Photonic entanglement-assisted quantum low-density parity-check encoders and decoders

Ivan B. Djordjevic

Electrical and Computer Engineering, University of Arizona, 1230 E. Speedway Boulevard, Tucson, Arizona 85721, USA (ivan@ece.arizona.edu)

Received March 1, 2010; accepted March 13, 2010;
posted April 1, 2010 (Doc. ID 124768); published April 30, 2010

I propose encoder and decoder architectures for entanglement-assisted (EA) quantum low-density parity-check (LDPC) codes suitable for all-optical implementation. I show that two basic gates needed for EA quantum error correction, namely, controlled-NOT (CNOT) and Hadamard gates can be implemented based on Mach–Zehnder interferometer. In addition, I show that EA quantum LDPC codes from balanced incomplete block designs of unitary index require only one entanglement qubit to be shared between source and destination. © 2010 Optical Society of America

OCIS codes: 270.5565, 270.5585, 130.3120.

Quantum information processing (QIP) is an exciting research area with a very wide range of applications [1–3]. QIP relies on fragile superposition states, which are sensitive to interactions with environment and decoherence, resulting in errors. To deal with decoherence and quantum errors, QIP has to employ quantum error-correction codes (QECCs). Inspired by the conjecture that the best quantum error-correcting codes can be related to the best classical codes [1], MacKay *et al.* recently proposed [2] how to design the sparse dual-containing binary codes that can be used to construct quantum low-density parity-check (LDPC) codes belonging to the class of Calderbank–Shor–Steane codes [1]. Following MacKay's paper, a number of quantum LDPC code designs have been proposed recently. Most of the designs belong to the class of dual-containing Calderbank–Shor–Steane codes that are essentially girth-4 codes, which perform badly under the sum–product algorithm (commonly used in decoding of LDPC codes). On the other hand, it was shown in [3] that through the use of entanglement arbitrary classical codes can be used in correction of quantum errors, not only girth-4 codes; this class of quantum codes is known as entanglement-assisted (EA) QECCs [3].

In this Letter, I show that LDPC codes from balanced incomplete block designs (BIBDs) of unitary index require only one ebit to be shared between source and destination. Because these codes have a girth of at least 6, they are capable of significantly outperforming previously proposed dual-containing LDPC codes, as is shown below. I further propose several quite general classes of BIBDs of index unity suitable for design of EA LDPC codes of girth at least 6, with the number of required ebits being one. I further show that two basic quantum gates needed for the implementation of EA encoders and decoders in integrated optics or photonic crystal technology, CNOT (controlled-NOT) and Hadamard gates, can be implemented by using a Mach–Zehnder interferometer (MZI).

The EA-QECCs [3] use pre-existing entanglement between transmitter and receiver to improve the reliability of transmission. Because dual-containing LDPC codes are in fact girth-4 codes, the existence of short cycles causes the error performance to deteriorate by correlating extrinsic information in the decoding process. By using the EA-QECC concept, arbitrary classical code can be used as quantum code. That is, if classical codes are not dual-containing, they correspond to a set of stabilizer generators that do not commute. By providing the entanglement between source and destination, the corresponding generators can be embedded into larger set of commuting generators, which gives a well-defined code space. By using LDPC codes of girth at least 6 I can dramatically improve the performance and reliability of current quantum key distribution schemes, as shown in Fig. 5. The number of ebits required for EA-QECC is determined by $e=\mathrm{rank}(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}})$, as I indicated above. Notice that for dual-containing codes $\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{0}$, meaning that the number of required ebits is zero. Therefore, the minimum number of ebits in an EA-QECC is 1, and here we are concerned with the design of LDPC codes of girth $g\geq 6$ with $e=1$. For example, an EA quantum LDPC code of quantum check matrix $\boldsymbol{A}$, given below, has $\mathrm{rank}(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}})=1$ and girth 6:

$$\boldsymbol{A}=\begin{pmatrix}\boldsymbol{H} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{H}\end{pmatrix},\quad \boldsymbol{H}=\begin{bmatrix}1&0&1&1&1\\1&1&0&0&1\\0&1&1&1&0\end{bmatrix}. \tag{1}$$

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 $\boldsymbol{A}$ by adding $e=1$ column so that they can be embedded into a larger Abelian group; the procedure is known as Abelianization in abstract algebra. For example, adding a $(0\ 1\ 1)^{\mathrm{T}}$ column to the $\boldsymbol{H}$ matrix above yields a dual-containing quantum code, and the corresponding quantum-check matrix is given by

$$\boldsymbol{A}'=\begin{pmatrix}\boldsymbol{H}' & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{H}'\end{pmatrix},\quad \boldsymbol{H}'=\left(\begin{array}{ccccc|c}1&0&1&1&1&0\\1&1&0&0&1&1\\0&1&1&1&0&1\end{array}\right). \tag{2}$$

The last column in $\boldsymbol{H}'$ corresponds to the ebit, the qubit that is shared between the source and destina-

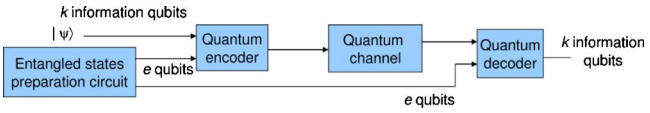

Fig. 1. (Color online) EA quantum code principle.

tion, which is illustrated in Fig. 1. The source encodes quantum information in state $|\psi\rangle$ with the help of local ancilla qubits $|0\rangle$ and the source half of shared ebits and then sends the encoded qubits over a noisy quantum channel (say, a free-space optical channel or optical fiber). 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 the shared ebits. We can further put such an obtained quantum-check matrix in standard form by Gauss–Jordan elimination:

$$\boldsymbol{A} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}. \quad (3)$$

The encoding circuit is shown in Fig. 2(a), while the decoding circuit is shown in Fig. 2(b). It is clear from Fig. 2 that for encoder and decoder implementation of quantum EA-LDPC codes Hadamard (H) and CNOT ($\oplus$) gates are sufficient.

I further discuss the implementation of Hadamard and CNOT gates in integrated optics or photonic crystal technology by using a MZI. The logical "0" is represented by a horizontal (H) photon $|\mathrm{H}\rangle \equiv |0\rangle$, and the logical "1" is represented by a vertical (V) photon $|\mathrm{V}\rangle \equiv |1\rangle$. The Hadamard gate can be implemented based on a MZI, as shown in Fig. 3(a). I use a polarization beam splitter (PBS) at the input of the quantum gate and a polarization beam combiner (PBC) at the output of the gate. The horizontal output (input) of the PBS (PBC) is denoted H, while the vertical output (input) of the PBS (PBC) is denoted V. The input qubit is denoted $|\psi\rangle = \psi_{\mathrm{H}}|0\rangle + \psi_{\mathrm{V}}|1\rangle = [\psi_{\mathrm{H}}\ \psi_{\mathrm{V}}]^{\mathrm{T}}$, while the output qubit is denoted $|\psi_{\mathrm{o}}\rangle = \psi_{\mathrm{o,H}}|0\rangle + \psi_{\mathrm{o,V}}|1\rangle = [\psi_{\mathrm{o,H}}\ \psi_{\mathrm{o,V}}]^{\mathrm{T}}$. It can be shown that output qubit is related by to the input qubit by

$$\begin{bmatrix} \psi_{o,H} \\ \psi_{o,V} \end{bmatrix} = U \begin{bmatrix} \psi_H \\ \psi_V \end{bmatrix}, \quad U = \begin{bmatrix} -\sin(\phi/2) & \cos(\phi/2) \\ \cos(\phi/2) & \sin(\phi/2) \end{bmatrix}. \quad (4)$$

By selecting $\phi = -\pi/2$, the corresponding unitary matrix U above is the same as the matrix representation of a Hadamard gate.

The implementation of the CNOT gate in integrated optics, based on a MZI, is shown in Fig. 3(b). Notice that some other proposals for implementation of CNOT gates [4] are probabilistic rather than deterministic. In addition, from Eq. (2) in [4] it is clear that the control qubit (in a directional coupler CNOT gate proposal) is affected by the target qubit, which violates the definition of a CNOT gate from [1]. In my proposal, shown in Fig. 3(b), I use the tap coupler to detect the presence of a photon in the c_{V} waveguide. In the absence of a c_{V} photon I apply corresponding control voltages to introduce the phase shifts of π rad. In the presence of a photon, the applied voltages are equal to 0 V. By using directional coupling theory it can be shown that output control $|C_{\mathrm{o}}\rangle = [c_{\mathrm{H,o}}\ c_{\mathrm{V,o}}]^{\mathrm{T}}$ and target qubits $|T_{\mathrm{o}}\rangle = [t_{\mathrm{H,o}}\ t_{\mathrm{V,o}}]^{\mathrm{T}}$ are related to corresponding input qubits by

$$\begin{pmatrix} c_{\mathrm{H,o}} \\ c_{\mathrm{V,o}} \\ t_{\mathrm{H,o}} \\ t_{\mathrm{V,o}} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \sin(\phi/2) & e^{j\alpha}\cos(\phi/2) \\ 0 & 0 & \cos(\phi/2) & -e^{j\alpha}\sin(\phi/2) \end{pmatrix} \begin{pmatrix} c_{\mathrm{H}} \\ c_{\mathrm{V}} \\ t_{\mathrm{H}} \\ t_{\mathrm{V}} \end{pmatrix}, \quad (5)$$

where ϕ is the phase shift introduced by the first phase trimmer and α is the phase shift introduced by the second phase trimmer. In the absence of a c_{V} photon the phase shifts $\phi = \alpha = \pi$ rad, and the gate described by Eq. (5) operates as a identity operator. In the presence of a c_{V} photon the phase shifts $\phi = \alpha = 0$ rad, and the gate operates as the CNOT gate.

In what follows, I provide several quite general BIBD-based LDPC code designs with $\mathrm{rank}(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}) = 1$ and girth at least 6. A BIBD(v, k, λ) is a collection of subsets (blocks) of a set V of size v, with the size of each block being k, so that (i) each pair of elements occurs in *exactly* λ of the subsets, and (ii) every element occurs in exactly r subsets. The incidence matrix of a BIBD(v, k, λ) with b blocks, which corresponds to a parity-check matrix of an LDPC code, is a $b \times v$ matrix $\boldsymbol{H} = (h_{ij})$ defined by $h_{ij} = 1$ if the ith block is contains the jth point; otherwise $h_{ij} = 0$. Because any two rows or columns in $\boldsymbol{H}$ overlap in exactly one position, providing that the row weight r is odd, the matrix $\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}$ is an all-one matrix of rank 1. Therefore, LDPC codes from BIBDs of unity index ($\lambda = 1$) and

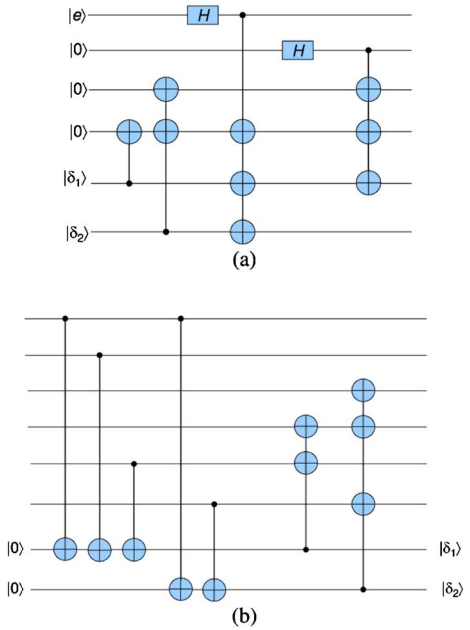

Fig. 2. (Color online) Encoding and decoding circuits for (5, 2) EA-LDPC code: (a) encoder configuration, and (b) decoder configuration. The states $|\delta_1\rangle$ and $|\delta_2\rangle$ are the information states.

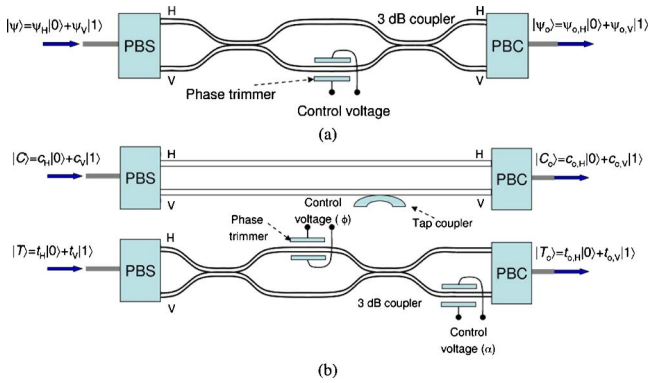

Fig. 3. (Color online) Implementation of basic quantum gates needed for EA-QECC in integrated optics based on a MZI: (a) Hadamard gate, and (b) CNOT gate. PBS/C, polarization-beam splitter/combiner.

odd r have $e=\mathrm{rank}(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}})=1$. The cycle of length four can be identified by searching the $\boldsymbol{H}$ matrix for four ones in the vertices of the rectangle. This cycle of length four exists if there are any two columns that overlap in two positions. Since in LDPC codes derived from BIBDs any two columns overlap in exactly one bit position, there are no cycles of length 4, and therefore, the girth of codes derived from BIBDs is 6. Because the girth of these codes is 6, they can significantly outperform quantum dual-containing LDPC codes (see Fig. 5). Below I describe two BIBDs of girth 6 with the property that $\mathrm{rank}(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}})=1$.

Design 1 (Steiner triple system). If $6t+1$ is a prime power and θ is a primitive root of $\mathrm{GF}(6t+1)$, then the following t initial blocks $(\theta^i, \theta^{2t+i}, \theta^{4t+i})$ $(i=0,1,\ldots,t-1)$ form BIBD$(6t+1,3,1)$ with $r=3t$. The BIBD is formed by adding the elements from $\mathrm{GF}(6t+1)$ to the initial blocks. The corresponding LDPC code has $\mathrm{rank}(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}})=1$ and girth of at least 6.

Design 2 (m-dimensional projective geometries). The finite projective geometries $\mathrm{PG}(m,p^s)$ are constructed by using $(m+1)$-tuples $\mathbf{x}=(x_0,x_1,\ldots,x_m)$ of elements x_i from $\mathrm{GF}(p^s)$ (p a prime, s a positive integer), not all simultaneously equal to zero, called "points." Two-dimensional projective geometries are known as projective planes. Two $(m+1)$-tuples $\boldsymbol{x}$ and $\mathbf{y}=(y_0,y_1,\ldots,y_m)$ represent the same point if $\boldsymbol{y}=\lambda\boldsymbol{x}$, where λ is a nonzero element from $\mathrm{GF}(p^s)$. Therefore, each point can be represented in p^s-1 ways

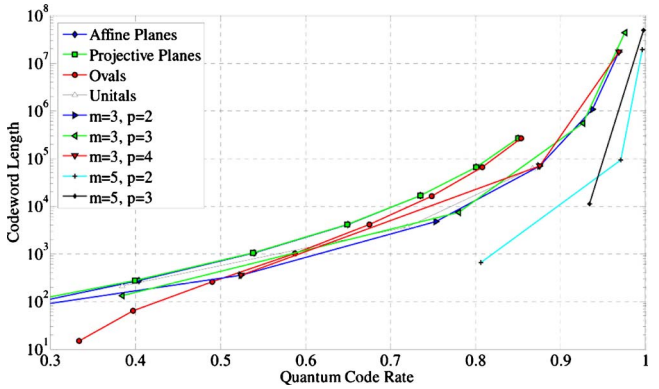

Fig. 4. (Color online) EA quantum LDPC codes from m-dimensional projective geometries.

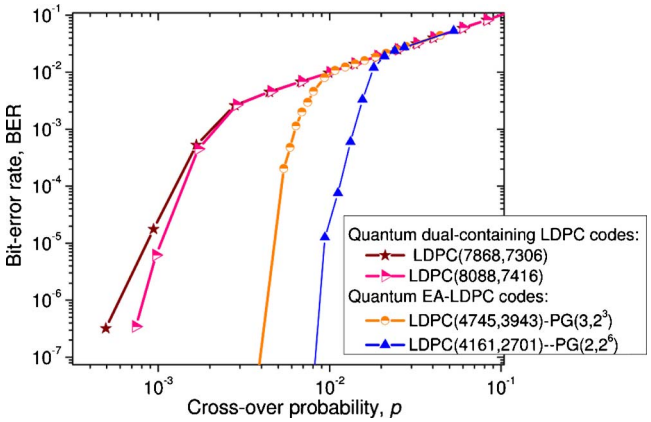

Fig. 5. (Color online) Bit error rates (BER) versus cross-over probability on a binary symmetric channel. The results are obtained assuming that the assisted entanglement state is a maximal entanglement state.

(an equivalence class). The number of points in $\mathrm{PG}(m,p^s)$ is $v=[p^{(m+1)s}-1]/(p^s-1)$. The points (equivalence classes) can be represented by $[\alpha^i]=\{\alpha^i,\beta\alpha^i,\cdots,\beta^{p^s-2}\alpha^i\}$ $(0\leqslant i\leqslant v)$, where $\beta=\alpha^v$. Let $[\alpha^i]$ and $[\alpha^j]$ be two distinct points in $\mathrm{PG}(m,p^s)$; then the line passing through them consists of points of the form $[\lambda_1\alpha^i+\lambda_2\alpha^j]$, where $\lambda_1,\lambda_2\in\mathrm{GF}(p^s)$. Because $[\lambda_1\alpha^i+\lambda_2\alpha^j]$ and $[\beta^k\lambda_1\alpha^i+\beta^k\lambda_2\alpha^j]$ represent the same point, each line in $\mathrm{PG}(m,p^s)$ consists of $k=(p^{ms}-1)/(p^s-1)$ points. The number of lines intersecting at a given point is given by k, and the number of lines in an m-dimensional projective geometry PG is $b=[p^{s(m+1)}-1](p^{sm}-1)/[(p^{2s}-1)(p^s-1)]$. The parity-check matrix is obtained as the incidence matrix $\boldsymbol{H}=(h_{ij})_{b\times v}$ with rows corresponding to the lines and columns to the points, and columns being arranged in the following order: $[\alpha^0],\ldots,[\alpha^v]$. Here $h_{ij}=1$ if the jth point belongs to the ith line, and zero otherwise. Each row has weight p^s+1, and each column has the weight k. Any two rows or columns have exactly one "1" in common, and the row weight (p^s+1) is odd. Therefore, the corresponding LDPC code has $\mathrm{rank}(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}})=1$.

In Fig. 4, I show the code length as a function of quantum code rate for EA LDPC codes derived from design 2, obtained for different values of $s=1-9$. The results of simulations are shown in Fig. 5 for 30 iterations in sum–product algorithm. The proposed EA quantum LDPC codes from design 2 are compared against dual-containing quantum LDPC codes. We can see that EA LDPC codes significantly outperform dual-containing LDPC codes.

References

1. M. A. Neilsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2000).
2. D. J. C. MacKay, G. Mitchison, and P. L. McFadden, IEEE Trans. Inf. Theory **50**, 2315 (2004).
3. T. Brun, I. Devetak, and M.-H. Hsieh, Science **314**, 436 (2006).
4. T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White, Phys. Rev. A **65**, 062324 (2002).