizer Codes

We now give our model for a bipartite quantum error correction protocol by constructing a bipartite code from a stabilizer quantum code. We assume that Alice would like to send k_A information qubits, Bob would like to send k_B information qubits, and both Alice and Bob would like to send k_{AB} nonlocal information qubits. An $[[n, k_A, k_B, k_{AB}; c_{AB}]]$ two-sender one-receiver quantum error-correcting code is one that exploits n total channel uses and c_{AB} ebits shared between Alice and Bob to send the aforementioned amounts of information qubits. Figure 1 depicts the operation of an $[[8, 1, 1, 1; 1]]$ two-sender one-receiver quantum code.

Let us consider a set of commuting generators that forms a valid stabilizer code [24]. Suppose that we have an $[n, k]$ stabilizer code S with generators $g_1, \ldots, g_{n-k}$. Suppose that we also have the $n + k$ generators of the normalizer $N(S)$ of this code. It is possible to determine the logical operators $\overline{X}_1, \ldots, \overline{X}_k, \overline{Z}_1, \ldots, \overline{Z}_k$ of this code by performing a symplectic Gram-Schmidt orthogonalization procedure on the generators of the normalizer $N(S)$ [48]—this procedure gives the $2k$ logical operators and the $n - k$ stabilizer generators.

Now let us assume that Alice possesses the first n_A qubits and Bob possesses the last n_B where $n_A + n_B = n$. We represent the stabilizer generators as follows:

$$g_1^{(A)} \otimes g_1^{(B)}, \ldots, g_{n-k}^{(A)} \otimes g_{n-k}^{(B)}.$$

The logical operators are as follows:

$$\overline{X}_1^{(A)} \otimes \overline{X}_1^{(B)}, \ldots, \overline{X}_k^{(A)} \otimes \overline{X}_k^{(B)},$$
$$\overline{Z}_1^{(A)} \otimes \overline{Z}_1^{(B)}, \ldots, \overline{Z}_k^{(A)} \otimes \overline{Z}_k^{(B)},$$

where the A superscript indicates the part of the generator corresponding to qubits that Alice possesses, and the B superscript indicates the part corresponding to qubits that Bob possesses. We can alternatively represent the stabilizer generators with an $(n - k) \times 2n$ binary check matrix H where

$$H \equiv \begin{bmatrix} H_Z \mid H_X \end{bmatrix}, \tag{4}$$

5

and the vertical bar divides the matrix into a "Z" part and an "X" part according to the Pauli-to-binary isomorphism (See Ref. [24]). We can further divide the matrix H into matrices corresponding to generators acting on Alice and Bob's respective qubits:

$$H \equiv \left[\, H_Z^A \; H_Z^B \,\middle|\, H_X^A \; H_X^B \,\right], \tag{5}$$

where H_Z^A and H_X^A are each $(n-k) \times n_A$ binary matrices and H_Z^B and H_X^B are each $(n-k) \times n_B$ binary matrices. Let H^A denote the following matrix:

$$H^A \equiv \left[\, H_Z^A \,\middle|\, H_X^A \,\right], \tag{6}$$

and let H^B denote the following matrix:

$$H^B \equiv \left[\, H_Z^B \,\middle|\, H_X^B \,\right]. \tag{7}$$

We can represent the normalizer $N(S)$ with an $(n+k) \times 2n$ binary matrix G where

$$G \equiv \left[\, G_Z \,\middle|\, G_X \,\right]. \tag{8}$$

There is a similar subdivided representation of the matrix G:

$$G \equiv \left[\, G_Z^A \; G_Z^B \,\middle|\, G_X^A \; G_X^B \,\right]. \tag{9}$$

Let G^A denote the following matrix:

$$G^A \equiv \left[\, G_Z^A \,\middle|\, G_X^A \,\right], \tag{10}$$

and let G^B denote the following matrix:

$$G^B \equiv \left[\, G_Z^B \,\middle|\, G_X^B \,\right]. \tag{11}$$

The rowspace of matrix H is in the rowspace of matrix G because the generators in group $N(S)$ normalize the generators in the group S.

We can formulate several *symplectic product matrices* [50, 48] that are useful for determining the local anticommutativity in the above generators. Let Ω_{H^A} be the "Alice" symplectic product matrix corresponding to Alice's local matrix H^A:

$$\Omega_{H^A} \equiv H_Z^A \left(H_X^A\right)^T + H_X^A \left(H_Z^A\right)^T,$$

where addition is binary. Let Ω_{H^B}, Ω_G, Ω_{G^A}, and Ω_{G^B} denote similar symplectic product matrices corresponding to matrices H^B, G, G^A, and G^B.

We can manipulate the generators of the stabilizer S into a form more suitable for representation as a bipartite code (this manipulation is similar to that of Theorem 1 in Ref. [22]). We freely abuse terminology by referring to a subgroup by its generating set. We first separate the generators in the stabilizer S into two subgroups with generators of the following forms:

$$S' \equiv \left\{ g_i^{(A)} \otimes g_i^{(B)} \right\},$$
$$S^B \equiv \left\{ I^{(A)} \otimes g_j^{(B)} \right\}. \tag{12}$$

It is possible to bring all generators into one of these two subgroups because the local "Alice" generators of S^B are dependent on the local "Alice" generators of S'. We further manipulate the generators to divide into three subgroups:

$$S^{AB} \equiv \left\{ g_i^{(A)} \otimes g_i^{(B)} \right\},$$
$$S^A \equiv \left\{ g_j^{(A)} \otimes I^{(B)} \right\},$$
$$S^B \equiv \left\{ I^{(A)} \otimes g_p^{(B)} \right\}, \tag{13}$$

by using the generators in S^B to remove any dependence of the local "Bob" generators of S'. We finally bring the generators of S into the following four subgroups by performing the symplectic Gram-Schmidt

orthogonalization procedure (see Ref.'s [50, 48]) on the local "Alice" part of the generators in S^{AB}. This last step further divides the subgroup S^{AB} into two subgroups S_{E}^{AB} and S_{NLI}^{AB}:

$$S_{\mathrm{E}}^{AB} \equiv \left\{ \begin{array}{c} g_i^{(A)} \otimes g_i^{(B)} \\ \overline{g}_i^{(A)} \otimes \overline{g}_i^{(B)} \end{array} \right\},$$

$$S_{\mathrm{NLI}}^{AB} \equiv \left\{ g_j^{(A)} \otimes g_j^{(B)} \right\},$$

$$S^A \equiv \left\{ g_p^{(A)} \otimes I^{(B)} \right\},$$

$$S^B \equiv \left\{ I^{(A)} \otimes g_q^{(B)} \right\}. \tag{14}$$

The entanglement subgroup S_{E}^{AB} consists of those generators in S^{AB} which have a locally anticommuting partner in S^{AB}, where the anticommutativity is with respect to the local "Alice" part of the generators. We denote a generator in S_{E}^{AB} by $g_i^{(A)} \otimes g_i^{(B)}$ and its locally anticommuting partner by $\overline{g}_i^{(A)} \otimes \overline{g}_i^{(B)}$. The generators in S_{E}^{AB} therefore correspond to ebits that Alice and Bob share before the quantum communication protocol begins.

The nonlocal information subgroup S_{NLI}^{AB} consists of those generators in S^{AB} which have no such locally anticommuting partner in S^{AB}. Its locally anticommuting partners are therefore in the normalizer $N(S)$. The generators in S_{NLI}^{AB} therefore correspond to nonlocal information qubits that Alice and Bob share before the quantum communication protocol begins. The local subgroups S^A and S^B correspond to ancilla qubits for Alice and Bob.

The following theorem shows how to produce an $[[n, k_A, k_B, k_{AB}; c_{AB}]]$ two-sender one-receiver quantum code from any $[[n, k]]$ stabilizer code, and furthermore, it computes the parameters k_A, k_B, k_{AB}, and c_{AB} as a function of the stabilizer group S and the normalizer $N(S)$ (it actually uses their corresponding binary representations).

Theorem 1 *From any $[[n, k]]$ stabilizer code, we can produce an $[[n, k_A, k_B, k_{AB}; c_{AB}]]$ two-sender one-receiver quantum code by choosing Alice to possess n_A qubits and choosing Bob to possess n_B qubits, where $n_A + n_B = n$. The two-sender one-receiver quantum code requires c_{AB} ebits where*

$$c_{AB} = \frac{1}{2} rank\left(\Omega_{H^A}\right) = \frac{1}{2} rank\left(\Omega_{H^B}\right).$$

It transmits k_A information qubits for Alice, k_B information qubits for Bob, and k_{AB} nonlocal information qubits where

$$k_{AB} = rank\left(H^A\right) + rank\left(H^B\right) + k - n - c_{AB},$$

$$k_A = \frac{1}{2} rank\left(\Omega_{G^A}\right) - c_{AB} - k_{AB},$$

$$k_B = \frac{1}{2} rank\left(\Omega_{G^B}\right) - c_{AB} - k_{AB}.$$

We can also compute k_{AB} with the following formula:

$$k_{AB} = \frac{1}{2}\left(rank\left(\Omega_{G^A}\right) + rank\left(\Omega_{G^B}\right) - rank\left(\Omega_G\right)\right) - 2c_{AB}.$$

Proof The method of proof is similar to that originally posted in Ref. [50] and later exploited in Ref. [48]. In this proof, we liberally go back and forth between the binary representation of Pauli generators and the groups generated by Pauli generators.

The number c_{AB} of ebits that the code requires is equal to the number of locally anticommuting pairs in S, with respect to either Alice's local part or Bob's local part. Ref. [50] shows that we can calculate the amount of anticommutativity in any set of generators by calculating the rank of its corresponding symplectic product matrix and dividing by two. Thus, the number of ebits that the code requires is equal to

$$c_{AB} = \frac{1}{2}\mathrm{rank}\left(\Omega_{H^A}\right) = \frac{1}{2}\mathrm{rank}\left(\Omega_{H^B}\right).$$

We now calculate the number k_{AB} of nonlocal information qubits. The number of generators in S, or equivalently, the number of rows in H, is equal to $n - k$. The size $\left|S^B\right|$ of the local subgroup S^B is equal

to $n - k$ reduced by the size $|S'|$ of the subgroup S' in (12). The size $|S'|$ of the subgroup S' in (12) is equal to $\text{rank}(H^A)$ because it consists of all the locally independent generators. Thus, the size $|S^B|$ is

$$|S^B| = n - k - \text{rank}(H^A).$$

A symmetric argument gives that

$$|S^A| = n - k - \text{rank}(H^B).$$

These results then imply that the size $|S^{AB}|$ of the subgroup S^{AB} in (13) is

$$\begin{aligned} |S^{AB}| &= n - k - |S^A| - |S^B| \\ &= \text{rank}(H^A) + \text{rank}(H^B) + k - n. \end{aligned}$$

We obtain the number k_{AB} of nonlocal information qubits, or equivalently, the size $|S^{AB}_{\text{NLI}}|$ of the nonlocal information subgroup S^{AB}_{NLI}, by reducing $|S^{AB}|$ by the number c_{AB} of ebits:

$$\begin{aligned} k_{AB} &= |S^{AB}| - c_{AB} \\ &= \text{rank}(H^A) + \text{rank}(H^B) + k - n - c_{AB}. \end{aligned}$$

We now calculate the number k_A of "Alice" local information qubits. For this task, we consider Alice's part G^A of the full normalizer matrix G. The anticommutativity in the generators corresponding to the rows of the matrix G^A is all and only due to ebits, nonlocal information qubits, and Alice's local information qubits. The anticommutativity from ebits is due to the local "Alice" generators in the subgroup S^{AB}_{E}, which are themselves in the rowspace of G^A. The anticommutativity from nonlocal information qubits is due in part to the local "Alice" generators of S^{AB}_{NLI} and the local part of the matching locally anticommuting partners in the local normalizer. Both of these local generators are in the rowspace of G^A. Alice's local information qubits have logical operators which contribute to the anticommutativity as well. We can calculate the overall number of anticommuting pairs due to ebits, nonlocal information qubits, and "Alice" local information qubits as $\text{rank}(\Omega_{G^A})/2$:

$$\frac{1}{2}\text{rank}(\Omega_{G^A}) = k_A + c_{AB} + k_{AB}. \tag{15}$$

Reducing the quantity $\text{rank}(\Omega_{G^A})/2$ by the number c_{AB} of ebits and the number k_{AB} of nonlocal information qubits produces the formula for k_A in the statement of the theorem. A symmetric argument gives that

$$\frac{1}{2}\text{rank}(\Omega_{G^B}) = k_B + c_{AB} + k_{AB}, \tag{16}$$

and, thus, gives the number k_B of local information qubits for Bob.

We can also calculate k_{AB} by recalling that $\text{rank}(\Omega_G)/2$ captures the number of logical operators of the code:

$$\frac{1}{2}\text{rank}(\Omega_G) = k_{AB} + k_A + k_B.$$

Combining the above equation with the equations (15) and (16) and solving for k_{AB} gives the following formula for k_{AB}:

$$k_{AB} = \frac{1}{2}\left(\text{rank}(\Omega_{G^A}) + \text{rank}(\Omega_{G^B}) - \text{rank}(\Omega_G)\right) - 2c_{AB}.$$

Finally, it is possible to produce local encoding circuits for the resulting two-sender one-receiver quantum code by first bringing the stabilizer generators into the form in (14) and applying the algorithm outlined in the appendix of Ref. [55] to the local parts of the generators (this algorithm, in turn, derives from the Grassl-Rötteler algorithm for encoding quantum convolutional codes [26]).

We now detail an example of an $[[8, 1, 1, 1; 3]]$ two-sender one-receiver quantum error-correcting code. Consider the $[[8, 3, 3]]$ stabilizer code from Grassl's table of quantum codes [25]. Its stabilizer generators are as follows:

$$\begin{matrix} X & I & Z & I & Y & Z & X & Y \\ I & X & Z & Z & Y & X & Y & I \\ I & I & X & Y & Z & Z & Y & X \\ Z & I & Z & X & I & Y & Y & Z \\ Z & Z & Z & Z & X & Z & Z & X \end{matrix}.$$

Let us suppose that Alice possesses the first four qubits and Bob possesses the second four qubits. Inspection of Alice's local generators reveals that they are an independent set of generators, and the same holds for Bob's local generators. Thus, the local subgroups S^A and S^B are empty.

We then perform the symplectic Gram-Schmidt orthogonalization procedure on Alice's local generators and produce the following set of generators:

$$\begin{matrix} X & I & Z & I & Y & Z & X & Y \\ I & I & X & Y & Z & Z & Y & X \\ I & X & Z & Z & Y & X & Y & I \\ Z & I & Y & Z & Z & X & I & Y \\ I & Y & Z & X & Z & I & Z & I \end{matrix}.$$

Notice that the first two generators form a locally anticommuting pair, the second two generators form a locally anticommuting pair, and the last generator does not have an anticommuting partner. Thus, the first four generators generate the entanglement subgroup, and the last generator generates the nonlocal subgroup.

Alice and Bob can each then perform local Clifford operations to reduce the above stabilizer to the following trivial one:

$$\begin{matrix} Z & I & I & I & Z & I & I & I \\ X & I & I & I & X & I & I & I \\ I & Z & I & I & I & Z & I & I \\ I & X & I & I & I & X & I & I \\ I & I & Z & I & I & I & Z & I \end{matrix}.$$

In the above stabilizer, we can plainly see that the first four generators correspond to two ebits that Alice and Bob share, and the last generator corresponds to a nonlocal information qubit (recall from Section 2.1 that the stabilizer of a nonlocal information qubit is ZZ). The operators acting on the fourth and eighth qubits are the identity for all stabilizer generators so that Alice can encode one local information qubit and Bob can encode one local information qubit. The error-correcting properties of the code are equivalent to the error-correcting properties of the original stabilizer code.

4 Applications to Fault-Tolerant Quantum Computation

The bipartite coding structure outlined in this paper is useful in fault-tolerant quantum computation [44, 3, 23]. This usefulness is due to the following two factors:

1. Bipartite codes derived from stabilizer codes maintain their error-correcting properties.
2. The encoding circuit consists of ebit preparations and local encoding circuits. For the example code in this section, the encoding circuit requires only nearest-neighbor interactions and has fewer malignant pairs than the encoding circuit for the baseline Steane code [3].

In this section, we represent the Steane code [40] as a bipartite quantum code and show how this representation gives a simplified, local encoding circuit. As a result, the simplified encoding circuit affects the "pseudothreshold" [46] for fault-tolerant quantum computation with the Steane code, under the assumption that quantum memory errors do not occur as frequently as quantum gate errors. We present the results of numerical simulations that demonstrate how the pseudothreshold improves under certain assumptions.
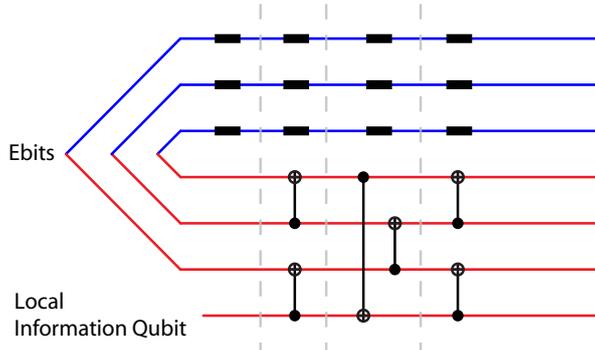
Fig. 2 (Color online) The encoding operations for the 3EA Steane code. We first prepare the seven-qubit register with three ebits and one local information qubit (the red qubits belong to the "inside party" and the blue qubits belong to the "outside party"). The black bars represent "wait gates," that model potential memory errors that may occur. The encoding consists of three rounds of local CNOT gates. Note that we place extra "memory decoherence" on the ebits to model preparation errors that may occur.

4.1 Steane Code as a Bipartite Stabilizer Code

Let us first recall the stabilizer generators of the Steane code (as presented in Ref. [3]):

$$
\begin{array}{ccccccc}
I & I & I & X & X & X & X \\
I & X & X & I & I & X & X \\
X & I & X & I & X & I & X \\
I & I & I & Z & Z & Z & Z \\
I & Z & Z & I & I & Z & Z \\
Z & I & Z & I & Z & I & Z
\end{array}
. \tag{17}
$$

We can write this code as a bipartite code by employing Theorem 1. In particular, let us give the first, second, and fourth qubits to an "outside" party, and the third, fifth, sixth, and seventh qubits to an "inside" party.[2] Figure 3 makes this nomenclature of "inside" and "outside" more clear. This bipartite cut yields a $[[7, 0, 1, 0; 3]]$ bipartite quantum code by employing the calculations in Theorem 1. It encodes one local information qubit with the help of three ebits shared between the inside party and the outside party. Note that this code is also a $[[4, 1, 3; 3]]$ entanglement-assisted code. We refer to this slight variation of the Steane code as the three-ebit entanglement-assisted Steane code (*3EA Steane code*).

4.2 Encoding Method

The advantage of the 3EA Steane code is that it is possible to encode it using only nearest-neighbor interactions on four qubits (if there is a good source of ebits available). This property is desirable for a fault-tolerant encoding circuit because the locality property ensures that errors propagate only to four qubits during encoding, under the assumption that gate errors occur more frequently than memory errors.

We now show how to encode the 3EA Steane code with local operations. Suppose that we initialize a seven-qubit quantum register with three ebits and one information qubit. We assume that the particular technology implementing the code possesses a good source of ebits, though note that we allow for memory errors to occur on both halves of the ebits after they have been prepared. The stabilizer corresponding

---

[2] Note that this distinction between parties is not particularly relevant in fault-tolerant quantum computation, but we make this distinction in order to appeal to the coding structure outlined before.
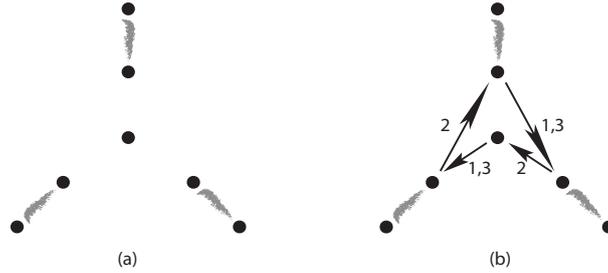
Fig. 3 The above figure depicts a particular geometric layout for encoding a set of qubits with the Steane code. The four inner qubits belong to the "inside" party and the three outer qubits belong to the "outside" party. (a) Three ebits surround an information qubit before the encoding takes place. (b) The encoding operations are local CNOT gates that interact the information qubit and the three local halves of the ebits. The arrows indicate the direction of the CNOT gates, and the number adjacent to an arrow indicates the time step at which the operation takes place.

to the unencoded state is as follows:

$$
\begin{array}{ccccccc}
I & I & I & X & X & I & I \\
I & X & X & I & I & I & I \\
X & I & I & I & I & I & X \\
I & I & I & Z & Z & I & I \\
I & Z & Z & I & I & I & I \\
Z & I & I & I & I & I & Z
\end{array}.
$$

The first round of encoding applies a CNOT gate from the third qubit to the fifth and from the sixth qubit to the seventh. The second round of encoding applies a CNOT gate from the seventh qubit to the third and from the fifth qubit to the sixth. The CNOT gates in the final round are the same as those in the first round. The result is that the stabilizer of the encoded state is as given in (17). Figure 2 depicts the encoding circuit in quantum circuit notation (with a permutation of the qubits for a simplified visual presentation). Note that that circuit includes memory errors that may occur on the outside party's share of the ebits (as explained in the caption of Figure 2). Figure 3 gives an alternative illustration of the encoding circuit that depicts a particular geometric layout of the qubits in the seven-qubit quantum register.

An analysis of this encoding circuit with publicly available fault-tolerant QASM tools [13,12] shows that it has 9,577 CNOT-CNOT malignant pairs, which are quite a bit fewer than the 13,245 CNOT-CNOT malignant pairs in the AGP Steane encoding circuit [3]. We then expect that the 3EA Steane code should outperform the baseline Steane code, when quantum memory errors occur less frequently than quantum gate errors. The results in the next section confirm this intuition.
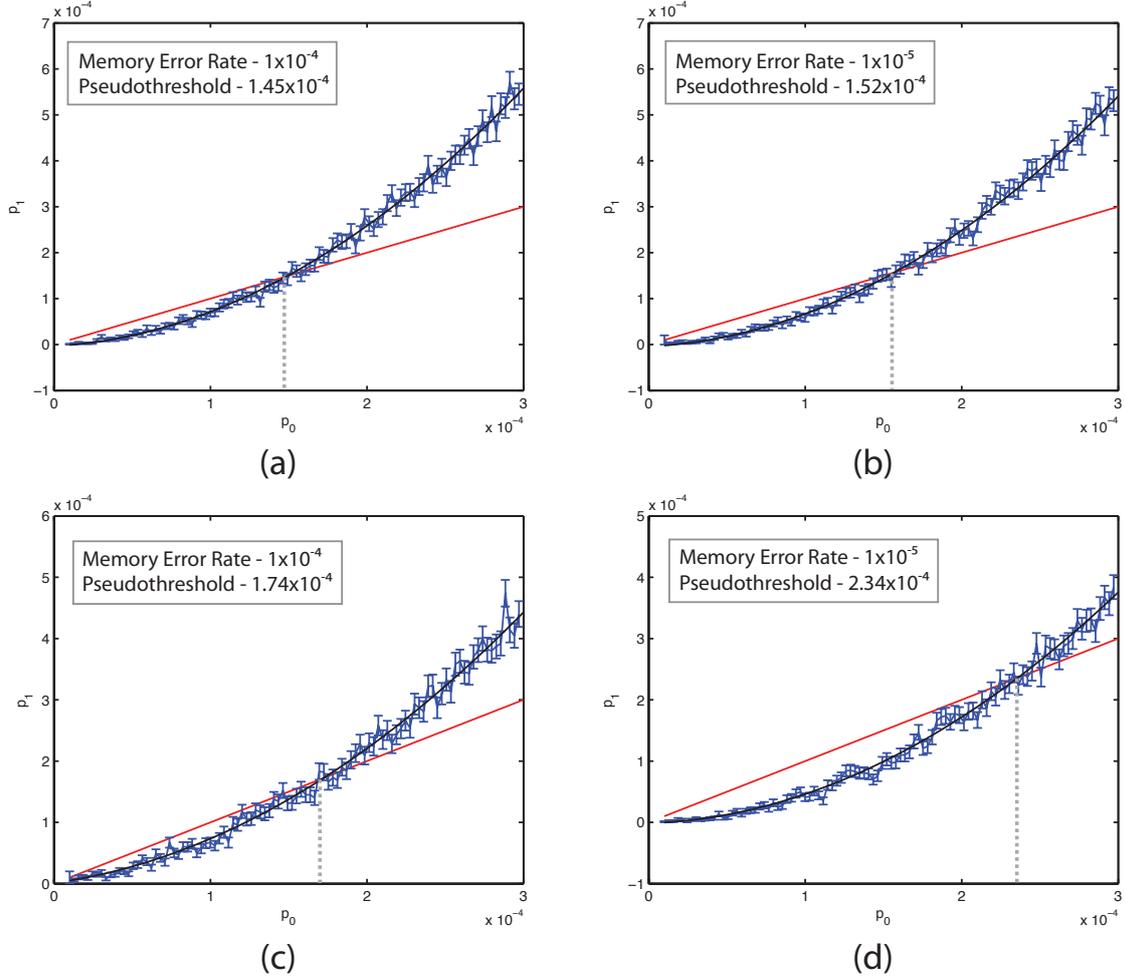
4.3 Simulation Results

We simulated the performance of the 3EA Steane code using publicly available QASM fault-tolerant simulation software [13,12]. In particular, we evaluated the encoding circuit of the 3EA Steane code in the CNOT extended rectangle (See Figure 11 of Ref. [3]). The CNOT extended rectangle performs "Steane error correction" [45] of two logical qubits (recall that "Steane error correction" is different from the "Steane code"), performs a logical CNOT between the two blocks, and performs Steane error correction again on the two blocks.

Figure 4 plots the results of the simulations with accompanying explanations. The result is that the 3EA Steane code gives an improvement in performance over the baseline Steane code, under the assumption that quantum memory errors occur less frequently than quantum gate errors.

5 Conclusion

The bipartite stabilizer formalism represents a new way of thinking about quantum error correction codes. Our main theorem shows how to divy up the qubits in a bipartite quantum code as local information

Fig. 4 (Color online) Various simulation results for the Steane code in the CNOT extended rectangle. Each plot graphs the probability of failure with encoding versus the probability of failure without encoding. The red line on each plot is the probability of failure when the encoding is trivial (i.e., there is no encoding). Each blue error bar is the result of 10^6 simulations, and there are 100 blue error bars on each plot. The black curve going through the error bars is a quadratic fit to the data points. The dashed line on each plot indicates the location of the pseudothreshold (the point at which the red curve intersects the black fitted curve). The result is that the 3EA Steane code gives an improvement over the baseline Steane code when memory errors occur less frequently than gate errors. (a) Baseline Steane code with memory error rate 1×10^{-4}. An estimate of the pseudothreshold is 1.45×10^{-4}. (b) Baseline Steane code with memory error rate 1×10^{-5}. An estimate of the pseudothreshold is 1.52×10^{-4}. (c) 3EA Steane code with memory error rate 1×10^{-4}. An estimate of the pseudothreshold is 1.74×10^{-4}. (d) 3EA Steane code with memory error rate 1×10^{-5}. An estimate of the pseudothreshold is 2.34×10^{-4}.

qubits, nonlocal information qubits, ancilla qubits, and ebits. Our original purpose was to show how the bipartite stabilizer formalism is useful for quantum communication, but it turns out to have use in fault-tolerant quantum computation as well. In particular, the 3EA Steane code improves the pseudothreshold for fault-tolerant quantum computation, under the assumption that there is a good source of ebits and quantum memory errors occur less frequently than quantum gate errors. This broad applicability reinforces the strong links between techniques for quantum communication and techniques for quantum computation.

We now list several open problems of interest for extensions in quantum communication topics.

- It would be interesting to develop quantum Shannon-theoretic protocols that include nonlocal information qubits. The state merging protocol may be useful here [29,30].
- The codes in this paper are relevant for a multiple-access channel, but it could be interesting to determine if there are useful codes for a broadcast channel. Yard *et al.* have already explored quantum

Shannon theoretic protocols for the quantum broadcast channel [58]. Perhaps techniques from that work will give insight into the design of quantum broadcast channel codes.

- It might also be interesting to explore bipartite convolutional codes as an extension of the work in Ref's. [55,49,51] and the work in this paper.
- There might be a way to develop multiparty codes that exploit a common secret key between multiple parties because of the connection between quantum privacy and quantum coherence [14,19,18].
- Finally, we are currently considering the extension of the ideas in this paper to the tripartite setting where the senders share quantum resources with the receiver (this extension would be similar to the way that Ref. [5] extends Ref. [22]).

It should also be interesting to explore further improvements that might arise in fault-tolerant simulations of the 3EA Steane when taking into account the nearest-neighbor interactions in its encoding circuit, similar to the way that Ref. [38] considered the impact of nearest-neighbor interactions for quantum Fourier transform circuits.

References

1. Ahlswede, R., Cai, N.: A strong converse theorem for quantum multiple access channels. Electronic Notes in Discrete Mathematics **21**, 137–141 (2005). General Theory of Information Transfer and Combinatorics
2. Aliferis, P., Cross, A.W.: Subsystem fault tolerance with the Bacon-Shor code. Physical Review Letters **98**(22), 220502 (2007). DOI 10.1103/PhysRevLett.98.220502
3. Aliferis, P., Gottesman, D., Preskill, J.: Quantum accuracy threshold for concatenated distance-3 codes. Quantum Information and Computation **6**, 97–165 (2006)
4. Bacon, D.: Operator quantum error correcting subsystems for self-correcting quantum memories. Physical Review A **73**, 012,340 (2006)
5. Bravyi, S., Fattal, D., Gottesman, D.: GHZ extraction yield for multipartite stabilizer states. Journal of Mathematical Physics **47**, 062,106 (2006)
6. Brun, T.A., Devetak, I., Hsieh, M.H.: Catalytic quantum error correction. arXiv:quant-ph/0608027 (2006)
7. Brun, T.A., Devetak, I., Hsieh, M.H.: Correcting quantum errors with entanglement. Science **314**(5798), 436–439 (2006)
8. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE Transactions on Information Theory **44**, 1369–1387 (1998)
9. Cerf, N.J., Cleve, R.: Information-theoretic interpretation of quantum error-correcting codes. Physical Review A **56**(3), 1721–1732 (1997). DOI 10.1103/PhysRevA.56.1721
10. Cirac, J.I., Ekert, A.K., Huelga, S.F., Macchiavello, C.: Distributed quantum computation over noisy channels. Physical Review A **59**(6), 4249–4254 (1999). DOI 10.1103/PhysRevA.59.4249
11. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Series in Telecommunication. John Wiley and Sons, New York (1991)
12. Cross, A.W.: QASM fault-tolerant simulation software. http://www.media.mit.edu/quanta/quanta-web/projects/qasm-tools/ (2006)
13. Cross, A.W., DiVincenzo, D.P., Terhal, B.M.: A comparative code study for quantum fault-tolerance. Quantum Information and Computation **9**, 541–572 (2009)
14. Devetak, I.: The private classical capacity and quantum capacity of a quantum channel. IEEE Transactions on Information Theory **51**(1), 44–55 (2005)
15. Devetak, I., Harrow, A.W., Winter, A.: A resource framework for quantum Shannon theory. IEEE Transactions on Information Theory **54**(10), 4587–4618 (2008)
16. Devetak, I., Harrow, A.W., Winter, A.J.: A family of quantum protocols. Physical Review Letters **93**, 239,503 (2004)
17. Devetak, I., Shor, P.W.: The capacity of a quantum channel for simultaneous transmission of classical and quantum information. Communications in Mathematical Physics **256**(2), 287–303 (2005)
18. Devetak, I., Winter, A.: Relating quantum privacy and quantum coherence: an operational approach. Physical Review Letters **93**, 080,501 (2004)
19. Devetak, I., Winter, A.: Distillation of secret key and entanglement from quantum states. Proceedings of the Royal Society A **461**, 207–235 (2005)
20. D'Hondt, E.: Distributed quantum computation: a measurement-based approach. Ph.D. thesis, Vrije Universiteit Brussel (2005)
21. Eisert, J., Jacobs, K., Papadopoulos, P., Plenio, M.B.: Optimal local implementation of nonlocal quantum gates. Physical Review A **62**(5), 052,317 (2000). DOI 10.1103/PhysRevA.62.052317
22. Fattal, D., Cubitt, T.S., Yamamoto, Y., Bravyi, S., Chuang, I.L.: Entanglement in the stabilizer formalism (2004). quant-ph/0406168
23. Gaitan, F.: Quantum Error Correction and Fault Tolerant Quantum Computing. CRC Press, Taylor and Francis Group (2008)
24. Gottesman, D.: Stabilizer codes and quantum error correction. Ph.D. thesis, California Institute of Technology (1997)

25. Grassl, M.: Encoding circuits for quantum error-correcting codes (Copyright 2007). URL `http://iaks-www.ira.uka.de/home/grassl/QECC/circuits/index.html`

26. Grassl, M., Rötteler, M.: Noncatastrophic encoders and encoder inverses for quantum convolutional codes. In: IEEE International Symposium on Information Theory (quant-ph/0602129), pp. 1109–1113. Seattle, Washington, USA (2006)

27. Grover, L.K.: Quantum Telecomputation. arXiv:quant-ph/9704012 (1997)

28. Harrow, A.W.: Coherent communication of classical messages. Physical Review Letters **92**, 097,902 (2004)

29. Horodecki, M., Oppenheim, J., Winter, A.: Partial quantum information. Nature **436**, 673–676 (2005)

30. Horodecki, M., Oppenheim, J., Winter, A.: Quantum state merging and negative information. Communications in Mathematical Physics **269**(1), 107–136 (2007)

31. Hsieh, M.H., Devetak, I., Winter, A.: Entanglement-assisted capacity of quantum multiple-access channels. IEEE Transactions on Information Theory **54**(7), 3078–3090 (2008)

32. Klimovitch, G.V., Winter, A.: Classical capacity of quantum binary adder channels. arXiv:quant-ph/0502055 (2005)

33. Kobayashi, H., Gall, F.L., Nishimura, H., Rötteler, M.: Perfect quantum network communication protocol based on classical network coding. arXiv:0902.1299 (2009)

34. Kremsky, I., Hsieh, M.H., Brun, T.A.: Classical enhancement of quantum-error-correcting codes. Physical Review A **78**(1), 012341 (2008). DOI 10.1103/PhysRevA.78.012341

35. Kribs, D., Laflamme, R., Poulin, D.: A unified and generalized approach to quantum error correction. Physical Review Letters **94**, 180,501 (2005)

36. Leung, D., Oppenheim, J., Winter, A.: Quantum network communication—the butterfly and beyond. arXiv:quant-ph/0608223 (2006)

37. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. Elsevier, Amsterdam (1977)

38. Maslov, D.: Linear depth stabilizer and quantum fourier transformation circuits with no auxiliary qubits in finite-neighbor quantum architectures. Physical Review A **76**(5), 052310 (2007). DOI 10.1103/PhysRevA.76.052310

39. Meter III, R.D.V.: Architecture of a quantum multicomputer optimized for shor's factoring algorithm. Ph.D. thesis, Keio University (quant-ph/0607065.) (2006)

40. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, New York (2000)

41. Poulin, D.: Stabilizer formalism for operator quantum error correction. Physical Review Letters **95**, 230,504 (2005)

42. Shaw, B., Wilde, M.M., Oreshkov, O., Kremsky, I., Lidar, D.: Encoding one logical qubit into six physical qubits. Physical Review A **78**, 012,337 (2008)

43. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Physical Review A **52**, 2493–2496 (1995)

44. Shor, P.W.: Fault tolerant quantum computation. In: Proceedings of the 37th Symposium on the Foundations of Computer Science, pp. 56–65. IEEE, Los Alamitos, CA (1996)

45. Steane, A.M.: Active stabilization, quantum computation, and quantum state synthesis. Physical Review Letters **78**(11), 2252–2255 (1997). DOI 10.1103/PhysRevLett.78.2252

46. Svore, K.M., Cross, A.W., Chuang, I.L., Aho, A.V.: A flow-map model for analyzing pseudothresholds in fault-tolerant quantum computing. Quantum Information and Computation **6**(3), 193–212 (2006)

47. Viterbi, A.J.: CDMA: Principles of Spread Spectrum Communication, 1st edn. Prentice Hall PTR (1995)

48. Wilde, M.M.: Logical operators of quantum codes. Physical Review A **79**, 062,322 (2009)

49. Wilde, M.M., Brun, T.A.: Entanglement-assisted quantum convolutional coding. arXiv:0712.2223 (2007)

50. Wilde, M.M., Brun, T.A.: Optimal entanglement formulas for entanglement-assisted quantum coding. Physical Review A **77**, 064,302 (2008)

51. Wilde, M.M., Brun, T.A.: Quantum convolutional coding with shared entanglement: General structure. arXiv:0807.3803 (2008)

52. Wilde, M.M., Brun, T.A.: Unified quantum convolutional coding. In: Proceedings of the IEEE International Symposium on Information Theory (arXiv:0801.0821), pp. 359–363 (2008)

53. Wilde, M.M., Brun, T.A., Dowling, J.P., Lee, H.: Coherent communication with linear optics. Physical Review A **77**(2), 022321 (2008). DOI 10.1103/PhysRevA.77.022321

54. Wilde, M.M., Krovi, H., Brun, T.A.: Coherent communication with continuous quantum variables. Physical Review A **75**(6), 060303 (2007). DOI 10.1103/PhysRevA.75.060303

55. Wilde, M.M., Krovi, H., Brun, T.A.: Convolutional entanglement distillation. arXiv:0708.3699 (2007)

56. Winter, A.: The capacity of the quantum multiple access channel. IEEE Transactions on Information Theory **47**, 3059–3065 (2001)

57. Yard, J.: Simultaneous classical-quantum capacities of quantum multiple access channels. Ph.D. thesis, Stanford University, Stanford, CA (2005). quant-ph/0506050

58. Yard, J., Hayden, P., Devetak, I.: Quantum broadcast channels. arXiv:quant-ph/0603098 (2006)

59. Yard, J., Hayden, P., Devetak, I.: Capacity theorems for quantum multiple-access channels: Classical-quantum and quantum-quantum capacity regions. IEEE Transactions on Information Theory **54**(7), 3091–3113 (2008)

60. Yeung, R.W.: A First Course in Information Theory. Springer (2002)