Bounds on the Expansion Properties of Tanner Graphs

Mingrui Zhu and Keith M. Chugg, *Member, IEEE*

***Abstract*—This work focuses on the expansion properties of a Tanner Graph because they are known to be related to the performance of associated iterative message-passing algorithms over various channels. By analyzing the eigenvalues and corresponding eigenvectors of the normalized incidence matrix representing a Tanner Graph, lower bounds on these expansion properties are derived. Specifically, for the binary erasure channel, these results lead to two lower bounds on stopping distance for any given binary linear code and an upper bound on stopping redundancy for the family of difference-set codes (type-I 2-D projective geometry low-density parity-check (LDPC) codes).**

***Index Terms*—Expansion of graphs, low-density parity-check (LDPC) codes, spectral graph theory, stopping distance and stopping redundancy, Tanner graphs.**

I. Introduction

There are two well known facts that motivate this work. First, eigenanalysis has been successfully used in spectral graph theory (SGT) [1] to reveal several fundamental properties of graphs, such as the spectrum of the graph, connectivity and routing, diameter and girth, etc. This correspondence uses techniques from SGT to bound parameters associated with vertex expansions of graphical models of binary linear codes. Second, to understand the behavior of iterative message-passing algorithms on loopy Tanner Graphs [2], several researchers have suggested that iterative decoding would perform well if the underlying Tanner Graphs had good expansion properties [3], [4]. Below we summarize expansion and related graph properties and introduce precise definitions as needed in this correspondence.

For Tanner Graphs, vertex expansion is a measure of the ratio between the number of vertices connected to a set of vertices and the number of edges incident on the same set of vertices. By carefully designing their iterative decoding algorithms, Sipser and Spielman [3] argued that, for the binary symmetric channel (BSC), their algorithms can correct a number of random errors if the minimum variable expansion of the underlying Tanner Graph is good enough. This argument was generalized by Burshtein and Miller [4] to analyze Gallager's hard-decision decoding and soft-decision decoding (with clipping) algorithms. Also in [3], the authors introduced a new family of asymptotically good, linear error-correcting codes, which are known as *expander codes*. It has been proved by Barg and Zémor [5] that expander codes attain the capacity under iterative decoding for BSC.

Manuscript received May 24, 2006; revised July 12, 2007. This work was supported in part by the Army Research Office DAAD19-01-1-0477. The material in this correspondence was presented in part at the 43rd Allerton Conference on Communication, Control, and Computing, Urbana-Champaign, IL, September 2005.

M. Zhu was with the Ming Hsieh Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089 USA. He is now with Amicus Wireless Technology, Sunnyvale, CA 94085 USA. (e-mail: mingrui.zhu@amicuswireless.com).

K. M. Chugg is with the Ming Hsieh Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089 USA. (e-mail: chugg@usc.edu).

Communicated by T. Richardson, Associate Editor for Coding Theory.

Color versions of Figures 1 and 2 in this correspondence are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2007.909127

Following this, several related graph properties have been defined and used in a number of cases to make this assertion more quantitative.

Specifically, *stopping set* was introduced in [6] to determine the performance of iterative decoding on the binary erasure channel (BEC). The size of the smallest stopping sets was defined as the *stopping distance* [7]. Focusing on Tanner Graph ensembles, Orlitsky, Viswanathan, and Zhang [8] demonstrated a linear relation between the degree distribution and the likely size of the smallest stopping sets. Bounds on the average block error probability were also derived in [8] by analyzing the asymptotic behavior of both the stopping distance and the distribution of stopping sets.

Giving the relationship between good expansion properties and performance, researchers have begun searching for other graphs that have better expansion properties than the standard Tanner Graphs. A primary example is a redundant parity-check matrix, where additional rows are added to the standard *parity-check matrix*. Previously, Schwartz and Vardy [7] introduced the concept of *stopping redundancy*, which is defined as the minimum number of rows in a redundant parity-check matrix of a linear code $\mathcal{C}$ such that the stopping distance equals its minimum distance. Furthermore, they provided bounds on stopping redundancy for the family of binary Reed–Muller codes, extended Golay Codes and maximum distance separable (MDS) codes. More recently, improved upper bounds on the stopping redundancy of MDS codes were provided by Han and Siegel [9].

In the literature, the concept of *pseudo-codeword* has also been used in [10]–[12] to analyze the convergence of iterative decoding. It is more general than stopping sets because pseudo-codewords for the iterative decoder are exactly stopping sets on the BEC whereas pseudo-codewords are not stopping sets on the additive white Gaussian noise (AWGN) channel. One therefore needs to consider *pseudo-weight* of pseudocodewords rather than the size of stopping sets to evaluate the performance of iterative decoding on the AWGN channel. Bounds on pseudo-weight for linear codes have been derived in [13], [14] by analyzing the structure of the decoder's *computation tree*. In this work, however, we will use a different approach to bound the expansion properties of general Tanner Graphs, which is directly related to stopping sets and stopping distance.

The main contribution of this work is twofold. In contrast to previous work, where minimum variable expansion on ensembles of Tanner Graphs was analyzed, we derive lower bounds on the expansion of both variable subsets and parity-check subsets for a specific Tanner Graph by generalizing the results in the literature of SGT, where lower bound on the minimum variable expansion for a given Tanner Graph is a simple extension. Furthermore, two lower bounds on stopping distance are derived, which generalize Tanner's bit-oriented and parity-oriented lower bounds on minimum distance to account for irregular Tanner Graphs. Our development also illustrates that Tanner's bounds are actually lower bounds on stopping distance. These lower bounds on stopping distance can then be used to derive an upper bound on the stopping redundancy of the family of difference-set codes, which provides an alternate proof of Vontobel's results [15] on projective geometry low-density parity-check (LDPC) codes, because the difference-set codes are also known as type-I two-dimensional projective geometry LDPC (2-D PG-LDPC) codes [16].

On the other hand, it is known that the performance of iterative decoding on loopy Tanner Graphs is not only related to the minimum variable expansion, but also a function of the distribution of the variable expansions [8], [15]. However, obtaining the exact distribution is difficult and often impractical [17]. Therefore, the concept of average variable expansion is introduced in this work as an indicator of the distribution of the variable expansions. Using techniques from spectral

graph theory, a lower bound on the average expansion properties for a specific code is derived.

The structure of the rest of the correspondence is as follows. After introducing the elements of graphical representation of linear codes and the associated matrices, we will prove a lemma by analyzing eigenvalues of the normalized incidence matrix. Next, expansion properties are defined and the previous lemma will be used to provide lower bounds on these expansion properties. We continue in Section IV to show two lower bounds on the stopping distance for binary linear codes and an upper bound on the stopping redundancy of difference-set codes. Conclusions are summarized in Section V.

II. Graph Representations and Eigenvalue Analysis

Considering an $[n, k, d_{\min}]$ binary linear code $\mathcal{C}$ specified by a $p \times n$ *incidence matrix* $\mathbf{H}_p$ with columns representing *bit variables*, rows representing *parity-checks* and $p \geq n - k = p_0$, the corresponding Tanner Graph [2] G_T is

$$G_T = (X_n \cup Y_p, E) = (\{x_0, .., x_{n-1}\} \cup \{y_0, .., y_{p-1}\}, E) \quad (1)$$

where X_n is the set of variables, Y_p is the set of single parity-check constraints and $E = \{(x, y) : x \in X_n,\ y \in Y_p\}$ is the set of edges. It can be shown that $\mathbf{H}_p = [h_{ij}]_{p\times n}$ is a *parity-check matrix* for the code $\mathcal{C}$. When $p = p_0$, $\mathbf{H}_p$ is a standard parity-check matrix for the code. For $p \geq p_0$, there are redundant parity-checks and we refer to $\mathbf{H}_p$ as a redundant parity-check matrix. In either case, $\mathbf{H}_p$ can be interpreted as both a parity-check matrix and the incidence matrix for the corresponding bipartite graph.

Let d_v denote the degree of vertex $v \in X_n \cup Y_p$, and let S denote a subset of vertices, i.e., $S \subseteq X_n \cup Y_p$, define

$$r_i = \text{weight of row } i \text{ of } \mathbf{H}_p = d_{y_i} \quad (2)$$

$$c_j = \text{weight of column } j \text{ of } \mathbf{H}_p = d_{x_j} \quad (3)$$

$$N(v) = \text{the set of neighbors of } v \quad (4)$$

$$N(S) = \text{the set of neighbors of } S \quad (5)$$

$$\text{vol}(S) = \text{the volume of } S = \sum_{v\in S} d_v \quad (6)$$

$$|E| = \text{the number of edges} = \text{vol}\,(X_n) = \text{vol}(Y_p) \quad (7)$$

where $0 \leq i \leq p-1$ and $0 \leq j \leq n-1$, and the $p \times n$ normalized incidence matrix is defined as

$$\mathbf{A}_p = [a_{ij}]_{p\times n} = \left[\frac{h_{ij}}{\sqrt{r_i \cdot c_j}}\right]_{p\times n}. \quad (8)$$

It is known that $\mathbf{A}_p^T\mathbf{A}_p$ and $\mathbf{A}_p\mathbf{A}_p^T$ share the same set of nonzero eigenvalues, among which the unique largest single eigenvalue is 1 [1]. Ordering the eigenvalues of $\mathbf{A}_p^T\mathbf{A}_p$ as $1 = \mu_0 > \mu_1 \geq \mu_2 \cdots \geq \mu_{p-1} \geq \mu_p = \cdots = \mu_{n-1} = 0$ if $p < n$ or $1 = \mu_0 > \mu_1 \geq \mu_2 \ldots \geq \mu_{n-1}$ otherwise, with corresponding orthonormal eigenvectors $\mathbf{e}_0, \mathbf{e}_1, \ldots \mathbf{e}_{n-1}$, it can also be shown that

$$\mathbf{e}_0 = \frac{\mathbf{T}_d^{1/2}\mathbf{1}_n}{\sqrt{\text{vol}(X_n)}} = \frac{\mathbf{T}_d^{1/2}\mathbf{1}_n}{\sqrt{|E|}} \quad (9)$$

where $\mathbf{T}_d = [t_{ij}]$ is a $n \times n$ diagonal matrix with $t_{jj} = c_j$, $0 \leq j \leq n-1$ and all entries of length-n column vector $\mathbf{1}_n$ are 1's. Similarly, let $\mathbf{e}'_0, \mathbf{e}'_1, \ldots \mathbf{e}'_{p-1}$ be the orthonormal eigenvectors of $\mathbf{A}_p\mathbf{A}_p^T$ corresponding to eigenvalues $1 = \mu_0 > \mu_1 \geq \mu_2 \ldots \geq \mu_{p-1}$, then

$$\mathbf{e}'_0 = \frac{(\mathbf{T}'_d)^{1/2}\mathbf{1}_p}{\sqrt{\text{vol}(Y_p)}} = \frac{(\mathbf{T}'_d)^{1/2}\mathbf{1}_p}{\sqrt{|E|}} \quad (10)$$

where $\mathbf{T}'_d = [t'_{ij}]$ is a $p \times p$ diagonal matrix with $t'_{ii} = r_i$, $0 \leq i \leq p-1$. Now we are ready to present our first lemma. However, it should be noted that this normalization technique has a long history and many applications in spectral graph theory. For more information about spectral graph theory, we direct the interested reader to [1].

Lemma 1: For any bipartite graph $G_T = (X_n \cup Y_p, E)$ and a subset S of X_n (or Y_p)

$$\frac{\text{vol}(N(S))}{\text{vol}(S)} \geq \frac{1}{\mu_1 + (1-\mu_1)\frac{\text{vol}(S)}{|E|}} \quad (11)$$

where μ_1 is the second largest eigenvalue of both $\mathbf{A}_p^T\mathbf{A}_p$ and $\mathbf{A}_p\mathbf{A}_p^T$.[1]

Proof: Considering $S \subseteq X_n$, define column vector $\boldsymbol{\psi}_S = (\psi_0, \psi_1, \ldots \psi_{n-1})^T$, where $\psi_j = 1$ if $x_j \in S$, and $\psi_j = 0$ otherwise. Expressing $\mathbf{T}_d^{1/2}\boldsymbol{\psi}_S$ as a linear combination of the orthonormal eigenvectors of $\mathbf{A}_p^T\mathbf{A}_p$

$$\mathbf{T}_d^{1/2}\boldsymbol{\psi}_S = \sum_{j=0}^{n-1}\langle \mathbf{T}_d^{1/2}\boldsymbol{\psi}_S, \mathbf{e}_j\rangle \mathbf{e}_j = \sum_{j=0}^{n-1} a_j \mathbf{e}_j \quad (12)$$

where

$$a_0 = \langle \mathbf{T}_d^{1/2}\boldsymbol{\psi}_S, \mathbf{e}_0\rangle = \frac{\text{vol}(S)}{\sqrt{|E|}} \quad (13)$$

$$\sum_{j=0}^{n-1} a_j^2 = \langle \mathbf{T}_d^{1/2}\boldsymbol{\psi}_S, \mathbf{T}_d^{1/2}\boldsymbol{\psi}_S\rangle = \text{vol}(S) \quad (14)$$

and $\langle\cdot,\cdot\rangle$ denotes the inner product of two column vectors, then

$$\langle \mathbf{A}_p\mathbf{T}_d^{1/2}\boldsymbol{\psi}_S, \mathbf{A}_p\mathbf{T}_d^{1/2}\boldsymbol{\psi}_S\rangle = \boldsymbol{\psi}_S^T\mathbf{T}_d^{1/2}\mathbf{A}_p^T\mathbf{A}_p\mathbf{T}_d^{1/2}\boldsymbol{\psi}_S \quad (15a)$$

$$= \sum_{j=0}^{n-1} a_j^2\mu_j \quad (15b)$$

$$\leq a_0^2 + (\sum_{j=1}^{n-1} a_j^2)\mu_1 \quad (15c)$$

$$= (1-\mu_1)\frac{|\text{vol}(S)|^2}{|E|} + \mu_1\text{vol}(S). \quad (15d)$$

Furthermore

$$\langle \mathbf{A}_p\mathbf{T}_d^{1/2}\boldsymbol{\psi}_S, \mathbf{A}_p\mathbf{T}_d^{1/2}\boldsymbol{\psi}_S\rangle = \sum_{u\in S}\sum_{v\in S}\sum_{\substack{y:(v,y)\in E \\ \text{and } (u,y)\in E}} \frac{1}{d_y} \quad (16a)$$

$$= \sum_{y\in N(S)}\left|\frac{N(y)\cap S}{\sqrt{d_y}}\right|^2 \quad (16b)$$

$$\geq \frac{\left(\sum_{y\in N(S)}\frac{|N(y)\cap S|}{\sqrt{d_y}}\sqrt{d_y}\right)^2}{\sum_{y\in N(S)} d_y} \quad (16c)$$

$$= \frac{|\text{vol}(S)|^2}{\text{vol}(N(S))} \quad (16d)$$

where (16a) and (16b) are generalized from [1, p. 97] and (16c) results from the Cauchy–Schwartz inequality. Combining (15d) and (16d) yields,

$$(1-\mu_1)\frac{|\text{vol}(S)|^2}{|E|} + \mu_1\text{vol}(S) \geq \frac{|\text{vol}(S)|^2}{\text{vol}(N(S))} \quad (17)$$

[1]Similar results can be found in [1] for the graphs of regular row/column weights. However, extensions to the irregular case discussed in [1] are not fully developed and draw invalid conclusions. The proof of Lemma 1 is based on similar techniques and can be considered as an extension of Chung's work.

and (11) is the direct result. Similarly, we can prove this lemma for $S \subseteq Y_p$ by using $\mathbf{e}_i'$'s and $\mathbf{T}_d'$ as defined in (10), and $\boldsymbol{\psi}_S' = (\psi_0', \psi_1', \ldots \psi_{p-1}')^T$, where $\psi_i' = 1$, if $y_i \in S$ and $\psi_i' = 0$ otherwise. □

III. Expansion Properties of Tanner Graphs

For a given Tanner Graph $G_T = (X_n \bigcup Y_p, E)$, considering a subset $S_m \subseteq X_n$ (or Y_p) of size m, its expansion is defined as the number of its neighbors divided by its volume,[2] i.e.,

$$\delta(S_m) = \frac{|N(S_m)|}{\mathrm{vol}(S_m)}. \tag{18}$$

Thus, the minimum and average variable expansion can be defined as

$$\delta_{\min}(m) = \min_{S_m} \delta(S_m) \tag{19}$$

$$\delta_{\mathrm{avg}}(m) = \frac{1}{\binom{n}{m}} \sum_{S_m} \delta(S_m) \tag{20}$$

where $S_m \subseteq X_n, |S_m| = m$ and $\binom{n}{m}$ is the binomial coefficient.

A. Relations to Previous Results

In [6]–[8], stopping sets were used to determine the performance of iterative decoding on erasure channels. For $S_m \subseteq X_n$, we say that S_m is a stopping set if all vertices in the neighborhood of S_m, i.e., vertices in $N(S_m)$, are connected to at least two different vertices in S_m. Thus, if S_m is a stopping set, $\delta(S_m) \leq \frac{1}{2}$. However, the converse is not necessarily true. Also, it can be shown that stopping distance [7] is lower bounded by the largest m such that $\delta_{\min}(m-1) > \frac{1}{2}$.

In [3], the authors discussed iterative decoding of (d_v, d_c)-regular LDPC codes on the BSC, and demonstrated that Spielman's simple sequential decoding algorithm can correct any $\alpha n/2$ or fewer random errors if every variable subset of the size αn or less expands by a factor of at least $3d_v/4$, where n is the number of variable vertices. Translating into our notation, it is equivalent to say that Spielman's simple sequential decoding can correct any pattern of $m/2$ or fewer errors if $\delta_{\min}(i) \geq 3/4$ for $1 \leq i \leq m$. Similar results were obtained in [18], where irregular LDPC codes were discussed. Thus, our goal in this correspondence is to establish lower bounds on expansion properties for a given Tanner Graph with these results in mind.

B. A Lower Bounds on $\delta(s_m)$

Theorem 2: For any subset S_m of X_n

$$\delta(S_m) \geq \frac{1}{r_{\max}} \cdot \frac{|E|}{\mu_1|E| + (1-\mu_1)\mathrm{vol}(S_m)} \tag{21}$$

and for any subset S_m of Y_p

$$\delta(S_m) \geq \frac{1}{c_{\max}} \cdot \frac{|E|}{\mu_1|E| + (1-\mu_1)\mathrm{vol}(S_m)} \tag{22}$$

where μ_1 is the second largest eigenvalue of both $\mathbf{A}_p^T\mathbf{A}_p$ and $\mathbf{A}_p\mathbf{A}_p^T$, $r_{\max} = \max_i r_i$ and $c_{\max} = \max_j c_j$.

[2]Strictly speaking, (18) only defines the "vertex" expansion, and the concept of "edge" expansion also exists in the literature of SGT. However, as only vertex expansion is considered throughout this work, we use the term expansion to refer to vertex expansion. Furthermore, it should be noted that, though the definition of vertex expansion is not restricted to variables, typically only subsets of variables, i.e., $S_m \subseteq X_n$, are considered to analyze the performance of iterative decoding.

Proof: Using the fact that, for $S_m \subseteq X_n$, $|N(S_m)| \geq \mathrm{vol}(N(S_m))/r_{\max}$, (21) follows directly from Lemma 1 and (18). Similarly, (22) can be proved. □

C. Lower Bounds on Minimum and Average Variable Expansion

A lower bound on minimum variable expansion follows from Theorem 2.

Theorem 3: For subsets of X_n with size m

$$\delta_{\min}(m) \geq \frac{1}{r_{\max}} \cdot \frac{|E|}{\mu_1|E| + (1-\mu_1)\cdot m \cdot c_{\max}} \tag{23}$$

where μ_1 is the second largest eigenvalue of both $\mathbf{A}_p^T\mathbf{A}_p$ and $\mathbf{A}_p\mathbf{A}_p^T$, $r_{\max} = \max_i r_i$ and $c_{\max} = \max_j c_j$.

Proof: Using the fact that, for $S_m \subseteq X_n, \mathrm{vol}(S_m) \leq m \cdot c_{\max}$, (23) follows from the definition of $\delta_{\min}(m)$ and (21). □

The derivation of lower bound on average variable expansion is more complicated, which is summarized in the following theorem.

Theorem 4: For a Tanner Graph $G_T = (X_n \bigcup Y_p, E)$ with largest variable degree of L and $|X_n| = n$, let n_l be the number of variable nodes of degree l and $d_l, 1 \leq l \leq L$, be integers such that $0 \leq d_l \leq n_l$, then

$$\delta_{\mathrm{avg}}(m) \geq \frac{\left(\underbrace{\sum^{n_1}\cdots\sum^{n_L}}_{d_1+\ldots+d_L=m} \binom{n_1}{d_1}\cdots\binom{n_L}{d_L}\sqrt{\sum_l l d_l}\right)^2}{r_{\max}\binom{n}{m}\sum_{j=0}^{n-1}\mu_j\widetilde{a}_j^2} \tag{24}$$

where μ_j's and $\mathbf{e}_j$'s are eigenvalues and corresponding eigenvectors of $\mathbf{A}_p^T\mathbf{A}_p$ and

$$\widetilde{a}_0^2 = \left(\binom{n-1}{m-1} - \binom{n-2}{m-2}\right)\mathbf{e}_0^T\mathbf{T}_d\mathbf{e}_0 + \binom{n-2}{m-2}|E| \tag{25a}$$

$$\widetilde{a}_j^2 = \left(\binom{n-1}{m-1} - \binom{n-2}{m-2}\right)\mathbf{e}_j^T\mathbf{T}_d\mathbf{e}_j \quad 1 \leq j \leq n-1. \tag{25b}$$

Proof: Considering $S_m \subseteq X_n$ and $|S_m| = m$, define column vector $\boldsymbol{\psi}_{S_m} = (\psi_0, \psi_1, \ldots \psi_{n-1})^T$, where $\psi_j = 1$ if $x_j \in S_m$, and $\psi_j = 0$ otherwise. Let

$$a_j(S_m) = \langle \mathbf{T}_d^{1/2}\boldsymbol{\psi}_{S_m}, \mathbf{e}_j\rangle = \mathbf{e}_j^T\mathbf{T}_d^{1/2}\boldsymbol{\psi}_{S_m} \tag{26}$$

combining (15b) and (16d) yields

$$\sum_{j=0}^{n-1}(a_j(S_m))^2\mu_j \geq \frac{|\mathrm{vol}(S_m)|^2}{\mathrm{vol}(N(S_m))}. \tag{27}$$

Summing the left side of the (27) over all $S_m \subseteq X_n$ such that $|S_m| = m$

$$\sum_{S_m}\sum_{j=0}^{n-1}(a_j(S_m))^2\mu_j = \sum_{j=0}^{n-1}\mu_j\sum_{S_m}(a_j(S_m))^2 \tag{28a}$$

$$= \sum_{j=0}^{n-1}\mu_j\sum_{S_m}|\langle\mathbf{T}_d^{1/2}\boldsymbol{\psi}_{S_m}, \mathbf{e}_j\rangle|^2 \tag{28b}$$

$$= \sum_{j=0}^{n-1} \mu_j \sum_{S_m} \mathbf{e}_j^T \mathbf{T}_d^{1/2} \boldsymbol{\psi}_{S_m} \boldsymbol{\psi}_{S_m}^T \mathbf{T}_d^{1/2} \mathbf{e}_j \tag{28c}$$

$$= \sum_{j=0}^{n-1} \mu_j \widetilde{a}_j^2 \tag{28d}$$

where

$$\widetilde{a}_j^2 = \sum_{S_m} \mathbf{e}_j^T \mathbf{T}_d^{1/2} \boldsymbol{\psi}_{S_m} \boldsymbol{\psi}_{S_m}^T \mathbf{T}_d^{1/2} \mathbf{e}_j$$
$$= \mathbf{e}_j^T \mathbf{T}_d^{1/2} \left(\sum_{S_m} \boldsymbol{\psi}_{S_m} \boldsymbol{\psi}_{S_m}^T \right) \mathbf{T}_d^{1/2} \mathbf{e}_j. \tag{29}$$

Using the definition of $\boldsymbol{\psi}_{S_m}$, we show that

$$\boldsymbol{\psi}_{S_m} \boldsymbol{\psi}_{S_m}^T = \begin{bmatrix} \psi_0\psi_0 & \psi_0\psi_1 & \cdot & \psi_0\psi_{n-1} \\ \psi_1\psi_0 & \psi_1\psi_1 & \cdot & \psi_1\psi_{n-1} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \psi_{n-1}\psi_{n-1} & \psi_{n-1}\psi_1 & \cdot & \psi_{n-1}\psi_{n-1} \end{bmatrix}$$

is a $n \times n$ binary symmetric matrix, where the entry at the intersection of the ith row and the jth column is 1 if and only if both x_i and x_j are in S_m. Furthermore, among all $\binom{n}{m}$ matrices of the form $\boldsymbol{\psi}_{S_m} \boldsymbol{\psi}_{S_m}^T$, $\binom{n-1}{m-1}$ have entry 1 at the intersection of the ith row and the ith column, $0 \le i \le n-1$, and $\binom{n-2}{m-2}$ have entry 1 at the intersection of the ith row and the jth column, $0 \le i \ne j \le n-1$, therefore

$$\sum_{S_m} \boldsymbol{\psi}_{S_m} \boldsymbol{\psi}_{S_m}^T = \begin{bmatrix} \binom{n-1}{m-1} & \binom{n-2}{m-2} & \cdot & \binom{n-2}{m-2} \\ \binom{n-2}{m-2} & \binom{n-1}{m-1} & \cdot & \binom{n-2}{m-2} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \binom{n-2}{m-2} & \binom{n-2}{m-2} & \cdot & \binom{n-1}{m-1} \end{bmatrix}$$
$$= \left(\binom{n-1}{m-1} - \binom{n-2}{m-2} \right) \mathbf{I}_n + \binom{n-2}{m-2} \mathbf{1}_n \mathbf{1}_n^T \tag{30}$$

where $\mathbf{I}_n$ is the $n \times n$ identity matrix and $\mathbf{1}_n$ is the $n \times 1$ all one column vector. Noting that $\mathbf{e}_0 = \frac{\mathbf{T}_d^{1/2} \mathbf{1}_n}{\sqrt{|E|}}$ and $\mathbf{e}_j$, $1 \le j \le n-1$, are the orthonormal eigenvectors of $\mathbf{A}_p^T \mathbf{A}_p$, (25a) and (25b) can be proved by combining (29) and (30).

Using the Cauchy–Schwartz inequality, it can also be shown that

$$\sum_{S_m} \frac{|\mathrm{vol}(S_m)|^2}{\mathrm{vol}(N(S_m))} \ge \frac{\left(\sum_{S_m} \sqrt{\mathrm{vol}(S_m)}\right)^2}{r_{\max} \binom{n}{m} \delta_{\mathrm{avg}}(m)}. \tag{31}$$

Combining (27), (28) and (31), we have

$$\delta_{\mathrm{avg}}(m) \ge \frac{\left(\sum_{S_m} \sqrt{\mathrm{vol}(S_m)}\right)^2}{r_{\max} \binom{n}{m} \sum_{j=0}^{n-1} \mu_j \widetilde{a}_j^2}. \tag{32}$$

As the final step, noting that for subsets of X_n with $m = d_1 + .. + d_L$ variable nodes, where d_l, $1 \le l \le L$, are integers such that $0 \le d_l \le n_l$, and n_l is the number of variable nodes of degree l, $\mathrm{vol}(S_m) = \sum_l l d_l$ and there are $\binom{n_1}{d_1} .. \binom{n_L}{d_L}$ $S_m \subseteq X_n$ satisfying these conditions, therefore

$$\sum_{S_m} \sqrt{\mathrm{vol}(S_m)} = \underbrace{\sum^{n_1} .. \sum^{n_L}}_{d_1 + .. + d_L = m} \binom{n_1}{d_1} .. \binom{n_L}{d_L} \sqrt{\sum_l l d_l} \tag{33}$$

and (24) follows. □

IV. Bounds on Stopping Distance and Stopping Redundancy

In this section, we will use results in the previous section to derive bounds on the stopping distance and the stopping redundancy for binary linear codes.

A. Lower Bounds on Stopping Distance

Considering $S \subseteq X_n$, define bit variables in S as *active bits* and parity-checks in the neighborhood of S as *active parity-checks* [19], respectively, then we say that S is a stopping set if all the neighbors of S, *i.e.,* all active parity-checks, are connected to S at least twice. The size of the smallest stopping set is defined as stopping distance.

Using Theorem 2, two lower bounds on stopping distance, denoted as $s(\mathbf{H}_p)$, of binary linear codes are derived. Since $s(\mathbf{H}_p) \le d_{\min}$, these lower bounds are also lower bounds on $d_{\min}$. In particular, they lead to Tanner's results [19] when the underlying Tanner Graph is regular. Thus, using Tanner's terminology, we call (34) and (35) bit-oriented bound and parity-oriented bound, respectively.

Theorem 5: For the $[n, k, d_{\min}]$ binary linear code $\mathcal{C}$ defined by the Tanner Graph $G_T = (X_n \cup Y_p, E)$ with $p \times n$ incidence matrix $\mathbf{H}_p$

$$d_{\min} \ge s(\mathbf{H}_p) \ge \frac{\frac{2}{r_{\max}} - \mu_1}{1 - \mu_1} \cdot \frac{|E|}{c_{\max}} \tag{34}$$

$$d_{\min} \ge s(\mathbf{H}_p) \ge \frac{1 + \frac{2c_{\min} - 2}{r_{\max}} - \mu_1 c_{\max}}{(1 - \mu_1) c_{\max}} \cdot \frac{2|E|}{c_{\max} r_{\max}} \tag{35}$$

where μ_1 is the second largest eigenvalue of $\mathbf{A}_p^T \mathbf{A}_p$, $r_{\max} = \max_i r_i$, $c_{\max} = \max_j c_j$ and $c_{\min} = \min_j c_j$.

Proof: Since stopping distance is always no larger than minimum distance [7], we only need to prove the second inequalities in (34) and (35).

Let $S_x \subseteq X_n$ be a smallest stopping set, it has been demonstrated, in Section III-A, that $\delta(S_x) \le \frac{1}{2}$. Then, (21) leads to

$$\frac{r_{\max}}{2} \ge \frac{|E|}{\mu_1 |E| + (1 - \mu_1) \mathrm{vol}(S_x)} \tag{36}$$

where μ_1 is the second largest eigenvalue of $\mathbf{A}_p^T \mathbf{A}_p$. Therefore

$$s(\mathbf{H}_p) = |S_x| \ge \frac{\mathrm{vol}(S_x)}{c_{\max}} \ge \frac{2/r_{\max} - \mu_1}{1 - \mu_1} \cdot \frac{|E|}{c_{\max}}. \tag{37}$$

To prove (35), let $S_y \subseteq Y_p$ be the set of active parity-checks of a smallest stopping set, and (22) leads to

$$\frac{|N(S_y)| c_{\max}}{\mathrm{vol}(S_y)} \ge \frac{|E|}{\mu_1 |E| + (1 - \mu_1) \mathrm{vol}(S_y)}. \tag{38}$$

Considering $N(S_y)$, it contains all active bits of the stopping set and some other bits that are not in the stopping set. For those active bits, all their neighbors are included in the set of S_y, and for the rest bits, some of their neighbors are in S_y but others are not. Therefore, let $c_{\mathrm{avg}}(N(S_y))$ be the average number of edges incident on $N(S_y)$ that are counted in $\mathrm{vol}(S_y)$, i.e., $|N(S_y)| c_{\mathrm{avg}}(N(S_y)) = \mathrm{vol}(S_y)$, then

$$\frac{c_{\max}}{c_{\mathrm{avg}}(N(S_y))} \ge \frac{|E|}{\mu_1 |E| + (1 - \mu_1) \mathrm{vol}(S_y)}. \tag{39}$$

Also, among the r_i neighbors of any node $y_i \in S_y$, at least 2 of them are active bits and the remaining $r_i - 2$ bits have at least one edge connected to S_y. In other words, assuming the r_i neighbors of y_i are

$x_1, x_2, .., x_{r_i}$, among which x_1 and x_2 are active bits and $x_3, ...x_{r_i}$ each has at least one edge connected to S_y, at least

$$(c_1 + c_2 + r_i - 2)/r_i = 1 + (c_1 + c_2 - 2)/r_i \geq 1 + (2c_{\min} - 2)/r_{\max}$$

edges connected to a neighbor of y_i are counted in $\mathrm{vol}(S_y)$ on average. Thus

$$c_{\mathrm{avg}}(N(S_y)) \geq 1 + (2c_{\min} - 2)/r_{\max}. \tag{40}$$

Combining (39) and (40), and noting that $s(\mathbf{H}_p)c_{\max} \geq 2|S_y| \geq \frac{2\mathrm{vol}(S_y)}{r_{\max}}$, (35) follows. □

Lower bounds on minimum distance and stopping distance when the underlying graph is regular can be considered as a special case of Theorem 5, which is summarized in the following corollary.

Corollary 6: The $d_{\min}$ and $s(\mathbf{H}_p)$ of regular LDPC codes defined by $p \times n$ parity-check matrix $\mathbf{H}_p$ satisfy

$$d_{\min} \geq s(\mathbf{H}_p) \geq \frac{n(2c - \eta_1)}{cr - \eta_1} \tag{41}$$

$$d_{\min} \geq s(\mathbf{H}_p) \geq \frac{2n(2c + r - 2 - \eta_1)}{r(cr - \eta_1)} \tag{42}$$

where $\eta_1 = \mu_1 cr$ is the second largest eigenvalue of $\mathbf{H}_p^T\mathbf{H}_p$.

Proof: If $\mathbf{H}_p$ is regular, i.e., $c_0 = \cdots = c_{n-1} = c$ and $r_0 = \cdots = r_{p-1} = r$, the $n \times n$ square matrix $\mathbf{H}_p^T\mathbf{H}_p$ has cr as its unique largest single eigenvalue and $\eta_1 = \mu_1 cr$ as its second largest eigenvalue, where μ_1 is the second largest eigenvalue of $\mathbf{A}_p^T\mathbf{A}_p$ and $\mathbf{A}_p$ is the normalized incidence matrix defined in (8). The proof is then straightforward by plugging $c_{\max} = c_{\min} = c$, $r_{\max} = r$, $|E| = nc$ and $\eta_1 = \mu_1 cr$ into (34) and (35) respectively. □

It can be seen that the part of (41) and (42) corresponding to $d_{\min}$ coincide with Tanner's bit-oriented bound and parity-oriented bound for regular LDPC codes [19, Ths. 3.1 and 4.1], respectively. We have noted that, lower bounds on both minimum BEC pseudo-weight and AWGN pseudo-weight of regular LDPC were derived in [12], which will also lead to Tanner's bounds. Also, lower bounds on $d_{\min}$ for block-wise irregular LDPC codes were derived in [20], where some degree of regularity is still necessary. Our main contributions are the derivation of low bounds for general LDPC codes and demonstrating that Tanner's bounds are actually lower bounds on stopping distance, and an immediate result of this is the explanation why Tanner's bounds on $d_{\min}$ are not tight.

B. An Upper Bound on the Stopping Redundancy of the Difference-Set Codes

Stopping redundancy, denoted as $\rho(\mathcal{C})$, was introduced in [7]. In this section, we will provide an upper bound on the stopping redundancy of the family of difference-set codes, which are also known as type-I 2-D PG-LDPC codes [16]. Specifically, assuming $\mathcal{C}$ is a difference-set code of length n, $\rho(\mathcal{C}) \leq n$.

Though there are relatively few codes in the family of difference-set codes, they are nearly as powerful as the best known cyclic codes in the range of practical interest [21]. Furthermore, several recent experiments [16], [22] suggested that this family of codes can perform very well under iterative decoding. It should also be noted that, in [15], pseudo-weight enumerators of pseudo-codewords of both type-I 2-D PG-LDPC and type-I 2-D Euclidean geometry LDPC (EG-LDPC) were discussed, and stopping redundancy of these two families of codes can be derived from their pseudo-weight enumerator as well.

To analyze the algebraic properties of cyclic codes, the components of a row vector[3] $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ are usually treated as coefficients of a polynomial, i.e., $\mathbf{v}(X) = v_0 + v_1X + v_2X^2 + \cdots + v_{n-1}X^{n-1}$. Since the mapping between $\mathbf{v}$ and $\mathbf{v}(X)$ is one-to-one, we use the terms "row vector" and "polynomial" interchangeably hereafter. Furthermore, for a given $\mathbf{v}(X)$ and its row vector $\mathbf{v} = \mathbf{v}_0$, we can work over rings of polynomials mod $(X^n + 1)$ and define a $p \times n$, $1 \leq p \leq n$, matrix as follows:

$$\mathbf{H}_p(\mathbf{v}) = \begin{bmatrix} \mathbf{v}^*(X) \bmod (X^n + 1) \\ X\,\mathbf{v}^*(X) \bmod (X^n + 1) \\ \cdot \\ \cdot \\ X^{p-1}\mathbf{v}^*(X) \bmod (X^n + 1) \end{bmatrix}_{p\times n} = \begin{bmatrix} \mathbf{v}_0^* \\ \mathbf{v}_1^* \\ \cdot \\ \cdot \\ \mathbf{v}_{p-1}^* \end{bmatrix}_{p\times n} \tag{43}$$

where $\mathbf{v}^*(X) = X^k\mathbf{v}(X^{-1})$ is the reciprocal of $\mathbf{v}(X)$ and $\mathbf{v}_i^*$, $0 \leq i \leq p-1$, are row vectors. This is called a *cyclic matrix* because $\mathbf{v}_i^*$ is the i-th cyclic shift of $\mathbf{v}_0^*$ to the right, $1 \leq i \leq p-1$.

To define a $[n, k, d_{\min}]$ binary cyclic code $\mathcal{C}$, one only needs to specify its *generator polynomial* [21, Ch.5], $\mathbf{g}(X) = 1 + g_1X + \cdots + g_{n-k-1}X^{n-k-1} + X^{n-k}$, which is the unique nonzero code polynomial of degree $n-k$ in $\mathcal{C}$, and all valid code polynomials can be written as $(u_0 + u_1X + \cdots + u_{k-1}X^{k-1})\mathbf{g}(X)$ where $u_0, u_1, \ldots u_{k-1}$ are the k information digits to be encoded. Noting that $\mathbf{g}(X)$ is a factor of $X^n + 1$ [21, Th. 5.5], there existes one degree k polynomial

$$\mathbf{h}(X) = 1 + h_1X + \cdots + h_{k-1}X^{k-1} + X^k \tag{44}$$

such that $X^n + 1 = \mathbf{g}(X)\mathbf{h}(X)$. This $\mathbf{h}(X)$ is defined as *parity polynomial* [21] of $\mathcal{C}$ because the generated cyclic matrix $\mathbf{H}_{p_0}(\mathbf{h})$, as defined in (43) with $p_0 = n - k$, is a parity-check matrix of $\mathcal{C}$, *i.e.,* an length-n row vector $\mathbf{c}$ is a valid codeword of $\mathcal{C}$ if and only if $\mathbf{H}_{p_0}(\mathbf{h})\mathbf{c} = \mathbf{0}$.

On the other hand, the parity-check matrix for a given cyclic code is usually not unique. One interesting result is the following lemma.

Lemma 7: Assuming that $\mathbf{h}(X)$ is the parity polynomial of an $[n, k, d_{\min}]$ binary cyclic code $\mathcal{C}$, if there exists another polynomial $\mathbf{z}(X) = \mathbf{h}(X)\mathbf{f}(X)$ such that

- $\mathbf{f}(X)$ is a nonzero polynomial of degree $f < p_0 = n - k$;
- the greatest common divisor of $\mathbf{f}(X)$ and $X^n + 1$ is 1, i.e., $\mathrm{GCD}(\mathbf{f}(X), X^n + 1) = 1$;

$\mathbf{H}_{p_0}(\mathbf{z})$, as defined in (43) with $p_0 = n-k$, is also a cyclic parity-check matrix for $\mathcal{C}$.

Proof: To show $\mathbf{H}_{p_0}(\mathbf{z})$ is a valid parity-check matrix of $\mathcal{C}$, it suffices to show that its row vectors belong to the row space of $\mathbf{H}_{p_0}(\mathbf{h})$, which follows from the definition of $\mathbf{z}^*(X)$ and the cyclic property of the row space of $\mathbf{H}_{p_0}(\mathbf{h})$, and they are linearly independent.

Assuming that the row vectors of $\mathbf{H}_{p_0}(\mathbf{z})$ are linearly dependent, thus there exist a set of variables $\alpha_i \in \{0, 1\}$, $0 \leq i \leq p_0 - 1$, such that not all of them are zero and

$$\alpha_0\mathbf{z}_0^* \oplus \alpha_1\mathbf{z}_1^* \oplus \cdots \oplus \alpha_{p_0-1}\mathbf{z}_{p_0-1}^* = \mathbf{0} \tag{45}$$

[3]Different from previous sections, where column vectors are used, row vectors are used here.

where $\oplus$ is modulo-2 addition and $\mathbf{0}$ is a zero row vector. Noting that $\mathbf{z}_i^* = X^i\mathbf{z}^*(X) \bmod (X^n+1)$, $0 \le i \le p_0 - 1$ and $\mathrm{GCD}(\mathbf{f}^*(X), X^n+1) = 1$

$$(45) \Leftrightarrow \alpha_0\mathbf{h}_0^* \oplus \alpha_1\mathbf{h}_1^* \oplus \cdots \oplus \alpha_{p_0-1}\mathbf{h}_{p_0-1}^* = \mathbf{0} \qquad (46)$$

contradicts with the fact that row vectors of $\mathbf{H}_{p_0}(\mathbf{h})$ are linearly independent. Thus, row vectors of $\mathbf{H}_{p_0}(\mathbf{z})$ are linearly independent. □

Definition 1: [21, Ch.5] Let $q = 2^\beta$ for positive integer β, $n = q(q+1)+1$, $k = 2^{2\beta} + 2^\beta - 3^\beta$ and $D = \{0, d_1, \ldots, d_q\}$ be a perfect simple difference set of order q, define polynomial $\mathbf{z}(X) = 1 + X^{d_1} + \cdots + X^{d_q}$ and $\mathbf{h}(X) = \mathrm{GCD}(\mathbf{z}(X), X^n+1)$. The cyclic code defined by the parity-check matrix with $\mathbf{H}_{p_0}(\mathbf{h}) = \mathbf{H}_{n-k}(\mathbf{h})$ is an $[n, k, d_{\min} = q+2]$ *difference-set code*. □

Theorem 8: The stopping redundancy of an $[n, k, d_{\min}]$ difference-set code is less than or equal to n.

Proof: From the definition of $\mathbf{z}(X)$ and $\mathbf{h}(X)$, it can be shown that there exists a polynomial $\mathbf{f}(X)$ such that $\mathbf{z}(X) = \mathbf{h}(X)\mathbf{f}(X)$ and $\mathrm{GCD}(\mathbf{f}(X), X^n+1) = 1$. Lemma 7 shows that $\mathbf{H}_{p_0}(\mathbf{z})$ is a parity-check matrix of $\mathcal{C}$. By adding row vectors corresponding to $X^i\mathbf{z}^*(X) \bmod (X^n+1)$, $p_0 \le i \le n-1$, to $\mathbf{H}_{p_0}(\mathbf{z})$, a $n \times n$ redundant parity-check matrix $\mathbf{H}_n(\mathbf{z})$ is formed

$$\mathbf{H}_n(\mathbf{z}) = \begin{bmatrix} \mathbf{z}^*(X) \bmod (X^n+1) \\ \cdot \\ X^{p_0-1}\mathbf{z}^*(X) \bmod (X^n+1) \\ \cdot \\ X^{n-1}\mathbf{z}^*(X) \bmod (X^n+1) \end{bmatrix}_{n\times n}. \qquad (47)$$

Since the rows of $\mathbf{H}_n(\mathbf{z})$ are cyclic shifts of $\mathbf{z}_0^*$, which is a row vector with $q+1$ non-zero elements, every row of $\mathbf{H}_n(\mathbf{z})$ is of weight $q+1$. On the other hand, as $\mathbf{H}_n(\mathbf{z})$ contains $\mathbf{z}_0^*$ and all its $n-1$ cyclic-shift to the right, the pigeonhole principle implies that every column of $\mathbf{H}_n(\mathbf{z})$ must have weight $q+1$ as well.

Let $D = \{0, d_1, \ldots, d_q\}$ be the simple difference set used to define $\mathbf{z}(X)$ and let $\mathbf{z}_i^*$, $0 \le i \le n-1$, be the row vector corresponding the reciprocal of $X^i\mathbf{z}(X) \bmod X^n+1$, the definition of D implies that

$$\mathbf{z}_i^* \cdot (\mathbf{z}_j^*)^T = \begin{cases} q+1, & 0 \le i = j \le n-1, \\ 1, & |i-j| \in D, 0 \le i \ne j \le n-1, \\ 0, & \text{otherwise.} \end{cases} \qquad (48)$$

Furthermore, let $\mathbf{A}_n(\mathbf{z})$ be the corresponding normalized incident matrix as defined in (8), (48) implies that $\mathbf{A}_n(\mathbf{z})^T\mathbf{A}_n(\mathbf{z})$ has diagonal entries of $\frac{1}{q+1}$ and off-diagonal entries of $\frac{1}{(q+1)^2}$. Then, $1 = \widetilde{\mu}_0 > \widetilde{\mu}_1 = \widetilde{\mu}_2 = \cdots = \widetilde{\mu}_{n-1} = \frac{q}{(q+1)^2}$ are eigenvalues of $\mathbf{A}_n(\mathbf{z})^T\mathbf{A}_n(\mathbf{z})$, and the bit-oriented bound, i.e., (41), is $q+2 = d_{\min}$. Therefore, the stopping redundancy of the family of difference-set codes $\rho(\mathcal{C}) \le n =$ the length of the code. □

Furthermore, for redundant parity-check matrix $\mathbf{H}_n(\mathbf{z})$, we can not only show that its stopping distance equals the minimum distance, but also the number of smallest stopping sets equals the number of minimum weight codewords, *i.e.,*

Theorem 9: For the family of $[n, k, d_{\min}]$ difference-set codes, the number of minimum weight codewords equal the number of smallest stopping sets in the Tanner Graph specified by $\mathbf{H}_n(\mathbf{z})$, which is defined in (47).

Proof: As a minimum weight codeword corresponds to a stopping set in Tanner graphical representation, it suffices to show that, by letting variables in a smallest stopping set be 1 and the rest be 0, every smallest stopping set corresponds to a minimum weight codeword. Without loss of generality, assuming that $\{x_1, x_2, \ldots, x_{q+2}\}$ forms a stopping set and $y_1, y_2, \ldots y_{q+1}$ are neighbors of x_1, there exists at least one x_j, $2 \le j \le q+2$, such that $y_i \in N(x_j)$ because $\{x_1, x_2, \ldots, x_{q+2}\}$ is a stopping set. However, as $|N(x_1) \bigcap N(x_2)| = \cdots = |N(x_1) \bigcap N(x_{q+2})| = 1$ and $|N(x_1)| = q+1$, by the pigeonhole principle there is only one such x_j for each y_i so that all neighbors of x_1 are of degree two. Similarly, we can prove this for x_j, $2 \le j \le q+2$. Thus, let $x_j = 1$ for $1 \le j \le q+2$ and $x_j = 0$ otherwise, a minimum weight codeword, which is of weight $q+2$, is formed. □

By Theorem 9, we can argue that, when the erasure probability is small, the performance of the iterative message-passing algorithm can be very close to that of the ML decoding. This can be demonstrated using the $[21, 11, 6]$ difference-set code $\mathcal{C}_{21}$ derived from the difference set $D = \{0, 3, 4, 9, 11\}$, where $\mathbf{h}(X) = \mathbf{z}(X) = 1 + X^3 + X^4 + X^9 + X^{11}$, and there are 168 codewords in $\mathcal{C}_{21}$ with Hamming weight $d_{\min} = 6$. Theorem 8 shows the stopping redundancy of $\mathcal{C}_{21}$ is upper bounded by $n = 21$, and Theorem 9 shows that there are 168 smallest stopping sets in $\mathbf{H}_{21}(\mathbf{z})$ of size 6. Therefore, the performance of iterative decoding over the BEC using the redundant parity-check matrix $\mathbf{H}_{21}(\mathbf{z})$ should be close to that of ML decoding and this is verified by the following simulation results.

Fig. 1 evaluates the performance of iterative decoding for $\mathcal{C}_{21}$ on the erasure channel as a function of p, the number of rows of the cyclic redundant parity-check matrix $\mathbf{H}_p(\mathbf{z})$ as defined in (43). It is known that the iterative decoding on the BEC performs better when redundant parity-checks are added to the Tanner Graph, which can be observed in this simulation as well. For example, when the channel erasure probability is 0.12, the probability of block error is 0.001 if $p = 10$, but this number is 0.00048 if $p = 15$ and 0.00047 when $p = 21$. The performance of ML decoding is also shown in Fig. 1 and is observed to be identical to that of the $p = 21$ iterative decoding algorithm.

Furthermore, Fig. 2 evaluates the performance of iterative decoding for $\mathcal{C}_{21}$ on the AWGN channel as a function of p. For the iterative decoding over AWGN channel, it is pseudocodewords not stopping sets that is used to analyze its performance and adding redundant parity- checks is not always useful because it can increase the number of pseudocodewords on the decoder's computation tree. However, Fig. 2 shows that our approach of adding parity-checks based on the distribution of stopping sets for $[21, 11, 6]$ difference-set code helps in AWGN scenario as well. By increasing the number of parity-checks from 10 to 21, there is a performance gain of 0.5 dB (in E_b/N_0) and the curve corresponding the $p = 21$ is only 0.25 dB away from that of the optimal ML decoding.

V. Conclusion

In this work, using techniques from spectral graph theory, we derived lower bounds on the expansion properties of Tanner Graphs. Specifically, for any given Tanner Graph represented by an incidence matrix, we showed that the expansion of both variables and parity-checks, the minimum and the average variable expansion, can be lower bounded by functions of the eigenvalues and corresponding eigenvectors of the normalized incidence matrix representing the graph.

This method can also be used to derive lower bounds on the stopping distance of binary linear codes defined by a given parity-check matrix, and we have pointed out the relationship between our bounds and Tanner's bit-oriented bound and parity-oriented bound on minimum distance for regular LDPC codes. Furthermore, these lower bounds can lead to an upper bound on stopping redundancy of the family of difference-set codes.

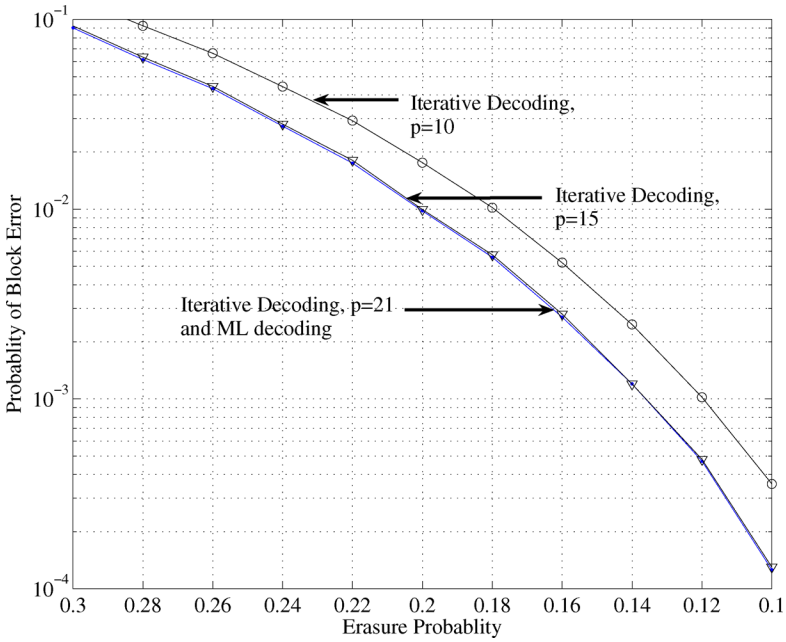

Fig. 1. Performance of iterative decoder as a function of p and maximum-likelihood decoder for $[21, 11, 6]$ difference-set code on BEC. Note that the curve of ML decoding and iterative decoding with $p = 21$ coincide.

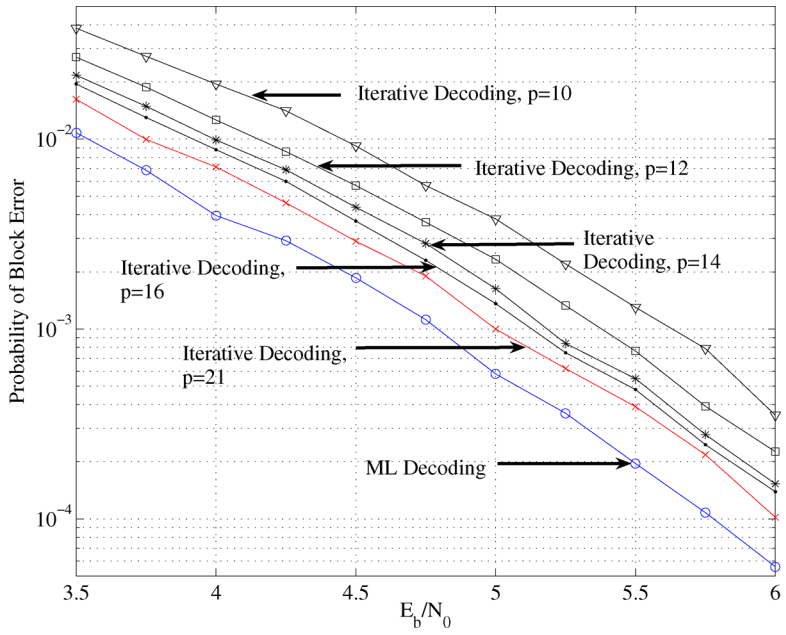

Fig. 2. Performance of iterative decoder as a function of p and maximum-likelihood decoder for $[21, 11, 6]$ difference-set code on AWGN channel.

An interesting open problem is how to properly add redundant parity-checks to the Tanner graphical representation to improve the performance of iterative decoding. In this work, we showed that this can be done for the family of difference-set codes. The generated redundant parity-check matrix has stopping distance equal minimum distance, and the number of minimum stopping sets is the same as minimum weight codewords. Therefore, the performance of iterative decoding and ML decoding are close to each other.

Acknowledgment

The authors are grateful to the reviewers for their valuable comments, which improved the presentation of this correspondence.

References

[1] F. R. K. Chung, *Spectral Graph Theory*. New York: American Mathematical Society, 1997.
[2] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, pp. 533–547, Sep. 1981.
[3] M. Sipser and D. A. Spielman, "Expander codes," *IEEE Trans. Inf. Theory*, vol. 42, pp. 1710–1722, Nov. 1996.
[4] D. Burshtein and G. Miller, "Expander graph arguments for message-passing algorithms," *IEEE Trans. Inf. Theory*, vol. 47, pp. 782–790, Feb. 2001.
[5] A. Barg and G. Zémor, "Error exponents of expander codes," *IEEE Trans. Inf. Theory*, vol. 48, pp. 1725–1730, Jun. 2002.
[6] C. Di, D. Proietti, I. E. Telatar, T. J. Richardson, and R. L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erarue channel," *IEEE Trans. Inf. Theory*, vol. 48, pp. 1570–1579, Jun. 2002.

[7] M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes," *IEEE Trans. Inf. Theory*, submitted for publication.
[8] A. Orlitsky, K. Viswananathan, and J. Zhang, "Stopping set distribution of low-density parity-check code ensembles," *IEEE Trans. Inf. Theory*, vol. 51, pp. 929–953, Mar. 2005.
[9] J. Han and P. H. Siegel, "Improved upper bounds on stopping redundancy," *IEEE Trans. Inf. Theory*, submitted for publication.
[10] N. Wiberg, "Codes and Decoding on General Graphs," Ph.D. dissertation, Linköping University, Linköping, Sweden, 1996.
[11] G. A. Horn, "Iterative Decoding and Pseudocodewords," Ph.D, California Inst. of Technol., Pasadena, CA, 1999.
[12] P. O. Vontobel and R. Koetter, "Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes," *IEEE Trans. Inf. Theory*, 2005, submitted for publication.
[13] P. O. Vontobel and R. Koetter, "Lower bounds on the minimum pseudo-weight of linear codes," in *Proc. IEEE Symp. Inf. Theory*, Jun. 2004, p. 70.
[14] C. Kelley and D. Sridhara, "Pseudocodworks of Tanner graphs," *IEEE Trans. Inf. Theory*, submitted for publication.
[15] P. O. Vontobel, R. Smarandache, N. Kiyavash, J. Teutsch, and D. Vukobratovic, "On the minimal pseudo-codewords of codes from finite geometries," in *Proc. IEEE Symp. Inf. Theory*, Jun. 2005.
[16] Y. Kou, S. Lin, and P. C. Fossorier, "Low-density parity-check codes based on finite geometries: A rediscoverty and new results," *IEEE Trans. Inf. Theory*, vol. 47, pp. 2711–2736, Nov. 2001.
[17] K. M. Krishnan and P. Shankar, "On the complexity of finding stopping distance in Tanner graphs," *IEEE Trans. Inf. Theory*, vol. 51, 2005.
[18] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Improved low-density parity-check codes using irregular graphs," *IEEE Trans. Inf. Theory*, vol. 47, Feb. 2001.
[19] R. M. Tanner, "Minimum-distance bounds by graph analysis," *IEEE Trans. Inf. Theory*, vol. 47, pp. 808–820, Feb. 2001.
[20] M. H. Shin, J. S. Kim, and H. Y. Song, "Generalization of Tanner's minimum distance bounds for LDPC acodes," *IEEE Commun. Lett.*, vol. 9, pp. 240–242, Mar. 2005.
[21] S. Lin and D. Costello Jr.*, Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1983.
[22] M. Zhu and K. M. Chugg, "Lower bounds on stopping distance and their applications," in *Proc. Allerton Conf. Commun., Contr. Comput.*, Sep. 2005.