Journal of Mathematical Research with Applications
May, 2013, Vol. 33, No. 3, pp. 330–336
DOI:10.3770/j.issn:2095-2651.2013.03.007
Http://jmre.dlut.edu.cn

A Construction of Low-Density Parity-Check Codes

Xiuling SHAN[1,2], **Tienan LI**[2,*]
1. *Department of Mathematics, Beijing Jiaotong University, Beijing* 100044*, P. R. China;*
2. *College of Mathematic and Information Science, Hebei Normal University,*
Hebei 050016*, P. R. China*

Abstract Low-density parity-check (*LDPC*) codes were first presented by Gallager in 1962. They are linear block codes and their bit error rate (BER) performance approaches remarkably close to the Shannon limit. The *LDPC* codes created much interest after the rediscovery by Mackay and Neal in 1995. This paper introduces some new LDPC codes by considering some combinatorial structures. We present regular *LDPC* codes based on group divisible designs which have Tanner graphs free of four-cycles.

Keywords low-density parity-check code; iterative decoding; group divisible design.

MR(2010) Subject Classification 05B05; 51D20

1. Introduction

Low-density parity-check (*LDPC*) codes were first presented by Gallager [1] in 1962. *LDPC* codes can achieve near-optimum performance with iterative decoding when used for transmission over white additive Gaussian noise (AWGN) channels. It became a challenge to construct codes that would come as close as possible to the Shannon limit [2]. The *LDPC* codes created much interest after the rediscovery by Mackay and Neal [3] in 1995. 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 parts: random codes [1, 3, 4] and structured codes [5–10]. Random *LDPC* codes are often constructed by computer search while structured *LDPC* codes are constructed by algebra 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. So the complexity drawbacks of random *LDPC* codes can be overcome by structured *LDPC* codes. Several structured *LDPC* codes have been known, including those based on combinatorial designs (such as *BIBD*s, mu-

Received November 6, 2011; Accepted May 22, 2012
Supported by the National Natural Science Foundation of China (Grant Nos. 11071056; 11201114).
* Corresponding author
E-mail address: xiulingshan@sina.com (Xiuling SHAN), tienanli@sina.com (Tienan LI)

tually orthogonal Latin rectangles, partial geometries) [5–9], finite geometries (such as conics, ovals [10]).

A binary regular $LDPC$ code is defined as the null space of a sparse parity-check matrix H over $GF(2)$ with the following properties: 1) each row has weight ρ; 2) each column has weight γ; 3) no two rows (or two columns) have more than one 1-component in common; 4) both ρ and γ are small compared to the code length. The $LDPC$ code defined above is called (γ, ρ)-regular. If not all the columns or rows of H have constant weight, then the null space of H gives an irregular $LDPC$ code. A useful way to describe $LDPC$ code is the Tanner graph which displays the relationship between codeword bits and parity-checks. Each of the n code bits and b parity-checks in the parity-check matrix H is represented by a vertex in the graph. An edge of the graph joins a code bit vertex to the vertex of the parity-checks that include it. The girth of a Tanner graph is the size of its smallest cycle. But the existence of short cycles in the Tanner graph prevents an exact error-probability analysis of iterative decoding procedures. Without 4-cycles in the graph of codes, the iterative sum-product decoding algorithm can be performed well. $LDPC$ codes based on combinatorial designs, such as Steiner 2-designs has girth at least 6.

The aim of this paper is to design regular $LDPC$ codes based on another combinatorial design: group divisible design. The paper is organized as follows. In Section 2, we show the connection between GDD and strongly regular (α, β)-geometry. In Section 3, we describe some properties of such codes such as the minimum distance, the number of 6-girth of the Tanner graph and the 2-rank of the parity-check matrix.

2. The connection with strongly regular (α, β)-geometry

A graph G is said to be regular if each vertex is connected to exactly k other vertices. If any two connected vertices of G are both connected together to exactly λ other vertices, and two unconnected vertices are both connected to exactly μ vertices together, the graph is called strongly regular and specified by the parameters (v, k, λ, μ) (see [11]).

Next, we will give the definition of strongly regular (α, β)-geometries. A (finite) (α, β)-geometry with parameters (s, t) is an incidence structure $(\mathcal{P}, \mathcal{L})$, where $\mathcal{P}$ is a finite non-empty set of elements (called points), $\mathcal{L}$ is a family of subsets (called lines) of $\mathcal{P}$, the incidence contains the following properties:

(1) Any two distinct points are incident with at most one line;

(2) Each line is incident with exactly $s + 1$ points;

(3) Each point is incident with exactly $t + 1$ lines;

(4) For any point $x \in \mathcal{P}$ and any line $L \in \mathcal{L}$ not containing x there are exactly α or β points on L collinear with x.

We call a line L not incident with a point x an α-line with respect to x if there are exactly α lines joining x to a point of L. β-lines are defined similarly. (α, β)-geometries were first defined in [12] where the problem of linear embedding was examined. We say an (α, β)-geometry is strongly regular if there exist integers p and r such that the following conditions are satisfied.

(1) If points x and y are collinear, there exist p lines on x that are α-lines with respect to y.

(2) If points x and y are not collinear, there exist r lines on x that are α-lines with respect to y.

We call s, t, p and r the parameters of the strongly regular (α, β)-geometry. A simple count shows that the number of lines of the geometry is $b = v(t+1)/(s+1)$, where v is the number of points.

N. Hamilton and R. Mathon [13] had shown that the point graph of a strongly regular (α, β)-geometry with parameters s, t, p and r is strongly regular with

$$\begin{aligned} &k = s(t+1),\\ &\lambda = p(\alpha-1) + (t-p)(\beta-1) + s - 1,\\ &\mu = r\alpha + \beta(t+1-r),\\ &v = \frac{k(k-\lambda-1)}{\mu} + k + 1. \end{aligned}$$

If for any point $x \in \mathcal{P}$ and any line $L \in \mathcal{L}$ not containing x there are exactly α points on L collinear with x, then the (α, β)-geometry is called a partial geometry of order (s, t) (see [14]). It is clear that the point graph of a partial geometry is strongly regular.

A group divisible design (GDD) is a triple $(X, \mathcal{G}, \mathcal{B})$ which satisfies the following properties.

(1) $\mathcal{G} = \{G_1, G_2, \ldots, G_m\}$ is a partition of a v-set X into subsets (called groups).

(2) $\mathcal{B}$ is a collection of subsets (called blocks) of X, such that a group and a block contain at most one element in common.

(3) Each pair of elements from distinct groups occurs in precisely λ (called the index) blocks. Each pair of elements from the same group does not appear in any block.

Let $K = \{|B| : B \in \mathcal{B}\}$. The multiset $\{|G_1|, |G_2|, \ldots, |G_m|\}$ is called the type of the GDD. We usually use exponential notation to describe the type: G has the type $t_1^{u_1} t_2^{u_2} \cdots t_m^{u_m}$ if G contains u_1 groups of size t_1, u_2 groups of size $t_2, \ldots, u_m$ groups of size t_m. If $K = \{k\}$, such GDD is often denoted as a k-GDD of type $t_1^{u_1} t_2^{u_2} \cdots t_m^{u_m}$. If each group $|G_i| = 1$ for $1 \le i \le m$, such GDD is just a $(m, k, 1)$-$BIBD$.

An automorphism of a GDD $(X, \mathcal{G}, \mathcal{B})$ is a permutation π on X with the property that $\pi(B) \in \mathcal{B}$ for each $B \in \mathcal{B}$. A GDD $(X, \mathcal{G}, \mathcal{B})$ is cyclic if it has an automorphism which permutes the elements in each group $G \in \mathcal{G}$ in a $|G|$-cycle. A cyclic k-GDD is denoted by k-$CGDD$. For further details, one can see [15].

Theorem 1 *An l-GDD of type g^u is a strongly regular $(l-1, l)$-geometry with parameters*

$$\begin{aligned} &s = l-1, \quad t = \frac{g(u-1)}{l-1} - 1,\\ &p = g-1, \quad r = t+1,\\ &\lambda = g(u-2), \quad \mu = g(u-1). \end{aligned}$$

Proof Let $(X, \mathcal{B})$ be an l-GDD of type g^u. The fact of s, t can be easily obtained by the definition of GDD. For any point $x \in X$ and any line $L \in \mathcal{B}$ not containing x, if L does not meet the group containing x, there are exactly l points on L collinear with x, otherwise there are exactly $l-1$ points on L collinear with x. So $(X, \mathcal{B})$ is an $(l-1, l)$-geometry.

If points x and y are collinear with line L, i.e., x and y belong to different groups, denote the lines containing x to be $L, L_1, L_2, \ldots, L_t$. Here $y \notin L_i$ for $1 \leq i \leq t$. If the line L_i meets the group containing y, L_i is an $(l-1)$-block with respect to y, otherwise an l-block with respect to y. There are $g-1$ $(l-1)$-blocks with respect to y in all. Thus $p = g-1$ and $\lambda = p(\alpha - 1) + (t-p)(\beta - 1) + s - 1 = g(u-2)$.

If points x and y are not collinear, i.e., x and y belong to the same group, y is not on each line containing x. This means that each line on x is an l-block with respect to y. So $r = t+1$ and $\mu = r\alpha + \beta(t+1-r) = g(u-1)$.

3. *GDD-LDPC* codes

For constructing $LDPC$ codes, we are only interested in GDDs with $\lambda = 1$ and equal group size. Let $(X, \mathcal{G}, \mathcal{B})$ be an l-GDD of type g^u with $|X| = gu$ and $|\mathcal{B}| = b = \frac{g^2u(u-1)}{l(l-1)}$. Instead of a list of the blocks, a GDD can be efficiently described by a $gu \times b$ matrix $H = [h_{ij}]$ over $GF(2)$ where each row in H represents an element $x \in X$ and each column a block $B \in \mathcal{B}$ such that

$$h_{ij} = \begin{cases} 1, & \text{if } x \in B \\ 0, & \text{otherwise.} \end{cases}$$

It is easy to see from the properties of a GDD that the incidence matrix H has constant row weight and constant column weight, and any two rows of H have exactly one 1-component in common. So the incidence matrix H can be considered as a parity-check matrix of a binary regular $LDPC$ code defined earlier. Therefore, the null space of H gives a (γ, ρ)-regular $LDPC$ code, which is denoted by GDD-$LDPC$ code of length b.

The GDD-$LDPC$ codes can be presented by $C = \{c : cH^T = 0, c \in GF(2)^b\}$ with v parity checks and code length b. In the parity-check matrix H, all columns have weight l and all rows have weight $\rho = \frac{g(u-1)}{l-1}$. As in the case for random constructions of parity-check matrix, the H constructed in this way is not necessarily of full rank. In this case the number of message bits in the code is $k = b - \text{rank}_2(H)$ where $\text{rank}_2(H)$ is the rank of H over $GF(2)$. But the rank of H is usually difficult to determine. For given block length l, the codes quickly become high rate since the code length $b = \frac{gu(u-1)}{l(l-1)}$ increases with nearly square of the number of parity checks. It would be useful to have codes with the properties of GDD but with a wider range of available rates for each codeword length.

Next, we will use the properties of strongly regular graph to derive the minimum distance of GDD-$LDPC$ code, the number of 6-girth of its Tanner graph and the 2-rank of its parity-check matrix.

The minimum distance of a code is equal to the minimum nonzero number of columns in the parity-check matrix for which a nontrivial linear combination sums to zero [16]. The properties of the *GDD* ensure that all columns in the parity-check matrix have weight l, and that no two columns share more than one element. Thus it needs at least $l+1$ columns to sum to zero and $d_{\min} \geq l+1$ for the *GDD-LDPC* codes.

Since the index of the l-*GDD* of type g^u is one, the Tanner graph of the *GDD-LDPC* code cannot contain 4-cycle. So the girth is at least six. In fact, the number of 6-cycles $N(6)$ in the *GDD-LDPC* code can be enumerated exactly.

Theorem 2 *The exact number of* 6*-cycles in the Tanner graph of the above GDD-LDPC code is*

$$N(6) = \frac{g^2u(u-1)(gu-2g-l+2)}{6}.$$

Proof Let $(X, \mathcal{G}, \mathcal{B})$ be an l-*GDD* of type g^u. Suppose x, y are distinct points of X and appear in the block $B \in \mathcal{B}$. By Theorem 1, we have $t = \frac{g(u-1)}{l-1} - 1$.

The point x is incident with t blocks $B_1, B_2, \ldots, B_t$ other than B, none of which contain the point y. Without loss of generality, we assume that the first $g-1$ blocks meet the group containing y, i.e., $B_1, B_2, \ldots, B_{g-1}$. On each of these $g-1$ blocks, there are $l-2$ points, $y_{i1}, \ldots, y_{i(l-2)}$ $(1 \leq i \leq g-1)$, which lies in different groups with x and y. So the pair $\{y_{ij}, y\}$ must appear in another block B'_j. Then there are $(g-1)(l-2)$ 6-cycles containing both x and y, which is of the type $(B, x, B_i, y_{ij}, B'_j, y)$. Similarly, the rest $t-g+1$ blocks $B_{g-1}, B_g, \cdots, B_t$ must not meet the group containing y. On each of these $t-g+1$ blocks, there are $l-1$ points which lie in different groups with x and y. There are $(t-g+1)(l-1)$ 6-cycles in which points x and y are connected. It is easy to see that there exist no other 6-cycles containing both x and y. Since a 6-cycle includes three pairs of distinct points, the number of 6-cycles is

$$\begin{aligned} N(6) &= \frac{1}{3} \times \frac{u(u-1)g^2}{l(l-1)} \times [(g-1)(l-2) + (t-g+1)(l-1)] \times \frac{l(l-1)}{2} \\ &= \frac{g^2u(u-1)(gu-2g-l+2)}{6}. \end{aligned}$$

The following two lemmas will help us to obtain the 2-rank of H.

Lemma 3 ([17]) *Let G be a strongly regular graph with parameters (v, k, λ, μ) and A be the adjacent matrix of G. Then the eigenvalues of A are k, r and m where*

$$r = \frac{(\lambda-\mu)+\Delta}{2}, \quad m = \frac{(\lambda-\mu)-\Delta}{2}.$$

The multiplicities of k, r and m are $1, f$ and h, respectively, where

$$f = \frac{1}{2}[(v-1) + \frac{(v-1)(\mu-\lambda)-2k}{\Delta}], \; h = \frac{1}{2}[(v-1) - \frac{(v-1)(\mu-\lambda)-2k}{\Delta}],$$

$$\Delta = \sqrt{(\lambda-\mu)^2 + 4k(k-\mu)}.$$

Lemma 4 ([18]) *For a strongly regular (α, β)-geometry D with incidence matrix N and adjacent matrix A, A and N are related by the expression $A = NN^T - (t+1)I$.*

From Lemma 3 it follows that if r is an eigenvalue of A with multiplicity f, then $r + (t+1)$ is an eigenvalue of NN^T with multiplicity f. For the case $u = l$, the *GDD* is the transversal design, which forms a partial geometry and has been discussed in [8]. Combining with Theorem 1 gives the following result.

Theorem 5 *Let $u \neq l$. The rate of the LDPC code which is derived from an l-GDD of type g^u is $1-\frac{l(l-1)}{g(u-1)}$.*

Proof By Theorem 1, an l-*GDD* of type g^u is a strongly regular $(l-1,l)$-geometry. Its adjacent matrix A has three eigenvalues $k=g(u-1)$, $r=0$, $m=-g$ with multiplicity $1, f=u(g-1)$, $h=u-1$, respectively. Let H be the incidence matrix of the *GDD*. Then, by Lemma 3 $HH^T=A+(t+1)I$ has eigenvalues

$$\theta_0=\frac{lg(u-1)}{l-1},\ \theta_1=\frac{g(u-1)}{l-1},\ \theta_2=\frac{g(u-1)}{l-1}-g$$

with multiplicities 1, $f=u(g-1)$, $h=u-1$, respectively. If $u\neq l$, we must have $u>l$ by the definition of the *GDD*. And all the three eigenvalues are not zero. Thus $\mathrm{rank}_2(HH^T)=gu$. Further, $\mathrm{rank}_2(H)\geq \mathrm{rank}_2(HH^T)=gu$. The code rate of the derived *GDD-LDPC* code is $R=\frac{b-v}{b}=1-\frac{l(l-1)}{g(u-1)}$.

If the desired *GDD* is a cyclic l-*GDD* of type g^u, the parity-check matrix of the *GDD-LDPC* code has special structure formed by some circulant sub-matrices.

Example Let $(X,\mathcal{G},\mathcal{B})$ be a 3-*GDD* of type g^5 with $X=Z_{5g}$ and $g=12s+3$. The block set $\mathcal{B}$ contains the following $8s+2$ base blocks [19]:

$$\begin{array}{ll}\{0,10s+1,20s+4\}, & \{0,10s+2,30s+8\},\\ \{0,10s-1-10r,20s+3-5r\}, & \{0,10s-2-10r,30s+6-5r\},\\ \{0,10s-4-10r,20s+2-5r\}, & \{0,10s-3-10r,30s+4-5r\},\\ \{0,10s-6-10r,20s+1-5r\}, & \{0,10s-7-10r,30s+2-5r\},\\ \{0,10s-9-10r,20s-1-5r\}, & \{0,10s-8-10r,30s+3-5r\}\end{array}$$

where $r=0,1,\ldots,s-1$. Each base block contributes to a distinct cirsulant matrix. Then the incidence matrix contains row of circulants, as

$$H=[H_1,H_2,\ldots,H_{8s+2}],$$

where H_i is the $5g\times 5g$ circulant matrix. Thus we need not store the entire H matrix for decoder action and hence the decoder memory requirement and implementation complexity reduces significantly. The rate of the desired *GDD-LDPC* code is $1-\frac{1}{8s+2}$. For different values of s, a sequence of codes with various lengths and rates can be implemented.

References

[1] R. G. GALLAGER. *Low-density parity-check codes.* IEEE Trans. Inform. Theory, 1962, **8**: 21–28.

[2] R. LUCAS, M. P. C. FOSSORIER, Y. KOU, et al. *Iterative dcoding of one-step majority logic decodeable codes based on belief propagation.* IEEE Trans. Commun., 2000, **48**: 931–937.

[3] D. J. C. MACKAY, R. M. NEAL. *Near Shannon limit performance of low-density parity-check codes.* Electron. Lett., 1996, **32**: 1645–1646.

[4] D. J. C. MACKAY. *Good error-correcting codes based on very sparse matrices.* IEEE Trans. Inform. Theory, 1999, **45**(2): 399–431.

[5] Yu KOU, Shu LIN, M. P. C. FOSSORIER. *Low-density parity-check codes based on finite geometries: a rediscovery and new results.* IEEE Trans. Inform. Theory, 2001, **47**(7): 2711–2736.

[6] B. AMMAR, B. HONARY, Yu KOU, et al. *Construction of low-density parity-check codes based on balanced incomplete block designs.* IEEE Trans. Inform. Theory, 2004, **50**(6): 1257–1268.

[7] Xiuli LI, Chen ZHANG, Jun SHEN. *Regular LDPC codes from semipartial geometries.* Acta Appl. Math., 2008, **102**(1): 25–35.

[8] S. J. JOHNSON, S. R. WELLER. *Codes for iterative decoding from partial geometries.* IEEE Trans. Commun., 2004, **52**: 236–243.

[9] B. VASIC, E. M. KURTAS, A. V. KUZNETSOV. *LDPC codes based on mutually orthogonal latin rectangles and their application in perpendicular magnetic recording.* IEEE Trans. Magnetics, 2002, **38**: 2346–2348.

[10] S. R. WELLER, S. J. JOHNSON. *Regular low-density parity-check codes from oval designs.* Eur. Trans. Telecommun., 2003, **14**: 399–409.

[11] J. H. VAN LINT, R. M. WILSON. *A Course in Combinatorics.* Cambridge University Press, Cambridge, 1992.

[12] F. DE CLERCK, M. VAN MALDEGHEM. *On linear representations of (α,β)-geometries.* European J. Combin., 1994, **15**(1): 3–11.

[13] N. HAMILTON, R. MATHON. *Strongly regular (α,β)-geometries.* J. Combin. Theory Ser. A, 2001, **95**(2): 234–250.

[14] R. C. BOSE. *Strongly regular graphs, partial geometries and partial designs.* Pacific J. Math., 1963, **13**: 389–419.

[15] C. J. COLBOURN, J. H. DINITZ. *The CRC Handbook of Combinatorial Designs* (2nd Ed.). CRC Press, Boca Raton, FL, 2006.

[16] S. B. WICKER. *Error Control Systems for Digital Communication and Storage.* Upper Saddle River, NJ: Prentice-Hall, 1995.

[17] P. J. CAMERON, J. H. VAN LINT. *Graphs, Codes and Designs.* Cambridge University Press, Cambridge-New York, 1980.

[18] F. BUEKENHOUT. *Handbook of Incidence Geometry.* North-Holland, Amsterdam, 1995.

[19] R. P. GALLANT, Zhike JIANG, A. C. H. LING. *The spectrum of cyclic group divisible designs with block size three.* J. Combin. Des., 1999, **7**(2): 95–105.