An Overview of Low Density Parity Check Codes

¹Abid Yahya, ¹Farid Ghani, ¹R. Badlishah and ²Raj Malook ¹School of Computer and Communication Engineering, Universiti Malaysia Perlis, Perlis, Malaysia ²IT Center Taif University, Kingdom of Saudi Arabia

INTRODUCTION

Low Density Parity Check (LDPC) codes (Gallager, 1963), have acquired considerable attention due to its near-capacity error execution and powerful channel coding technique, with an adequately long codeword length. The performance of LDPC codes is investigated, at many events of interests and is encountered to outperform turbo codes with good error correction (Berrou et al., 1993; MacKay, 1999; Chung et al., 2001).

The proof of the minimum distance of the code, for most existing classes of algebraic codes makes important use of the algebraic structure of the code (Tanner et al., 2001). The minimum distance for each class of codes is usually recognized by using a proof method exact to that precise class, and the minimum distance of codes in a new class may not be easily accomplished (MacKay, 1999; Tanner et al., 2001). Tanner et al. (2001) presented a class of codes called Sparse Difference Codes, in which the parity check matrix of the resultant linear code is a block structure as a permutation matrix. The so-called array codes have parity-check matrices with powers of permutation matrices, and can be considered as LDPC codes (Fan, 2000). Eleftheriou and Olcer (2002) proposed this class of LDPC codes for an application in Digital Subscriber Lines (DSL) that employ discrete multitone modulation. Authors emphasize on further investigation in order to completely utilize the LDPC coding for DSLs, together with very high DSL, and to evaluate performance with actual loop and noise characteristics. The simulation results show that, even under rigid latency constraints, good net coding gains can be achieved by LDPC coding. Moreover, LDPC codes do not exhibit error floors at the low bit-error rates of interest for DSL transmission. Furthermore, Kim et al. (2002) proposed explicit construction of LDPC codes based on partial row construction with girth at least eight.

Authors propose construction of LDPC codes based on partial row construction and also the Sparness of codes are not well defined. Moreover, authors observe no error floor but at low SNR, while error floor occurs at high SNR. This leads to design codes which exhibit no error floors at high SNR. Simulation results show that the proposed method improves the code rate only at low girth codes

Algebraically structured QC-LDPC codes: The construction of LDPC codes from circulant permutation matrices is investigated by Fossorier (2004). It is observed from simulation results that such codes cannot have a Tanner graph representation with larger girth and their minimum distance cannot be increased by increasing the code length and as a result, the girth as for random constructions. Fossorier derives a simple necessary and sufficient condition for the Tanner graph (Tanner, 1981) of the Quasi-Cyclic (QC) LDPC codes to have a given girth. It is shown from the simulation results that the proposed codes have a girth g of at most 12, which generalizes the result simulated by Tanner et al. (2001). In case of girth g = 6, the condition is very easy to construct QC-LDPC codes, which perform significantly better at moderate block lengths , when iteratively decoded with the Belief Propagation (BP) algorithm (MacKay, 1999). Actually, Fossorier employs an upper bound on the minimum Hamming distance of QC LDPC codes and necessary condition to reach this bound. Fossorier has found that an appropriate coset weight distribution (MacKay and Postol, 2003) has to be considered when constructing families of LDPC codes. Another family of structured LDPC codes with girth six is introduced by Milenkovic and Laendner (2004) based on a class of idempotent, symmetric Latin and modified Latin squares. The proposed codes have a block structure with permutation block, which ascertains that both their corresponding girth and minimum distance are at least equal to six. The proposed method significantly reduces the number of six-cycles by shorten the codes and by removing block-columns of the parity-check matrix in a structured manner.

A QC-LDPC code can be counted as one of such algebraic constructions, which is based on circulant permutation matrices. It is essential to figure out the

proper shift values, which construct no short cycles, since the cycle structures in QC-LDPC codes are ascertained by the shift values of circulant permutation matrices, either randomly or algebraically (Miladinovic and Fossorier, 2004; Tanner et al., 2001). In case of random selection numbers of computations are required to find the proper shift values, which yield a large girth. As a result, algebraic methods are desirable to find good shift values. Few promising methods are experienced to guarantee a large girth and Tanner's QC-LDPC code (Tanner et al., 2001) is one of such constructions. Tanner et al. (2001) investigated a class of LDPC block codes, which is known to guarantee a large girth. These quasi-cyclic group-structured regular LDPC codes have highly symmetric graphs based on simple algebraic description. When the length of the basic cycle p is large, the graphs appear to have a relatively large girth for the graph size and vertex degrees, reaching the maximum girth of twelve for many of the (3, 5) codes. Simulation results show that the proposed codes perform significantly better than randomly generated (3, 5) LDPC codes for lengths of 1055 or less. In the random selection of shift values, it acquires too much computation to figure out the proper shift values, which yield a large girth. Hence, it is suitable to adopt algebraic methods to locate good shift values. Kim et al. (2006) examined the cycles of Tanner (3, 5) QC-LDPC codes and derive their girth values. Conditions in the proposed method are expressed for cycles of different lengths in Tanner (3, 5) QC-LDPC codes as simple polynomial equations in a primitive 15th root of unity in prime field. Simulation results depict that when p is 31, the girth of the code is 8, and when p is 61 or 151, the girth of the proposed code is 10. Correspondingly to the (3, 5) case, the other Tanner (J, L) quasi-cyclic LDPC codes can also be easily examined. Another class of algebraically structured QC-LDPC codes and their convolutional counterparts is presented by Tanner and Woodard (2004). Structure of multiplicative groups in the set of integers modulo m is used to place circulant matrices with a parity check matrix, so as to shape regular QC-LDPC block codes with short to moderate block lengths and rates and find the performance of proposed codes comparably to random LDPC codes.

In the work presented by Tanner *et al.* (2001) and other researchers, their constructed LDPC codes are from short to moderate block lengths. Authors replicate the constraint structure of the QC-LDPC block code to infinity and modified construction of the proposed codes to yield irregular LDPC codes, which do significantly well in the low SNR regime, but some suffer from poor distance especially, at high SNR due to error floor. They employ search method to find the girth of graph which acquires

too much computation to figure out the proper shift values and resultantly with many short cycles of length 4. A novel method is required to save the shift value of matrix in order to save the time and memory. Additionally, a robust method requires finding the highest girth by avoiding unnecessary short cycles.

Encoding and decoding of QC-LDPC based on belief propagation: A novel methodology for designing structured quasi-cyclic generalized LDPC (G-LDPC) codes is presented by Liva et al. (2008). A pragmatic approach for designing good codes is proposed, based on the insertion of powerful constraint nodes in LDPC bipartite graphs. Approach of the proposed code is based on the substitution of check nodes in the protograph of a LDPC code with stronger nodes based, such as, on Hamming codes. It is observed that such a design approach, extends to low-rate quasi-cyclic G-LDPC codes with outclass performance in both the error floor and waterfall regions on the AWGN channel. The decoder uses in the proposed work is the standard belief-propation algorithm (MacKay, 1999) with maximum a posteriori decoding at each variable node and check node. Analysis of the iterative decoding properties of a G-LDPC code's design is based on Density Evolution (DE) analysis (Luby et al., 2001; Richardson and Urbanke, 2001b; Richardson et al., 2001), constituting a controlling tool for code designers. Another technique for the design of QC-LDPC codes is proposed by Liu and Schniter (2008) based on generalized combining method. The proposed method designs a much larger class of QC-LDPC codes with similar performance by loosening the condition for ascertaining the intermediate parameters. In the proposed work a lot of QC-LDPC codes with much less 6-cycles and better performance are designed, by permuting the block rows of the parity check matrices of the component codes. It is shown that the proposed QC-LDPC codes designed by the generalized combining method outperform those designed by the Chinese Remainder Theorem (CRT) combining method by 0.5 dB at a BER of 10⁻¹. The performance of irregular LDPC codes is investigated by Ohhashi and Ohtsuki (2004a) with three BP based decoding algorithms, specifically the Uniformly Most Powerful (UMP) BP-based algorithm, the normalized BP-based algorithm, and the offset BP-based algorithm on a fast Rayleigh fading channel by employing density evolution. It is observed from the study of proposed method that the performance and decoding complexity of irregular LDPC codes with the offset BP-based algorithm can be very close to that with the BP algorithm on the fast Rayleigh fading channel. After successful evolution of irregular LDPC codes, Ohhashi and Ohtsuki (2004b) then

analyze the performance of regular LDPC codes with the normalized BP-based algorithms on the fast Rayleigh fading channel. Formulas for short and long regular LDPC codes are derived based on the Probability Density Function (PDF) of the initial likelihood information and DE for the normalized BP-based algorithm on the fast Rayleigh fading channel. Performance of the long regular LDPC codes with the normalized BP-based algorithm in the proposed method outperforms the BP algorithm and the UMP BP-based algorithm on fast Rayleigh fading channel.

Sullivan et al. (2005) employed seed matrix for construction of LDPC codes, which is the chain of two relative incidence matrices for Fano planes and circulant permutation matrices. The effect on decoding performance is investigated by employing sum-product algorithm for column weight 3. Authors show by using BER simulations that large girth codes perform better than those with lower girths. A new necessary and adequate condition for determining the girth of QC-LDPC codes is derived by Wu et al. (2008) based on the theory of adjacency matrices, without an explicit enumeration of cycles. It is shown from simulation results that the obtained codes are often with performance comparable to the LDPC codes constructed by progressive-edge-growth (PEG) algorithm (Hu et al., 2001; Hu et al., 2002). The performance error for regular QC-LDPC and PEG-LDPC codes are plotted with iterative sum-product decoding (Chung et al., 2001), with same code rate and observe that the PEG-LDPC codes are frequently with smaller girth than the proposed QC-LDPC code by adopting concentrated parity-check degree distribution. There is considerable work on optimizing girth in LDPC codes.

A large girth LDPC codes construction based on linear congruence is proposed by Jing et al. (2007). Based on graph-theoretic method, three kinds of special paths are designed in the proposed method to ensure that the Tanner graph of the parity check matrix mapped from the connection graph, based on without short cycles. The proposed method is competent of generating a class of regular QC-LDPC codes with a girth of 12 and a minimum Hamming distance of no less than 24. The simulation results show that the proposed LDPC codes significantly outperform random codes and the QC block LDPC code with similar block lengths and rates. Another method for constructing large girth QC-LDPC codes from graphical models is proposed by Huang et al. (2008). The proposed QC-LDPC codes based on circulant permutation matrices with girths 16 and 18, by employing a simple quadratic congruential equation. The simulation results show that the proposed codes perform better than the randomly constructed LDPC codes for short to moderate block lengths and have almost the same performance as the Sridhara-Fuja-Tanner (SFT) (Tanner *et al.*, 2001) codes for different block lengths and rates.

Yang et al. (2008) proposed Parallel-Input Parallel-Output (PIPO) structure for QC-LDPC codes to execute a faster and more efficient QC-LDPC encoder than that based on conventional Serial-Input Parallel-Output (SIPO) Parallel-Input Serial-Output (PISO) structure. Experimental results reveal that the proposed PIPO encoding structure for QC-LDPC codes perform significantly better than the conventional SIPO and PISO structures in terms of speed and complexity. The proposed scheme shows that the number of LC registers required by PIPO at the same encoding speed, is linearly proportional to the block size of the submatrix in the generator matrix. While in case of SIPO and PISO, it is proportional squarely. Additionally, the combinationals required by SIPO are about 2 to 3 times as much as that PIPO requires. The encoding architecture is investigated, based on the proposed PIPO structure for multi-rate QC-LDPC codes, employed by Chinese Digital Television Terrestrial Broadcasting (DTMB), with less logic complexity compared with SIPO architecture. It is shown from simulation results that PIPO proposes more flexible trade-offs between encoding speed and encoding complexity, which points that the maximal throughput has the potential over 1Gbps.

With the requirements, defined by MacKay et al. (2004) for the check matrix of quantum LDPC, Zhou et al. (2008) proposed a novel construction method of quantum LDPC based on classical quasi-cyclic sparse sequence, which can fix both bit flip and phase shift errors. The results show that quantum LDPC code can correct the bit error efficiently, and the proposed construction method of quantum LDPC code is available. It is observed from the proposed work that quantum error correction code based on classical LDPC code is a promising research area in quantum communications and quantum computation.

In many ways, LDPC codes can be considered serious competitors to turbo codes. In particular, LDPC codes show an asymptotically better performance than turbo codes and they admit a broad range of tradeoffs between performance and decoding complexity (Richardson and Urbanke, 2001a). The foremost criticism concerning LDPC codes is their apparent high encoding complexity. Richardson and Urbanke (2001a) considerd the encoding problem for codes determined by sparse parity-check matrices. In the proposed work the encoding complexity is upper bounded by n+g², where g , the gap, measures in some way to be made specific shortly, the distance of the given parity-check matrix to a lower triangular matrix. For the (3, 6)-regular LDPC code, the

complexity of encoding is essentially quadratic in the block length (n). The proposed work shows that even the large block lengths admit practically feasible encoders, because of the extremely small constant factor.

Hocevar (2003a, b) design encoder-decoder solution for Irregular Partitioned Permutation (IPP) LDPC codes, for both software and hardware based on Sridhara, Fuja and Tanner (SFT) method (Tanner et al., 2001). Two approaches are discussed by Hocevar, first is the preimplementation phase involving matrix factorization, and second approach is the operation implementations for data encoding. The quasi-cyclic factorization or row reduction at the block level in the proposed scheme forms the core of the preimplementation portion and attains a high degree of parallelism, thus enabling very high data rate and flexible decoders. It is much faster, up to two orders of magnitude, and it is simpler than the standard quasi-cyclic approach that uses cyclic shifting. The prime advantage of the proposed method is that it does not need storing a matrix inverse in full binary form that would require a nontrivial memory, whether exploiting symmetry or not, and the solution hardware is trivial.

A simple yet low complex systematic LDPC encoding method proposed for class of QC-LDPC codes to let LDPC encoder attains an interchangeable structure, used in the With the proposed encoding scheme, implementation of the proposed encoder becomes much more hardware efficient than having a separate hardware due to LDPC encoder and decoder resource sharing. Additionally, the overall computational complexity of the proposed encoding scheme is lower than the well-known Richardson's efficient encoding scheme (Richardson and Urbanke, 2001a). Authors show that the proposed LDPC encoding scheme is directly applicable to current the WLAN and WiMAX standards. Another low complexity and fast encoding schemes, which has also reduced computational complexity from Richardson's is proposed by Kim et al. (2008). In that work, authors focus on computational complexity of Richardson's LDPC matrix, which is composed by matrix A, B, C, D, E and F (Richardson and Urbanke, 2001b) and propose two schemes for low complexity encoding. First approaches T $= \phi$ and confines D consisting of dual diagonal matrices and second makes $T = \phi = 1$ without cycle-4, resultantly achieve reducing the complexity to O(n). Proposed encoding schemes are very useful for high-rate and fast communication systems due to reduce complexity and efficiently omitted processes of encoding.

Authors in the aforesaid work construct QC-LDPC codes decoder based on density evolution in order to

compute the threshold of noise level for a large class of binary-input channels. But it is not able to estimate their performance in the case of finite length. Additionally, their interconnection increases the hardware complexity. The new proposed QC-LDPC codes with reduce hardware complexity because performance of LDPC codes of finite length may be affected by other elements such as cycle property and minimum distance not only by density evolution.

The codes constructed by the authors in the aforesaid systems are with high hardware complexity which makes them unusable at very large lengths. The unstructured interconnection comes up with routing complexity and obstruction in decoder implementations the number of row connections is almost uniformly distributed by first selecting randomly the rows with the least number of connections. The resultant codes are with rigid row and column weight. The decoders of aforesaid system run with maximum iteration even by achieving the task at early iteration. This will not only waste the time but also degrades the system performance. Moreover, the iterative techniques although improve the decoder throughput but on the other hand memory size is increased.

Abid et al. (2009a-d) keeping in mind the aforesaid system has proposed a novel construction of QC-LDPC code which reduces not only encoding complexity but improve the decoding part of the system. In order to simplify the hardware implementation, the proposed codes incorporate some form of structured decoder interconnections. In the proposed algorithm, the restructuring of the interconnections is invented by splitting the rows with the group size. Such a division guarantees a concentrated node degree distribution and reduces the hardware complexity. The new codes offer more flexibility in terms of high girth, multiple code rates and block length.

REFERENCES

Abid, Y., S. Othman, M.F.M. Salleh and G. Farid, 2009a. Lower computation and storage complexity of QC-LDPC codes in rayleigh fading channel. Int. J. Comput. Theory Eng., 1: 115-118.

Abid, Y., S. Othman, M.F.M. Salleh and A. Sardar, 2009b. An efficient encoding-decoding of large girth LDPC codes based on quasi-cyclic. Aust. J. Basic Applied Sci., 3: 1734-1739.

Abid, Y., S. Othman, M.F.M. Salleh and G. Farid, 2009c. A new quasi-cyclic low density parity check codes. Proceedings of IEEE Symposium on Industrial Electronics and Applications, Oct. 4-6, Kuala Lumpur, Malaysia, pp. 329-342.

- Abid, Y., S. Othman, M.F.M. Salleh and G. Farid, 2009d. Row division method to generate QC-LDPC codes. Proceedings of IEEE 5th Advanced International Conference on Telecommunications, May 24-28, Venice, Mestre, Italy, pp:183-187.
- Berrou, C., A. Glavieux and P. Thitimajshima, 1993. Near shannon limit error correcting coding and decoding: Turbo-codes. Proceedings of the IEEE International Conference on Communication, May 23-26, Geneva, Switzerland, pp. 1064-1070.
- Chung, S.Y., T.J. Richardson and R.L. Urbanke, 2001. Analysis of sum-product decoding of low-density parity-check codes using a gaussian approximation. IEEE Trans. Inform. Theory, 47: 657-670.
- Eleftheriou, E. and S. Olcer, 2002. Low-density parity-check codes for digital subscriber lines. IEEE Int. Conf. Commun., 3: 1752-1757.
- Fan, J.L., 2000. Array codes as low-density parity-check codes. Proceedings of the 2nd International Symposium on Turbo Codes and Related Topics, Sept. 4-7, Brest, France, pp. 545-546.
- Fossorier, M.P.C., 2004. Quasi-cyclic low density parity check codes from circulant permutation matrices. IEEE Trans. Inform. Theory, 50: 1788-1794.
- Gallager, R.G., 1963. Low-Density Parity-Check Code. MIT Press, Cambridge, MA, pp. 90.
- Hocevar, D.E., 2003a. LDPC code construction with flexible hardware implementation. Proc. IEEE Int. Conf. Commun., 4: 2708-2712.
- Hocevar, D.E., 2003b. Efficient encoding for a family of quasi-cyclic LDPC codes. Proceedings of the IEEE Conference on Global Telecommunication, Dec. 5-1, Dallas, TX, USA., pp. 3996-4000.
- Hu, X.Y. E. Eleftheriou and D.M. Arnold, 2001.
 Progressive edge-growth tanner graphs.
 Proceedings of the IEEE Conference on Global Telecommunications, Nov. 25-29, Dallas, pp: 995-1001.
- Hu, X.Y. E. Eleftheriou and D.M. Arnold, 2002. Irregular progressive edge growth (PEG) tanner graphs. Proceedings of the IEEE International Symposium on Information Theory, July 30-35, Lausanne, Switzerland, pp. 480-480.
- Huang, C.M., J.F. Huang and C.C. Yang, 2008. Construction of quasi-cyclic LDPC codes from quadratic congruences. IEEE Commun. Lett., 12: 313-315.
- Jing, L.J., J.L. Lin and W.L Zhu, 2007. Design of quasi-cyclic low-density parity check codes with large girth. ETRI J., 29: 381-389.

- Kim, J.L., U. Peled, I. Perepelitsa and V. Pless, 2002. Explicit construction of families of LDPC codes with girth at least six. Proceedings of the 40th Annual Allerton Conference on Communications, Control and Computing, Oct. 2-4, Univ. of Illi. at Urbana-Champaign, IL, pp. 1024-1031.
- Kim, S., J.S. No, H. Chung and D.J. Shin, 2006. On the girth of tanner's (3, 5) quasi-cyclic LDPC codes. IEEE Trans. Inform. Theory, 52: 1739-1744.
- Kim, J.K., S.P. Balakannan, M.H. Lee and C.J. Kim, 2008. Low complexity encoding of LDPC codes for high-rate and high-speed communication. Proceedings of the 1st International Conference on Distributed Framework and Applications, Oct 21-22, Penang, pp: 189-193.
- Liu, H. and P. Schniter, 2008. Iterative frequency-domain channel estimation and equalization for single-carrier transmissions without cyclic-prefix. IEEE Trans. Wireless Commun., 7: 3686-3691.
- Liva, G., W.E. Ryan and M. Chiani, 2008. Quasi-cyclic generalized LDPC codes with low error floors. IEEE Trans. Commun., 56: 49-57.
- Luby, M.G., M. Mitzenmacher, M.A. Shokrollahi and D.A. Spielman, 2001. Analysis of low density codes and improved designs using irregular graphs. IEEE Trans. Inform. Theory, 47: 585-598.
- MacKay, D.J.C., 1999. Good error-correcting codes based on very sparse matrices. IEEE Trans. Inform. Theory, 45: 399-431.
- MacKay, D.J.C. and M.S. Postol, 2003. Weaknesses of margulis and ramanujan-margulis low-density paritycheck codes. Electronic Notes Theoretical Comput. Sci., 74: 97-104.
- MacKay, D., G. Mitchison and P.L. McFadden, 2004. Sparse graph codes for quantum error correction. IEEE Trans. Inform. Theory, 50: 2315-2330.
- Miladinovic, N. and M. Fossorier, 2004. Systematic recursive construction of LDPC codes. IEEE Commun. Lett., 8: 302-304.
- Milenkovic, O. and S. Laendner, 2004. Analysis of the cycle-structure of LDPC codes based on Latin squares. Proceedings of the IEEE International Conference on Communications, June 20-24, Boulder, CO, USA., pp: 777-781.
- Ohhashi, A. and T. Ohtsuki, 2004a. Performance analysis of BP-based algorithms for irregular low-density parity-check codes on fast Rayleigh fading channel. Proceedings of the IEEE 60th Conference on Vehicular Technology, Sept 26-29, Chiba, Japan, pp: 2530-2534.

- Ohhashi, A. and T. Ohtsuki, 2004b. Regular low-density parity-check (LDPC) code with normalized and UMP BP-based algorithms on fast Rayleigh fading channel. Proceedings of the IEEE 60th Conference on Vehicular Technology, Sept 26-29, Noda, Japan, pp: 2520-2524.
- Richardson, T.J. and R.L. Urbanke, 2001a. Efficient encoding of low-density parity-check codes. IEEE Trans. Inform. Theory, 47: 638-656.
- Richardson, T.J. and R.L. Urbanke, 2001b. The capacity of low density parity-check codes under message-passing decoding. IEEE Trans. Inform. Theory, 47: 599-618.
- Richardson, T.J., A. Shokrollahi and R. Urbanke, 2001. Design of capacity-approaching irregular low-density parity-check codes. IEEE Trans. Inform. Theory, 47: 619-637.
- Sullivan, M.E.O., J. Brevik and R. Wolski, 2005. The performance of LDPC codes with large girth. 43rd Allerton Conference on Communication Control and Computing. http://pompone.cs.ucsb.edu/~rich/publications/g4.pdf.
- Tanner, R., 1981. A recursive approach to low complexity codes. IEEE Trans. Inform. Theory, 27: 533-547.

- Tanner, R.M., D. Sridhara and T.E. Fuja, 2001. A class of group-structured LDPC codes. Proceedings of the International Conference on Information Systems Technology and its Applications, June 13-15, Ambleside, England, pp. 282-282.
- Tanner, R. and J. Woodard, 2004. WCDMA Requirements and Practical Design. Wiley, Chichester, West Sussex, ISBN: 978-0-470-86177-6.
- Wu, X., X. You and C. Zhao, 2008. A necessary and sufficient condition for determining the girth of quasi-cyclic LDPC codes. IEEE Trans. Commun., 56: 854-857.
- Yang, Z., Q. Xie, K. Peng and J. Fu, 2008. A fast and efficient encoding structure for QC-LDPC codes. Proceedings of the International Conference on Communications, Circuits and Systems, May 19-23, Beijing, China, pp: 16-20.
- Zhou, B., L. Zhang, J. Kang, Q. Huang, Y.Y. Tai, S. Lin and M. Xu, 2008. Non-binary LDPC codes vs. Reed-Solomon codes. Proceedings of the Workshop on Information Theory and Applications, Jan. 27-Feb. 1, San Diego, CA., pp. 175-184.