Photonic Quantum Dual-Containing LDPC Encoders and Decoders

Ivan B. Djordjevic, *Member, IEEE*

***Abstract*—We propose encoder and decoder architectures for quantum low-density parity-check (LDPC) codes suitable for all-optical implementation, based on controlled-NOT (CNOT) and Hadamard gates only. Given the fact that the CNOT gate can be implemented using directional couplers, and Hadamard gate by using π-hybrid, the proposed encoders/decoders architectures are suitable for implementation in integrated optics. In addition, we propose several quantum LDPC codes based on balanced incomplete block designs.**

***Index Terms*—Calderbank–Shor–Steane (CSS) codes, integrated optics circuits, low-density parity-check (LDPC) codes, quantum error-correction.**

I. INTRODUCTION

QUANTUM information processing is an exciting research area with a very wide range of applications including quantum computing, quantum memories, quantum key distribution (QKD), quantum metrology, quantum lithography, and quantum communications [1]. Quantum information processing relies on fragile superposition states, which are sensitive to interactions with environment, resulting in decoherence. Decoherence introduces errors, and thus quantum information processing has to rely on quantum error-correction.

Inspired by the conjecture that the best quantum error-correcting codes can be related to the best classical codes [1] MacKay *et al.* proposed recently in [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 (CSS) codes [1]. Most of the constructions introduced in [2] are obtained by computer search. In our recent paper [3], we proposed a series of quantum LDPC codes based on the balanced incomplete block designs (BIBDs) [4].

Quantum error control coding (QECC) can be implemented in a variety of potential technologies [1]. One such realization, based on three beryllium atomic-ion qubits, has been reported in [5]. This QECC scheme, however, is not compatible with many potential applications such as QKD, deep-space optical communications, and free-space interchip/intrachip optical communications. A novel QECC scheme is needed that is compatible with different photonic quantum applications. Given that a controlled-NOT (CNOT) gate has recently been implemented in silica-on-silicon waveguides [6], in this letter, we consider the possibility for an *all-optical* implementation of encoders and decoders for quantum LDPC codes based on CNOT and Hadamard gates only. Namely, the CNOT gate can be implemented based on directional couplers [6], while the Hadamard gate can be implemented using a π-hybrid. Those two gates are basic building blocks that can be used to implement an arbitrary quantum LDPC encoder/decoder, as shown in Section II. In addition to encoder/decoder architectures for all-optical implementation, we describe in Section III several quantum LDPC codes of high quantum rate (>0.9).

II. PHOTONIC QUANTUM LDPC ENCODERS/DECODERS

In this section, we describe encoder/decoder implementation so that only CNOT and Hadamard gates are required. In what follows, the logical "0" is represented by a horizontal (H) photon $|H\rangle \equiv |0\rangle$ and the logical "1" is represented by a vertical (V) photon $|V\rangle \equiv |1\rangle$. The CSS codes [1], can be designed using a pair of conventional linear codes satisfying the twisted property (one code includes the dual of another code). The CSS codes based on dual-containing codes [2] are simplest to implement. Their (quantum) check matrix can be represented by

$$\boldsymbol{A} = \left[\begin{array}{c|c} \boldsymbol{H} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{H} \end{array}\right] \tag{1}$$

where $\boldsymbol{H}\boldsymbol{H}^T = 0$, 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 requirement $\boldsymbol{H}\boldsymbol{H}^T = 0$ is satisfied when rows of $\boldsymbol{H}$ have an even number of 1s, and any two of them overlap by an even number of 1s [2]. The LDPC codes satisfying these two requirements were designed by exhaustive computer search in [2], while in [3], they were designed by using the combinatorial objects known as BIBDs [4]. A BIBD(v, b, r, k, λ) is a collection of subsets of a set V of size v, with a size of each subset being k, so that 1) each pair of elements occurs in *exactly* λ of the subsets, and 2) every element occurs in exactly r subsets. The code rate of quantum codes is lower bounded by $R_Q \geq [b - 2\mathrm{rank}(\boldsymbol{H})]/b$, where $\mathrm{rank}(\boldsymbol{H})$ is the rank of $\boldsymbol{H}$-matrix, and b is the codeword length (related to the number of subsets in a BIBD). The advantages of BIBD-based quantum LDPC codes compared to other codes include 1) high rate, 2) regular structure in corresponding parity-check $(\boldsymbol{H}-)$ matrices leads to low complexity encoders/decoders, 3) their sparse $\boldsymbol{H}$-matrices require a small number of interactions per qubit to determine the error location, and 4) excellent error correction capabilities. For example, $\boldsymbol{H}$-matrix from BIBD(3,6,4,4,2) is given below and satisfies the condition $\boldsymbol{H}\boldsymbol{H}^T = 0$. The quantum check matrix corresponding to $\boldsymbol{H}$-matrix is given below as $\boldsymbol{A}$-matrix

$$\boldsymbol{A} = \left[\begin{array}{c|c} \boldsymbol{H} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{H} \end{array}\right] \quad \boldsymbol{H} = \begin{bmatrix} 100111 \\ 111001 \\ 011110 \end{bmatrix}. \tag{2}$$

Similarly as in [1] and [2], we adopt the *stabilizer* framework. A stabilizer group S consists of a set of Pauli matrices (X, Y, Z

Manuscript received January 12, 2009; revised March 08, 2009. First published April 03, 2009; current version published June 10, 2009. This letter was supported in part by the NSF under Grant IHCS-0725405.

The author is with the Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721 USA (e-mail: ivan@ece.arizona.edu).

Color versions of one or more of the figures in this letter are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LPT.2009.2019262

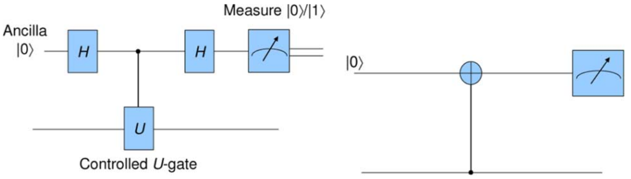

Fig. 1. (left) Quantum circuit for measurement of a single qubit U-operator, $U \in \{X, Z\}$; and (right) the equivalent circuit for measurement of Z-operator.

together with multiplicative factors $\pm 1, \pm j$), with a property that any two operators in group S commute so they can be simultaneously measured. In the stabilizer framework, a codeword is defined to be a ket $|\psi\rangle$ that is a $+1$ eigenket of all stabilizers S_i, so that $S_i|\psi\rangle = |\psi\rangle$ for all i. Any Pauli vector on b-qubits can be written uniquely as a product of X- and Z-operators together with the phase factor (± 1 or $\pm j$). The quantum LDPC code is obtained by replacing ones in the left half of $\boldsymbol{A}$, in the example above, with X-operators and zeros with I-operators (identity operators), and replacing ones in the right half of $\boldsymbol{A}$ with Z-operators and zeros with I-operators. The corresponding stabilizers S_i are obtained by reading-off the ith rows of such a modified $\boldsymbol{A}$-matrix. For example, by reading off the first row, we obtain the stabilizer $S_1 = XIIXXX = X_1X_4X_5X_6$, and by reading off the sixth row, we obtain $S_6 = IIIIIIIZZZZI = Z_8Z_9Z_{10}Z_{11}$, where the subscripts are used to denote the positions of corresponding X- or Z-operators. An interesting property of CSS codes is that stabilizers S_i do not mix up X- and Z-operators; we can, therefore, correct the qubit flip and phase errors independently. From (1), it follows that providing the $\boldsymbol{H}$-matrix of dual-containing code is sparse, the corresponding $\boldsymbol{A}$-matrix will be sparse as well, while corresponding stabilizers will be of low weight.

The quantum circuit to measure a single unitary qubit operator $U \in \{X, Y, Z\}$, based on controlled U-gate, is shown in Fig. 1(left). Because the Y-operator equals ZX (up to the multiplicative phase constant$-j$), we are only concerned with X- and Z-operators. Notice that either discrete or continuous error operator E can be decomposed using a discrete set of errors: I (no error); X (qubit flip error); Z (phase flip error); and Y (simultaneous qubit and phase flip error). Based on Fig. 1(right), we conclude that X- and Z-operators can be measured based on CNOT and Hadamard (H)-gates. The H-gate can be implemented based on a 50 : 50 directional coupler, Y-junction, or π-hybrid, which is shown in Fig. 2(a). The output electrical fields ($E_{o,1}$ and $E_{o,2}$) are related to the input electrical fields ($E_{i,1}$ and $E_{i,2}$) by $E_{o,1} = (E_{i,1} + E_{i,2})\sqrt{1-k}$ and $E_{o,2} = (E_{i,1} + E_{i,2}\exp(-j\phi))\sqrt{k}$, where k is the power splitting ratio and ϕ is the phase shift introduced by a phase trimmer. By selecting $k = 1/2$ and $\phi = \pi$, the corresponding scattering matrix is the same as the matrix representation of a Hadamard-gate

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{3}$$

For example, for the vertical photon $|1\rangle \equiv [01]^T$ (T is the transposition operation), at the input of H-gate, the corresponding output is $H|1\rangle = [11]^T/\sqrt{(2)} = (|0\rangle + |1\rangle)/\sqrt{(2)}$.

The corresponding integrated optics implementation of CNOT-gate is shown in Fig. 2(b). The control qubits are denoted with C, and target qubits are denoted by T. Using the directional coupler theory, it can be shown that target output V and H photons $(t_{V,o}, t_{H,o})$ are related to the input control photons (c_V, c_H) and the input target photons (t_V, t_H) by [5], [6]

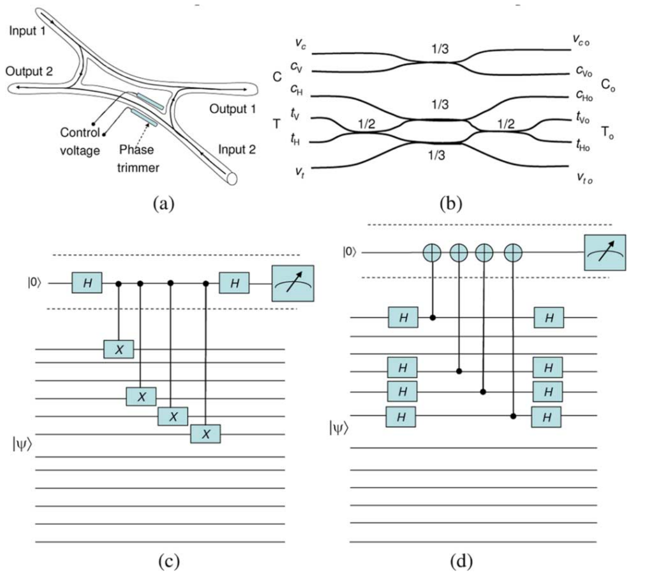

Fig. 2. Implementation of H- and CNOT-gates in integrated optics: (a) H-gate based on a π-hybrid, and (b) CNOT-gate based on a directional coupler. The syndrome quantum circuit for stabilizer $S_1 = X_1X_4X_5X_6$: (c) based on H- and controlled-X gates, and (d) based on H- and CNOT-gates.

$$t_{H,o} = \frac{1}{\sqrt{3}}(c_V + t_H) \quad t_{V,o} = \frac{1}{\sqrt{3}}(c_V + t_V). \tag{4}$$

Therefore, when the control qubit c_V is set to 1, the target qubit is flipped [see (4)]. The CNOT gate based on the directional coupler was implemented in [6] with an average logical basis fidelity of $94.3 \pm 0.2\%$. Notice also that the CNOT-gate can also be implemented using a hybrid as a building block. Namely we have to set the phase shift to zero and power splitting ratios to $k = 1/2$ and $k = 1/3$, and integrate hybrids as shown in Fig. 2(b).

Now we come to the point where we explain how to implement the quantum LDPC error detector for A, based on the H- and CNOT-gates described above. Let us observe the first stabilizer $S_1 = X_1X_4X_5X_6$ only; the whole error detector can be obtained by corresponding concatenation of remaining stabilizers. The transmission error is identified as an intersection of corresponding syndrome measurements. The syndrome quantum circuit for measurement of stabilizer S_1 is shown in Fig. 2(c) and (d). In Fig. 2(c), the quantum syndrome implementation circuit is based on H- and controlled-X gates, while in Fig. 2(d), the corresponding implementation is based on H- and CNOT-gates only, and can, therefore, be implemented in integrated optics. To implement the syndrome quantum circuit for stabilizer S_1, we have to integrate four CNOT-gates [Fig. 2(b)] and eight H-gates [Fig. 2(a)], as shown in Fig. 2(d). The main advantage of quantum LDPC codes compared to other classes of quantum codes is the sparseness of quantum check matrix, and therefore, a small number of interactions is required in corresponding stabilizers.

To simplify the implementation of encoders for quantum LDPC codes, we have to put the quantum check matrix A in a systematic form by Gaussian elimination first [1]

$$\boldsymbol{A} \equiv \left[\begin{array}{ccc|ccc} \boldsymbol{I} & \boldsymbol{A_1} & \boldsymbol{A_2} & \boldsymbol{B} & \boldsymbol{C_1} & \boldsymbol{C_2} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{D} & \boldsymbol{I} & \boldsymbol{E} \end{array}\right]. \tag{5}$$

For a quantum CSS (N, K), we have to add K Z_i-operators $(i = 1, 2, \ldots, K)$ independent of stabilizers $S_i(i = 1, \ldots, N-K)$ as follows $\bar{\boldsymbol{Z}} = [\mathbf{000} \,|\, \boldsymbol{A}_2^T \mathbf{0}\boldsymbol{I}]$. To encode, we first need to prepare the system in $|0\rangle^{\otimes N}$ state (the notation $\otimes$ stands for the tensor product), measure the observables $S_1, S_2, \ldots, S_{N-K}, Z_1, Z_2, \ldots, Z_K$, and stabilize the system with corresponding Pauli operators. To prepare the system in $|0\rangle^{\otimes N}$ state, we can use the multiphoton entanglement from distant single photon sources, as described in [7].

III. Quantum BIBD Codes, Results, and Conclusion

In addition to quantum BIBD-based codes we introduced in [3], below we describe several BIBD-based codes suitable for quantum error correction.

Construction 1: If $2(2\lambda+1)t+1$ is a prime power and θ is a primitive root of $GF[2(2\lambda+1)t+1]$, then the following t initial sets $S_i = (\theta^i, \theta^{2t+i}, \theta^{4t+i}, \ldots, \theta^{4\lambda t+i})(i = 0, 1, \ldots, t-1)$ form a BIBD $(2(2\lambda+1)t+1, t[2(2\lambda+1)t+1], (2\lambda+1)t, 2\lambda+1, \lambda)$. The BIBD is formed by adding the elements from $GF[2(2\lambda+1)t+1]$ to the initial blocks S_i. For any even index λ and even parameter t (the row weight is even), the corresponding LDPC code is a dual-containing code ($\boldsymbol{H}\boldsymbol{H}^T = 0$). The quantum code rate for this construction is lower bounded by $R_Q \geq (1 - 2/t)$, and the minimum distance is lower bounded by $d_{\min} \geq 2\lambda + 2$. For any odd index λ design we have to add an additional block $(1, 2, \ldots, 2(2\lambda+1)t+1)$, so that the row weight of $\boldsymbol{H}$ becomes even.

Construction 2: If $2(2\lambda-1)t+1$ is a prime power and θ is a primitive root of $GF[2(2\lambda-1)t+1]$, then the following t initial sets $S_i = (0, \theta^i, \theta^{2t+i}, \ldots, \theta^{(4\lambda-1)t+i})$ form a BIBD$(2(2\lambda-1)t+1, [2(2\lambda-1)t+1]t, 2\lambda t, 2\lambda, \lambda)$. For any even index λ, the corresponding LDPC codes are dual containing codes. The quantum LPDC code rate is lower bounded by $R_Q \geq (1-2/t)$, and the minimum distance is lower bounded by $d_{\min} \geq 2\lambda+1$.

Construction 3: If $(\lambda-1)t$ is a prime power and θ is a primitive root of $GF[(\lambda-1)t+1]$, then the following t initial sets $(0, \theta^i, \theta^{t+i}, \ldots, \theta^{(\lambda-2)t+i})$ form a BIBD$[(\lambda-1)t+1, ((\lambda-1)t+1)t, \lambda t, \lambda, \lambda]$. Again for an even index λ, the quantum LDPC code of rate $R_Q \geq (1-2/t)$ is obtained, whose minimum distance is lower bounded by $d_{\min} \geq \lambda+1$. Similarly as in the previous two constructions, for any odd index λ design, we have to add an additional block $(1, 2, \ldots, (\lambda-1)t)$. The example used in Section II belongs to this construction, and was obtained for $\lambda = t = 2$.

Construction 4: If $2\,k-1$ is a prime power and θ is a primitive root of $GF(2k-1)$, then the following initial sets:

$$\begin{aligned}&(0, \theta^i, \theta^{i+2}, \ldots, 0^{i+2k-4})\\&(\infty, \theta^{i+1}, \theta^{i+3}, \ldots, 0^{i+2k-3}), \qquad (i = 0, 1)\end{aligned}$$

form a BIBD$(2k, 4(2k-1), 2(2k-1), k, 2(k-1))$. For even k, the quantum code rate is lower bounded by $R_Q \geq [1 - 1/(2k-1)]$, the codeword length is determined by $4(2k-1)$, and the minimum distance is lower bounded by $d_{\min} \geq k+1$.

The results of simulations are shown in Fig. 3 for 30 iterations in a sum-product-with-correction-term algorithm. Bit-error-rate (BER) curves are obtained by counting the errors only on those codewords from C not belonging to $C^{\perp}$ and represent BER$(C/C^{\perp})$. Three quantum LDPC codes of quantum rate above 0.9 are designed by employing Construction 1 and 2: 1) quantum LDPC$(7868, 7306, 0.9285, \geq 6)$ code (the parameters in brackets represent codeword length, information word length, code rate, and lower bound on minimum distance, respectively) from Construction 1 by setting $t = 28$ and $\lambda = 2$, 2) quantum LDPC$(8702, 8246, 0.946, \geq 5)$ code from Construction 2 by setting $t = 38$ and $\lambda = 2$, and 3) quantum LDPC$(8088, 7416, 0.917, \geq 9)$ from Construction 2 by setting $t = 24$ and $\lambda = 4$. For comparison purposes, two curves for quantum LDPC codes from [3] are plotted as well. The BIBD codes proposed here outperform the codes from [3] for BERs around 10^{-7}. The code from BIBD with index $\lambda = 4$ and Construction 2 outperforms the codes with index $\lambda = 2$ from both Constructions, because it has larger minimum distance. The code with index $\lambda = 2$ from Construction 1 outperforms corresponding code from Construction 2.

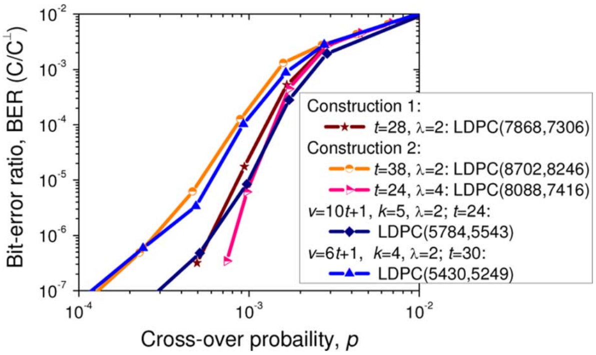

Fig. 3. BERs against crossover probability on a binary symmetric channel.

In conclusion, we propose encoder and decoder architectures for quantum LDPC codes suitable for implementation in integrated optics, based on CNOT and Hadamard gates only, implemented by using directional couplers and π-hybrids, respectively. We also propose several quantum LDPC codes of high quantum code rate (above 0.9) based on BIBDs, outperforming previously proposed codes. The quasi-cyclic structure and sparseness of the parity-check matrix of proposed LDPC codes have several advantages: 1) the quantum syndrome can be measured with sparse number of interactions; 2) the quasi-cyclic structure of parity check matrix leads to low decoder complexity compared to random codes; 3) there exist practical decoding algorithms; 4) high quantum code rates; and 5) excellent error correction capabilities.

References

[1] M. A. Neilsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge: Cambridge Univ. Press, 2000.

[2] 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.

[3] I. B. Djordjevic, "Quantum LDPC codes from balanced incomplete block designs," *IEEE Commun. Lett.*, vol. 12, no. 5, pp. 389–391, May 2008.

[4] I. Anderson, *Combinatorial Designs and Tournaments*. Oxford: Oxford Univ. Press, 1997.

[5] J. Chiaverini *et al.*, "Realization of quantum error correction," *Nature*, vol. 432, pp. 1476–4687, Dec. 2, 2005.

[6] A. Politi, M. Cryan, J. Rarity, S. Yu, and J. L. O'Brien, "Silica-on-silicon waveguide quantum circuits," *Science*, vol. 320, pp. 646–649, 2008.

[7] A. Beige, Y. Lim, and C. Schön, "Multi-photon entanglement from distant single photon sources on demand," *J. Mod. Opt.*, vol. 54, pp. 397–407, Jan. 2007.