LOWER BOUNDS ON STOPPING DISTANCE OF LINEAR CODES AND THEIR APPLICATIONS

Mingrui Zhu and Keith M. Chugg

Communication Sciences Institute
Department of Electrical Engineering
Viterbi School of Engineering
University of Southern California, Los Angeles 90089-2565
{mingruiz,chugg}@csi.usc.edu

Abstract

One of the most important open problems in the communication society is to determine the performance of iterative message passing algorithms over loopy graphs. Some recent work addresses this problem for loopy Tanner graphs by introducing the concepts of stopping distance and stopping redundancy. By analyzing the eigenvalues and eigenvectors of the normalized incidence matrix representing a Tanner graph, we derive lower bounds on its stopping distance. Using these lower bounds, an upper bound on stopping redundancy of the difference-set codes is derived as well.

I. INTRODUCTION

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 [1] G is:

$$G = (B \cup Y, E) = (\{b_0, b_1, ..., b_{n-1}\} \cup \{y_0, y_1, ..., y_{p-1}\}, E) \tag{1}$$

where B is the set of variables, Y is the set of single parity-check constraints and $E = \{(b, y) : \ b \in B, \ y \in Y\}$ is the set of edges. It can be shown that the correspondence between $\mathbf{H}_p$ and the traditional *parity-check matrix* representing $\mathcal{C}$ is one-to-one. Furthermore, as Y may contain more than necessary parity-checks, we usually refer $\mathbf{H}_p$ as parity-check matrix when $p = n - k = p_0$, and redundant parity-check matrix otherwise.

Considering $S \subseteq B$, define bit variables in S as *active bits* and parity-checks in the neighborhood of S as *active parity-checks* [2], respectively. 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. It is known that, for binary erasure channels (BEC), the performance of iterative decoding over G is completely determined by its stopping sets [3]. The size of the smallest stopping sets was defined as *stopping distance* [4], which is usually denoted as $s(\mathbf{H}_p)$ to emphasize that it is a function of the specific (redundant) parity-check matrix representing the code.

Previous investigations [3], [5] have considered the properties of random ensembles of linear codes. In contrast, we focus on the parameters of an arbitrary linear code and will analyze eigenvalues and eigenvectors of the *"normalized" incidence matrix* representing the code. Using this technique, we will derive two lower bounds on stopping distance. Since the stopping distance is always no larger than $d_{\min}$, these lower bounds are also lower bounds on minimum distance. In particular, if the graph is regular, they are Tanner's bit-oriented bound and parity-oriented bound [2], respectively, *i.e.,* we demonstrate that Tanner's bounds are actually lower bounds on $s(\mathbf{H}_p)$ for regular Tanner graphs.

Also, these lower bounds can be used to derive upper bounds on *stopping redundancy*, denoted as $\rho(\mathcal{C})$, which is defined as the minimum number of rows in a (redundant) parity-check matrix $\mathbf{H}_p$ for $\mathcal{C}$ such that $s(\mathbf{H}_p) = d_{\min}$ [4]. Previously, Schwartz and Vardy [4] proved

that stopping redundancy is well defined and provided bounds on $\rho(\mathcal{C})$ for the family of binary Reed-Muller codes, extended Golay Codes and maximum distance separable (MDS) codes. In this work, we will provide an upper bound on $\rho(\mathcal{C})$ for the family of *simple difference-set codes*, *i.e.*,$\rho(\mathcal{C}) \leq n$, where n is the length of the code.

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, this lemma will be used to provide lower bounds on stopping distance for linear codes, which will also lead to Tanner's bit-oriented bound and parity-oriented bound on $d_{\min}$ for regular Low-Density Parity-Check (LDPC) codes [6]. We continue in Section IV to show connections between our work and the work of Schwartz and Vardy by providing an upper bound on stopping redundancy of the difference-set codes. Conclusions and future work are discussed in Section V.

II. Graph Representations and Eigenvalue Analysis

Let d_v denote the degree of vertex $v \in B \cup Y$, and $S \subseteq B \cup Y$

$$
\begin{aligned}
r_i &= \text{weight of row } i \text{ of } \mathbf{H}_p = d_{y_i} \quad 0 \leq i \leq p-1 && (2)\\
c_j &= \text{weight of column } j \text{ of } \mathbf{H}_p = d_{b_j} \quad 0 \leq j \leq n-1 && (3)\\
N(v) &= \text{the set of neighbors of } v = \{u : (v,u) \in E \ \text{ or } \ (u,v) \in E\} && (4)\\
N(S) &= \text{the set of neighbors of } S && (5)\\
\text{vol}(S) &= \text{the volume of } S = \sum_{v \in\ S} d_v && (6)\\
A_d[\omega, \mathcal{C}] &= \text{number of weight } \omega \text{ codewords} && (7)\\
A_s[|S|, \mathbf{H}_p] &= \text{number of size } |S| \text{ stopping sets} && (8)
\end{aligned}
$$

Furthermore, define

$$
r_{\max} = \max_i r_i \quad r_{\min} = \min_i r_i \quad c_{\max} = \max_j c_j \quad c_{\min} = \min_j c_j \tag{9}
$$

and the $p \times n$ normalized incidence matrix :

$$
\mathbf{A}_p = [a_{ij}]_{p \times n} = \left[\frac{h_{ij}}{\sqrt{r_i \cdot c_j}} \right]_{p \times n} \tag{10}
$$

It can be shown that $\mathbf{A}_p^T \mathbf{A}_p$ and $\mathbf{A}_p \mathbf{A}_p^T$ share the same set of non-zero eigenvalues, among which the unique largest single eigenvalue is 1 [7]. Ordering the eigenvalues of $\mathbf{A}_p^T \mathbf{A}_p$ as $1 = \mu_0 > \mu_1 \geq \mu_2 ... \geq \mu_{p-1} > \mu_p = ... = \mu_{n-1} = 0$ if $p < n$ or $1 = \mu_0 > \mu_1 \geq \mu_2 ... \geq \mu_{n-1}$ otherwise, with corresponding orthonormal eigenvectors $\mathbf{e}_0, \mathbf{e}_1, ...\mathbf{e}_{n-1}$, it can also be shown that

$$
\mathbf{e}_0 = \frac{\mathbf{T}_d^{1/2} \mathbf{1}_n}{\sqrt{\text{vol}(G)}} \tag{11}
$$

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 $\mathbf{e}'_0, \mathbf{e}'_1, ...\mathbf{e}'_{p-1}$ be the orthonormal eigenvectors of $\mathbf{A}_p \mathbf{A}_p^T$ corresponding to eigenvalues $1 = \mu_0 > \mu_1 \geq \mu_2 ... \geq \mu_{p-1}$, then,

$$
\mathbf{e}'_0 = \frac{(\mathbf{T}'_d)^{1/2} \mathbf{1}_p}{\sqrt{\text{vol}(G)}} \tag{12}
$$

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 [7].

Lemma 1: For an arbitrary bipartite graph $G = (B \cup Y, E)$ with edges between B and Y and a subset S of B (or Y), we have

$$\frac{\text{vol}(N(S))}{\text{vol}(S)} \geq \frac{1}{\mu_1 + (1-\mu_1)\frac{\text{vol}(S)}{\text{vol}(G)}} = \frac{\text{vol}(G)}{\mu_1 \text{vol}(G) + (1-\mu_1)\text{vol}(S)} \tag{13}$$

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 of Lemma 1: Considering $S \subseteq B$, define a $n \times 1$ column vector ψ_S as $(\psi_0, \psi_1, ...\psi_{n-1})^T$, where $\psi_j = 1$, if $b_j \in S$ and $\psi_j = 0$, otherwise. Expressing $\mathbf{T}_d^{1/2}\psi_S$ as a linear combination of the orthonormal eigenvectors of $\mathbf{A}_p^T \mathbf{A}_p$,

$$\mathbf{T}_d^{1/2}\psi_S = \sum_{j=0}^{n-1} \langle \mathbf{T}_d^{1/2}\psi_S, \mathbf{e}_j \rangle \mathbf{e}_j = \sum_{j=0}^{n-1} a_j \mathbf{e}_j \tag{14}$$

and

$$a_0 = \langle \mathbf{T}_d^{1/2}\psi_S, \mathbf{e}_0 \rangle = \frac{\psi_S^T \mathbf{T}_d \mathbf{1}_n}{\sqrt{\text{vol}(G)}} = \frac{\text{vol}(S)}{\sqrt{\text{vol}(G)}} \tag{15}$$

$$\sum_{j=0}^{n-1} a_j^2 = \langle \mathbf{T}_d^{1/2}\psi_S, \mathbf{T}_d^{1/2}\psi_S \rangle = \psi_S^T \mathbf{T}_d \psi_S = \text{vol}(S) \tag{16}$$

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

$$\langle \mathbf{A}_p \mathbf{T}_d^{1/2}\psi_S, \mathbf{A}_p \mathbf{T}_d^{1/2}\psi_S \rangle = \psi_S^T \mathbf{T}_d^{1/2} \mathbf{A}_p^T \mathbf{A}_p \mathbf{T}_d^{1/2} \psi_S = \sum_{j=0}^{n-1} a_j^2 \mu_j \tag{17a}$$

$$\leq a_0^2 + (\sum_{j=1}^{n-1} a_j^2)\mu_1 \tag{17b}$$

$$= (1-\mu_1)\frac{(\text{vol}(S))^2}{\text{vol}(G)} + \mu_1 \text{vol}(S) \tag{17c}$$

Furthermore,

$$\langle \mathbf{A}_p \mathbf{T}_d^{1/2}\psi_S, \mathbf{A}_p \mathbf{T}_d^{1/2}\psi_S \rangle = \sum_{u \in S} \sum_{v \in S} \sum_{\substack{y\,:\,(v,y)\in E \\ \text{and } (u,y)\in E}} \frac{1}{d_y} = \sum_{y \in N(S)} \left| \frac{N(y) \cap S}{\sqrt{d_y}} \right|^2 \tag{18a}$$

$$\geq \frac{\left(\sum_{y \in N(S)} \frac{|N(y) \cap S|}{\sqrt{d_y}} \sqrt{d_y} \right)^2}{\sum_{y \in N(S)} d_y} \tag{18b}$$

$$= \frac{(\text{vol}(S))^2}{\text{vol}(N(S))} \tag{18c}$$

[1]Similar results can be found in [7] for the graphs of regular row/column weights. However, extensions to the irregular case discussed in [7] 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.

where (18a) is generalized from [7, Page 97] and (18b) results from Cauchy-Schwartz inequality. Combining (17c) and (18c),

$$(1-\mu_1)\frac{|\text{vol}(S)|^2}{\text{vol}(G)}+\mu_1\text{vol}(S)\geq\langle\mathbf{A}_p\mathbf{T}_d^{1/2}\psi_S,\mathbf{A}_p\mathbf{T}_d^{1/2}\psi_S\rangle\geq\frac{|\text{vol}(S)|^2}{\text{vol}(N(S))} \tag{19}$$

and (13) is the direct result. Similarly, we can prove this lemma for $S\subseteq Y$ by using $\mathbf{e}_i'$'s and $\mathbf{T}_d'$ defined at the end of section II, and $\psi_S'=(\psi_0',\psi_1',...\psi_{p-1}')^T$, where $\psi_i'=1$, if $y_i\in S$ and $\psi_i'=0$ otherwise. □

III. Lower Bounds of $s(\mathbf{H}_p)$

Using lemma 1,we will derive lower bounds on stopping distance of linear codes. Since $s(\mathbf{H}_p)\leq d_{\min}$, these lower bounds are also lower bounds on $d_{\min}$. In particular, they lead to Tanner's results [2] when the underlying Tanner graph is regular. Thus, using Tanner's terminology, we call (20) and (21) bit-oriented bound and parity-oriented bound, respectively.

A. Bit-oriented and parity-oriented bounds on $s(\mathbf{H}_p)$

Theorem 2: For the $[n,k,d_{\min}]$ linear code $\mathcal{C}$ defined by the Tanner graph $G=(B\cup Y,E)$ with $p\times n$ incidence matrix $\mathbf{H}_p$, define $c_{\max}$, $c_{\min}$ and $r_{\max}$ as in (9), then the following are true:

$$d_{\min}\geq s(\mathbf{H}_p)\geq\frac{(2/r_{\max})-\mu_1}{1-\mu_1}\cdot\frac{\text{vol}(G)}{c_{\max}} \tag{20}$$

$$d_{\min}\geq s(\mathbf{H}_p)\geq\frac{1+(2c_{\min}-2)/r_{\max}-\mu_1c_{\max}}{(1-\mu_1)c_{\max}}\cdot\frac{2\text{vol}(G)}{c_{\max}r_{\max}} \tag{21}$$

where μ_1 is the second largest eigenvalue of $\mathbf{A}_p^T\mathbf{A}_p$ and $\mathbf{A}_p$ as defined in (10).

The bit-oriented bound, *i.e.,* (20), becomes meaningless if $\mu_1>2/r_{\max}$. However, $1+(2c_{\min}-2)/r_{\max}-\mu_1c_{\max}$ may still be positive which makes parity-oriented bound meaningful.

Proof of Theorem 2: Since stopping distance is always no larger than minimum distance [4], we only need to prove the second inequalities of (20) and (21).

Let $S_1\subseteq B$ be a smallest stopping set, $N(S_1)$ is then the set of active parity-checks and $s(\mathbf{H}_p)=|S_1|$. Applying lemma 1,

$$\frac{|N(S_1)|r_{\max}}{\text{vol}(S_1)}\geq\frac{\text{vol}(N(S_1))}{\text{vol}(S_1)}\geq\frac{\text{vol}(G)}{\mu_1\text{vol}(G)+(1-\mu_1)\text{vol}(S_1)} \tag{22}$$

where μ_1 is the second largest eigenvalue of $\mathbf{A}_p^T\mathbf{A}_p$. Since any active parity-check in $N(S_1)$ must be connected to at least two active bits, $|N(S_1)|\leq\frac{1}{2}\text{vol}(S_1)$. Therefore,

$$\frac{r_{\max}}{2}\geq\frac{\text{vol}(G)}{\mu_1\text{vol}(G)+(1-\mu_1)\text{vol}(S_1)} \tag{23}$$

$$\Rightarrow s(\mathbf{H}_p)=|S_1|\geq\frac{\text{vol}(S_1)}{c_{\max}}\geq\frac{2/r_{\max}-\mu_1}{1-\mu_1}\cdot\frac{\text{vol}(G)}{c_{\max}} \tag{24}$$

To prove (21), let $S_2\subseteq Y$ be the set of active parity-checks of a smallest stopping set,

$$\frac{|N(S_2)|c_{\max}}{\text{vol}(S_2)}\geq\frac{\text{vol}(N(S_2))}{\text{vol}(S_2)}\geq\frac{\text{vol}(G)}{\mu_1\text{vol}(G)+(1-\mu_1)\text{vol}(S_2)} \tag{25}$$

Considering $N(S_2)$, 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_2, and for the rest bits, some of their neighbors are in S_2 but others are not. Therefore,

let $c_{avg}(N(S_2))$ be the average number of edges connected to $N(S_2)$ that are counted in $\text{vol}(S_2)$, *i.e.*, $|N(S_2)|c_{avg}(N(S_2)) = \text{vol}(S_2)$, then

$$(25) \Rightarrow \frac{c_{\max}}{c_{avg}(N(S_2))} \geq \frac{\text{vol}(G)}{\mu_1 \text{vol}(G) + (1-\mu_1)\text{vol}(S_2)} \tag{26}$$

Also, among the r_i neighbors of any node $y_i \in S_2$, at lease 2 of them are active bits and the remaining $r_i - 2$ bits have at least one edge connected to S_2. In other words, assuming the r_i neighbors of y_i are $b_1, b_2, .., b_{r_i}$, among which b_1 and b_2 are active bits and $b_3, ..b_{r_i}$ each has at least one edge connected to S_2, it can be shown that 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 $\text{vol}(S_2)$ on average. Thus,

$$c_{avg}(N(S_2)) \geq 1 + (2c_{\min} - 2)/r_{\max} \tag{27}$$

$$\begin{aligned} (26) \quad &\Rightarrow \quad \frac{c_{\max} r_{\max}}{2c_{\min} + r_{\max} - 2} \geq \frac{\text{vol}(G)}{\mu_1 \text{vol}(G) + (1-\mu_1)\text{vol}(S_2)} \\ &\Leftrightarrow \quad \text{vol}(S_2) \geq \frac{1 + (2c_{\min} - 2)/r_{\max} - \mu_1 c_{\max}}{(1-\mu_1)c_{\max}} \cdot \text{vol}(G) \end{aligned} \tag{28}$$

Noting that $s(\mathbf{H}_p)c_{\max} \geq 2|S_2| \geq 2\text{vol}(S_2)/r_{\max}$, (21) is obtained. □

Lower bounds on minimum distance and stopping distance when the underlying graph is regular can be considered as a special case of Theorem 2, which is summarized in the following corollary.

Corollary 3: The $d_{\min}$ of regular LDPC codes defined by $p \times n$ parity-check matrix $\mathbf{H}_p$ satisfies

$$d_{\min} \quad \geq \quad s(\mathbf{H}_p) \geq \frac{n(2c - \eta_1)}{cr - \eta_1} \tag{29}$$

$$d_{\min} \quad \geq \quad s(\mathbf{H}_p) \geq \frac{2n(2c + r - 2 - \eta_1)}{r(cr - \eta_1)} \tag{30}$$

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

Proof of Corollary 3: It can be shown that, if $\mathbf{H}_p$ is regular, *i.e.*, $c_0 = ... = c_{n-1} = c$ and $r_0 = ... = r_{p-1} = r$, 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 (10). The proof of Corollary 3 is then straightforward by plugging $c_{\max} = c_{\min} = c$, $r_{\max} = r$, $\text{vol}(G) = nc$ and $\eta_1 = \mu_1 cr$ into (20) and (21) respectively. □

It can be seen that the part of (29) and (30) corresponding to $d_{\min}$ coincide with Tanner's bit-oriented bound and parity-oriented bound for regular LDPC codes [2, Theorem 3.1,Theorem 4.1], respectively. We have also noted that Shin [8] generalized Tanner's work by deriving lower bounds on $d_{\min}$ for Quasi-cyclic LDPC codes, where some degree of regularity is still necessary. Our contributions are the derivation of low bounds for general LDPC codes and demonstrating that Tanner's bounds are indeed lower bounds on stopping distance.

Considering Gallager's $(20, 3, 4)$ regular LDPC code [6, Figure 2.1], it has $d_{\min} = 6$, and the given redundant parity-check matrix has stopping distance of 6, $r = 4$, $c = 3$ and $\mu_1 = 0.5$. The bit-oriented bound does not apply, the parity-oriented bound is, however, 4.

IV. An upper bound on stopping redundancy of the difference-set codes

Stopping redundancy was introduced by Schwartz and Vardy [4]. Lower and upper bounds were also provided for binary and ternary extended Golay codes, the family of Reed-Muller codes and Maximum-Distance Separable (MDS) codes. In this section, we will provide an upper bound on stopping redundancy of the family of difference-set codes. Specifically, assuming $\mathcal{C}$ is a difference-set code of length n and minimum distance $d_{\min}$, we will show that there exists a $n \times n$ redundant parity-check matrix $\mathbf{H}_n$ such that $s(\mathbf{H}_n) = d_{\min}$, therefore $\rho(\mathcal{C}) \leq n$. 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 [9].

To analyze the algebraic properties of cyclic codes, the components of a row vector[2] $\mathbf{v} = (v_0, v_1, ..., v_{n-1})$ are usually treated as coefficients of a polynomial, *i.e.,* $\mathbf{v}(X) = v_0 + v_1 X + v_2 X^2 + ... + v_{n-1} X^{n-1}$. Since the correspondence between $\mathbf{v}$ and $\mathbf{v}(X)$ is one-to-one, we use the terms "row vector" and "polynomial" interchangeably hereafter.

It is known that a cyclic code is uniquely specified by its *parity polynomial* [9], which is of degree k and defined as:

$$\mathbf{h}(X) = 1 + h_1 X + h_2 X^2 + ... + h_{k-1} X^{k-1} + X^k \tag{31}$$

The corresponding parity-check matrix can be written as:

$$\mathbf{H}_{p_0} = \begin{bmatrix} \mathbf{h}^*(X) \bmod (X^n+1) \\ X\ \mathbf{h}^*(X) \bmod (X^n+1) \\ \cdot \\ \cdot \\ X^{p_0-1}\mathbf{h}^*(X) \bmod (X^n+1) \end{bmatrix}_{p_0 \times n} = \begin{bmatrix} \mathbf{h}^*(X) \\ X\ \mathbf{h}^*(X) \\ \cdot \\ \cdot \\ X^{p_0-1}\mathbf{h}^*(X) \end{bmatrix}_{p_0 \times n} = \begin{bmatrix} \mathbf{h}_0^* \\ \mathbf{h}_1^* \\ \cdot \\ \cdot \\ \mathbf{h}_{p_0-1}^* \end{bmatrix}_{p_0 \times n} \tag{32}$$

where $p_0 = n - k$, $\mathbf{h}^*(X) = X^k \mathbf{h}(X^{-1})$ is the reciprocal of $\mathbf{h}(X)$ and $\mathbf{h}_i^*$, $0 \leq i \leq p_0 - 1$, are row vectors. A parity-check matrix of this form is called a *cyclic parity-check matrix* because $\mathbf{h}_i^*$ is the i-th cyclic shift of $\mathbf{h}_0^*$ to the right, $1 \leq i \leq p_0 - 1$.

It is also known that the parity-check matrix for a given cyclic code is usually not unique. One interesting result is the following lemma.

Lemma 4: Assuming that $\mathbf{h}(X)$ is the parity polynomial of an $[n,k,d_{\min}]$ 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 non-zero polynomial of degree $f < p_0 = n - k$;
- the greatest common divisor of $\mathbf{f}(X)$ and $X^n + 1$ is 1, *i.e.,* GCD$(\mathbf{f}(X), X^n + 1) = 1$;

then,

$$\mathbf{H}_{p_0}(\mathbf{z}) = \begin{bmatrix} \mathbf{z}^*(X) \bmod (X^n+1) \\ X\ \mathbf{z}^*(X) \bmod (X^n+1) \\ \cdot \\ \cdot \\ X^{p_0-1}\mathbf{z}^*(X) \bmod (X^n+1) \end{bmatrix}_{p_0 \times n} = \begin{bmatrix} \mathbf{z}_0^* \\ \mathbf{z}_1^* \\ \cdot \\ \cdot \\ \mathbf{z}_{p_0-1}^* \end{bmatrix}_{p_0 \times n} \tag{33}$$

is also a cyclic parity-check matrix for $\mathcal{C}$, where

$$\mathbf{z}^*(X) = X^{k+f}\mathbf{z}(X^{-1}) = X^k \mathbf{h}(X^{-1}) X^f \mathbf{f}(X^{-1}) = \mathbf{h}^*(X)\mathbf{f}^*(X) \tag{34}$$

is the reciprocal of $\mathbf{z}(X)$.

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

Proof of Lemma 4: 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 $\mathbf{H}_{p_0}$ and they are linearly independent. Since the row space of $\mathbf{H}_{p_0}$ is of dimension p_0, the row space of $\mathbf{H}_{p_0}(\mathbf{z})$ is then the same as the row space of $\mathbf{H}_{p_0}$. Therefore, $\mathbf{H}_{p_0}(\mathbf{z})$ is a cyclic parity-check matrix for $\mathcal{C}$.

Noting that $\mathbf{z}^*(X) = \mathbf{h}^*(X)\mathbf{f}^*(X)$ and GCD$(\mathbf{f}^*(X), X^n + 1) = 1$, $\mathbf{z}_0^*$ is a non-zero row vector and is a linear combination of the row vectors of $\mathbf{H}_{p_0}$. Also, the cyclic property of the row space of $\mathbf{H}_{p_0}$ guarantees that it contains all the cyclic shift of $\mathbf{z}_0^*$ to the right.

To prove part two, 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

$$\alpha_0\mathbf{z}_0^* \oplus \alpha_1\mathbf{z}_1^* \oplus ... \oplus \alpha_{p_0-1}\mathbf{z}_{p_0-1}^* = \mathbf{0} \tag{35}$$

where $\oplus$ is modulo-2 addition and $\mathbf{0}$ is a zero row vector. Equivalently,

$$\alpha_0\mathbf{z}^*(X) \oplus \alpha_1 X\mathbf{z}^*(X) \oplus ... \oplus \alpha_{p_0-1}X^{p_0-1}\mathbf{z}^*(X) \equiv 0 \bmod (X^n + 1) \tag{36a}$$

$$\mathbf{f}^*(X)\left[\alpha_0\mathbf{h}^*(X) \oplus \alpha_1 X\mathbf{h}^*(X) \oplus ... \oplus \alpha_{p_0-1}X^{p_0-1}\mathbf{h}^*(X)\right] \equiv 0 \bmod (X^n + 1) \tag{36b}$$

Noting that GCD$(\mathbf{f}^*(X), X^n + 1) = 1$, thus

$$[\alpha_0 \oplus \alpha_1 X \oplus ... \oplus \alpha_{p_0-1}X^{p_0-1}]\mathbf{h}^*(X) \equiv 0 \bmod (X^n + 1) \tag{37a}$$

$$\Leftrightarrow \alpha_0\mathbf{h}_0^* \oplus \alpha_1\mathbf{h}_1^* \oplus ... \oplus \alpha_{p_0-1}\mathbf{h}_{p_0-1}^* = \mathbf{0} \tag{37b}$$

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

A. An upper bound on stopping redundancy of the difference-set codes

Definition 1: [9][Ch.5] Let $D = \{d_0, d_1, ..., d_q\}$ be a set of $q + 1$ non-negative integers such that $0 \leq d_0 < d_1 < ... < d_q \leq q(q + 1)$, and for each $0 < t < q(q + 1)$, there exist one and only one ordered pair $0 \leq i \neq j \leq q$ such that $d_i - d_j \equiv t \bmod q(q + 1)$, then D is a perfect simple **difference set** of order q. □

It can be shown that, if D is perfect simple difference set, $D' = \{0, d_1 - d_0, d_2 - d_0, ..., d_{q-1} - d_0, d_q - d_0\}$, $\overline{D} = \{q(q+1) - d_q, q(q+1) - d_{q-1}, ..., q(q+1) - d_1, q(q+1) - d_0\}$ and $\overline{D}' = \{0, d_q - d_{q-1}, ..., d_q - d_1, d_q - d_0\}$ are also perfect simple difference sets. It is also known that perfect simple difference sets exist for order $q = \alpha^\beta$, where α is prime and β is any positive integer. However, the case of $q = 2^\beta$ corresponds to the most commonly studied difference-set codes.

Definition 2: [9] Let $D = \{0, d_1, ..., d_q\}$ be a perfect simple difference set of order $q = 2^\beta$, define the polynomial $\mathbf{z}(X) = 1 + X^{d_1} + X^{d_2} + ... + X^{d_q}$. Let $n = q(q+1)+1 = 2^{2\beta} + 2^\beta + 1$, $k = 2^{2\beta} + 2^\beta - 3^\beta$ and $\mathbf{h}(X)$ be the greatest common divisor of $\mathbf{z}(X)$ and $X^n + 1$, *i.e.,* $\mathbf{h}(X) =$ GCD$(\mathbf{z}(X), X^n + 1)$, the cyclic code defined by the parity-check matrix with $p_0 = n - k$,

$$\mathbf{H}_{p_0} = \begin{bmatrix} \mathbf{h}^*(X) \\ X\ \mathbf{h}^*(X) \\ \cdot \\ \cdot \\ X^{p_0-1}\mathbf{h}^*(X) \end{bmatrix}_{p_0 \times n} = \begin{bmatrix} \mathbf{h}_0^* \\ \mathbf{h}_1^* \\ \cdot \\ \cdot \\ \mathbf{h}_{p_0-1}^* \end{bmatrix}_{p_0 \times n} \tag{38}$$

is an $[n, k, d_{\min} = q + 2]$ **difference-set code**, where $\mathbf{h}^*(X)$ is the reciprocal of $\mathbf{h}(X)$. □

Theorem 5: The stopping redundancy of an $[n,k,d_{\min}]$ difference-set code is less than or equal to n, where $n = q^2 + q + 1$, $k = q^2 + q - 3^\beta$, $d_{\min} = q + 2$ and $q = 2^\beta$.

Proof of Theorem 5: Since $\mathbf{h}(X) = \text{GCD}(\mathbf{z}(X), X^n + 1)$, where polynomial $\mathbf{z}(X)$ corresponds to the perfect simple difference set D of order $q = 2^\beta$, there exists a polynomial $\mathbf{f}(X)$ such that $\mathbf{z}(X) = \mathbf{h}(X)\mathbf{f}(X)$ and $\text{GCD}(\mathbf{f}(X), X^n + 1) = 1$. Using Lemma 4,

$$\mathbf{H}_{p_0}(\mathbf{z}) = \begin{bmatrix} \mathbf{z}^*(X) \bmod (X^n+1) \\ X\ \mathbf{z}^*(X) \bmod (X^n+1) \\ \cdot \\ \cdot \\ X^{p_0-1}\mathbf{z}^*(X) \bmod (X^n+1) \end{bmatrix}_{p_0 \times n} = \begin{bmatrix} \mathbf{z}_0^* \\ \mathbf{z}_1^* \\ \cdot \\ \cdot \\ \mathbf{z}_{p_0-1}^* \end{bmatrix}_{p_0 \times n} \tag{39}$$

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,

$$\mathbf{H}_n(\mathbf{z}) = \begin{bmatrix} \mathbf{z}^*(X) \bmod (X^n+1) \\ \cdot \\ X^{p_0-1}\mathbf{z}^*(X) \bmod (X^n+1) \\ \cdot \\ X^{n-1}\mathbf{z}^*(X) \bmod (X^n+1) \end{bmatrix}_{n \times n} = \begin{bmatrix} \mathbf{z}_0^* \\ \cdot \\ \mathbf{z}_{p_0-1}^* \\ \cdot \\ \mathbf{z}_{n-1}^* \end{bmatrix}_{n \times n} \tag{40}$$

which has both rows and columns weight $q+1$. Then

$$\mathbf{A}_n(\mathbf{z}) = \frac{1}{(q+1)^2}\mathbf{H}_n(\mathbf{z}) \tag{41}$$

Furthermore, $1 = \widetilde{\mu}_0 > \widetilde{\mu}_1 = \widetilde{\mu}_2 ... \widetilde{\mu}_{n-1} = \frac{q}{(q+1)^2}$ are eigenvalues of $\mathbf{A}_n(\mathbf{z})^T\mathbf{A}_n(\mathbf{z})$, which has diagonal entries of $\frac{1}{q+1}$ and off-diagonal entries of $\frac{1}{(q+1)^2}$. Then, the bit-oriented bound is

$$s(\mathbf{H}_n(\mathbf{z})) \ge \frac{\frac{2}{q+1} - \frac{q}{(q+1)^2}}{1 - \frac{q}{(q+1)^2}}(q^2+q+1) = q+2 = d_{\min} \tag{42}$$

Therefore, the stopping distance of $\mathbf{H}_n(\mathbf{z})$ equals $d_{\min}$ of the code, and 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 6: For the family of $[n, k, d_{\min}]$ difference-set code,

$$A_d[d_{\min}, \mathcal{C}] = A_s[s(\mathbf{H}_n(\mathbf{z})), \mathbf{H}_n(\mathbf{z})] \tag{43}$$

Proof of Theorem 6: To show (43), it suffices to show that, by letting variables in it be 1 and the rest be 0, every smallest stopping set corresponds to a minimum weight codeword. Without loss of generality, assuming that $\{b_1, b_2, ..., b_{q+2}\}$ forms a stopping set and y_1, y_2, ... y_{q+1} are neighbors of b_1, there exists at least one b_j, $2 \le j \le q+2$, such that $y_i \in N(b_j)$ because $\{b_1, b_2, ..., b_{q+2}\}$ is a stopping set. However, as $|N(b_1) \bigcap N(b_2)| = ... = |N(b_1) \bigcap N(b_{q+2})| = 1$ and $|N(b_1)| = q+1$, it can be shown that there is only one such b_j for each y_i so that all neighbors of b_1 are of degree two. Similarly, we can prove this for b_j, $2 \le j \le q+2$. Thus, let $b_j = 1$ for $1 \le j \le q+2$ and $b_j = 0$ otherwise, a minimum weight codeword, which is of weight $q+2$, is formed. □

Using (43), 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 verified using the $[21, 11, 6]$ difference-set code $\mathcal{C}_{21}$ derived from the difference set $D = \{0, 3, 4, 9, 11\}$, where $\mathbf{h}(X) = \mathbf{z}(X) = 1 + X^3 + X^4 + X^9 + X^{11}$, $d_{\min} = 6$

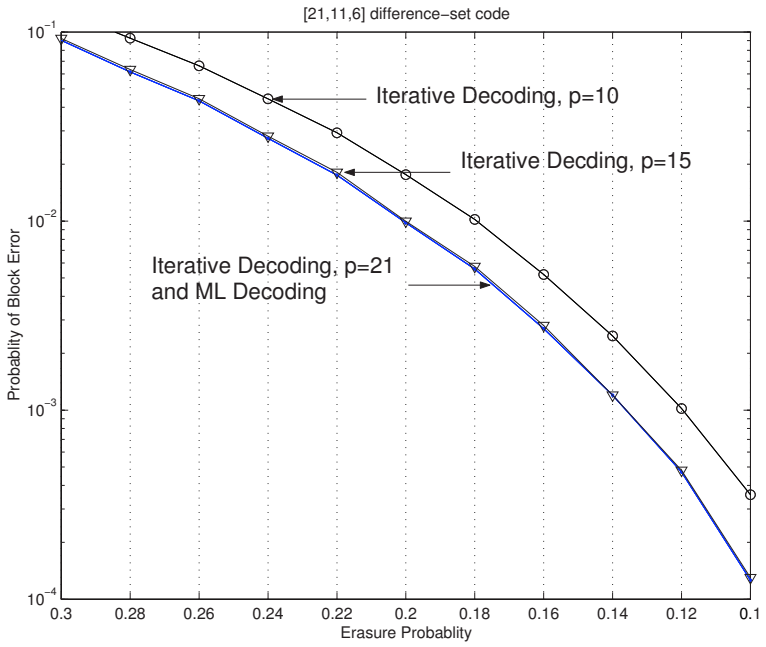

Fig. 1. Performance of iterative decoder as a function of p and Maximum-Likelihood decoder for $[21, 11, 6]$ difference-set code on BEC. Note that the curve of ML decoding and iterative decoding with $p = 21$ coincide.

and $A_d[6, \mathcal{C}_{21}] = 168$. It can be shown that $\rho(\mathcal{C}_{21}) \leq 12$, and $A_s[s(\mathbf{H}_p(\mathbf{z})), \mathbf{H}_p(\mathbf{z})] = 168$ if $p \geq 15$, where Theorem 5 and Theorem 6 provide bounds $\rho(\mathcal{C}_{21}) \leq 21$ and $p \geq 21$, respectively.

Figure 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 $\mathbf{H}_p(\mathbf{z})$ in the form similar to (40). The general belief, that the iterative decoder will perform better if redundant parity-checks are added to the Tanner Graph, is verified by this simulation. 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 1 and is observed to be identical to that of the $p = 21$ iterative decoding algorithm.

V. Conclusion and Future work

Using techniques of spectral graph theory, we derived lower bounds on stopping distance of linear codes defined by randomly generated parity-check matrices, and 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, using these lower bounds, we derived an upper bound on stopping redundancy of the family of difference-set codes.

References

[1] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Information Theory*, vol. 27, pp. 533–547, September 1981.

[2] R. M. Tanner, "Minimum-distance bounds by graph analysis," *IEEE Trans. Information Theory*, vol. 47, pp. 808–820, February 2001.

[3] 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. Information Theory*, vol. 48, pp. 1570 – 1579, June 2002.

[4] M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes," *Submitted to Information Theory*, 2005.

[5] A. Orlitsky, K. Viswananathan, and J. Zhang, "Stopping set distribution of ldpc code ensembles," *IEEE Trans. Information Theory*, vol. 51, pp. 929 – 953, March 2005.
[6] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.
[7] F. R. K. Chung, *Spectral Graph Theory*. American Mathematical Society, 1997.
[8] M. H. Shin, J. S. Kim, and H. Y. Song, "Generalization of tanner's minimum distance bounds for ldpc codes," *IEEE Communications Letters*, vol. 9, pp. 240–242, March 2005.
[9] S. Lin and J. D. Costello, *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, 1983.