Generalization of Tanner's Minimum Distance Bounds for LDPC Codes

Min-Ho Shin, Joon-Sung Kim and Hong-Yeop Song

***Abstract*— Tanner derived minimum distance bounds of regular codes in terms of the eigenvalues of the adjacency matrix by using some graphical analysis on the associated graph of the code. In this letter, we generalize Tanner's results by deriving a bit-oriented bound and a parity-oriented bound on the minimum distances of both regular and block-wise irregular LDPC codes.**

***Index Terms*— LDPC codes, bit-oriented bound, parity-oriented bound, QC-LDPC codes.**

I. Introduction

LOW-DENSITY parity check (LDPC) codes are error-correcting codes defined by sparse parity check matrices. LDPC codes with iterative decoding were first invented by Gallager in 1962 and recently much attention has been paid since they have been rediscovered to perform very close to the theoretical limit [1],[2],[3],[4]. Especially Luby *et al.* [3] introduced irregular LDPC codes with improved performances and Richardson *et al.* [4] presented near capacity achieving irregular LDPC codes by introducing density evolution technique which analyzes the asymptotic performance of the codes. However, relatively few papers have been presented on the distance property of the LDPC codes. Tanner [5] derived minimum distance bounds on the regular LDPC codes in terms of the eigenvalues of the associated graph by using the relationship between nodes on the graph and a minimum-weight codeword.

In this letter we generalize the Tanner's results. We derive a bit-oriented bound and a parity-oriented bound on the minimum distance of both regular and block-wise irregular LDPC codes. We present some examples of codes and discuss the usefulness of the bounds.

II. Tanner's Minimum Distance Bounds

An LDPC code with an $m \times n$ parity check matrix H can be thought as a bipartite graph with m check nodes and n bit nodes [5]. A bipartite graph is $B = (V_b \cup V_c, E)$, where $V_b = \{b_1, b_2, \ldots, b_n\}$, $V_c = \{c_1, c_2, \ldots, c_m\}$ and the edge set E consists of edge (c_i, b_j) in $V_c \times V_p$ corresponds to nonzero h_{ij} in H [6]. The connectivity of the graph is described by an $(m+n) \times (m+n)$ real-valued adjacency matrix with entry $a_{ij} = 1$ if and only if the ith node is connected by an edge to the jth node [6]. Thus

$$A = \begin{bmatrix} 0 & H \\ H^T & 0 \end{bmatrix}.$$

Tanner [5] derived minimum distance bounds by analyzing the properties of the subgraph of B related to a minimum-weight word. He defined active bit nodes as bit nodes corresponding to non-zeros in a minimum-weight word, active edges as the edges incident on active bit nodes, and active check nodes as the check nodes with at least one active incident edge. See Fig. 1 for an example.

Tanner presented the following bounds on the minimum distance d of a code with an $m \times n$ regular parity check matrix H. Let γ be the fixed column weight and ρ be the fixed row weight of H and μ_1, μ_2 be the largest and the second largest eigenvalues of HH^T respectively. Then we have the *bit-oriented bound* [5, Theorem 3.1]

$$d \geq \frac{n(2\gamma - \mu_2)}{\mu_1 - \mu_2},$$

and the *parity-oriented bound* [5, Theorem 4.1]

$$d \geq \frac{2n(2\gamma + \rho - 2 - \mu_2)}{\rho(\mu_1 - \mu_2)}.$$

Using these bounds, Tanner set up a heuristic rule that a code with a smaller ratio of second to first eigenvalues will have a good distance property [5].

III. Generalization of the Bounds

Tanner's bounds are applicable only to regular LDPC codes. In this section we generalize Tanner's results.

Theorem 1 (Bit-oriented bound): Let $\mu_1 > \mu_2 > \cdots > \mu_s$ be the ordered distinct eigenvalues of real valued matrix $H^T H$, where the parity check matrix H of a linear block code is in the form of $H = [H_1, H_2, \ldots, H_p]$. We assume that the associated graph of the code is connected. Let each $H_i, (1 \leq i \leq p)$ be an $m \times l$ matrix with fixed column weight γ_i and fixed row weight ρ_i with the assumption $\gamma_1 \leq \gamma_2 \leq \cdots \leq \gamma_p$.

Then the minimum distance d of the code satisfies

$$d \geq \frac{(2\gamma_1 - \mu_2) l \sum_{i=1}^{p} \gamma_i^2}{\gamma_p^2 (\sum_{i=1}^{p} \gamma_i \rho_i - \mu_2)}.$$

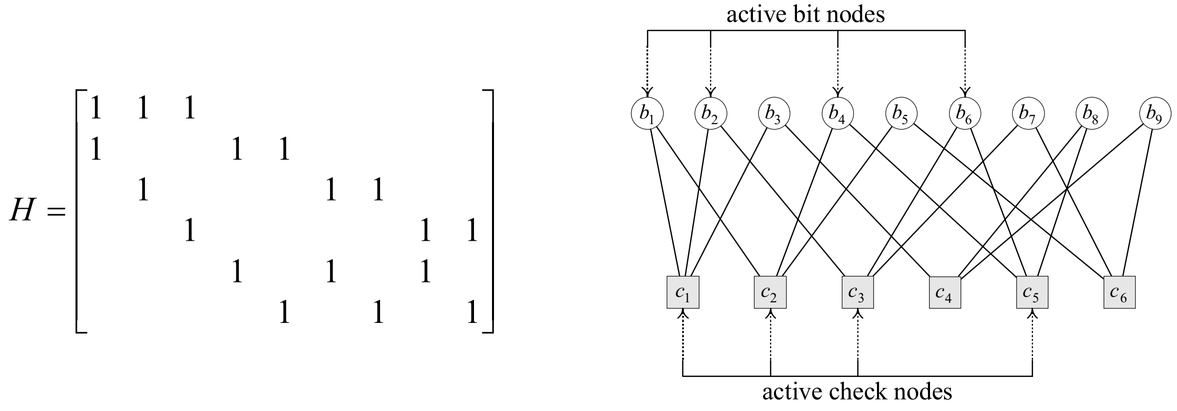
Proof: Let $\mathbf{c}$ be a real-valued vector of length-pl corresponding to a minimum-weight codeword with ones in every nonzero positions and zeros elsewhere. The first eigenvector of $H^T H$ can be taken to be

Manuscript received June 23, 2004. The associate editor coordinating the review of this letter and approving it for publication was Prof. Marc Fossorier. Support for this work was provided in part by Samsung Electronics under the project on 4G wireless communication systems. Part of this work was presented at ISIT'04.

The authors are with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul, Korea (e-mail: mh.shin@coding.yonsei.ac.kr).

Digital Object Identifier 10.1109/LCOMM.2005.03002.

1089-7798/05$20.00 © 2005 IEEE


$$H = \begin{bmatrix} 1 & 1 & 1 & & & & & & \\ 1 & & & 1 & 1 & & & & \\ & 1 & & & & 1 & 1 & & \\ & & 1 & & & & & 1 & 1 \\ & & & 1 & & 1 & & 1 & \\ & & & & 1 & & 1 & & 1 \end{bmatrix}$$

(a)

(b)

Fig. 1. This figure shows an example of regular LDPC code with length 9, fixed column weight 2, and fixed row weight 3. Active bit nodes and active check nodes are shown corresponding to a minimum-weight word (110101000). (a) Parity check matrix. (b) Associated bipartite graph.

$\mathbf{e}_1 = (\gamma_1, \ldots, \gamma_1, \gamma_2, \ldots, \gamma_2, \ldots, \gamma_p, \ldots, \gamma_p)^T / \sqrt{l \sum_{i=1}^{p} \gamma_i^2}$ with the corresponding eigenvalue $\mu_1 = \sum_{i=1}^{p} \gamma_i \rho_i$, and it is unique since the graph is connected [7]. Let d_i be the number of nonzeros of $\mathbf{c}$ in each l-portion corresponding to H_i, and let $\mathbf{c}_i$ be the projection of $\mathbf{c}$ onto the ith eigenspace. Clearly

$$\mathbf{c}^T\mathbf{c} = \|\mathbf{c}\|^2 = d, \tag{1}$$

$$\|\mathbf{c}_1\|^2 = \frac{(\sum_{i=1}^{p} d_i\gamma_i)^2}{l\sum_{i=1}^{p}\gamma_i^2} \le \frac{d^2\gamma_p^2}{l\sum_{i=1}^{p}\gamma_i^2}. \tag{2}$$

Let x_i be the weight on the ith check defined by $H\mathbf{c}$. Since each nonzero x_i must be even and at least two, we have

$$\|H\mathbf{c}\|^2 = \sum_{i=1}^{m} x_i^2 \ge 2\sum_{i=1}^{m} x_i = 2\sum_{i=1}^{p} d_i\gamma_i \ge 2\gamma_1 d. \tag{3}$$

Using the eigenspace representation we get

$$\|H\mathbf{c}\|^2 = \sum_{i=1}^{s} \mu_i\|\mathbf{c}_i\|^2 \le (\mu_1 - \mu_2)\|\mathbf{c}_1\|^2 + \mu_2\|\mathbf{c}\|^2. \tag{4}$$

Then substituting (1), (2), (3) into (4) gives the desired bound for d. ■

Theorem 2 (Parity-oriented bound): Let $\mu_1 > \mu_2 > \cdots > \mu_s$ be the ordered distinct eigenvalues of real valued matrix HH^T, where the parity check matrix H of a linear block code is in the form of $H = [H_1, H_2, \ldots, H_p]$. We assume that the associated graph of the code is connected. Let each $H_i, (1 \le i \le p)$ be an $m \times l$ matrix with fixed column weight γ_i and fixed row weight ρ_i with the assumption $\gamma_1 \le \gamma_2 \le \cdots \le \gamma_p$. Then the minimum distance d of the code satisfies

$$d \ge \frac{2m(2\gamma_1 + \sum_{i=1}^{p}\rho_i - 2 - \mu_2)}{\gamma_p(\sum_{i=1}^{p}\gamma_i\rho_i - \mu_2)}.$$

Proof: Let $\mathbf{p}$ be a length-m real-valued vector that has a 1 in every active check node position and 0 elsewhere, and let $\mathbf{p}_i$ be the projection of $\mathbf{p}$ onto the ith eigenspace of HH^T. The first eigenvector can be taken to be $\mathbf{e}_1 = (1, 1, \ldots, 1)^T/\sqrt{m}$ with $\mu_1 = \sum_{i=1}^{p}\gamma_i\rho_i$, and it is unique since the graph is connected [7]. If η is the number of 1's in $\mathbf{p}$, then $\mathbf{p}^T\mathbf{p} = \|\mathbf{p}\|^2 = \eta$ and $\|\mathbf{p}_1\|^2 = \eta^2/m$. Observe that $H^T\mathbf{p}$ assigns an integer weight distribution to bit nodes in H. Let y_i be the weight on the ith bit node so that

$$\|H^T\mathbf{p}\|^2 = \sum_{i=1}^{pl} y_i^2. \tag{5}$$

Each active check node is adjacent to an even number of nonzero bit nodes. For the jth active check node, let $u_j(w)$ be the number of adjacent nodes with weight w in $H^T\mathbf{p}$, $0 \le w \le \gamma_p$. The squared weight counted at the jth active check node is

$$\sum_{w=1}^{\gamma_p}(1/w)u_j(w)w^2 \ge 2\gamma_1 + \sum_{i=1}^{p}\rho_i - 2. \tag{6}$$

Then since there are η active check nodes,

$$\sum_{i=1}^{pl} y_i^2 \ge \eta(2\gamma_1 + \sum_{i=1}^{p}\rho_i - 2). \tag{7}$$

Using eigenspace representation we get

$$\|H^T\mathbf{p}\|^2 = \sum_{i=1}^{s}\mu_i\|\mathbf{p}_i\|^2 \le (\mu_1 - \mu_2)\|\mathbf{p}_1\|^2 + \mu_2\|\mathbf{p}\|^2. \tag{8}$$

Substituting from above gives

$$\eta \ge m(2\gamma_1 + \sum_{i=1}^{p}\rho_i - 2 - \mu_2)/(\mu_1 - \mu_2) \tag{9}$$

and $d\gamma_p \ge 2\eta$ gives the desired bound. ■

Corollary 3: Tanner's bounds are obtained by setting $p = 1$ or by setting $\gamma_1 = \gamma_2 = \cdots = \gamma_p$ and $\rho_1 = \rho_2 = \cdots = \rho_p$ in Theorems 1 and 2.

IV. Examples and Conclusions

To illustrate the use of the theorems, we calculate the bounds of the code in Fig. 1 and present examples of quasi-cyclic LDPC (QC-LDPC) codes. The parity check matrix of a quasi-cyclic code is in the form of a block matrix consists of $m \times m$ circulant matrices as blocks, where m is the order of circulant matrix. Each circulant matrix H_{ij} in H is completely

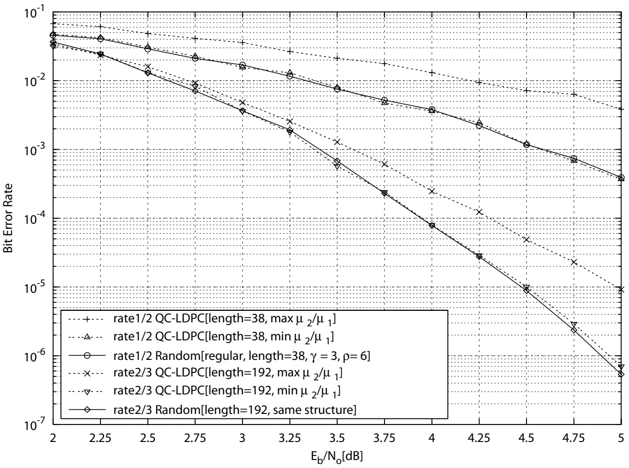


Fig. 2. BER performance of QC-LDPC codes compared with that of randomly constructed ones with the same structure [2] in AWGN channel. Sum-Product decoding algorithm with at most 100 iterations is applied.

described by the associated polynomial $h_{ij}(x)$ corresponding to the top row of H_{ij} [8],[9],[10]. More precisely, we have

$$h_{ij}(x) = \sum_{k=0}^{m-1} (H_{ij})_{0k} x^k. \tag{10}$$

We call the number of nonzero coefficients of the polynomial the weight of the polynomial.

Example 1: The code in Fig. 1 is a rate-4/9 [9,2,3]-regular LDPC code with $\mu_1 = 6$ and $\mu_2 = 3$. Note that non-zero eigenvalues of $H^T H$ and HH^T are the same [5],[6]. Hence the bit-oriented bound gives $d \geq 3$ and the parity-oriented bound gives $d \geq 4$. The actual minimum distance found through an exhaustive search is 4. Thus the parity-oriented bound gives the true minimum distance.

Example 2: Let $H = [H_1, H_2]$ with $h_1(x) = 1 + x + x^8, h_2(x) = 1 + x^2 + x^6 + x^{16}$, and $m = 19$. Then $\mu_1 = 25$ and $\mu_2 = 6$. In this example the bound from Theorem 1 becomes zero since $\mu_2 = 2\gamma_1$, whereas the bound from Theorem 2 gives $d \geq 2.5$. The actual minimum distance found through an exhaustive search is 7. One of the worst connected graphs with these code parameters is $H = [H_1, H_2]$ with $h_1(x) = 1 + x^5 + x^{12}, h_2(x) = 1 + x^2 + x^7 + x^{14}$. This code has $\mu_1 = 25$ and $\mu_2 = 22.29$ with the true minimum distance 4.

Example 3: Consider QC-LDPC codes with $H = [H_1, H_2, H_3]$ with $m = 64$. Let the weights of the associated polynomials are 3, 3, and 4 respectively. Then the largest eigenvalue is $\mu_1 = 34$. With this structure one of the best codes with girth 6 in terms of the theorems is $h_1(x) = 1 + x^5 + x^{56}, h_2(x) = 1 + x^{16} + x^{47}$ and $h_3(x) = 1 + x^2 + x^{30} + x^{57}$. The second largest eigenvalue of this code is $\mu_2 = 13.67$. Whereas one of the worst codes without 4-cycle is $h_1(x) = 1 + x + x^{18}, h_2(x) = 1 + x^{12} + x^{36}$ and $h_3(x) = 1 + x^5 + x^{11} + x^{34}$ with $\mu_2 = 28.19$.

The derived bounds have weak points due to some approximations used in the derivation. First if there are parity check equations in the minimum-weight word satisfied by four or more nonzero bits in the code, the inequality (3) will not be tight. Second, replacing all the smaller eigenvalues by μ_2 results in the loss of tightness. Third, replacing all the other weights into the maximum(or minimum) weight in (2), (3), (6) does the same. We observe that the bit-oriented bound becomes trivial as p increases both in regular and irregular cases, whereas the parity-oriented bound becomes meaningful for larger column and row weights.

The bounds, though might not be tight sometimes, still give a heuristic indicator for the distance property of an associated code. For an example, the weight enumerator of the first code in Example 2 is $A(z) = 1 + 38z^7 + 190z^8 + 4636z^{11} + \cdots$, while $A(z) = 1 + 19z^4 + 38z^6 + 95z^7 + 266z^8 + \cdots$ for the second one. Empirical results indicate the bounds give a heuristic rule that a code with a smaller ratio of second to first eigenvalue would have a good distance property as expected by Tanner in his analysis on the case of regular LDPC codes. This rule is also in accord with other criteria related to expander graphs [11]. Simulation results (Fig. 2) show that the derived bounds work well as a design criterion for the construction of irregular LDPC codes.

V. Acknowledgement

The authors would like to thank the editor and the anonymous reviewers for their constructive suggestions and comments.

References

[1] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 21-28, Jan. 1962.

[2] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, pp. 533-547, Mar. 1999.

[3] M. Luby *et al.*, "Improved low-density parity-check codes using irregular graphs and belief propagation," in *IEEE Trans. Inform. Theory*, vol. 47, pp. 585-598, Feb. 2001.

[4] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 619-637, Feb. 2001.

[5] R. M. Tanner, "Minimum distance bounds by graph analysis," *IEEE Trans. Inform. Theory*, vol. 47, pp. 808-821, Feb. 2001.

[6] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, 1992.

[7] L. W. Beineke and R. J. Wilson, *Graph Connections*, Oxford Science Publications, 1997.

[8] Henk van Tilborg, "On quasi-cyclic codes with rate 1/m," *IEEE Trans. Inform. Theory*, vol. 24, pp. 628-630, Sept. 1978.

[9] B. Vasic, "Structured iteratively decodable codes based on Steiner systems and their application in magnetic recoding," *Proc. IEEE GLOBECOM Conf.*, pp. 2954-2960, Nov. 2001.

[10] S. J. Johnson and S. R. Weller, "A family of irregular LDPC codes with low encoding complexity," *IEEE Commun. Lett.*, vol. 7, pp. 79-81, Feb. 2003.

[11] M. Sipser and D. Spielman, "Expander codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1710-1722, Nov. 1996.