

Construction of Quantum LDPC Codes From Classical Row-Circulant QC-LDPCs

Zunaira Babar, Panagiotis Botsinis, Soon Xin Ng, Dimitrios Alanis, and Lajos Hanzo

Abstract—Classical row-circulant quasi-cyclic (QC) low-density parity check (LDPC) matrices are known to generate efficient high-rate short and moderate-length QC-LDPC codes, while the comparable random structures exhibit numerous short cycles of length-4. Therefore, we conceive a general formalism for constructing nondual-containing Calderbank–Shor–Steane (CSS)-type quantum low-density parity check (QLDPC) codes from arbitrary classical row-circulant QC-LDPC matrices. We apply our proposed formalism to the classical balanced incomplete block design (BIBD)-based row-circulant QC-LDPC codes for demonstrating that our designed codes outperform their dual-containing CSS-type counterparts as well as the entanglement-assisted (EA)-QLDPC codes.

Index Terms—Quantum error correction, low density parity check codes, iterative decoding.

I. INTRODUCTION

QUANTUM-domain parallel processing provides a plausible solution for achieving full-search based multi-stream detection [1], which is vital for future gigabit-wireless systems. The peculiar laws of quantum mechanics have also spurred interest in the absolutely-secure quantum-based communication systems [2], [3]. Unfortunately, quantum decoherence imposes a hitherto insurmountable impairment on the practical implementation of quantum computation as well as on quantum communication systems. More specifically, decoherence perturbs the fragile quantum states, which may be characterized either by bit-flips or phase-flips - or in fact possibly both - inflicted on the constituent qubits. Analogously to the classical error correction codes, these detrimental effects of decoherence may be overcome with the aid of efficient quantum error correction codes (QECCs).

Meritorious families of QECCs can be constructed from the known classical binary as well as quaternary codes by invoking the stabilizer formalism [4]. In particular, the astounding performance of the classical low density parity check (LDPC) codes achieved at an affordable decoding complexity has inspired the community to construct their stabilizer-based quantum counterparts, i.e. quantum low density parity check (QLDPC) codes. In

this letter, we focus our attention on the construction of QLDPC codes from the family of classical row-circulant quasi-cyclic (QC)-LDPC matrices, which are known to generate efficient high-rate short and moderate-length QC-LDPC codes [5]–[7]. The balanced incomplete block design (BIBD) [6] and the cyclic difference family based LDPC code structures [7] are particularly significant in this respect. The resultant classical codes have at least a girth of 6, while the randomly constructed LDPC codes of comparable code length have numerous cycles of length 4, which impair the performance of the associated decoding algorithm.

In [8], Mackay *et al.* presented generalized methods, namely ‘bicycle’ and ‘unicycle’ codes, for constructing dual-containing Calderbank-Shor-Steane (CSS)-type QLDPC codes from arbitrary classical LDPCs. Later Djordjevic [9] extended these ideas for constructing the family of BIBD-based high-rate QLDPC codes. Unfortunately, these dual-containing CSS structures have numerous unavoidable short cycles of length-4. Inspired by the concept of entanglement-assisted (EA)-QLDPC codes [10], which do not exhibit the unavoidable length-4 cycles in the binary formalism, Djordjevic [11] conceived the EA counterparts of the BIBD-based designs of [9]. The resultant EA-QLDPC codes required a single pre-shared entangled qubit (ebit), which constitutes a valuable resource, because maintaining a noiseless entangled state is not a trivial task. Furthermore, both the dual-containing CSS codes as well as the EA-QLDPC codes of [9] constitute a class of homogeneous CSS codes, which have numerous short cycles in the Galois field $GF(4)$ formalism. In contrast to these developments, we propose a general formalism for constructing non-dual-containing CSS-type QLDPC codes from arbitrary classical row-circulant QC-LDPC matrices. The proposed construction brings with it the following plausible benefits:

- Since the constructed codes are non-dual-containing, they do not suffer from having unavoidable short cycles in the binary formalism and have fewer short cycles in the $GF(4)$ formalism than their homogeneous counterparts.
- Pre-shared ebits are not required.

We apply our proposed methodology to the family of classical BIBD-based row-circulant QC-LDPC codes for evaluating the performance of the resultant QLDPC codes.

This letter is organized as follows. In Section II, we review the BIBD-based classical Row-Circulant QC-LDPC codes, while the proposed construction method is presented in Section III. Our results are discussed in Section IV, while our conclusions are offered in Section V.

Manuscript received June 22, 2015; accepted October 20, 2015. The associate editor coordinating the review of this paper and approving it for publication was H. Saeedi.

The authors are with the University of Southampton, Southampton SO16 1BJ, U.K. (e-mail: zb2g10@ecs.soton.ac.uk).

Digital Object Identifier 10.1109/LCOMM.2015.2494020

II. CLASSICAL BIBD-BASED ROW-CIRCULANT QC-LDPCs

The BIBD constructions proposed by Bose [12] constitute the family of classical row-circulant QC-LDPC codes. A BIBD characterized by the parameters (v, b, r, k, λ) divides all the v elements of a set V into b blocks of size k so that each pair of elements occurs in exactly λ of the blocks, whilst every element occurs in exactly r blocks and the number of elements k in each block is small as compared to the size v of the set V . Based on this notation, Bose proposed the following BIBD [12] constructions, which are suitable for conceiving the row-circulant QC-LDPCs [6].

1) Type-I Bose BIBDs: Given that t is a positive integer so that $(12t + 1)$ is a power of a prime, then there exists a prime Galois field $\text{GF}(12t + 1)$ having elements ranging from 0 to $12t$, which constitute the finite set V of the BIBD. Furthermore, let α be the primitive element of $\text{GF}(12t + 1)$, which satisfies the following condition:

$$\alpha^{4t} - 1 = \alpha^c, \quad (1)$$

where c is an integer in the range $0 < c < 12t + 1$. Based on this notation, Bose [12] proposed that there exists a BIBD having the parameters $v = (12t + 1)$, $b = t(12t + 1)$, $r = 4t$, $k = 4$ and $\lambda = 1$, whose t base blocks are given by:

$$B_i = \{0, \alpha^{2i}, \alpha^{2i+4t}, \alpha^{2i+8t}\}, \quad (2)$$

for $0 \leq i < t$. We can then proceed by creating $(12t + 1)$ blocks from the base block B_i by adding each element of the Galois field to each element of the base block, hence creating a total of $t(12t + 1)$ blocks. The incidence matrix of this BIBD is a $(12t + 1) \times t(12t + 1)$ matrix, which is as follows:

$$H_{\text{BIBD}} = (H_0, H_1, \dots, H_{t-1}), \quad (3)$$

where the i th submatrix H_i is a $(12t + 1) \times (12t + 1)$ -element circulant matrix corresponding to the base block B_i . Furthermore, the matrix H_{BIBD} has a row weight of $4t$ and a column weight of 4. Since the incidence matrix of Eq. (3) has the required properties of a QC-LDPC matrix, a subarray of H_{BIBD} , having m submatrices for $0 < m < t$, can be used for constructing a classical row-circulant $(12t + 1) \times m(12t + 1)$ -element LDPC code is at least 5 and the coding rate is approximately $(m - 1)/m$.

2) Type-II Bose BIBDs: Let t be a positive integer so that $(20t + 1)$ is a power of a prime, then there exists a prime Galois field $\text{GF}(20t + 1)$ having elements ranging from 0 to $20t$, which constitute the finite set V of the BIBD. In contrast to Eq. (1), the primitive element α of $\text{GF}(20t + 1)$ has to satisfy the condition:

$$\alpha^{4t} + 1 = \alpha^c, \quad (4)$$

where c is an integer in the range $0 < c < 20t + 1$. Bose [12] proposed that we can construct a BIBD having the parameters of $v = (20t + 1)$, $b = t(20t + 1)$, $r = 5t$, $k = 5$ and $\lambda = 1$, whose t base blocks are given by:

$$B_i = \{\alpha^{2i}, \alpha^{2i+4t}, \alpha^{2i+8t}, \alpha^{2i+12t}, \alpha^{2i+16t}\}, \quad (5)$$

for $0 \leq i < t$. Similar to the Type-I design, $(12t + 1)$ blocks can be constructed for each base block B_i . The incidence matrix of the resultant BIBD is a $(20t + 1) \times t(20t + 1)$ -element matrix, which is formed by t submatrices, as previously shown in Eq. (3). For the Type-II design, the matrix H_{BIBD} has a row weight of $5t$ and a column weight of 5. Again, we can construct a row-circulant QC-LDPC of size $(20t + 1) \times m(20t + 1)$ by using a subarray of H_{BIBD} .

III. PROPOSED QLDPC CODE CONSTRUCTION

The family of CSS codes, invented independently by Calderbank and Shor [13] as well as by Steane [14], constitute a special class of stabilizer codes, which facilitate the design of quantum codes from a pair of classical binary codes. More explicitly, an $[n, k_1 - k_2]$ CSS code, which is capable of correcting $(d - 1)/2$ bit-flips as well as phase-flips, can be constructed from the classical linear block codes $C_1(n, k_1)$ and $C_2(n, k_2)$, provided that we have $C_2 \subset C_1$, and that C_1 as well as the dual of C_2 , i.e. C_2^\perp , have a minimum Hamming distance of d . If H_z and H_x are the parity check matrices (PCMs) of C_1 and C_2^\perp , respectively, then the resultant CSS code assumes the following form [8]:

$$\begin{pmatrix} H_z & 0 \\ 0 & H_x \end{pmatrix}. \quad (6)$$

More explicitly, H_z is used for bit-flip correction, while H_x corrects the phase-flips. Furthermore, since $C_2 \subset C_1$, the PCMs H_z and H_x must satisfy the symplectic criterion, which may be defined as:

$$H_z H_x^T = 0. \quad (7)$$

When $H_z = H_x$, the constraint of Eq. (7) reduces to $H_z H_z^T = 0$, which is referred to as a ‘dual-containing’ CSS code. In the context of the QLDPC codes, this dual-containing structure results in numerous unavoidable short cycles in the associated Tanner graph, which in turn degrade the performance of the decoding algorithm. Furthermore, if the symplectic criterion is not intrinsically satisfied, then pre-shared ebits may be used. The resultant codes constitute the family of EA codes.

We may also view the PCM of Eq. (6) in the $\text{GF}(4)$ formalism as [15]:

$$\hat{H} = \begin{pmatrix} \omega H_z \\ H_x \end{pmatrix}, \quad (8)$$

where $\{0, 1, \omega, \bar{\omega}\} \in \text{GF}(4)$. When both H_z and H_x are the same, as in the family of dual-containing CSS and EA-QLDPC codes¹, we may refer to them as homogeneous CSS codes. The $(m \times n)$ -element² PCM \hat{H} of a homogeneous code exhibits numerous short cycles in its Tanner graph, because the i th and $(i + m/2)$ th rows completely overlap, i.e. they have non-zero values at the same indices. These short cycles, resulting from

¹To the best of our knowledge, all the CSS-type EA-QLDPC codes proposed to date are homogeneous.

²Please note that m denotes the number of rows of the PCM \hat{H} , while n represents the number of submatrices of H_{BIBD} used in an LDPC matrix.

178 the global homogeneous code structure, appear in addition to
 179 the short cycles within the local structures of the PCMs H_z and
 180 H_x , or, equivalently, in addition to the short cycles observed
 181 in the binary formalism of Eq. (6). It is pertinent to mention
 182 here that short cycles in the GF(4) formalism are a by-product
 183 of the symplectic criterion of Eq. (7), which cannot be completely
 184 eliminated even if both H_z and H_x have a girth of 6
 185 in the binary formalism [16]. However, the number of short
 186 cycles may be reduced by adopting a non-dual-containing (or
 187 equivalently non-homogeneous) design, having $H_x \neq H_z$.

188 In contrast to both the dual-containing and to the EA structures,
 189 which suffer from numerous unavoidable short cycles, non-dual-containing
 190 codes may be designed, so that they have at least a girth of 6 in the
 191 binary formalism of Eq. (6) and fewer short cycles in the GF(4) formalism
 192 of Eq. (8) by virtue of their non-homogeneous nature. Therefore, we focus
 193 our attention on the non-dual-containing structure for constructing
 194 QLDPC codes from the pair of classical row-circulant QC-LDPC matrices
 195 H_z and H_x , each having a girth of at least 6. Let us consider a
 196 row-circulant QC-LDPC matrix H , which is a subarray of H_{BIBD} of Eq. (3),
 197 assuming that it consists of an even number of square circulant submatrices.
 198 Inspired by the non-dual-containing CSS-type QC-QLDPC codes of [17], we
 199 propose that if we formulate H_z and H_x as follows:
 200
 201

$$H_z = H,$$

$$H_x = \left(H_{\frac{m}{2}}^T, H_{\frac{m}{2}+1}^T, \dots, H_{m-1}^T, H_0^T, H_1^T, \dots, H_{\frac{m}{2}-1}^T \right), \quad (9)$$

202 where m is even, then the resultant CSS code satisfies the symplectic
 203 criterion of $H_z H_x^T = 0$. This may be readily shown as follows:
 204

$$\begin{pmatrix} H_{\frac{m}{2}} \\ H_{\frac{m}{2}+1} \\ \vdots \\ H_{m-1} \\ H_0 \\ H_1 \\ \vdots \\ H_{\frac{m}{2}-1} \end{pmatrix} \begin{pmatrix} H_0 & H_1 & \dots & H_{\frac{m}{2}-1} & H_{\frac{m}{2}} & H_{\frac{m}{2}+1} & \dots & H_{m-1} \end{pmatrix}$$

$$= H_0 H_{\frac{m}{2}} + H_1 H_{\frac{m}{2}+1} + \dots + H_{\frac{m}{2}-1} H_{m-1} + H_{\frac{m}{2}} H_0 + H_{\frac{m}{2}+1} H_1 + \dots + H_{m-1} H_{\frac{m}{2}-1}. \quad (10)$$

205 Since the multiplication of circulant matrices is commutative,
 206 the two parts of Eq. (10), i.e. $(H_0 H_{\frac{m}{2}} + H_1 H_{\frac{m}{2}+1} + \dots + H_{\frac{m}{2}-1} H_{m-1})$
 207 and $(H_{\frac{m}{2}} H_0 + H_{\frac{m}{2}+1} H_1 + \dots + H_{m-1} H_{\frac{m}{2}-1})$
 208 are equal. Hence, the modulo 2 addition of Eq. (10) yields 0;
 209 thus, satisfying the symplectic criterion. Furthermore, the resultant
 210 quantum coding rate is approximately $(m-2)/m$.

211 Let us now scrutinize the girth of the PCMs H_z and H_x
 212 in the binary formalism. The constituent $(l \times l)$ -element circulant
 213 submatrix H_i of Eq. (3), which has a row weight and a column weight
 214 of γ , is uniquely and unambiguously characterized by the polynomial
 215 $h_i(x) = x^{d_{i,0}} + x^{d_{i,1}} + \dots + x^{d_{i,\gamma-1}}$, where $d_{i,j}$ denotes the
 216 column index of the j th non-zero entry in the first row of H_i .
 217 For example, if the first row of H_i

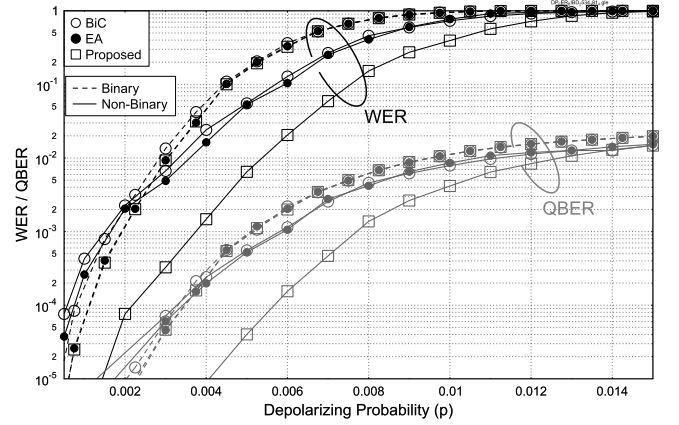


Fig. 1. Comparison of the achievable WER/QBER performance of our proposed [2534, 2172] QLDPC code (labeled 'Proposed') with the bicycle code of Eq. (11) (labeled 'BiC') and the EA-QLDPC code of Eq. (12) (labeled 'EA') over a quantum depolarizing channel.

218 has a 1 at index 0, 5 and 8, then the polynomial is given by
 219 $1 + x^5 + x^8$. The PCM H has a girth of at least 6 if every
 220 difference $(d_{i,j_1} - d_{i,j_2})$ modulo l , for $0 \leq i \leq (m-1)$ and
 221 $0 \leq j_1, j_2 \leq (\gamma-1)$, is a unique integer between 0 and $(l-1)$.
 222 Furthermore, the polynomial transpose is defined as $h_i(x)^T =$
 223 $x^{l-d_{i,1}} + x^{l-d_{i,2}} + \dots + x^{l-d_{i,\gamma-1}}$, which would yield the same
 224 differences as $h_i(x)$. Hence, since in Eq. (9) we are taking the
 225 transpose of all the sub-matrices H_i and just permuting their
 226 location, the differences $(d_{i,j_1} - d_{i,j_2})$ for H_z and H_x are
 227 the same and consequently they both have the same girth³.

IV. RESULTS AND DISCUSSIONS

228 To evaluate the performance of our proposed design, we considered
 229 the Type-I design of Eq. (2) having $t = 15$ and the primitive root
 230 $\alpha = 2$. Since our design requires m to be even, we arbitrarily
 231 chose $m = 14$, which yields a [2534, 2172] QLDPC code having a
 232 coding rate of 0.857. We compare our design both to an equivalent
 233 bicycle QLDPC code, whose PCM is given by:
 234

$$H_x = H_z = [H_0, H_1, \dots, H_{\frac{m}{2}-1}, H_0^T, H_1^T, \dots, H_{\frac{m}{2}-1}^T], \quad (11)$$

235 and to a comparable EA-QLDPC, which requires a single ebit
 236 and has:

$$H_x = H_z = [H_0, H_1, \dots, H_{m-1}]. \quad (12)$$

237 Fig. 1 compares the word error rate (WER) as well as the qubit
 238 error rate (QBER) performance of our QLDPC code (labeled 'Proposed')
 239 to that of the bicycle code of Eq. (11) (labeled 'BiC') and to that of
 240 the EA-QLDPC code of Eq. (12) (labeled 'EA'), when operating over
 241 a quantum depolarizing channel. We have evaluated the performance of
 242 both the binary as well as the non-binary QLDPC decoder, which
 243 operate over the PCMs of Eq. (6) and Eq. (8), respectively. We
 244 invoked a maximum

³Following the usual convention [6], we assume that each row of H_i is a cyclic right-shift of the row above it. However, if the direction of cyclic shift is reversed, then the resulting PCM H_i is symmetric and therefore $H_i^T = H_i$.

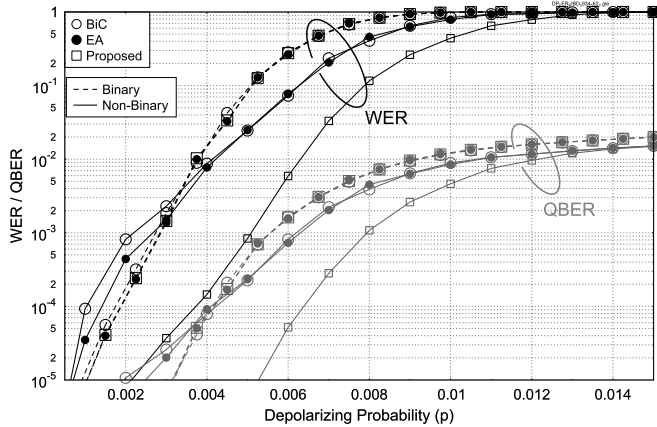


Fig. 2. Comparison of the achievable WER/QBER performance of our proposed [3934, 3372] QLDPC code (labeled ‘Proposed’) with the bicycle code of Eq. (11) (labeled ‘Bic’) and the EA-QLDPC code of Eq. (12) (labeled ‘EA’) over a quantum depolarizing channel.

of 100 iterations. Each decoding algorithm iterates until either a valid error is found or the maximum number of iterations is reached. Furthermore, the WER metric here counts the detected as well as the undetected block errors. We may observe in Fig. 1 that the performance of the designed QLDPC is exactly the same as that of the EA-QLDPC code for binary decoding, while that of the bicycle QLDPC code is slightly worse, which is due to the presence of length-4 cycles. By contrast, when non-binary decoding is invoked, then the performance of our proposed design improves significantly as compared to both the bicycle code as well as the EA-QLDPC. More specifically, the bicycle code achieves a WER of 10^{-4} at $p = 0.00055$, which increases to $p = 0.0007$ when an EA-QLDPC is used. By contrast, our construction exhibits a WER of 10^{-4} at $p = 0.00215$, which is almost three times better than that of the EA-QLDPC. As discussed in Section III, unlike the bicycle and EA-QLDPC codes, which have numerous short cycles in their GF(4) formalism by virtue of their homogeneous nature, non-homogeneous structures have fewer short cycles in the GF(4) formalism. Consequently, our QLDPC outperforms its comparable bicycle and EA counterparts, when non-binary decoding is invoked.

As an another example, we construct a QLDPC code using the Type-II design of Eq. (2) having $t = 14$ and the primitive root $\alpha = 3$. The resultant QLDPC code has dimensions of [3934, 3372] and a coding rate of 0.857, when $m = t$. Fig. 2 compares the performance of our non-dual-containing [3934, 3372] QLDPC code both to the comparable bicycle code and to the EA-QLDPC codes. It may be observed that the performance curves of Fig. 2 exhibit the same trend as those of Fig. 1.

V. CONCLUSIONS

In this letter, we have conceived a generalized formalism for constructing non-dual-containing CSS-type QLDPC codes from the known classical row-circulant high-rate QC-LDPC codes, which operate efficiently at short and moderate lengths. Since our design is merely based on the transpose and column permutation operations, the characteristics of the underlying

classical LDPC matrix are not compromised. In particular, we applied our formalism to the BIBD-based classical LDPCs for evaluating their performance. Furthermore, we invoked both binary as well as non-binary decoding. It was demonstrated that our QLDPC codes have the same performance as the EA-QLDPC codes, when binary decoding is invoked, while they outperform their EA counterparts in case of non-binary decoding. As compared to a dual-containing code, our QLDPC codes exhibit a superior performance both for binary as well as for non-binary decoding.

REFERENCES

- [1] P. Botsinis, S. X. Ng, and L. Hanzo, “Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design,” *IEEE Access*, vol. 1, pp. 94–122, 2013.
- [2] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, “Secure communication with single-photon two-qubit states,” *J. Phys. A Math. Gen.*, vol. 35, no. 28, p. L407, 2002.
- [3] J. Li, X.-B. Chen, G. Xu, Y.-X. Yang, and Z.-P. Li, “Perfect quantum network coding independent of classical network solutions,” *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 115–118, Feb. 2015.
- [4] D. Gottesman, “Stabilizer codes and quantum error correction,” Ph.D. dissertation, California Institute of Technology, Pasadena, CA, USA, 1997.
- [5] H. Tang, J. Xu, Y. Kou, S. Lin, and K. Abdel-Ghaffar, “On algebraic construction of Gallager and circulant low-density parity-check codes,” *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1269–1279, Jun. 2004.
- [6] B. Ammar, B. Honary, Y. Kou, J. Xu, and S. Lin, “Construction of low-density parity-check codes based on balanced incomplete block designs,” *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1257–1269, Jun. 2004.
- [7] S. Johnson and S. R. Weller, “A family of irregular LDPC codes with low encoding complexity,” *IEEE Commun. Lett.*, vol. 7, no. 2, pp. 79–81, Feb. 2003.
- [8] D. MacKay, G. Mitchison, and P. McFadden, “Sparse-graph codes for quantum error correction,” *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2315–2330, Oct. 2004.
- [9] I. B. Djordjevic, “Quantum LDPC codes from balanced incomplete block designs,” *IEEE Commun. Lett.*, vol. 12, no. 5, pp. 389–391, May 2008.
- [10] M.-H. Hsieh, T. A. Brun, and I. Devetak, “Entanglement-assisted quantum quasicyclic low-density parity-check codes,” *Phys. Rev. A*, vol. 79, p. 032340, Mar. 2009.
- [11] 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.
- [12] R. Bose, “On the construction of balanced incomplete block designs,” *Ann. Eugenics*, vol. 9, pp. 353–399, 1939.
- [13] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” *Phys. Rev. A*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996.
- [14] A. Steane, “Multiple-particle interference and quantum error correction,” *Roy. Soc. London Proc. Ser. A*, vol. 452, pp. 2551–2577, Nov. 1995.
- [15] Y.-J. Wang, B. Sanders, B.-M. Bai, and X.-M. Wang, “Enhanced feedback iterative decoding of sparse quantum codes,” *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 1231–1241, Feb. 2012.
- [16] T. Camara, H. Ollivier, and J.-P. Tillich, “A class of quantum LDPC codes: Construction and performances under iterative decoding,” in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 811–815.
- [17] M. Hagiwara and H. Imai, “Quantum quasi-cyclic LDPC codes,” in *Proc. Int. Symp. Inf. Theory*, Aug. 2010, pp. 806–810.

QUERY

Q1: Please check and confirm the insertion of author group and affiliation.
Please provide department name with affiliation as well.