Quantum LDPC Codes from Balanced Incomplete Block Designs

Ivan B. Djordjevic, *Member, IEEE*

***Abstract*— We present a series of structured LDPC codes suitable for use in quantum error correction. Those codes belong to the class of dual-containing Calderbank-Shor-Steane (CSS) codes. The component CSS code is designed using the combinatorial object known as balanced incomplete block design (BIBD) with an even index. The quantum LDPC codes have the rate around 0.9. Several examples of quantum LDPC codes from BIBDs from unity index, extended by addition of an all-ones column, are introduced as well. To improve the BER performance, we employed the method of removing the cycles of length four in corresponding bipartite graph.**

***Index Terms*— Low-density parity-check (LDPC) codes, quantum error-correction, Calderbank-Shor-Steane codes.**

I. Introduction

THE quantum information processing is an exciting research area with applications ranging from cryptography to complexity theory [1]. It can be used to efficiently solve some hard problems in classical computation, e.g. integer factorization, and quantum-based computers are much more powerful than Turing machines. The quantum information processing, however, relies on fragile superposition states required to manipulate the quantum information, which are sensitive to the interactions with environment-decoherence. Decoherence introduces the errors, and someone has to rely on quantum error-correction. Fortunately, it was shown by Calderbank and Shor in [2], and Steane in [3], that good quantum error-correcting codes exist. Moreover, it has been shown that quantum information processing can be done fault-tolerantly [1].

It is well known in classical error correction that Shannon limit can be closely approached by low-density parity-check (LDPC) codes. Inspired by the conjecture that the best quantum error-correcting codes can be related to the best classical codes [1]-[3] D. J. C. MacKay *at el.* proposed recently in [4] how to design the sparse dual-containing binary codes that can be used to construct quantum LDPC codes belonging to the class of Calderbank-Shor-Steane (CSS) codes [1]. Most of the constructions introduced in [4] are obtained by computer search, and several researchers recently addressed the problem of designing quantum LDPC codes by using some other approaches [5],[6].

In this paper we propose to design quantum LDPC codes using the combinatorial concepts [7]. It was recently shown in [8] that combinatorial constructions can successfully be used to design good classical LDPC codes. The codes from combinatorial objects exhibit highly regular structure, which might facilitate the quantum implementation. The good classical LDPC codes are codes of high girth (at least six), and several interesting constructions are given in [8]. Unfortunately, it was shown in [4],[5] that quantum stabilizer LDPC codes and quantum self-dual containing CSS codes are girth-4 codes, so that combinatorial designs proposed in [8] are not applicable here. Novel combinatorial constructions resulting in girth-4 LDPC codes with even overlap between any two rows and even row weight are needed.

We propose a series of quantum LDPC codes designed using the combinatorial object known as balanced incomplete block design (BIBD) [7]. The quantum LDPC codes, introduced in this letter, have the high code rate (around 0.9). We also show how to modify some of BIBDs used to design classical LDPC codes, so that they can be used to design quantum sparse codes as well. To improve the bit-error rate (BER) performance we employed an efficient algorithm due to Sankaranarayanan and Vasic [10] to remove the cycles of length four from corresponding bipartite graph (the modified bipartite graph is used only in decoding phase).

II. Quantum LDPC Codes from BIBDs

It has been shown by Calderbank, Shor and Steane [2]-[3] that the quantum codes, now known as CSS codes, can be designed using a pair of conventional linear codes satisfying the *twisted property*, that is one of the codes includes the dual of another code. Among them, particularly are simple the CSS codes based on dual-containing codes [4], whose (quantum) check matrix can be represented by [1],[4]

$$A = \begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix}, \tag{1}$$

where $HH^T = 0$, which is equivalent to $C^{\perp}(H) \subset C(H)$, where $C(H)$ is the code having H as the parity check matrix, and $C^{\perp}(H)$ is its corresponding dual code. It has been shown in [4] that the requirement $HH^T = 0$ is satisfied when rows of H have even number of 1s, and any two of them overlap by an even number of 1s. The LDPC codes satisfying these two requirements in [4] were designed by exhaustive computer search, in [5] they were designed as codes over GF(4) by identifying the Pauli operators I, X, Y, Z with elements from GF(4), while in [6] they were designed in quasi-cyclic fashion. In what follows, we will show how to design the dual-containing LDPC codes using the combinatorial objects known as BIBDs [7]. Notice that the theory behind BIBDs is well known (see [7]), and BIBDs of unity index have already been used to design LDPC codes of girth-6 [8]. Notice, however, that dual-containing LDPC are girth-4 LDPC codes, and they can be designed based on BIBDs with even index. A balanced incomplete block design, denoted as BIBD(v, b, r, k, λ), is a collection of subsets (also known as blocks) of a set V of size v, with a size of each subset being k, so that: (i) each pair of elements (also known as points) occurs in exactly λ of the subsets,

Manuscript received January 18, 2008. The associate editor coordinating the review of this letter and approving it for publication was V. Stankovic. This work is supported by the National Science Foundation under Grant IHCS-0725405.

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

Digital Object Identifier 10.1109/LCOMM.2008.080083.

and (ii) every element occurs in exactly r subsets. The BIBD parameters satisfy the following two conditions [7]: a) $vr = bk$, and b) $\lambda(v-1) = r(k-1)$. Because the BIBD parameters are related (conditions a) and b)) it is sufficient to identify only three of them: v, k and λ. It can be easily verified [8] that a point-block incident matrix represents a parity-check matrix H of an LDPC code of the code rate R lower bounded by $R \geq [b - \text{rank}(H)]/b$, where b is the codeword length, and with rank( ) we denoted the rank of the parity-check matrix. The parameter k corresponds to the column weight, r to the row weight and v to the number of parity-checks. The corresponding quantum code rate is lower bounded by $R_Q \geq [b - 2\text{rank}(H)]/b$. By selecting the index of BIBD $\lambda = 1$, the parity-check matrix has the girth of at least 6. For a classical LDPC code to be applicable in quantum error-correction the following two conditions are to be satisfied [4]: (1) the LDPC code must contain its dual or equivalently any two rows of the parity-check matrix must have even overlap and the row weight must be even ($HH^T = 0$), and (2) the code must have rate greater than 1/2. The BIBDs with even index λ satisfy the condition (1). The parameter λ corresponds to the number of ones in which two rows overlap. For example, the parity check matrix from BIBD(7,7,4,4,2)=$\{\{1,2,4,6\},\{2,6,3,7\},\{3,5,6,1\},\{4,3,2,5\},\{5,1,7,2\},\{6,7,5,4\},\{7,4,1,3\}\}$, given as H_1-matrix at the bottom of this column, has the rank 3, the even overlap between any two rows, and row weight is even as well (or equivalently $H_1H_1^T = 0$). Notice that so called λ-configurations (in definition of BIBD the word exactly from condition (i) is replaced by at most) are not applicable here. However, the *H*-matrix from BIBD of unity index can be converted to *H*-matrix satisfying condition (1) by adding a column with all-ones, which is equivalent to adding an additional block to unity index BIBD having all elements from V. For example, the parity check matrix from BIBD(7,7,3,3,1), after the addition of a column with all ones, is given as H_2-matrix at the bottom, and satisfies the condition $H_2H_2^T = 0$. The following method due to Bose [9] is a powerful method to design many different BIBDs with desired index λ. Let S be a set of elements. Associate to each element *u* from *S n* symbols $u_1, u_2, \ldots, u_n$. Let sets $S_1, \ldots, S_t$ satisfy the following three conditions: (i) every set $S_i (i = 1, \ldots, t)$ contains k symbols (the symbols from the same set are different from one another); (ii) among *kt* symbols in *t* sets exactly *r* symbols belong to each of *n* classes ($nr = kt$); and (iii) the differences from *t* sets are symmetrically repeated so that each repeats λ times.

$$H_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$H_2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

If *s* is an element from S, from each S_i set we are able to form another set S_i, s by adding *s* to S_i keeping the class number (subscript) unchanged; then sets $S_{i,s} (i = 1, \ldots, t; s \in S)$ represent a (mn, nt, r, k, λ) BIBD. By observing the elements from BIBD blocks as position of ones in corresponding columns of a parity-check matrix, the code rate of an LDPC code such obtained is lower bounded by $R \geq 1 - m/t$ ($R_Q \geq 1 - 2m/t$), and the codeword length is determined by $b = nt$. In the rest of this Section we introduce several constructions employing the method due to Bose.

Construction 1: If $6t+1$ is a prime or prime power and θ is a primitive root of GF$(6t+1)$, then the following t initial sets $S_i = (0, \theta^i, \theta^{2t+i}, \theta^{4t+i}) (i = 0, 1, \ldots, t-1)$ form a BIBD$(6t+1, t(6t+1), 4t, 4, 2)$. The BIBD is formed by adding the elements from GF(6t+1) to the initial blocks S_i. Because the index of BIBD is even ($\lambda = 2$), and row weight $r = 4t$ is even, the corresponding LDPC code is a dual-containing code ($HH^T = 0$). The quantum code rate for this construction, and constructions 2 and 3 as well, is lower bounded by $R_Q \geq (1 - 2/t)$. The BIBD(7,7,4,4,2) given above is obtained using this construction method. For $t = 30$ a dual-containing LDPC(5430,5249) code is obtained. The corresponding quantum LDPC code has the rate 0.934, which is significantly higher than any of the codes introduced in [4] ($R_Q = 1/4$).

Construction 2: If $10t+1$ is a prime or prime power and θ is a primitive root of GF$(10t+1)$, then the following t initial sets $S_i = (\theta^i, \theta^{2t+i}, \theta^{4t+i}, \theta^{6t+i})$ form a BIBD$(10t+1, t(10t+1), 4t, 4, 2)$. For example, for $t = 24$ dual-containing LDPC(5784,5543) code is obtained, and corresponding CSS code has the rate 0.917.

Construction 3: If $5t+1$ is a prime or prime power and θ is a primitive root of GF$(5t+1)$, then the following t initial sets $(\theta^i, \theta^{2t+i}, \theta^{4t+i}, \theta^{6t+i}, \theta^{8t+i})$ form a BIBD$(5t+1, t(5t+1), 5t, 5, 4)$. Notice that parameter *t* is to be even for LDPC code to satisfy the condition (1). For example, for $t = 30$, the dual-containing LDPC(4530,4379) code is obtained, and corresponding CSS LDPC code has the rate 0.934.

Construction 4: If $2t+1$ is a prime or prime power and θ is a primitive root of GF$(2t+1)$, then the following $5t+2$ initial sets

$$\begin{array}{c} (\theta_1^i, \theta_1^{t+i}, \theta_3^{i+a}, \theta_3^{t+i+a}, 0_2)(i = 0, 1, ..., t-1) \\ (\theta_2^i, \theta_2^{t+i}, \theta_4^{i+a}, \theta_4^{t+i+a}, 0_3)(i = 0, 1, ..., t-1) \\ (\theta_3^i, \theta_3^{t+i}, \theta_5^{i+a}, \theta_5^{t+i+a}, 0_4)(i = 0, 1, ..., t-1) \\ (\theta_4^i, \theta_4^{t+i}, \theta_1^{i+a}, \theta_1^{t+i+a}, 0_5)(i = 0, 1, ..., t-1) \\ (\theta_5^i, \theta_5^{t+i}, \theta_2^{i+a}, \theta_2^{t+i+a}, 0_1)(i = 0, 1, ..., t-1) \\ (0_1, 0_2, 0_3, 0_4, 0_5), (0_1, 0_2, 0_3, 0_4, 0_5) \end{array} \tag{2}$$

form a BIBD$(10t+5, (5t+2)(2t+1), 5t+2, 5, 2)$. Similarly as in previous construction, the parameter *t* is to be even. The quantum code rate is lower bounded by $R_Q \geq [1 - 2 \cdot 5/(5t+2)]$, and the codeword length is determined by $(5t+2)(2t+1)$. For $t = 30$, the dual-containing LDPC(5490,5307) is obtained, and corresponding quantum LDPC codes has the rate 0.934. The following two constructions are obtained by converting unity index BIBD into $\lambda = 2$ BIBD.

Construction 5: If $12t+1$ is a prime or prime power and θ is a primitive root of GF$(12t+1)$, then the following t initial sets $(0, \theta^i, \theta^{4t+i}, \theta^{8t+i}) (i = 0, 2, \ldots, 2t-2)$ form a BIBD$(12t+1, t(12t+1), 4t, 4, 1)$. To convert this unity index BIBD into $\lambda = 2$ BIBD we have to add an additional block (1,2,...,12*t*+1).

Construction 6: If $20t+1$ is a prime or prime power and θ is a primitive root of GF(20t+1), then the following *t* initial sets $(\theta^i, \theta^{4t+i}, \theta^{8t+i}, \theta^{12t+i}, \theta^{16t+i}) (i = 0, 2, \ldots, 2t-2)$ form a BIBD$(20t+1, t(20t+1), 5t, 5, 1)$. Similarly as we did in

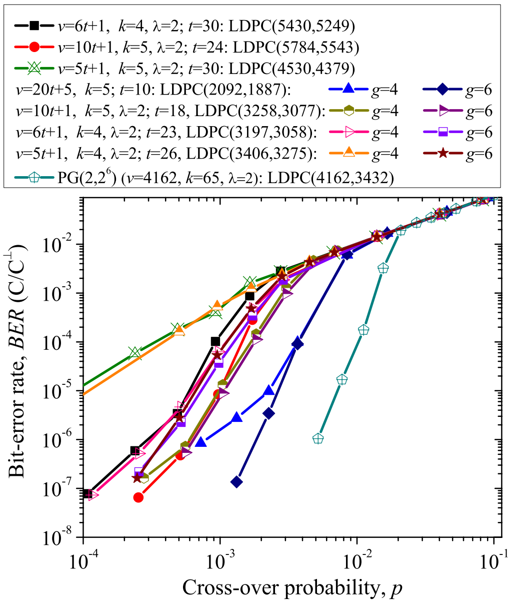

Fig. 1. BERs against crossover probability on BSC.

previous construction, in order to convert this unity index BIBD into $\lambda = 2$ BIBD we have to add an additional block $(1, 2, \ldots, 20t + 1)$.

III. Numerical Results

We performed the simulations for error-correcting performance of proposed codes as the function of noise level by Monte Carlo simulations. We simulated the classical binary symmetric channel (BSC), to be compatible with current literature [4]-[6]. The results of simulations are shown in Fig. 1 for 30 iterations in sum-product-with-correction-term algorithm due to H. Xiao-Yu *et al.* [11]. We simulated dual-containing LDPC codes of high-rate and moderate lengths, so that corresponding quantum LDPC code has the rate around 0.9. BER curves correspond to $C/C^{\perp}$ case, and are obtained by counting the errors only on those codewords from C not belonging to $C^{\perp}$. The codes from BIBD with index $\lambda = 2$ outperform the codes with index $\lambda = 4$. The codes derived from unity index BIBDs by adding all 1's column outperform the codes derived from BIBDs of even index. In simulations presented in Fig. 1 the codes with parity-check matrices with column weight $k = 4$ or 5 are observed. The code from projective geometry (PG) is an exception. It is based on BIBD$(s^2 + s + 1, s + 1, 1)$, where s is a prime power, in our example parameter s was set to 64. The LDPC(4162,3432) code based on this BIBD outperforms other codes, however, the code rate is lower (R=0.825), and the column weight is large (65). For more details on PG codes and secondary structures developed from them an interested reader is referred to [12]. To improve the BER performance of proposed high-rate sparse dual-containing codes we employed an efficient algorithm due to Sankaranarayanan and Vasic, for removing the cycles of length four in corresponding bipartite graph. As shown in Fig. 1, this algorithm can significantly improve the BER performance, especially for weak (index four BIBD based) codes. For example, with LDPC(3406,3275) code the BER of 10^{-5} can be achieved at cross-over probability $1.14 \cdot 10^{-4}$ if sum-product-with-correction-term algorithm [11] is employed ($g = 4$ curve), while the same BER can be achieved at cross-over probability $6.765 \cdot 10^{-4}$ when the algorithm proposed in [10] is employed ($g = 6$ curve). Notice that this algorithm modifies the parity-check matrix by adding the auxiliary variables and checks, so that the 4-cycles are removed in the modified parity-check matrix. The algorithm attempts to minimize the required number of auxiliary variable/check nodes while removing the 4-cycles. The modified parity-check matrix is used only in decoding phase, while the encoder remains the same.

IV. Conclusion

We have shown that sparse dual-containing codes suitable for use in quantum error-correction can be designed in combinatorial fashion, based on BIBDs, instead of using exhaustive computer search. We present four constructions based on even index BIBDs, and two constructions based on unity index BIBDs. All those constructions belong to the class of dual-containing CSS codes. The quantum LDPC codes have the rate around 0.9. In order to keep complexity of decoder low we design moderate length LDPC codes of column weight k=4 or 5. To improve the BER performance, we employed the method of removing the cycles of length four in corresponding bipartite graph. Notice that a BIBD does not exist for arbitrary v, k and $\lambda = 2$, but only for those parameters that satisfy simultaneously conditions a) and b) in definition of BIBD. Another interesting fact to notice is that by using the concepts from this paper, and allowing the BIBD blocks to be of different size we can design quantum irregular LDPC codes, which might outperform quantum regular LDPC codes proposed here. The possible applications of quantum LDPC codes introduced in this paper include deep-space optical communications, interchip/intrachip optical communications, and quantum key distribution (QKD).

References

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

[2] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” *Phys. Rev. A*, vol. 54, pp. 1098-1105, 1996.

[3] A. M. Steane, “Error correcting codes in quantum theory,” *Phys. Rev. Lett.*, vol. 77, p. 793, 1996.

[4] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, “Sparse-graph codes for quantum error correction,” *IEEE Trans. Inform. Theory*, vol. 50, pp. 2315-2330, 2004.

[5] T. Camara, H. Ollivier, and J.-P. Tillich, “Constructions and performance of classes of quantum LDPC codes,” 2005. quant-ph/0502086.

[6] M. Hagiwara and H. Imai, “Quantum quasi-cyclic LDPC codes,” 2007. quant-ph/0701020.

[7] I. Anderson, *Combinatorial Designs and Tournaments*. Oxford University Press, 1997.

[8] B. Vasic and O. Milenkovic, “Combinatorial constructions of low-density parity-check codes for iterative decoding,” *IEEE Trans. Inform. Theory*, vol. 50, pp. 1156-1176, June 2004.

[9] R. C. Bose, “On the construction of balanced incomplete block designs,” *Ann. Eugen.*, vol. 9, pp. 353-399, 1939.

[10] S. Sankaranarayanan and B. Vasic, “Iterative decoding of linear block codes: a parity-check orthogonalization approach,” *IEEE Trans. Inform. Theory*, vol. 51, pp. 3347-3353 Sept. 2005.

[11] H. Xiao-Yu, E. Eleftheriou, D.-M. Arnold, and A. Dholakia, “Efficient implementations of the sum-product algorithm for decoding of LDPC codes,” in *Proc. IEEE Globecom*, vol. 2, pp. 1036-1036, 2001.

[12] 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, pp. 3696-3701, Nov. 2005.