

LDPC Codes Based on α – Resolvable BIB and Group Divisible Designs

Shyam Saurabh¹ and Kishore Sinha²

¹*Ranchi University, Ranchi, India*

²*Birsa Agricultural University, Ranchi, India*

Abstract

Structured LDPC codes have been constructed using balanced incomplete block (BIB) designs, resolvable BIB designs, mutually orthogonal Latin rectangles, partial geometries, group divisible designs, resolvable group divisible designs and finite geometries. Here we have constructed LDPC codes from α – resolvable BIB and Group divisible designs. The sub-matrices of incidence matrix of such block design are used as a parity – check matrix of the code which satisfy row – column constraint. Here the girth of the proposed code is at least six and the corresponding LDPC code (or Tanner graph) is free of 4– cycles.

Keywords: LDPC Codes; Tanner graph; Resolvable designs; BIB designs; Group divisible designs

1. Introduction

Low– density parity– check (LDPC) codes were introduced by Gallager (1962). In recent years, these codes have become strong competitor to Turbo codes for error control in many digital storage and communication systems where high reliability is required. Based on the methods of constructions, LDPC codes can be divided into two types: random codes and structured codes. Random LDPC codes are constructed by computer search while structured LDPC codes are constructed by algebraic and combinatorial methods. Despite the excellent error– correcting properties of some known random LDPC codes, they often have the high complexity. A large amount of information is necessary to specify the positions of the non– zero elements in the parity– check matrix. These complexity drawbacks of random LDPC codes can be overcome by structured LDPC codes. A coverage on the constructions of structured LDPC codes using balanced incomplete block (BIB) and resolvable BIB designs, mutually orthogonal

¹ Corresponding Author

Email: shyamsaurabh785@gmail.com

²Email: kishore.sinha@gmail.com

Kishore Sinha is former Professor (Statistics) and presently at: # 201 Maitry Residency, Kalkere Main Road, Bangalore - 560043.

Latin rectangles, partial geometries, group divisible designs, resolvable group divisible designs and finite geometries may be found in Kou *et al.* (2001), Ammar *et al.* (2004), Li *et al.* (2008), Johnson and Weller (2001, 2003, 2004), Vasic *et al.* (2002), Weller and Johnson (2003), Lan *et al.* (2008) and Xu *et al.* (2015, 2019), among others.

A binary (γ, ρ) – regular LDPC code is defined as the null space of an $m \times n$ sparse parity– check matrix H with entries from $\{0, 1\}$ having the following properties: 1) each row has ρ nonzero elements; 2) each column has γ nonzero elements; 3) $\rho \ll n$ and $\gamma \ll m$. The code rate of a (γ, ρ) – regular LDPC code is $1 - \gamma/\rho$ provided that the parity check matrix has full rank. The Tanner graph of an LDPC code is a bipartite graph in which two types of nodes are variable nodes (representing coded symbol variables) and check nodes (representing the local check– sum constraints) respectively. The size of the shortest cycle is called the girth of the Tanner graph (or LDPC code). The shortest cycles affect the decoding performance with iterative algorithm based on belief propagation, especially the 4 – cycles. In order to create an LDPC code free of 4 – cycle, a structural property is imposed on H : no two distinct columns (or two distinct rows) have more than one nonzero element in common. This constraint on H is known as the row– column constraint (or RC constraint), see Diao *et al.* (2013). The RC– constraint ensures that the girth of the LDPC codes generated by such H is at least six.

The aim of this paper is to construct LDPC codes free of four cycles from α – resolvable BIB and Group divisible designs. A submatrix of incidence matrix of such block design is used as parity – check matrix of the code which satisfies row – column constraint. Hence the girth of the proposed code is at least six and the corresponding LDPC code (or Tanner graph) is free of 4 – cycles.

2. Preliminaries

Suppose b blocks of a block design $D(v, b, r, k)$ can be divided into $t = r/\alpha$ classes, each of size $\beta = v\alpha/k$ such that in each class of β blocks every point of D is replicated α times. Then these t classes are known as α – resolution (or parallel) classes and the design is called α – resolvable design. When $\alpha=1$ the design is said to be resolvable and the classes are called resolution classes.

A $2 - (v, k, \lambda)$ or a BIB design is an arrangement of v points into a collection of sets of size k , called *blocks*, such that each pair of distinct points occurs in exactly λ blocks.

A *Group divisible (GD) design* is defined as an arrangement of $v (= mn; m, n \geq 2; m$ groups of n points) points into b blocks such that each block contains $k (<v)$ distinct points, each point occurs r times and any pair of distinct points which are first associates occur together in λ_1 blocks and in λ_2 blocks if they are second associates. Furthermore, if $r - \lambda_1 = 0$ then the GD design is singular; if $r - \lambda_1 > 0$ and $rk - v\lambda_2 = 0$ then it is semi-regular (*SR*); and if $r - \lambda_1 > 0$ and $rk - v\lambda_2 > 0$, the design is regular (*R*).

SRX and *RX* numbers are from Clatworthy (1973). For terminologies and constructions of designs, see Raghavarao (1988), Raghavarao and Padgett (2005), Dey (2010), among others. If resolvable BIB and GD designs are not available then we go for α - resolvable BIB and GD designs respectively. α - resolvable solutions of GD designs used in this paper may be found in Clatworthy (1973) and Saurabh *et al.* (2021). In this paper we abbreviate resolution classes for α - resolution classes.

3. Construction Methods

3.1. Construction from α - resolvable BIB designs

Consider α - resolvable BIB design: $v, b, r, k, \lambda = 1$ and Let R^1, R^2, \dots, R^t be the resolution classes where $t = r/\alpha$. Let I_1, I_2, \dots, I_t be the $v \times (v\alpha/k)$ matrices corresponding to t resolution classes. Then each row sum of I_i ($1 \leq i \leq t$) is α . Such matrices are of full rank. Combining any p ($1 \leq p \leq t$) resolution classes of such design we obtain a sequence of LDPC codes with length $v\alpha p/k$ and rate about $1 - k/\alpha p$.

Johnson and Weller (2001, 2003) constructed $(3, \rho)$ - and $(4, \rho)$ - regular LDPC codes from Kirkman triple systems (KTS) which are resolvable Steiner triple systems (STS). Here we construct LDPC codes from α - resolvable $v, b, r, k, \lambda = 1$ design. In addition some series of resolvable BIB designs: $v, b, r, k, \lambda = 1$ are reported which yield LDPC codes as discussed in Johnson and Weller (2003).

The following resolvable series may be found in Furino *et al.* (1996) where s is a prime or prime power:

Series I: $v = (s + 1)(s^2 + 1), b = (s^2 + 1)(s^2 + s + 1), r = s^2 + s + 1, k = s + 1, \lambda = 1.$

Series II: $v = s^2, b = s(s + 1), r = s + 1, k = s, \lambda = 1.$

Series III: $v = s^3, b = s^2(s^2 + s + 1), r = s^2 + s + 1, k = s, \lambda = 1$.

Remark 1: Series I, II and III yield $(s+1, \rho) -$, $(s+1, \rho) -$ and $(s, \rho) -$ regular LDPC codes with different lengths and rates.

The following theorem may be found in Raghavarao (1988) and 3 – resolvability follows from Bose’s first module theorem, see Kageyama and Mohan (1983).

Theorem 1: When $v = 6s + 1$ is a prime or prime power and x be a primitive root of GF (v). Then the s initial sets $(x^0, x^{2s}, x^{4s}); (x, x^{2s+1}, x^{4s+1}); \dots, (x^{s-1}, x^{3s-1}, x^{5s-1})$ give a solution of the 3 – resolvable BIB design with parameters: $v = 6s + 1, b = s(6s + 1), r = 3s, k = 3, \lambda = 1$.

Example 1: For $s = 7$ in Theorem 1 we obtain a 3 – resolvable BIB design with parameters: $v = 43, b = 301, r = 21, k = 3, \lambda = 1$.

Let $N = (I_1|I_2|I_3|I_4|I_5|I_6|I_7)$ be the incidence matrix. Suppose we take combination of 3, 4, 5 and 6 resolution classes respectively. Then we can construct a sequence of LDPC codes of lengths 129, 172, 215, 258 with rates 0.66, 0.75, 0.80, 0.83 respectively.

3. 2. Construction from α – resolvable Group divisible designs

Consider a Group divisible design with parameters:

$$v, b, r, k, \lambda_i \in \{0, 1\}; |\lambda_i - \lambda_j| = 1, i \neq j; i, j \in \{1, 2\} \quad (1)$$

Let B_i and B_j be two distinct blocks of the design. Since any two elements occur in either one block or no block, we have $|B_i \cap B_j| \leq 1$ and hence any two distinct columns of the incidence matrix N have at most one nonzero element common. That is, every pair of points of the design is contained in at most one block and also every pair of blocks contains at most one point. Hence no two rows (or columns) in incidence matrix N have more than one position where they both have 1–component in common. If we consider N as parity– check matrix then it satisfies the RC – constraint and the constructed LDPC code (or Tanner graph) is free of 4 – cycles. Also each column and row sum of N is k and r respectively. Hence the LDPC code is $(k, r) -$ regular.

Xu *et al.* (2015) constructed LDPC codes from resolvable GD designs. If (1) represents α – resolvable GD design then we can construct LDPC codes as discussed in Section 3. 1.

Theorem 2 [Banerjee and Kageyama (1996)]: The existence of α – resolvable GD design with parameters:

$$v = mn, b, r, k = 3, \lambda_1 = 0, \lambda_2 = 1$$

implies the existence of another 2α – resolvable GD design with parameters:

$$v^* = m^*n^* = 2v, b^* = 4b, r^* = 2r, k = 3, \lambda_1 = 0, \lambda_2 = 1, m^* = m, n^* = 2n.$$

Using Theorem 2 repeatedly to α – resolvable GD design, we obtain following series:

Series IV: A 2 – resolvable solution of SR30: $v = 18, b = 36, r = 6, k = 3, \lambda_1 = 0, \lambda_2 = 1, m = 3, n = 6$ yields a series of 2^{x+1} – resolvable SRGD designs with parameters:

$$v = 18 \cdot 2^x, b = 36 \cdot 4^x, r = 6 \cdot 2^x, k = 3, \lambda_1 = 0, \lambda_2 = 1, m = 3, n = 6 \cdot 2^x (x \geq 1).$$

Example 2: For $x = 3$, we obtain a 16 – resolvable GD design with parameters:

$$v = 144, b = 2304, r = 48, k = 3, \lambda_1 = 0, \lambda_2 = 1, m = 3, n = 48.$$

Let $N = (I_1|I_2|I_3)$ be the incidence matrix. Suppose we take combination of any two resolution classes. Then we can construct a sequence of LDPC codes of length 1536 with rate 0.90.

Series V: A 2 – resolvable solution of SR34: $v = 30, b = 100, r = 10, k = 3, \lambda_1 = 0, \lambda_2 = 1, m = 3, n = 10$ yields a series of 2^{x+1} – resolvable SRGD designs with parameters:

$$v = 30 \cdot 2^x, b = 100 \cdot 4^x, r = 10 \cdot 2^x, k = 3, \lambda_1 = 0, \lambda_2 = 1, m = 3, n = 10 \cdot 2^x (x \geq 1).$$

Example 3: For $x = 2$, we obtain a 8 – resolvable GD design with parameters: $v = 120, b = 1600, r = 40, k = 3, \lambda_1 = 0, \lambda_2 = 1, m = 3, n = 40$.

Let $N = (I_1|I_2|I_3|I_4|I_5)$ be the incidence matrix. Suppose we take combination of 2, 3 and 4 resolution classes respectively. Then we can construct a sequence of LDPC codes of lengths 640, 960, 1080 with rates 0.81, 0.88, 0.91 respectively.

Series VI: A resolvable solution of $R91$: $v = 21, b = 63, r = 9, k = 3, \lambda_1 = 0, \lambda_2 = 1, m = 7, n = 3$ yields a series of 2^x -resolvable RGD designs with parameters:

$$v = 21 \cdot 2^x, b = 63 \cdot 4^x, r = 9 \cdot 2^x, k = 3, \lambda_1 = 0, \lambda_2 = 1, m = 7, n = 3 \cdot 2^x (x \geq 1).$$

Example 4: For $x = 3$, we obtain a 8 - resolvable GD design with parameters:

$$v = 168, b = 4032, r = 72, k = 3, \lambda_1 = 0, \lambda_2 = 1, m = 7, n = 24.$$

Let $N = (I_1|I_2|I_3|I_4|I_5|I_6|I_7|I_8|I_9)$ be the incidence matrix. Suppose we take combination of 5, 7 and 8 resolution classes respectively. Then we can construct a sequence of LDPC codes of lengths 2240, 3136, 3584 with rates 0.92, 0.94, 0.95 respectively.

Remark 2: Resolvable solutions of $SR31, SR32, SR33$ and a 2 - resolvable solution of $R88$ will also yield series of GD designs which are applicable in the construction of LDPC codes.

References

- [1] Ammar, B., Honary, B. and Kou, Y., *Construction of low-density parity-check codes based on balanced incomplete block designs*. IEEE Trans. Inform. Theory, 2004, 50(6): 1257–1268.
- [2] Banerjee, S. and Kageyama, S. (1996). Non-isomorphic solutions of group divisible designs with $k=3$ and $\lambda_1=0$. *J. Statist. Plan. Inference*, **56**, 23–32.
- [3] Dey, A. (2010). *Incomplete Block Designs*. Hindustan Book Agency, New Delhi.
- [4] Diao, Q., Tai, Y., Lin, S. and Abdel - Ghaffar, K., “LDPC codes on partial geometries: construction, trapping set structure, and puncturing,” *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 7898–7914, Dec. 2013.
- [5] Furino, S., Miao, Y. and Jianxing, Y. (1996). *Frames and Resolvable Designs: Uses, Constructions and Existence*. Boca Roca, United States: Taylor & Francis Inc.
- [6] Gallager, R. G., *Low-density parity-check codes*. IEEE Trans. Inform. Theory, 1962, 8: 21–28.
- [7] Johnson, S. J. and Weller, S. R. “Construction of low-density parity-check codes from Kirkman triple systems,” In *Proc. IEEE Globecom Conf.*, San Antonio, TX, vol. 2, pp. 970–974, Nov. 2001.
- [8] Johnson, S. J. and Weller, S. R., Resolvable 2 - design for regular low-density parity-check codes. *IEEE Trans. on Communications*, 2003, 51 (9), 1413 – 1419.

- [9] Johnson, S. J. and Weller, S. R., *Codes for iterative decoding from partial geometries*. IEEE Trans. On Commun., 2004, 52: 236– 243.
- [10] Kageyama, S. and Mohan, R. N., On μ – resolvable BIB designs. Discrete Mathematics, 1983, 45, 113 – 121.
- [11] Kou, Y., Lin, S. and Fossonier, M. P. C., *Low–density parity–check codes based on finite geometries: a rediscovery and new results*. IEEE Trans. Inform. Theory, 2001, 47(7): 2711–2736.
- [12] Lan, L., Tai, Y., Lin, S., Memari, B. and Honary, B. “New constructions of quasi–cyclic LDPC codes based on special classes of BIBDs for the AWGN and binary erasure channels,” *IEEE Trans. Commun.*, vol. 56, no. 1, pp. 39–48, Jan. 2008.
- [13] Li, Xiuli , Zhang, X. C. and Shen, J. *Regular LDPC codes from semipartial geometries*. Acta Appl. Math., 2008, 102(1): 25–35.
- [14] Raghavarao, D. (1988). *Constructions and Combinatorial Problems in Design of Experiments*. John Wiley, New York.
- [15] Raghavarao, D. and Padgett, Lakshmi V. (2005). Block designs. Analysis, combinatorics and applications. *Series on Applied Mathematics*, **17**, World Scientific, Singapore.
- [16] Saurabh, S. and Sinha, K. (2021). A survey of resolvable solutions of partially balanced designs, *Communications in Statistics – Theory and Methods*, DOI: 10.1080/03610926.2021.1942049
- [17] Vasic, B., Kurtas, E. M. and Kuznetsov, A. V. *LDPC codes based on mutually orthogonal latin rectangles and their application in perpendicular magnetic recording*. IEEE Trans. Magnetics, 2002, 38: 2346–2348.
- [18] Weller, S. R. and Johnson, S. J., *Regular low–density parity–check codes from oval designs*. Eur. Trans. Telecommun., 2003, 14: 399–409.
- [19] Xu, H., Feng, D. Sun, C. and Bai, B. (2015). Construction of LDPC codes based on resolvable Group divisible designs. 2015 International Workshop on High Mobility Wireless Communications (HMWC), DOI: [10.1109/HMWC.2015.7354346](https://doi.org/10.1109/HMWC.2015.7354346) 111–115.
- [20] Xu, H., Yu, Z., Feng, D. and Zhu, H. (2019). New construction of partial geometries based on group divisible designs and their associated LDPC codes. *Physical Communication*, <https://doi.org/10.1016/j.phycom.2019.100970>.