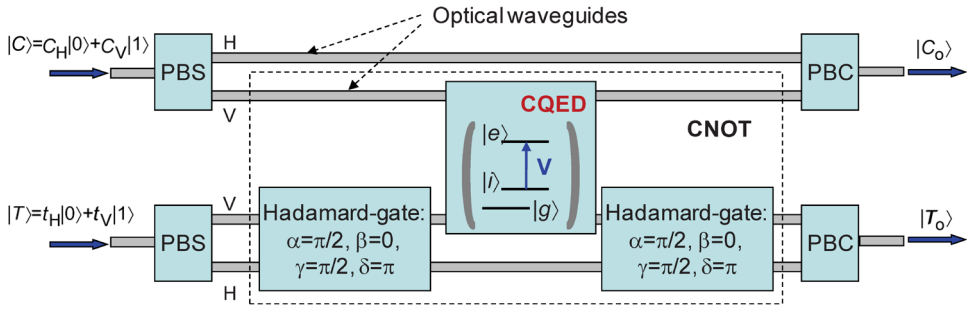
IEEE Photonics Journal
An IEEE Photonics Society Publication

Cavity Quantum Electrodynamics (CQED)-Based Quantum LDPC Encoders and Decoders

Volume 3, Number 4, August 2011

Ivan B. Djordjevic, Senior Member, IEEE



DOI: 10.1109/JPHOT.2011.2162315
1943-0655/$26.00 ©2011 IEEE

Cavity Quantum Electrodynamics (CQED)-Based Quantum LDPC Encoders and Decoders

Ivan B. Djordjevic, *Senior Member, IEEE*

Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721 USA

DOI: 10.1109/JPHOT.2011.2162315
1943-0655/$26.00 ©2011 IEEE

Manuscript received June 20, 2011; revised July 10, 2011; accepted July 12, 2011. Date of publication July 18, 2011; date of current version August 5, 2011. This work was supported in part by the National Science Foundation (NSF) under Grant CCF-0952711 and in part by NSF through the Center for Integrated Access Networks ERC under Grant EEC-0812072. Corresponding author: I. B. Djordjevic (e-mail: ivan@ece.arizona.edu).

Abstract: Quantum information processing (QIP) relies on delicate superposition states that are sensitive to interactions with environment, resulting in errors. Moreover, the quantum gates are imperfect so that the use of quantum error correction coding (QECC) is essential to enable the fault-tolerant computing. The QECC is also important in quantum communication and teleportation applications. The most critical gate, i.e., the CNOT gate, has been implemented recently as a probabilistic device by using integrated optics. CNOT gates from linear optics provide only probabilistic outcomes and, as such, are not suitable for any meaningful quantum computation (on the order of thousand qubits and above). In this paper, we show that arbitrary set of universal quantum gates and gates from Clifford group, which are needed in QECC, can be implemented based on cavity quantum electrodynamics (CQED). Moreover, in CQED technology, the use of the controlled-Z gate instead of the CNOT gate is more appropriate. We then show that encoders/decoders for quantum low-density parity-check (LDPC) codes can be implemented based on Hadamard and controlled-Z gates only using CQED. We also discuss quantum dual-containing and entanglement-assisted codes and show that they can be related to combinatorial objects known as balanced incomplete block designs (BIBDs). In particular, a special class of BIBDs—Steiner triple systems (STSs)— yields to low-complexity quantum LDPC codes. Finally, we perform simulations and evaluate the performance of several classes of large-girth quantum LDPC codes suitable for implementation in CQED technology against that of lower girth entanglement-assisted codes and dual-containing quantum codes.

Index Terms: Quantum information processing (QIP), quantum error correction coding (QECC), cavity quantum electrodynamics (CQED), Clifford group, quantum low-density parity-check (LDPC) codes.

1. Introduction

Quantum information processing (QIP) is an exciting research area with various applications [1], [2]. In order to perform an arbitrary quantum computation, a minimum number of gates, known as universal quantum gates, are needed. The QIP, unfortunately, relies on delicate superposition states, which are sensitive to interactions with environment, resulting in decoherence. Moreover, the quantum gates are imperfect, and the use of quantum error correction coding (QECC) is necessary to enable the fault-tolerant computing and to deal with quantum errors [3]–[7]. QECC is also essential in quantum communication and quantum teleportation applications. The QECC based on structured quantum low-density parity-check (LDPC) codes [3], [7] offers a number of

advantages thanks to the sparseness of corresponding quantum check-matrix, which results in small number of interactions per syndrome measurement. It has been recently demonstrated by author that universal quantum gates can be implemented in integrated optics and all-fiber technologies [5]–[7]. The most critical gate, the CNOT gate has been recently implemented as a probabilistic device in integrated optics [8]–[10]. The CNOT gates from linear optics provide only probabilistic outcomes and as such are not suitable for large-scale computation (on the order of thousand and above). On the other hand, the nonlinear Kerr phase shift up to $\pi/4$ at the single-photon has been demonstrated by Fushman *et al.* [11] by using the cavity quantum electrodynamics (CQED)-based devices, which can be used as a starting point toward the deterministic CNOT-gate implementation. Moreover, since the following equality is valid $HZH = X$ (H is the Hadamard gate; X, Y, and Z are Pauli gates), and the controlled-Z gate is easier to implement in CQED technology than CNOT gate, the controlled-Z gate should be used instead as an element of universal set of quantum gates such as {H, phase (P), $\pi/8$ (T), controlled-Z}. The CQED techniques can be used on many different ways to perform quantum computation, including the following: i) The quantum information can be represented by photon states wherein the cavities with atoms are used to provide the nonlinear interaction between photons [12], [13]; ii) the quantum information can be represented using atoms wherein the photons can be used to communicate between atoms [14]; and iii) the quantum information can represented using quantum interface between a single photon and the spin state of an electron trapped in a quantum dot [15].

In this paper, we show that arbitrary set of universal quantum gates, including {H, P, T, controlled-Z}, can be implemented based on CQED. We then show that the quantum gates from Clifford group needed in QECC can also be implemented using the same technology. We further show that encoders and decoders for quantum LDPC codes can be implemented based only on Hadamard and controlled-Z gates using CQED. We further describe two classes of quantum LDPC codes, namely dual-containing and entanglement-assisted, and relate them to balanced incomplete block designs (BIBDs) of unitary index. In particular, the Steiner triple systems (STS)-based codes have low-decoding complexity. Finally, we perform the Monte Carlo simulations and evaluate performance of several classes of quantum large-girth LDPC codes suitable for implementation in CQED technology. Two CQED-based implementations are studied, namely the photon number states and polarization states-based implementations.

The paper is organized as follows. In Section 2, we describe how to implement the quantum gates needed for the Clifford group and the universal gates in CQED technology. In Section 3, we describe two classes of quantum LDPC codes, i.e., dual-containing and entanglement-assisted LDPC codes, and show that corresponding encoders and decoders can be implemented in the same technology. In Section 4, we provide numerical results in which the performance of two classes of codes are compared. Finally, some important concluding remarks are provided in Section 5.

2. CQED-Based Clifford Group and Universal Quantum Gates

The quantum error correction code can be defined as mapping from K-qubit space to N-qubit space. To facilitate its definition, we introduce the concept of Pauli operators, using a definition due to MacKay *et al.* [3]. A *Pauli operator on N qubits* has the following form $cO_1O_2,\ldots,O_N$, where $O_i \in \{I, X, Y, Z\}$ (X, Y, and Z are Pauli operators), and $c = 1, -1$, i or $-$i (where $\mathrm{i}^2 = 1$). This operator takes $|i_1 i_2,\ldots,i_N\rangle$ to $cO_1|i_1\rangle \otimes O_2|i_2\rangle \ldots \otimes O_N|i_N\rangle$. The set of Pauli operators on N-qubits form the *multiplicative Pauli group* G_N. For multiplicative group we can define the *Clifford operator* [16] U as the operator that preserves the elements of Pauli group under conjugation, namely $\forall\ O \in G_N :\ UOU^{\dagger} \in G_N$. The encoded operator for quantum error correction typically belongs to the Clifford group. To implement any unitary operator from the Clifford group, the use of the CNOT gate U_{CNOT} or an equivalently controlled-Z gate, Hadamard gate H, and phase gate P is sufficient. The Gottesman-Knill theorem [2] showed that gates from the Clifford group are not sufficient to perform arbitrary quantum operation. However, the Clifford set of gates can be extended by either the Toffoli (U_T) or $\pi/8$ (T) gate to obtain a universal set of quantum gates.

We turn our attention now to the CQED implementation of the following set {H, P, T, U_{CNOT}, or controlled-Z} of universal quantum gates using CQED technology by employing option i) from the introduction, namely by representing the quantum information by photon states and by using the cavities with atoms to provide the nonlinear interaction between photons [12], [13]. The H, P, and T gates are single-qubit gates and can be implemented based on one mode of radiation field inside the cavity by passing a two-level atom through the cavity. In the middle of the passage of the atom through the cavity, a short classical pulse of amplitude A_p is to be applied. Let the ground state and excited state of atom be denoted by $|g\rangle$ and $|e\rangle$, respectively, and let the photon number states $|0\rangle$ and $|1\rangle$ represent logic 0 and 1, respectively. The interaction Hamiltonian can be represented by [17]

$$H_{\text{int}} = \hbar\Omega\left(a|e\rangle\langle g| + a^{\dagger}|g\rangle\langle e|\right) \tag{1}$$

where a and $a^{\dagger}$ denote the photon annihilation and creation operators, and Ω is the corresponding vacuum Rabi frequency associated with interaction of the cavity mode with atom states. Based on (1), the time-evolution operator can be derived [17]:

$$U(t) = \cos(\Omega t\sqrt{a^{\dagger}a+1})|g\rangle\left\langle g\right| + \cos(\Omega t\sqrt{a^{\dagger}a+1})\left|e\right\rangle \times \left\langle e\right|-i\frac{\sin(\Omega t\sqrt{a^{\dagger}a+1})}{\sqrt{a^{\dagger}a+1}}a\left|e\right\rangle\left\langle g\right|-ia^{\dagger}\frac{\sin(\Omega t\sqrt{a^{\dagger}a+1})}{\sqrt{a^{\dagger}a+1}}\left|g\right\rangle\langle e| \tag{2}$$

and the time-evolution of initial state $|\psi(0)\rangle$ can be described by $|\psi(t)\rangle = U(t)|\psi(0)\rangle$. The atom-field state $|\psi(0)\rangle = |e,0\rangle$ get unaffected after $\Delta t = \pi/2\Omega$, while $|\psi(0)\rangle = |e,1\rangle$ moves to $-i|g,0\rangle$. After the initial time $\Delta t = \pi/2\Omega$, the pulse of amplitude A_p is applied, which prepares the atom in superposition state [13]:

$$|g\rangle \rightarrow \cos\theta|g\rangle + ie^{-i\phi}\sin\theta|e\rangle,\ |e\rangle \rightarrow ie^{i\phi}\sin\theta|g\rangle + \cos\theta|e\rangle;\ \theta = \omega t/2,\ \omega = |d|A_p/\hbar \tag{3}$$

where $d = |d|e^{i\phi}$ is the dipole moment. The atom again interacts with the cavity field for the same duration $\Delta t = \pi/2\Omega$ so that the initial cavity modes are transformed to [13]:

$$|0\rangle \rightarrow \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle,\ |1\rangle \rightarrow e^{-i\phi}\sin\theta|0\rangle - \cos\theta|1\rangle \tag{4}$$

which is equivalent to the one-qubit unitary operator $U(\theta,\phi)$:

$$U(\theta,\phi) = \begin{bmatrix} \cos\theta & e^{i\phi}\sin\theta \\ e^{-i\phi}\sin\theta & -\cos\theta \end{bmatrix}. \tag{5}$$

For example, by setting $\theta = \pi/4$ and $\phi = 0$, the unitary gate $U(\pi/4,0)$ becomes the Hadamard gate H:

$$U(\pi/4,0) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H. \tag{6}$$

The Z gate is obtained by setting $\theta = \phi = 0$:

$$U(0,0) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z. \tag{7}$$

The P and T gates and other Pauli gates can be obtained by properly selecting θ and ϕ and/or by concatenation of two U-gates with properly chosen parameters. The quantum phase shift gate based on CQED, in which two qubits are represented as two radiation modes inside of cavity in

combination with a three-level atom that provides the desired control interaction, is described in [13]. Namely, the quantum phase shift gate operation can be described by

$$C(U_\alpha) = |0_1 0_2\rangle\langle 0_1 0_2| + |0_1 1_2\rangle\langle 0_1 1_2| + |1_1 0_2\rangle\langle 1_1 0_2| + e^{i\alpha}|1_1 1_2\rangle\langle 1_1 1_2|. \tag{8}$$

By setting $\alpha = \pi$, the controlled-Z, known as $C(Z)$, gate is obtained. The CNOT gate can be obtained simply applying two Hadamard gates on second qubit before and after $C(Z)$ gate as follows:

$$\underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\end{bmatrix}}_{I\otimes H}\underbrace{\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{bmatrix}}_{C(Z)}\underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\end{bmatrix}}_{I\otimes H} = \frac{1}{2}U_{CNOT}, \quad U_{CNOT} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}. \tag{9}$$

More details, about the quantum phase shift gate and underlying operation principle can be found in [13]. Notice that, as indicated in introduction, because of equality $HZH = X$, the controlled-Z gate can be used instead of CNOT gate. The main challenge for CNOT-gate/controlled-Z-gate implementation is to introduce the phase shift of π rad. One approach that was able to introduce the nonlinear Kerr phase shift up to $\pi/4$ at the single-photon was based on the quantum dot in photonic crystal [11], which is, however, insufficient for desired $C(Z)$-operation. The approach described above was based on the photon number states. Below we describe an approach that is based on *photon polarization* and cavity-assisted interaction to achieve the control operation, which is more compatible with existing fiber-optics communication systems. This implementation is also suitable for photonic integration.

In what follows, the logical "0" is represented by a horizontal (H) photon $|\mathrm{H}\rangle \equiv |0\rangle = (1\ 0)^{\mathrm{T}}$, and the logical "1" is represented by a vertical (V) photon $|\mathrm{V}\rangle \equiv |1\rangle = (0\ 1)^{\mathrm{T}}$. We use a polarization beam splitter (PBS) at the input of quantum gate and a polarization beam combiner (PBC) at the output of the gate. The one output (input) of PBS (PBC) is denoted by H, while the other output (input) of PBS (PBC) is denoted by V. The input qubit is denoted by $|\psi\rangle = \psi_{\mathrm{H}}|0\rangle + \psi_{\mathrm{V}}|1\rangle = [\psi_{\mathrm{H}}\ \psi_{\mathrm{V}}]^{\mathrm{T}}$, while the output qubit is denoted by $|\psi_{\mathrm{o}}\rangle = \psi_{\mathrm{o,H}}|0\rangle + \psi_{\mathrm{o,V}}|1\rangle = [\psi_{\mathrm{o,H}}\ \psi_{\mathrm{o,V}}]^{\mathrm{T}}$. In Fig. 1(a), we show an implementation based on single directional coupler, and in Fig. 1(b), we show an implementation based on single optical hybrid (OH), while in Fig. 1(c), we show the corresponding implementation based on single Mach–Zehnder interferometer (MZI). The power splitting ratio k of OH is parameterized as follows $k = \cos^2(\phi/2)$. In all three schemes, the output qubit is related to the input qubit by

$$\begin{bmatrix}\psi_{o,H}\\ \psi_{o,V}\end{bmatrix} = U\begin{bmatrix}\psi_H\\ \psi_V\end{bmatrix}, \qquad U = \begin{bmatrix}\cos\left(\frac{\phi}{2}\right)e^{i(\alpha-\beta/2-\delta/2)} & -\sin\left(\frac{\phi}{2}\right)e^{i(\alpha-\beta/2+\delta/2)}\\ \sin\left(\frac{\phi}{2}\right)e^{i(\alpha+\beta/2-\delta/2)} & \cos\left(\frac{\phi}{2}\right)e^{i(\alpha+\beta/2+\delta/2)}\end{bmatrix}. \tag{10}$$

The U-matrix in (10) represents the matrix representation of an arbitrary single-qubit quantum gate according to the decomposition theorem [2]. For OH, the corresponding phase shifts α, β, δ can be introduced by phase trimmer either thermally or electrooptically, while the proper power splitting ratio $k = \cos^2(\phi/2)$ should be set in fabrication phase. By setting $\phi = \delta = 0$ rad, $\alpha = \pi/4$ and $\beta = \pi/2$ rad U-gate described by (10) operates as the phase gate; by setting $\phi = \delta = 0$ rad, $\alpha = \pi/8$, and $\beta = \pi/4$ rad, the U-gate operates as $\pi/8$ gate, while by setting $\phi = \pi/2$, $\alpha = \pi/2$, $\beta = 0$ rad, and $\delta = \pi$, the U-gate given by (10) operates as Hadamard gate. The Y-gate is obtained by setting $\gamma = \pi$, $\beta = \delta = 0$ rad, and $\alpha = \pi/2$; the Z-gate is obtained by setting $\phi = \delta = 0$ rad, $\alpha = \pi/2$, and $\beta = \pi$; and the X-gate is obtained by setting $\phi = \pi$, $\delta = 0$ rad, $\alpha = \pi/2$, and $\beta = -\pi$. As an illustration, let us provide the derivation of (10) for directional coupler-based gate [see Fig. 1(a)]. We can write the unitary operator U as the product of three unitary operators: i) U_1

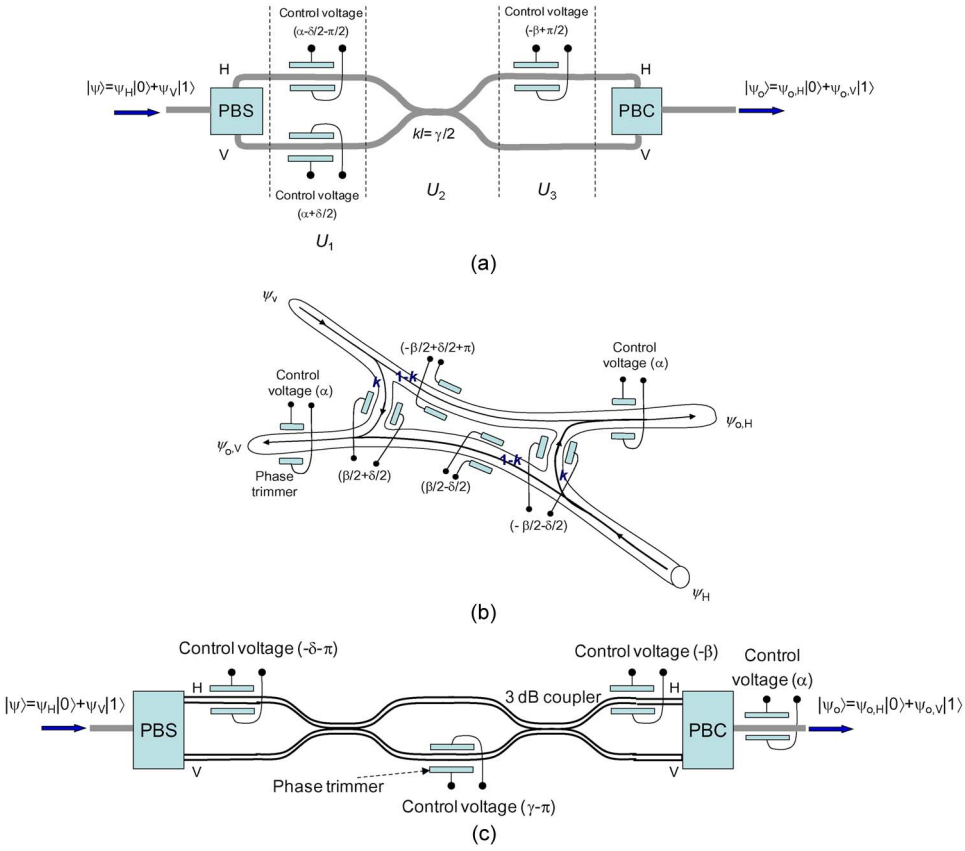


Fig. 1. Photonic implementation of arbitrary single-qubit gate based on (a) single directional coupler, (b) optical hybrid, and (c) Mach–Zehnder interferometer. PBS/C: polarization beam splitter/combiner.

corresponding to the first phase section; ii) U_2 corresponding to the directional coupler section; and iii) U_3 corresponding to the second phase section. When the photon is present in upper branch of the first phase section, it will experience the phase shift $\exp[\mathrm{i}(-\alpha-\delta/2-\pi/2)]$, and the phase shift $\exp[\mathrm{i}(\alpha+\delta/2)]$ when in lower branch, meaning that the matrix representation of this section is

$$U_1 = \begin{bmatrix} e^{i(\alpha-\delta/2-\pi/2)} & 0 \\ 0 & e^{i(\alpha+\delta/2)} \end{bmatrix}. \tag{11}$$

In similar fashion, when the photon is present in upper branch of the second phase section it will experience the phase shift $\exp[\mathrm{i}(-\beta+\pi/2)]$, and no phase shift when in lower branch, indicating that the matrix representation of this section is

$$U_3 = \begin{bmatrix} e^{i(-\beta+\pi/2)} & 0 \\ 0 & 1 \end{bmatrix}. \tag{12}$$

The direction coupler action on H- and V-photons can be described by the creation (annihilation) operators a $(a^\dagger)$ and b $(b^\dagger)$. The action of directional coupler is given by

$$U_2 = e^{-i(\phi/2)(a^\dagger b + ab^\dagger)} = e^{-i(\phi/2)G}, \qquad G = a^\dagger b + ab^\dagger. \tag{13}$$

By using the Baker–Campbell–Hausdorf formula:

$$e^{\lambda G} A e^{-\lambda G} = \sum_{n=0}^{\infty} \frac{\lambda^n}{n!} C_n;\ C_0 = A_0, \qquad C_n = [G, C_{n-1}],\ n = 1, 2, \cdots;\ C_n = \begin{cases} a, & n \text{ - even} \\ -b, & n \text{ - odd} \end{cases} \tag{14}$$

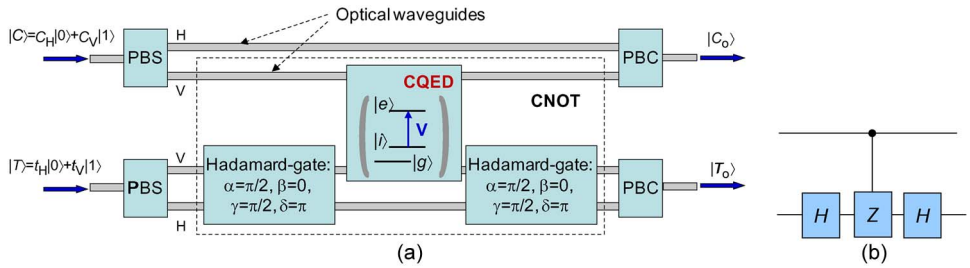


Fig. 2. Deterministic CNOT gate. (a) Possible implementation based on CQED and (b) an equivalent scheme.

we can show that

$$U_2 a U_2^\dagger = e^{-i(\phi/2)G} a e^{+i(\phi/2)G} = \sum_{n=0}^{\infty} \frac{(-i\phi/2)^n}{n!} C_n$$

$$= \sum_{n-\text{even}} \frac{(-i\phi/2)^n}{n!} a - \sum_{n-\text{odd}} \frac{(-i\phi/2)^n}{n!} b = a\cos(\phi/2) + ib\sin(\phi/2)$$

$$U_2 b U_2^\dagger = e^{-i(\phi/2)G} b e^{+i(\phi/2)G} = ia\sin(\phi/2) + b\cos(\phi/2). \tag{15}$$

The corresponding matrix representation is given by

$$U_2 = \begin{bmatrix} \cos(\phi/2) & i\sin(\phi/2) \\ i\sin(\phi/2) & \cos(\phi/2) \end{bmatrix} \tag{16}$$

which is the same as the corresponding expression derived from directional coupler theory. The overall operation of gate from Fig. 1(a) is then

$$\begin{bmatrix} \psi_{o,H} \\ \psi_{o,V} \end{bmatrix} = U_3 U_2 U_1 \begin{bmatrix} \psi_H \\ \psi_V \end{bmatrix} = \begin{bmatrix} e^{i(-\beta+\pi/2)} & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \cos(\phi/2) & i\sin(\phi/2) \\ i\sin(\phi/2) & \cos(\phi/2) \end{bmatrix} \begin{bmatrix} e^{i(\alpha-\delta/2-\pi/2)} & 0 \\ 0 & e^{i(\alpha+\delta/2)} \end{bmatrix} \begin{bmatrix} \psi_H \\ \psi_V \end{bmatrix} \tag{17}$$

proving, therefore, (10). Since the phase shifts can be introduced in integrated optics on single qubits (see [18, Figs. 6 and 7] for more details on fabrication), the proposed quantum gates are implementable in integrated optics technology.

To complete the implementation of the set {H, P, T, U_{CNOT}, or controlled-Z} of universal quantum gates, the implementation of CNOT-gate/controlled-Z-gate is needed. One possible implementation based on CQED, compatible with photon polarization states, is shown in Fig. 2. We also provide an equivalent scheme to facilitate the explanation. To enable the interaction of vertical photons, we use an optical cavity with single trapped 3-level atom, as illustrated in Fig. 2(a). The atom has three relevant levels: the ground $|g\rangle$, the intermediate $|i\rangle$, and the excited $|e\rangle$ states.

The ground and intermediate states are close to each other and can be the hyperfine states. The atom has initially been prepared in superposition state $|\psi_A\rangle = (|g\rangle + |i\rangle)/\sqrt{2}$. The transition $|i\rangle \rightarrow |e\rangle$ is coupled to a cavity mode in vertical polarization, and it is resonantly driven by the vertical photon from the input.

When the incoming photon is in vertical polarization and the atom is in the ground state, the incoming photon is resonant with the cavity mode. It interacts with the atom and after interaction, the atom goes back to the initial state, while the V-photon acquires the phase shift of π rad. If, on the other hand, the atom was in intermediate state, the frequency corresponding to the entangled mode is significantly detuned from the frequency of the input photon, and the photon leaves the cavity

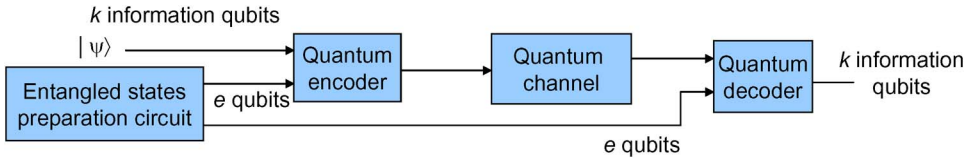


Fig. 3. Entanglement-assisted quantum code.

with no phase change. The operation of gate shown in Fig. 2, by ignoring the Hadamard gates, can be described by

$$U_{AC}R_A(-\theta)U_{AT}R_A(\theta)U_{AC}|CT\rangle|\psi_A\rangle \tag{18}$$

where $|\psi_A\rangle$ denotes the initial atom state $(|g\rangle + |i\rangle)/\sqrt{2}$, $|CT\rangle$ is the input two-qubit state, U_{AC} (U_{AT}) denotes the operator describing atom-control-photon (atom-target-photon) interaction, and $U_A(\theta)$ is the atom-rotation operator performed by applying the θ-pulse on the atom. In the absence of control-vertical photon the action of operators above is simply identity operator since $R_A(-\theta)R_A(\theta) = I$ and $U_{AC}^2 = I$. In the presence of control-vertical photon, the sequence of operators is as follows: i) The vertical-control-photon interacts with the atom; ii) the rotation operator is applied on the atom; iii) the target-vertical-photon interacts with the atom; iv) the de-rotation operator is applied on the atom; and v) the vertical-target-photon interacts with the atom. After this sequence of operators, the control-photon and atom go back to initial states, while the target-photon achieves the π phase shift. Therefore, the overall action is controlled-Z operation. The additional two Hadamard gates are used to perform the following transformation: $HZH = X$, resulting in CNOT-gate operation. Someone may follow a more rigorous derivation by applying the similar procedure to that provided in [13]. From Fig. 2, it is evident that the use of the controlled-Z gate instead of the CNOT gate for quantum computing applications and quantum teleportation is more appropriate in CQED technology, since the controlled-Z gate implementation is simpler (two Hadamard gates from Fig. 2 are not needed for controlled-Z-gate implementation). The quantum gate shown in Fig. 2 is suitable for implementation in photon crystal technology [19]. For proper operation, the on-chip integration is required. The first step toward this implementation would be achieving the coherent control of quantum $|CT\rangle$ states from Z (18). The quantum-error correction-based fault-tolerant concepts should be used to facilitate this implementation. Given this description of universal quantum gates, in the next section, we describe the design and implementation of quantum LDPC coding using CQED technology.

3. CQED-Based Quantum LDPC Encoders and Decoders

In this section, we describe two classes of sparse-graph quantum codes, i.e., i) quantum dual-containing LDPC codes and ii) entanglement-assisted LDPC codes, and show that corresponding encoders and decoders can be implemented in CQED technology. The block-scheme of entanglement-assisted quantum code, which requires a certain number of entangled qubits to be shared between the source and destination, is shown in Fig. 3.

The number of needed pre-existing entanglement qubits (also known as ebits [4]) can be determined by $e = \text{rank}(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}})$, where $\boldsymbol{H}$ is the parity-check matrix of a classical code (and rank(.) is the rank of a given matrix). The source encodes quantum information in state $|\psi\rangle$ with the help of local ancilla qubits $|0\rangle$ and source-half of shared ebits and then sends the encoded qubits over a noisy quantum channel (e.g., free-space or fiber-optic channel). The receiver performs decoding on all qubits to diagnose the channel error and performs a recovery unitary operation to reverse the action of the channel.

Notice that the channel does not affect the receiver's half of shared ebits at all. By omitting the ebits, the conventional quantum coding scheme is obtained.

Most practical quantum codes belong to the class of CSS codes [1]–[3] and can be designed using a pair of conventional linear codes satisfying the twisted property (one code includes the dual

of another code). Their quantum-check matrix has the form

$$\boldsymbol{A} = \left[\begin{array}{c|c} \boldsymbol{H} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{G} \end{array}\right], \quad \boldsymbol{H}\boldsymbol{G}^{T} = \boldsymbol{0} \tag{19}$$

where $\boldsymbol{H}$ and $\boldsymbol{G}$ are $M \times N$ matrices. The condition $\boldsymbol{H}\boldsymbol{G}^{\mathrm{T}} = \boldsymbol{0}$ ensures that twisted product condition is satisfied. Each row in (19) represents a stabilizer, with ones in the left-half of $\boldsymbol{A}$ corresponding to the positions of X-operators and ones in the right-half ($\boldsymbol{G}$) corresponding to the positions of Z-operators. As there are $2M$ stabilizer conditions applying to N qubit states, $N - 2M$ qubits are encoded in N qubits. The commutativity of stabilizers now appears as *orthogonality of rows* with respect to a *twisted* (*sympletic*) *product*, which are formulated as follows: If the kth row in $\boldsymbol{A}$ is $r_k = (x_k; z_k)$, where x_k is the X binary string and z_k is the Z binary string, then the twisted product of rows k and l is defined by [3]

$$r_k \odot r_l = x_k \cdot z_l + x_l \cdot z_k \bmod 2 \tag{20}$$

where $x_k \cdot z_l$ is dot (scalar) product defined by $x_k \cdot z_l = \sum_j x_{kj} z_{lj}$. The twisted product is zero if and only if there is an even number of places where the operators corresponding to rows k and l differ (and are neither the identity), i.e., if the operators commute. The CSS codes based on dual-containing codes are simplest to implement. Their (quantum) check matrix can be represented by [1]–[3]

$$\boldsymbol{A} = \left[\begin{array}{c|c} \boldsymbol{H} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{H} \end{array}\right] \tag{21}$$

where $\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}} = 0$, which is equivalent to $C^{\perp}(\boldsymbol{H}) \subset C(\boldsymbol{H})$, where $C(\boldsymbol{H})$ is the code having $\boldsymbol{H}$ as the parity-check matrix, and $C^{\perp}(\boldsymbol{H})$ is its corresponding dual code. The quantum LDPC codes have many advantages over other classes of quantum codes, thanks to the sparseness of their parity-check matrices [3], [7]. From (21), it follows that by providing that the $\boldsymbol{H}$-matrix of a dual-containing code is sparse, the corresponding $\boldsymbol{A}$-matrix will be sparse as well, while corresponding stabilizers will be of low weight. For example, the $\boldsymbol{H}$-matrix given below satisfies the condition $\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}} = 0$ and can be used in quantum check matrix (21) as dual-containing code:

$$\boldsymbol{H} = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

The main drawback of dual-containing LDPC codes is the fact that they are essentially girth-4 codes,[1] which do not perform well under sum-product algorithm (commonly used in decoding of LDPC codes). On the other hand, it was shown in [6] that the use of entanglement arbitrary classical codes can be used in correction of quantum errors and not only girth-4 codes. Because quantum key distribution (QKD) and quantum teleportation systems assume the use of entanglement, this approach does not increase the complexity of the system *at all*.

The number of entanglement qubits (ebits) needed in EA LDPC codes is $e = \mathrm{rank}(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}})$, as indicated above, so that minimum number of required EPR pairs (Bell states) is one, which is

[1]Girth represents the shortest cycle in corresponding bipartite graph representation of a parity-check matrix of classical code.

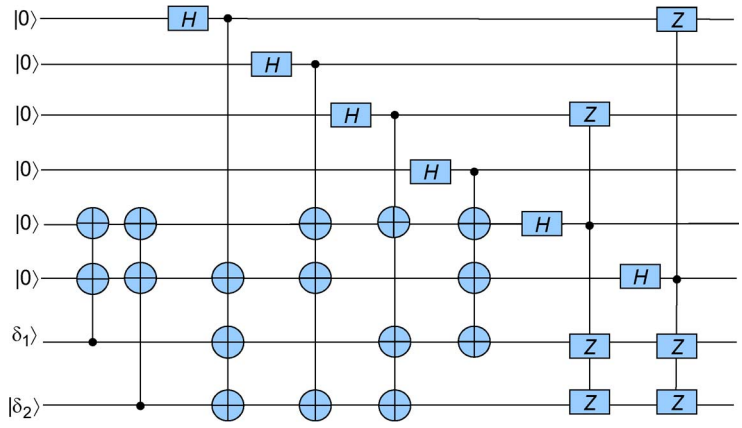


Fig. 4. Encoding circuit for quantum (8,2) LDPC code. $|\delta_1\delta_2\rangle$ are information qubits.

exactly the same as already in use in certain QKD schemes. For example, an LDPC code given below has rank$(\boldsymbol{H}_1\boldsymbol{H}_1^{\mathrm{T}}) = 1$ and girth 6:

$$\boldsymbol{H}_1 = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

and requires only one ebit to be shared between source and destination. Since arbitrary classical codes can be used with this approach, including LDPC code of girth $g \geq 6$, the performance of quantum LDPC codes can significantly be improved. Notice that $\boldsymbol{H}$-matrix above is obtained from $\boldsymbol{H}_1$-matrix by adding all 1's column.

Because two Pauli operators on N-qubits commute if and only if there is an even number of places in which they differ (neither of which is the identity I operator), we can extend the generators in $\boldsymbol{A}$ (for $\boldsymbol{H}_1$) by adding the $e = 1$ column so that they can be embedded into a larger Abelian group; the procedure is known as Abelianization in abstract algebra. One may use a stabilizer version of Gram–Schmidt orthogonalization algorithm to simplify this procedure, as indicated in [4].

For example, by performing Gauss–Jordan elimination, the quantum check matrix (21) can be put in standard form (see [16] for definition of standard form representation of quantum check matrix):

$$\boldsymbol{A} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

The corresponding generators in standard form are

$$g_1 = X_1X_6X_7X_8, \quad g_2 = X_2X_5X_6X_8, \quad g_3 = X_3X_5X_7X_8$$
$$g_4 = X_4X_5X_6X_7, \quad g_5 = Z_3Z_5Z_7Z_8, \quad g_6 = Z_1Z_6Z_7Z_8$$

where the subscripts are used to denote the positions of corresponding X- and Z-operators. The encoding circuit is shown in Fig. 4. We use the efficient implementation of encoders introduced by Gottesman [16]. It is clear from Fig. 4 that for encoder implementation of quantum LDPC codes,

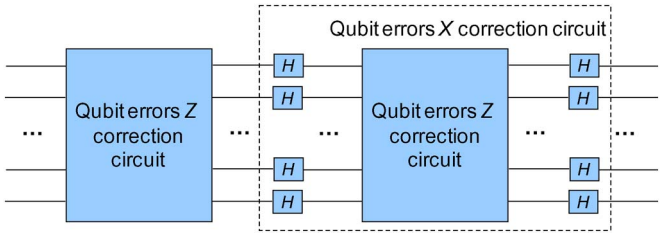


Fig. 5. Quantum LDPC decoder of CSS type implementation based only on controlled-Z gates.

Hadamard (H), CNOT ($\oplus$), and controlled-Z gates are sufficient, whose implementation in CQED technology is already discussed in Section 2. From Fig. 2, it is clear that controlled-X gate in CQED technology is typically implemented based on one controlled-Z and two H-gates. Therefore, by using the equivalency shown in Fig. 2(b), the quantum LDPC encoder can be implemented based only on Hadamard and controlled-Z gates, and their implementation is therefore compatible with CQED technology. Because $\mathrm{H}^2 = I$, the corresponding circuit based on H-gates and controlled-Z gates can be simplified. It can be shown in similar fashion that the corresponding decoder can be implemented based only on H-gates and controlled-Z gates. (Notice that simplest decoder is obtained by using stabilizer formalism, as we described in [5].) By closer inspection of (21), we can conclude that generators for CSS design employ exclusively either X- or Z-gates but not both. This is also evident from the example above (generators g_1, g_2, g_3, and g_4 contain only X-operators, while generators g_5 and g_6 contain only Z-operators). Therefore, quantum LDPC decoders of CSS type can be implemented based on controlled-Z gates only, as shown in Fig. 5. For entanglement-assisted LDPC decoder implementation, we need to follow procedure described above, in text related to Fig. 4.

We turn our attention now to the design of quantum LDPC codes based on STSs [20]. The STS represents a particular instance of a BIBD [20]. The BIBD(v, k, λ) is defined as collection of blocks of length k for the set V of integers of size v, such that each pair of elements of V occur together in exactly λ of the blocks. The STS(v) is defined as an BIBD$(v, 3, 1)$. We have shown in [7] that BIBD of even λ can be used to design the quantum LDPC codes belonging to CSS codes, by using dual-containing classical codes. We also shown in [6] that BIBDs of unitary index $(\lambda = 1)$ can be used to design the entanglement-assisted LDPC codes that require only one ebit to be shared between source and destination, since rank$(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}) = 1$. For example, the STS(7) is given by the following collection of blocks of length $k = 3$: {2, 4, 6}, {6, 3, 7}, {5, 6, 1}, {3, 2, 5}, {1, 7, 2}, {7, 5, 4}, {4, 1, 3}. By identifying these blocks with non-zero positions of corresponding parity-check matrix, we obtain an LDPC code of girth-6 satisfying the property rank$(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}) = 1$. For example, $\boldsymbol{H}_1$-matrix above is obtained from STS(7). By adding all 1's column to such obtain matrix, we obtain a dual-containing code since rank$(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}) = 0$. The $\boldsymbol{H}$-matrix above is obtained using this simple approach. Therefore, both entanglement-assisted codes and dual-containing quantum codes can be obtained by using STSs. By selectively removing the blocks from STSs, we can increase the girth of corresponding LDPC code and, therefore, improve BER performance, at the expense of increasing the complexity of an equivalent entanglement-assisted LDPC codes since now rank$(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}) > 1$. For more details about various STSs, see [20, Ch. 6]. Notice that the codes from STSs are easy to implement because column-weight of corresponding classical parity-check matrices is only 3, while the parity-check matrices' column-weight of projective geometry (PG)-based codes [6], [20], which also satisfy rank$(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}) = 1$ property, is huge (see Fig. 6).

4. Performance Analysis of Entanglement-Assisted Large-Girth LDPC Codes

In Fig. 6, we provide comparison of EA LDPC codes of girth $g = 6, 8, 10,$ and 12 against dual-containing LDPC code $(g = 4)$. With parameter c, we denoted the column-weight of corresponding parity-check matrix. The dual contained code of girth-4 is designed based on the BIBDs we

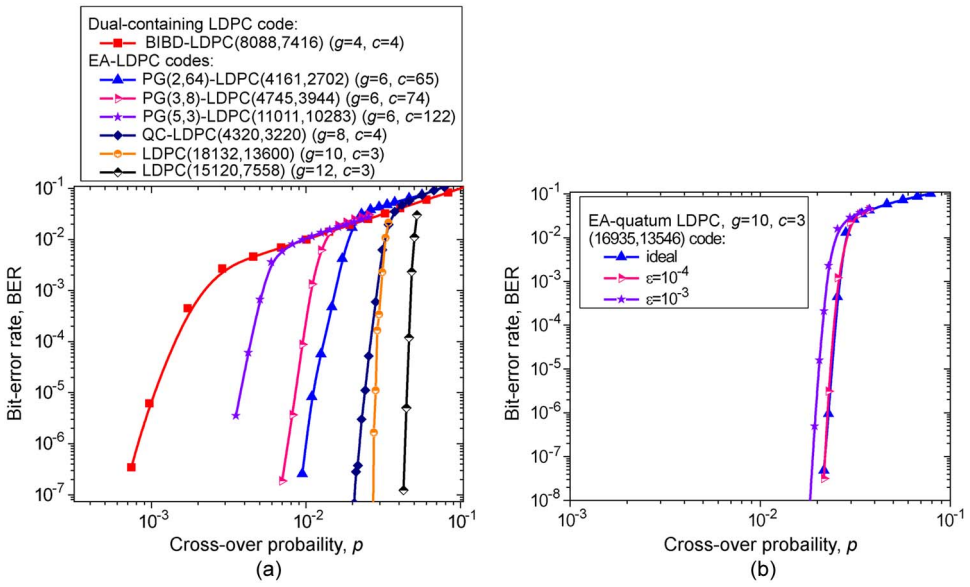


Fig. 6. BER performance of various quantum codes. (a) Assuming that gates are perfect, and (b) assuming that gates are imperfect. BIBD: balanced incomplete block design, PG: projective geometry, QC: quasi-cyclic code, EA: entanglement-assisted codes. The parameters g and c denote girth and column-weight of corresponding parity-check matrix, respectively.

described in [7]. The entanglement-assisted codes from PGs are designed as we described in [6] (see also [21] and [22]). These codes are of girth-6 but require only one ebit to be shared between source and destination. The entanglement-assisted codes of girth 10 and 12 are obtained in a similar fashion to STS described above by selectively removing the blocks from the design.

From Fig. 6(a), it is clear that EA LDPC codes outperform for more than an order of magnitude, in terms of cross-over probability, the corresponding dual-containing LDPC code. It is also evident that as we increase the girth, we get better performance, at the expense of increased entanglement-complexity since $\text{rank}(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}) > 1$ for $g > 6$ codes and increases as girth increases. Notice, however, that finite geometry codes [21], [22] typically have large column-weight (see Fig. 6) so that although they require a small number of ebits, their decoding complexity is high because of huge column-weight. In practice, we will need to make a compromise between decoding complexity, number of required ebits, and BER performance. The results shown in Fig. 6(a) are obtained by assuming that quantum gates are perfect. In Fig. 6(b), we study the influence of imperfect quantum gates on BER performance for girth-8 EA LDPC (16935, 13546) code. Namely, some practical problems such as dissipation through lossy cavity and atomic decoherence will affect the operation of gates, causing the controlled-Z gate (or equivalently CNOT gate) to fail with certain probability. When gates fail with probability $\varepsilon = 10^{-4}$, the BER performance loss is negligible. On the other hand, when the gates fail with probability $\varepsilon = 10^{-3}$, the BER performance loss is small but noticeable.

5. Conclusion

We have shown that an arbitrary set of universal quantum gates, including {H, P, T, controlled-Z}, can be implemented based on CQED technology. We have also shown how to implement various gates operators from the Clifford group, which are needed in quantum error correction, by using the same technology. Because the QIP relies on delicate superposition states and quantum gates are imperfect, the use of QECC is necessary. The use of QECC is also essential in quantum communications and teleportation applications. We have shown that the encoders and decoders for arbitrary quantum error correcting code can be implemented based on CQED. In particular, the quantum LDPC codes are discussed because they offer several advantages compared with other class of quantum codes thanks to the sparseness of their quantum-check matrix.

For the completeness of presentation, we have shown that BIBDs can be used to design both dual-containing quantum codes and entanglement-assisted quantum codes. In particular, the codes designed from STSs are simple to implement compared with finite geometry codes [21], [22]. We further show that the basic building blocks for quantum LDPC codes are Hadamard and controlled-Z gates, and their implementation is compatible with CQED technology. Finally, we have performed Monte Carlo simulations and shown that that the entanglement-assisted LDPC codes of large-girth significantly outperform corresponding dual-containing and lower-girth entanglement-assisted LDPC codes.

Because dissipation through lossy cavity and atomic decoherence affect the operation of gates, to account for these practical problems, we assumed that the controlled-Z gate (or equivalently CNOT gate) fails with certain probability, and we evaluate the performance of EA-quantum LDPC (16935, 13546) with faulty gates [see Fig. 6(b)]. We have shown that when gates fail with probability $\varepsilon = 10^{-3}$, the BER performance loss is small but noticeable.

An important practical problem to be addressed in the future is related to the trapping of the atom within the cavity that requires ultra-cold conditions. As a solution, instead, the quantum-dot approach can be used as indicated in [11].

References

[1] F. Gaitan, *Quantum Error Correction and Fault Tolerant Quantum Computing*. Boca Raton, FL: CRC, 2008.
[2] M. A. Neilsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.
[3] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2315–2330, Oct. 2004.
[4] T. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, Oct. 2006.
[5] I. B. Djordjevic, "Photonic implementation of quantum relay and encoders/decoders for sparse-graph quantum codes based on optical hybrid," *IEEE Photon. Technol. Lett.*, vol. 22, no. 19, pp. 1449–1451, Oct. 2010.
[6] I. B. Djordjevic, "Photonic entanglement-assisted quantum low-density parity-check encoders and decoders," *Opt. Lett.*, vol. 35, no. 9, pp. 1464–1466, May 2010.
[7] I. B. Djordjevic, "Quantum LDPC codes from balanced incomplete block designs," *IEEE Commun. Lett.*, vol. 12, no. 5, pp. 389–391, May 2008.
[8] T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White, "Linear optical controlled-NOT gate in the coincidence basis," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 6, pp. 062324-1–062324-5, Jun. 2002.
[9] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature*, vol. 409, no. 6816, pp. 46–52, Jan. 2001.
[10] A. Politi, M. Cryan, J. Rarity, S. Yu, and J. L. O'Brien, "Silica-on-silicon waveguide quantum circuits," *Science*, vol. 320, no. 5876, pp. 646–649, May 2008.
[11] I. Fushman, D. Englund, A. Faraon, N. Stoltz, P. Petroff, and J. Vuckovic, "Controlled phase shifts with a single quantum dot," *Science*, vol. 320, no. 5877, pp. 769–772, May 2008.
[12] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, "Measurement of conditional phase shifts for quantum logic," *Phys. Rev. Lett.*, vol. 75, no. 25, pp. 4710–4713, Dec. 1995.
[13] M. S. Zubairy, M. Kim, and M. O. Scully, "Cavity-QED-based quantum phase gate," *Phys. Rev. A, Gen. Phys.*, vol. 68, no. 3, p. 033820, Sep. 2003.
[14] C.-H. Su, A. D. Greentree, W. J. Munro, K. Nemoto, and L. C. L. Hollenberg, "High-speed quantum gates with cavity quantum electrodynamics," *Phys. Rev. A, Gen. Phys.*, vol. 78, no. 6, p. 062336, Dec. 2008.
[15] C. Bonato, F. Haupt, S. S. R. Oemrawsingh, J. Gudat, D. Ding, M. P. van Exter, and D. Bouwmeester, "CNOT and bell-state analysis in the weak-coupling cavity QED regime," *Phys. Rev. Lett.*, vol. 104, no. 16, p. 160503, Apr. 2010.
[16] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, Calif. Inst. Technol., Pasadena, CA, 1997.
[17] M. O. Scully and M. S. Zubairy, *Quantum Optics*. Cambridge, U.K.: Cambridge Univ. Press, 1997.
[18] A. Politi, J. C. F. Matthews, M. G. Thompson, and J. L. O'Brien, "Integrated quantum photonics," *IEEE J. Sel. Topics Quantum Electron.*, vol. 15, no. 6, pp. 1673–1684, Nov./Dec. 2009.
[19] A. Faraon, A. Majumdar, D. Englund, E. Kim, M. Bajcsy, and J. Vuckovic, "Integrated quantum optical networks based on quantum dots and photonic crystals," *New J. Phys.*, vol. 13, p. 055025, May 2011.
[20] I. Anderson, *Combinatorial Designs and Tournaments*. London, U.K.: Oxford Univ. Press, 1997.
[21] I. B. Djordjevic, S. Sankaranarayanan, and B. Vasic, "Projective plane iteratively decodable block codes for WDM high-speed long-haul transmission systems," *J. Lightw. Technol.*, vol. 22, no. 3, pp. 695–702, Mar. 2004.
[22] S. Sankaranarayanan, I. B. Djordjevic, and B. Vasic, "Iteratively decodable codes on m-flats for WDM high-speed long-haul transmission," *J. Lightw. Technol.*, vol. 23, no. 11, pp. 3696–3701, Nov. 2005.