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 \([n,k,d_{\text{min}}]\) binary linear code \(C\) specified by a \(p \times n\) incidence matrix \(H_p\) with columns representing bit variables, rows representing parity-checks and \(p \geq n-k = p_0\), the corresponding Tanner graph \([1]\) \(G\) is:

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

(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 \(H_p\) and the traditional parity-check matrix representing \(C\) is one-to-one. Furthermore, as \(Y\) may contain more than necessary parity-checks, we also refer \(H_p\) 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 \(s(H_p)\) 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 \(d_{\text{min}}\), 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 \(s(H_p)\) for regular Tanner graphs.

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

This work was supported in part by the Army Research Office DAAD19-01-1-0477
that stopping redundancy is well defined and provided bounds on $\rho(C)$ 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 $\rho(C)$ for the family of simple difference-set codes, i.e., $\rho(C) \leq n$, 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 $S \subseteq B \cup Y$

$$r_i = \text{weight of row } i \text{ of } \textbf{H}_p = d_{yi}, \quad 0 \leq i \leq p - 1$$

$$c_j = \text{weight of column } j \text{ of } \textbf{H}_p = d_{bj}, \quad 0 \leq j \leq n - 1$$

$$N(v) = \text{the set of neighbors of } v = \{ u : (v, u) \in E \text{ or } (u, v) \in E \}$$

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

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

$$A_d[\omega, C] = \text{number of weight } \omega \text{ codewords}$$

$$A_s[|S|, \textbf{H}_p] = \text{number of size } |S| \text{ stopping sets}$$

Furthermore, define

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

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

$$A_p = [a_{ij}]_{p \times n} = \left[ \frac{h_{ij}}{\sqrt{r_i \cdot c_j}} \right]_{p \times n}$$

It can be shown that $A_p^T A_p$ and $A_p A_p^T$ share the same set of non-zero eigenvalues, among which the unique largest single eigenvalue is 1 [7]. Ordering the eigenvalues of $A_p^T A_p$ as $1 = \mu_0 > \mu_1 \geq \mu_2 \ldots \geq \mu_{p-1} > \mu_p = \ldots = \mu_{n-1} = 0$ if $p < n$ or $1 = \mu_0 > \mu_1 \geq \mu_2 \ldots \geq \mu_{n-1} = 0$ otherwise, with corresponding orthonormal eigenvectors $e_0, e_1, \ldots e_{n-1}$, it can also be shown that

$$e_0 = \frac{T_d^{1/2} 1_n}{\sqrt{\text{vol}(G)}}$$

where $T_d = [t_{ij}]$ 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 $1_n$ are 1’s. Similarly, let $e'_0, e'_1, \ldots e'_{p-1}$ be the orthonormal eigenvectors of $A_p A_p^T$ corresponding to eigenvalues $1 = \mu_0 > \mu_1 \geq \mu_2 \ldots \geq \mu_{p-1}$, then,

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

where $T'_d = [t'_{ij}]$ 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 $G = (B \cup Y, E)$ and a subset $S$ of $B$ (or $Y$),

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

where $\mu_1$ is the second largest eigenvalue of both $A_p^T A_p$ and $A_p A_p^T$.

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

$$T_d^{1/2} \psi_S = \sum_{j=0}^{n-1} \langle T_d^{1/2} \psi_S, e_j \rangle e_j = \sum_{j=0}^{n-1} a_j e_j$$ (14)

and

$$a_0 = \langle T_d^{1/2} \psi_S, e_0 \rangle = \frac{\psi_S^T T_d 1_n}{\sqrt{\text{vol}(G)}} = \frac{\text{vol}(S)}{\sqrt{\text{vol}(G)}}$$ (15)

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

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

$$\langle A_p T_d^{1/2} \psi_S, A_p T_d^{1/2} \psi_S \rangle = \psi_S^T T_d^{1/2} A_p^T A_p T_d^{1/2} \psi_S = \sum_{j=0}^{n-1} a_j^2 \mu_j$$ (17a)

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

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

Furthermore,

$$\langle A_p T_d^{1/2} \psi_S, A_p T_d^{1/2} \psi_S \rangle = \sum_{u \in S} \sum_{v \in S} \sum_{y : (v, y) \in E \text{ and } (u, y) \in E} \frac{1}{d_y} = \sum_{y \in N(S)} \frac{|N(y) \cap S|^2}{\sqrt{d_y}}$$ (18a)

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

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

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

$$(1 - \mu_1) \frac{(\text{vol}(S))^2}{\text{vol}(G)} + \mu_1 \text{vol}(S) \geq \langle A_p T_d^{1/2} \psi_S, A_p T_d^{1/2} \psi_S \rangle \geq \frac{(\text{vol}(S))^2}{\text{vol}(N(S))}$$ (19)

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

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.
III. LOWER BOUNDS OF $s(H_p)$

Using lemma 1, we will derive lower bounds on stopping distance of linear codes. Since $s(H_p) \leq d_{\min}$, 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 $s(H_p)$

Theorem 2: For the $[n, k, d_{\min}]$ linear code $C$ defined by the Tanner graph $G = (B \cup Y, E)$ with $p \times n$ incidence matrix $H_p$, define $c_{\max}$, $c_{\min}$ and $r_{\max}$ as in (9), it can be shown that:

$$d_{\min} \geq s(H_p) \geq \frac{(2/r_{\max}) - \mu_1}{1 - \mu_1} \cdot \frac{\text{vol}(G)}{c_{\max}}$$

(20)

$$d_{\min} \geq s(H_p) \geq \frac{1 + (2c_{\min} - 2)/r_{\max} - \mu_1 c_{\max}}{(1 - \mu_1)c_{\max}} \cdot \frac{2\text{vol}(G)}{c_{\max}r_{\max}}$$

(21)

where $\mu_1$ is the second largest eigenvalue of $A_p^T A_p$ and $A_p$ as defined in (10).

The bit-oriented bound, i.e., (20), becomes meaningless if $\mu_1 > 2/r_{\max}$. However, $1 + (2c_{\min} - 2)/r_{\max} - \mu_1 c_{\max}$ may still be positive which makes the 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 $s(H_p) = |S_1|$. Applying lemma 1,

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

(22)

where $\mu_1$ is the second largest eigenvalue of $A_p^T A_p$. 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,

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

(23)

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

(24)

To prove (21), let $S_2 \subseteq Y$ be the set of active parity-checks of a smallest stopping set, $N(S_2)$, 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 $c_{\text{avg}}(N(S_2))$ be the average number of edges connected to $N(S_2)$ that are counted in $\text{vol}(S_2)$, i.e., $|N(S_2)| c_{\text{avg}}(N(S_2)) = \text{vol}(S_2)$, then

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

(25)

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

(26)

Also, among the $r_i$ neighbors of any node $y_i \in S_2$, at least 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 $(c_1 + c_2 + r_i - 2)/r_i = \frac{|N(S_2)|}{\text{vol}(S_2)} \geq \frac{\text{vol}(N(S_2))}{\text{vol}(S_2)} \geq \frac{\text{vol}(G)}{\mu_1 \text{vol}(G) + (1 - \mu_1) \text{vol}(S_2)}$
1 + (c_1 + c_2 - 2)/r_i \geq 1 + (2c_{\text{min}} - 2)/r_{\text{max}} \text{ edges connected to a neighbor of } y_i \text{ are counted in } \text{vol}(S_2) \text{ on average. Thus, }
\begin{equation}
c_{\text{avg}}(N(S_2)) \geq 1 + (2c_{\text{min}} - 2)/r_{\text{max}}
\end{equation}

\begin{equation}
(26) \iff \frac{c_{\text{max}}r_{\text{max}}}{2c_{\text{min}} + r_{\text{max}} - 2} \geq \frac{\text{vol}(G)}{\mu_1\text{vol}(G) + (1 - \mu_1)\text{vol}(S_2)}
\end{equation}

\begin{equation}
\implies \text{vol}(S_2) \geq \frac{1 + (2c_{\text{min}} - 2)/r_{\text{max}} - \mu_1c_{\text{max}}}{(1 - \mu_1)c_{\text{max}}} \cdot \text{vol}(G)
\end{equation}

Noting that \( s(H_p)c_{\text{max}} \geq 2|S_2| \geq 2\text{vol}(S_2)/r_{\text{max}} \), (21) is obtained. \[ \square \]

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 \( d_{\text{min}} \) and \( s(H_p) \) of regular LDPC codes defined by \( p \times n \) parity-check matrix \( H_p \) satisfy

\begin{equation}
d_{\text{min}} \geq s(H_p) \geq \frac{n(2c - \eta_1)}{cr - \eta_1}
\end{equation}

\begin{equation}
d_{\text{min}} \geq s(H_p) \geq \frac{2n(2c + r - 2 - \eta_1)}{r(c\eta - \eta_1)}
\end{equation}

where \( \eta_1 = \mu_1cr \) is the second largest eigenvalue of \( H_p^T H_p \). \[ \square \]

**Proof of Corollary 3:** It can be shown that, if \( H_p \) is regular, i.e., \( c_0 = \ldots = c_{n-1} = c \) and \( r_0 = \ldots = r_{p-1} = r \), the \( n \times n \) square matrix \( H_p^T H_p \) has \( cr \) as its unique largest single eigenvalue and \( \eta_1 = \mu_1cr \) as its second largest eigenvalue, where \( \mu_1 \) is the second largest eigenvalue of \( A_p^T A_p \) and \( A_p \) is the normalized incidence matrix defined in (10). The proof of Corollary 3 is then straightforward by plugging \( c_{\text{max}} = c_{\text{min}} = c \), \( r_{\text{max}} = r \), \( \text{vol}(G) = nc \) and \( \eta_1 = \mu_1cr \) into (20) and (21) respectively. \[ \square \]

It can be seen that the part of (29) and (30) corresponding to \( d_{\text{min}} \) 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 \( d_{\text{min}} \) 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 \( d_{\text{min}} = 6 \), 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 \( C \) is a difference-set code of length \( n \) and minimum distance \( d_{\text{min}} \), we will show that there exists a \( n \times n \) redundant parity-check matrix \( H_n \) such that \( s(H_n) = d_{\text{min}} \), therefore \( \rho(C) \leq n \). 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]. Also, the family of difference-set codes is known as the type-I two-dimensional projective geometry LDPC, or 2-D PG-LDPC, codes [10].
To analyze the algebraic properties of cyclic codes, the components of a row vector\(^2\) \(v = (v_0, v_1, ..., v_{n-1})\) are usually treated as coefficients of a polynomial, i.e., \(v(X) = v_0 + v_1X + v_2X^2 + ... + v_{n-1}X^{n-1}\). Since the correspondence between \(v\) and \(v(X)\) 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:

\[
h(X) = 1 + h_1X + h_2X^2 + ... + h_{k-1}X^{k-1} + X^k
\]

(31)

The corresponding cyclic parity-check matrix can be written as:

\[
H_{p_0} = \begin{bmatrix}
    h^*(X) \mod (X^{n+1}) \\
    X \ h^*(X) \mod (X^{n+1}) \\
    \cdot \\
    \cdot \\
    X^{p_0-1}h^*(X) \mod (X^{n+1})
\end{bmatrix}_{p_0 \times n}
= \begin{bmatrix}
    h^*(X) \\
    X \ h^*(X) \\
    \cdot \\
    \cdot \\
    X^{p_0-1}h^*(X)
\end{bmatrix}_{p_0 \times n}
\begin{bmatrix}
    h^*_0 \\
    h^*_1 \\
    \cdot \\
    \cdot \\
    h^*_{p_0-1}
\end{bmatrix}_{p_0 	imes n}
\]

(32)

where \(p_0 = n - k\), \(h^*(X) = X^kh(X^{-1})\) is the reciprocal of \(h(X)\) and \(h^*_i\), \(0 \leq i \leq p_0 - 1\), are row vectors. A parity-check matrix of this form is called a cyclic parity-check matrix because \(h^*_i\) is the \(i\)-th cyclic shift of \(h^*_0\) 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 \(h(X)\) is the parity polynomial of an \([n,k,d_{\min}]\) cyclic code \(C\), if there exists another polynomial \(z(X) = h(X)f(X)\) such that:

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

then,

\[
H_{p_0}(z) = \begin{bmatrix}
    z^*(X) \mod (X^{n+1}) \\
    X \ z^*(X) \mod (X^{n+1}) \\
    \cdot \\
    \cdot \\
    X^{p_0-1}z^*(X) \mod (X^{n+1})
\end{bmatrix}_{p_0 \times n}
= \begin{bmatrix}
    z^*_0 \\
    z^*_1 \\
    \cdot \\
    \cdot \\
    z^*_{p_0-1}
\end{bmatrix}_{p_0 \times n}
\]

(33)

is also a cyclic parity-check matrix for \(C\), where

\[
z^*(X) = X^{k+f}z(X^{-1}) = X^kh(X^{-1})X^{f}f(X^{-1}) = h^*(X)f^*(X)
\]

(34)

is the reciprocal of \(z(X)\).

**Proof of Lemma 4:** To show \(H_{p_0}(z)\) is a valid parity-check matrix of \(C\), it suffices to show that its row vectors belong to the row space of \(H_{p_0}\) and they are linearly independent. Since the row space of \(H_{p_0}\) is of dimension \(p_0\), the row space of \(H_{p_0}(z)\) is then the same as the row space of \(H_{p_0}\). Therefore, \(H_{p_0}(z)\) is a cyclic parity-check matrix for \(C\).

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

To prove part two, assuming that the row vectors of \(H_{p_0}(z)\) 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

\[
\alpha_0z^*_0 \oplus \alpha_1z^*_1 \oplus ... \oplus \alpha_{p_0-1}z^*_{p_0-1} = 0
\]

(35)

\(^2\)Different from previous sections, where column vectors are used, row vectors are used here.
\[
\alpha_0 z^*(X) + \alpha_1 Xz^*(X) + \cdots + \alpha_{p_0-1} X^{p_0-1}z^*(X) \equiv 0 \mod (X^n + 1) \quad (36a)
\]
\[
f^*(X) \left[ \alpha_0 h^*(X) + \alpha_1 Xh^*(X) + \cdots + \alpha_{p_0-1} X^{p_0-1}h^*(X) \right] \equiv 0 \mod (X^n + 1) \quad (36b)
\]
Noting that \( \text{GCD}(f^*(X), X^n + 1) = 1 \), thus
\[
[\alpha_0 + \alpha_1 X + \cdots + \alpha_{p_0-1} X^{p_0-1}]h^*(X) \equiv 0 \mod (X^n + 1) \quad (37a)
\]
\[\Leftrightarrow \alpha_0 h_0^* + \alpha_1 h_1^* + \cdots + \alpha_{p_0-1} h_{p_0-1}^* = 0 \quad (37b)\]
contradicts with the fact that row vectors of \( H_{p_0} \) are linearly independent. Thus, row vectors of \( H_{p_0}(z) \) are linearly independent.

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

\textbf{Definition 1:} [9][Ch.5] Let \( D = \{d_0, d_1, \ldots, d_q\} \) be a set of \( q + 1 \) non-negative integers such that \( 0 \leq d_0 < d_1 < \cdots < d_q \leq q(q+1) \), 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 \( d_i - d_j \equiv t \mod q(q+1) \), then \( D \) is a perfect simple \textbf{difference set} of order \( q \).

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

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

\[
H_{p_0} = \begin{bmatrix}
h^*(X) \\
X h^*(X) \\
\vdots \\
X^{p_0-1}h^*(X)
\end{bmatrix}_{p_0 \times n}
\begin{bmatrix}
h_0^* \\
h_1^* \\
\vdots \\
h_{p_0-1}^*
\end{bmatrix}_{p_0 \times n}
\]

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

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

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

\[
H_{p_0}(z) = \begin{bmatrix}
z^*(X) \mod (X^n + 1) \\
X z^*(X) \mod (X^n + 1) \\
\vdots \\
X^{p_0-1}z^*(X) \mod (X^n + 1)
\end{bmatrix}_{p_0 \times n}
\begin{bmatrix}
z_0^* \\
z_1^* \\
\vdots \\
z_{p_0-1}^*
\end{bmatrix}_{p_0 \times n}
\]

is a parity-check matrix of \( C \). By adding row vectors corresponding to \( X^i z^*(X) \mod (X^n + 1) \), \( p_0 \leq i \leq n - 1 \), to \( H_{p_0}(z) \), a \( n \times n \) redundant parity-check matrix \( H_n(z) \) is formed,

\[
H_n(z) = \begin{bmatrix}
z^*(X) \mod (X^n + 1) \\
X^{p_0-1}z^*(X) \mod (X^n + 1) \\
X^{n-1}z^*(X) \mod (X^n + 1)
\end{bmatrix}_{n \times n}
\begin{bmatrix}
z_0^* \\
z_{p_0-1}^* \\
z_{n-1}^*
\end{bmatrix}_{n \times n}
\]
which has both rows and columns weight $q + 1$. Then
\[
A_n(z) = \frac{1}{(q+1)^2} H_n(z) \tag{41}
\]
Furthermore, $1 = \tilde{\mu}_0 > \tilde{\mu}_1 = \tilde{\mu}_2 ... \tilde{\mu}_{n-1} = \frac{q}{(q+1)^2}$ are eigenvalues of $A_n(z)^T A_n(z)$, 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
\[
s(H_n(z)) \geq \frac{2}{q+1} - \frac{q}{(q+1)^2} (q^2 + q + 1) = q + 2 = d_{\min} \tag{42}
\]
Therefore, the stopping distance of $H_n(z)$ equals $d_{\min}$ of the code, and the stopping redundancy of the family of difference-set codes, $\rho(C) \leq n = \text{the length of the code.}$

Furthermore, for redundant parity-check matrix $H_n(z)$, 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,
\[A_d[d_{\min}, C] = A_s[s(H_n(z)), H_n(z)] \tag{43}\]

**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, assume 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 $b_j, 2 \leq j \leq q + 2$, such that $y_j \in N(b_j)$ because $\{b_1, b_2, ..., b_{q+2}\}$ is a stopping set. However, as $|N(b_1) \cap N(b_2)| = ... = |N(b_1) \cap N(b_{q+2})| = 1$ and $|N(b_j)| = q + 1$, it can be shown that there is only one such $b_j$ for each $y_j$ so that all neighbors of $b_1$ are of degree two. Similarly, we can prove this for $b_{j'}, 2 \leq j' \leq q + 2$. Thus, let $b_j = 1$ for $1 \leq j \leq q + 2$ 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 $C_{21}$ derived from the difference set $D = \{0, 3, 4, 9, 11\}$, where $h(X) = z(X) = 1 + X^3 + X^4 + X^9 + X^{11}, d_{\min} = 6$ and $A_d[6, C_{21}] = 168$. It can be shown that $\rho(C_{21}) \leq 12$, and $A_s[s(H_p(z)), H_p(z)] = 168$ if $p \geq 15$, where Theorem 5 and Theorem 6 provide bounds $\rho(C_{21}) \leq 21$ and $p \geq 21$, respectively.

Figure 1 evaluates the performance of iterative decoding for $C_{21}$ on the erasure channel as a function of $p$, the number of rows of the cyclic redundant parity-check matrix $H_p(z)$ 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.
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.

REFERENCES