IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

DOI:10.1587/transfun.2024EAL2062

Publicized:2024/11/12

This advance publication article will be replaced by the finalized version after proofreading.

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY

The Institute of Electronics, Information and Communication Engineers

Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

LETTER

Binary Cycle Codes Have Optimal Stopping Redundancy*

Yingnan QI[†,††a)], **Chuhong TANG**[†,††b)], **Haiyang LIU**[†c)], ***Nonmembers**, and* **Lianrong MA**[†††d)], ***Member***

SUMMARY In this letter, we prove that binary cycle codes constructed from simple connected graphs have optimal stopping redundancy. For such a code, we also obtain a full-rank parity-check matrix whose number of minimum-size stopping sets is equal to the number of minimum-weight codewords of the code.
key words: *Binary cycle codes, minimum distance, stopping distance, stopping redundancy*

1. Introduction

It has been shown that the performance of iterative decoding of a binary linear code over the binary erasure channel (BEC) depends on the choice of the parity-check matrix of the code [1]-[3]. To be specific, suppose $\boldsymbol{H}$ is a parity-check matrix of a binary linear code C whose minimum distance is d. The performance of iterative decoding over the BEC can be characterized by certain combinatorial structures, called *stopping sets*, of $\boldsymbol{H}$. The minimum size of the non-empty stopping sets is called the *stopping distance* of $\boldsymbol{H}$ and is denoted by $s(\boldsymbol{H})$, which should be maximized for desirable performance. It can be shown that the inequality $s(\boldsymbol{H}) \leq d$ holds for any parity-check matrix $\boldsymbol{H}$ of C. The *stopping redundancy* of C, $\rho(C)$, is defined as the minimum number of rows in a parity-check matrix $\boldsymbol{H}$ of C for which $s(\boldsymbol{H}) = d$. (Note that there always exists such a parity-check matrix $\boldsymbol{H}$ for a code C [2].)

In particular, if $\rho(C)$ is equal to the redundancy of C, then C is said to have *optimal stopping redundancy*. In other words, there exists a full-rank parity-check matrix $\boldsymbol{H}$ (i.e., the rows in $\boldsymbol{H}$ are linearly independent) of C for which $s(\boldsymbol{H}) = d$. It is known from [2, Theorem 3] that any binary linear code with minimum distance ≤ 3 has optimal stopping redundancy. On the other hand, finding binary linear codes with minimum distance ≥ 4 as well as optimal stopping redundancy is an interesting but challenging research problem [4]. To date, only sporadic families of binary linear codes are proved to have optimal stopping redundancy [4]-[7]. Due to its theoretical significance, it is deserved to find more binary linear codes that have optimal stopping redundancy.

In this letter, we focus on *binary cycle codes* (also known as circuit codes), an important class of graph-theoretic codes that have nice structural properties [8]. From the practical point of view, the structural properties allow us to design efficient algorithms for these codes. For instance, the encoding and decoding processes of a binary cycle code can be performed iteratively, with complexity linear in the code length. From the theoretical point of view, these codes are amenable to analysis thanks to their structural properties. Several structural parameters of these codes have been determined in the previous works (see e.g., [9]-[12]), which is helpful in understanding the code performances.

We consider binary cycle codes constructed from simple connected graphs in this letter. By construction, a parity-check matrix $\boldsymbol{H}$ of a binary cycle code C is the incidence matrix of the graph from which C is constructed. It is known that $\boldsymbol{H}$ contains one redundant row. We show that $\boldsymbol{H}'$ is a full-rank parity-check matrix of C, where $\boldsymbol{H}'$ is obtained by removing a row from $\boldsymbol{H}$. Then we prove that $\boldsymbol{H}'$ has the following property: A stopping set of $\boldsymbol{H}'$ with size $\leq d$ is a stopping set of $\boldsymbol{H}$ and vice versa, where d is the minimum distance of C. The property, together with the known results, indicates that C has optimal stopping redundancy. As a byproduct, we conclude from the property that the number of minimum-size stopping sets of $\boldsymbol{H}'$ is equal to that of minimum-weight codewords in C. This implies that the iterative decoding of a binary cycle code from a simple connected graph using a parity-check matrix with the minimum number of rows is asymptotically optimal over the BEC.

2. Preliminaries

In this section, we introduce the concepts and known results that will be used in the following discussions. First, let us introduce some specific notations. We let $\mathbb{F}_2 = \{0, 1\}$ be the binary Galois field. Suppose $\boldsymbol{A}$ is a binary matrix, $\mathrm{rank}(\boldsymbol{A})$ is the rank of $\boldsymbol{A}$ over $\mathbb{F}_2$. The support of a vector $\boldsymbol{a}$ is the set $\{i : a_i \neq 0\}$, where a_i is the i-th entry of $\boldsymbol{a}$. The size of the support of $\boldsymbol{a}$ is called the Hamming weight (in brief, weight) of $\boldsymbol{a}$. For a finite set $\mathcal{A}$, $|\mathcal{A}|$ is the size of $\mathcal{A}$. Suppose $\mathcal{S}$ is a subset of column indices of $\boldsymbol{A}$, the restriction of $\boldsymbol{A}$ onto the set $\mathcal{S}$ is denoted by $\boldsymbol{A}_{\mathcal{S}}$, i.e., $\boldsymbol{A}_{\mathcal{S}}$ is a submatrix of $\boldsymbol{A}$ that contains the columns whose indices are in $\mathcal{S}$.

[†]Institute of Microelectronics, Chinese Academy of Sciences, Beijing 100029, China.
[††]University of Chinese Academy of Sciences, Beijing 100049, China.
[†††]Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China.
*This work is supported by the National Natural Science Foundation of China (NSFC) under Grant 62271482.
a) E-mail: qiyingnan@ime.ac.cn
b) E-mail: tangchuhong@ime.ac.cn
c) E-mail: liuhaiyang@ime.ac.cn (Corresponding author)
d) E-mail: malian@tsinghua.edu.cn

2.1 Stopping sets, stopping distance and stopping redundancy

Assume that C is an $[n, k, d]$ binary linear code specified by a parity-check matrix $\boldsymbol{H} \in \mathbb{F}_2^{m\times n}$, where n, k, and d are the length, dimension, and minimum distance of C, respectively. In this work, $\boldsymbol{H}$ is allowed to have redundant rows, so we have $m \geq \mathrm{rank}(\boldsymbol{H}) = n - k$, where the equality holds if and only if $\boldsymbol{H}$ is of full-rank.

Definition 1 ([2]): Suppose $\boldsymbol{H}$ is a parity-check matrix of binary linear code C. A subset $\mathcal{S}$ of column indices of $\boldsymbol{H}$ is said to be a *stopping set* if $\boldsymbol{H}_{\mathcal{S}}$ does not contain a row of weight 1. The *stopping distance* of $\boldsymbol{H}$, denoted by $s(\boldsymbol{H})$, is the minimum size of the non-empty stopping sets of $\boldsymbol{H}$.

Note that the stopping set and stopping distance depend on the specific parity-check matrix that describes a binary linear code. Note also that the empty set is a trivial stopping set for any parity-check matrix. In the following, we only consider the non-empty stopping sets.

Lemma 1 ([2]): Let C be a binary linear code and $\boldsymbol{H}$ be a parity-check matrix of C. It holds that $s(\boldsymbol{H}) \leq d$.

It is known that there always exists a parity-check matrix $\boldsymbol{H}$ for a binary linear code C satisfying $s(\boldsymbol{H}) = d$ [2]. From the practical point of view, it is desirable to find such a parity-check matrix whose number of rows is as small as possible in order to maintain a reasonable decoding complexity.

Definition 2: Suppose C is an $[n, k, d]$ binary linear code and $\boldsymbol{H}$ is a parity-check matrix of C. The *stopping redundancy* $\rho(C)$ is defined as the minimum number of rows in $\boldsymbol{H}$ such that $s(\boldsymbol{H}) = d$ holds. If $\rho(C) = n - k$, then C is said to have *optimal stopping redundancy*.

Remark 1: We know from the above definition that we can find a full-rank parity-check matrix $\boldsymbol{H}$ such that $s(\boldsymbol{H}) = d$ holds for a binary linear code C that has optimal stopping redundancy.

Apart from the stopping distance, the number $S_{\min}(\boldsymbol{H})$ of minimum-size stopping sets in a parity-check matrix $\boldsymbol{H}$ is crucial in the evaluation of the performance of iterative decoding over the BEC. In particular, it is of great interest to find a parity-check matrix $\boldsymbol{H}$ for C satisfying $s(\boldsymbol{H}) = d$ as well as $S_{\min}(\boldsymbol{H}) = A_{\min}$, where $A_{\min}$ is the number of minimum-weight codewords in C.† In this case, we can expect the performance of iterative decoding of C using $\boldsymbol{H}$ is close to that of optimal decoding, especially when the channel erasure probability is small. For a more detailed discussion, see e.g., [3].

2.2 Binary cycle codes

A binary cycle code is a linear code constructed from a graph. In the following discussions, we always assume that a graph is simple and connected. For terminologies in graph theory, the readers can refer to [13].

†In general, we have $S_{\min}(\boldsymbol{H}) \geq A_{\min}$ for a parity-check matrix $\boldsymbol{H}$ such that $s(\boldsymbol{H}) = d$. There always exists a parity-check matrix such that the lower bound is tight [3].

Definition 3: Suppose $\mathcal{G}$ is a simple connected graph that contains m vertices and n edges. The incidence matrix of $\mathcal{G}$, $\boldsymbol{H} := \boldsymbol{H}(\mathcal{G})$, is a binary matrix of size $m \times n$. Let C be a binary linear code specified by the parity-check matrix $\boldsymbol{H}$. Then the code C is called a *binary cycle code*.

Note that each column of $\boldsymbol{H}$ is of weight 2, since two vertices are incident with an edge. Note also that each codeword in C corresponds to a simple cycle of $\mathcal{G}$ or a union of simple cycles with disjoint edges, which indicates that the minimum distance of C is equal to the girth of $\mathcal{G}$, i.e., the length of the shortest cycle in $\mathcal{G}$.

For the analysis of iterative decoding, it is convenient to represent $\boldsymbol{H}$ by a bipartite graph $\mathcal{T}$, called the Tanner graph of $\boldsymbol{H}$ [14], which can be obtained by associating each vertex (resp., edge) of $\mathcal{G}$ with a check node (resp., variable node) in $\mathcal{T}$, respectively. Denote the girth of $\mathcal{T}$ (resp., $\mathcal{G}$) by g (resp., g_d). By construction, we can obtain $g_d = g/2$.

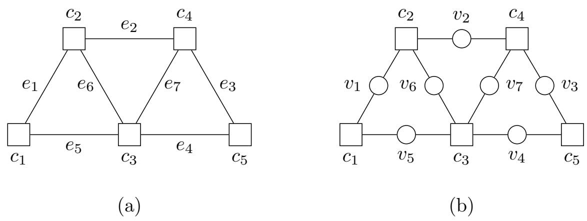

Fig. 1 An illustrative example. (a) A graph $\mathcal{G}$ with 5 vertices and 7 edges. For convenience, each vertex in $\mathcal{G}$ is denoted by a square. The incidence matrix $\boldsymbol{H}$ of $\mathcal{G}$ specifies a $[7, 3, 3]$ binary cycle code. (b) The Tanner graph $\mathcal{T}$ of $\boldsymbol{H}$. For convenience, each check (resp., variable) node in $\mathcal{T}$ is denoted by a square (resp., cycle). The edges in $\mathcal{T}$ are not labelled for notational simplicity.

In order to illustrate these concepts, consider the illustrative example in Figure 1. Figure 1(a) provides a simple connected graph $\mathcal{G}$, whose incidence matrix is

$$\boldsymbol{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix},$$

where the j-th row of $\boldsymbol{H}$ corresponds to the vertex c_j in $\mathcal{G}$, and the i-th column of $\boldsymbol{H}$ corresponds to the edge e_i in $\mathcal{G}$. The Tanner graph $\mathcal{T}$ of $\boldsymbol{H}$ is shown in Figure 1(b), where the variable node v_i corresponds to the edge e_i in $\mathcal{G}$. By inspection, we know that $\boldsymbol{H}$ is the parity-check matrix of a $[7, 3, 3]$ binary cycle code.

Lemma 2 ([8]): Let $\boldsymbol{H}$ be the incidence matrix of a simple connected graph $\mathcal{G}$. If $\boldsymbol{H}$ has m rows, then $\mathrm{rank}(\boldsymbol{H}) = m - 1$.

3. Main Results

In this section, we present the main results of this letter. The following lemma states the stopping distance and the number of minimum-size stopping sets of a binary cycle code specified by a parity-check matrix that is the incidence matrix of a simple connected graph.

Lemma 3: Let $\boldsymbol{H}$ be the incidence matrix of a simple connected graph with girth g_d. Suppose C is a binary cycle code with parity-check matrix $\boldsymbol{H}$. Then we have $s(\boldsymbol{H}) = d = g_d$ and $S_{\min}(\boldsymbol{H}) = A_{\min}$.

Proof: In fact, the equality $s(\boldsymbol{H}) = g/2$ follows from the results in [15, Section II], where g is the girth of the Tanner graph of $\boldsymbol{H}$. Since C is a binary cycle code, we have $d = g_d = g/2$. Therefore, we have $s(\boldsymbol{H}) = d = g_d$.

For a parity-check matrix $\boldsymbol{H}$ with uniform column weight γ, we know from [16, Corollary 1] that the equality $S_{\min}(\boldsymbol{H}) = A_{\min}$ holds if $d = d_L$, where

$$d_L = \begin{cases} 1+\gamma+\sum\limits_{i=1}^{(g-6)/4}\gamma(\gamma-1)^i, & g/2 \text{ odd},\\ 1+\gamma+\sum\limits_{i=1}^{(g-8)/4}\gamma(\gamma-1)^i+(\gamma-1)^{(g-4)/4}, & g/2 \text{ even}.\end{cases}$$

Hence, we only need to prove that $d_L = d = g/2$ for the incidence matrix $\boldsymbol{H}$ of a simple connected graph. In this case, we have $\gamma = 2$. If $g/2$ is odd, we can let $g/2 = 2t+1$, where t is a positive integer. Then we have $d_L = 1+2+2(t-1) = 2t+1 = g/2$. If $g/2$ is even, we can also prove that $d_L = g/2$ in a similar manner. □

Remark 2: Note that the authors use the notation d to represent the column weight of a parity-check matrix in [15]. In this letter, we follow the convention of coding theory and use the notation d to represent the minimum distance of a code.

The following two lemmas are necessary for establishing our results.

Lemma 4: Let C be a binary cycle code specified by an $m \times n$ parity-check matrix $\boldsymbol{H}$ that is the incidence matrix of a simple connected graph. Then the matrix $\boldsymbol{H}'$ is a full-rank parity-check matrix of C, where $\boldsymbol{H}'$ is obtained by removing a row from $\boldsymbol{H}$.

Proof: Assume that the m rows in $\boldsymbol{H}$ are $\boldsymbol{h}_1, \dots, \boldsymbol{h}_{m-1}$ and $\boldsymbol{h}$, where $\boldsymbol{h}_1, \dots, \boldsymbol{h}_{m-1}$ are the rows of $\boldsymbol{H}'$. Since each column of $\boldsymbol{H}$ is of weight 2, we have $\boldsymbol{h}+\sum_{i=1}^{m-1}\boldsymbol{h}_i = \boldsymbol{0}$, where $\boldsymbol{0}$ is the zero vector of length n. In other words, it holds that $\boldsymbol{h} = \sum_{i=1}^{m-1}\boldsymbol{h}_i$.

Suppose $\bar{\boldsymbol{h}}$ is a vector in the row space of $\boldsymbol{H}$. Then $\bar{\boldsymbol{h}}$ is the linear combination of the rows $\boldsymbol{h}_1, \dots, \boldsymbol{h}_{m-1}$ and $\boldsymbol{h}$. Because $\boldsymbol{h} = \sum_{i=1}^{m-1}\boldsymbol{h}_i$, we conclude that $\bar{\boldsymbol{h}}$ is the linear combination of the $m-1$ rows $\boldsymbol{h}_1, \dots, \boldsymbol{h}_{m-1}$. This, together with the fact that $\mathrm{rank}(\boldsymbol{H}) = m-1$, indicates that $\boldsymbol{h}_1, \dots, \boldsymbol{h}_{m-1}$ are linearly independent. As a consequence, $\boldsymbol{H}'$ is a full-rank parity-check matrix of C. □

Lemma 5: Let C be a binary cycle code specified by an $m \times n$ parity-check matrix $\boldsymbol{H}$ that is the incidence matrix of a simple connected graph $\mathcal{G}$. Let $\mathcal{S}$ be a subset of column indices of $\boldsymbol{H}$, where $|\mathcal{S}|$ is less than or equal to the minimum distance of C. Suppose $\boldsymbol{H}'$ is obtained by removing a row from $\boldsymbol{H}$. Then $\mathcal{S}$ is a stopping set of $\boldsymbol{H}'$ *if and only if* $\mathcal{S}$ is a stopping set of $\boldsymbol{H}$.

Proof: Since the graph from which binary cycle code C is constructed is simple, we have $d \geq 3$, where d is the minimum distance of C. Hence, both $\boldsymbol{H}'$ and $\boldsymbol{H}$ do not contain stopping sets with size less than 3. (Suppose to the contrary. Let $\mathcal{S}$ be a stopping set of $\boldsymbol{H}'$ or $\boldsymbol{H}$ with size less than 3. We construct a binary vector $\boldsymbol{x}$ of length n whose support is $\mathcal{S}$. Because $\boldsymbol{H}'_{\mathcal{S}}$ or $\boldsymbol{H}_{\mathcal{S}}$ does not contain a row of weight 1, we conclude that $\boldsymbol{x}$ is a codeword in C whose weight is less than 3, a contradiction.) In the following, we assume that $|\mathcal{S}| = s \geq 3$. Since the minimum distance of C is equal to g_d, we have $s \leq g_d$.

We first prove the "if" part of the lemma. With proper row permutations, $\boldsymbol{H}_{\mathcal{S}}$ can be written as

$$\boldsymbol{H}_{\mathcal{S}} = \begin{bmatrix} \boldsymbol{H}'_{\mathcal{S}} \\ \boldsymbol{h}_{\mathcal{S}} \end{bmatrix}.$$

Since $\mathcal{S}$ is a stopping set of $\boldsymbol{H}$ and $\boldsymbol{H}'_{\mathcal{S}}$ is a submatrix of $\boldsymbol{H}_{\mathcal{S}}$, $\boldsymbol{H}'_{\mathcal{S}}$ does not contain a row of weight 1. This indicates that $\mathcal{S}$ is a stopping set of $\boldsymbol{H}'$.

Now we prove the "only if" part of the lemma. Assume that $\mathcal{S}$ is a stopping set of $\boldsymbol{H}'$ but $\mathcal{S}$ is not a stopping set of $\boldsymbol{H}$. Under the assumption, we conclude that $\boldsymbol{h}_{\mathcal{S}}$ is a row vector of weight 1 and $\boldsymbol{H}'_{\mathcal{S}}$ does not contain a row of weight 1. Denote the entry in the j-th row and the i-th column of $\boldsymbol{H}'_{\mathcal{S}}$ by h_{ji}. Without loss of generality, we can assume that $\boldsymbol{h}_{\mathcal{S}} = [1\ 0\ \cdots\ 0]$. We know that the first column of $\boldsymbol{H}'_{\mathcal{S}}$ is of weight 1. Without loss of generality, we can let $h_{11} = 1$. Since $\boldsymbol{H}'_{\mathcal{S}}$ does not contain a row of weight 1, there exists at least one more entry 1 in the first row. With proper column permutations, we can let $h_{12} = 1$. Because the weight of the second column of $\boldsymbol{H}'_{\mathcal{S}}$ is 2, there is an entry 1 in the last $m-2$ rows of the column. With proper row permutations, we can assume that $h_{22} = 1$. Using the fact that $\boldsymbol{H}'_{\mathcal{S}}$ does not contain a row of weight 1, we conclude that there exists at least one more entry 1 in the second row, which can be assumed in the third column, i.e., $h_{23} = 1$. Because the weight of the third column of $\boldsymbol{H}'_{\mathcal{S}}$ is 2, there is an entry 1 in the column in addition to h_{23}. If this entry 1 is in the first row, i.e., $h_{13} = 1$, we conclude that the Tanner graph of $\boldsymbol{H}$ has a cycle of length 4. Equivalently, $\mathcal{G}$ has a cycle of length 2, a contradiction. As a result, this entry 1 is in the last $m-3$ rows of the third column. With proper row permutations, we can assume that $h_{33} = 1$. Repeat the above processes, we can obtain the following matrix of size $(s-1) \times (s-1)$,

$$\begin{bmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & 1 & \ddots & \\ & & & \ddots & 1 \\ & & & & 1 \end{bmatrix},$$

which is a submatrix of $\boldsymbol{H}'_{\mathcal{S}}$ after proper row and column permutations.

Let us consider the $(s-1)$-th row. Using the fact that $\boldsymbol{H}'_{\mathcal{S}}$ does not contain a row of weight 1, we conclude that there exists at least one more entry 1 in this row. Moreover, this entry 1 cannot be in any of the first $s-1$ columns. With proper column permutations, we can suppose that $h_{s-1,s}=1$. Because the weight of the s-th column of $\boldsymbol{H}'_{\mathcal{S}}$ is 2, there is an entry 1 in the column in addition to $h_{s-1,s}$. If $h_{i,s}=1 (1 \le i \le s-2)$, we conclude that the Tanner graph of $\boldsymbol{H}$ has a cycle of length $2(s-i)$. In other words, $\mathcal{G}$ has a cycle of length $s-i \le g_d - i < g_d$, a contradiction. As a consequence, the vector $[0 \cdots 0\ 1]$ of length s is a row of $\boldsymbol{H}'_{\mathcal{S}}$. This, however, contradicts the assumption that $\mathcal{S}$ is a stopping set of $\boldsymbol{H}'$. □

Theorem 1: With the above notations, we have $s(\boldsymbol{H}') = g_d = d$ and $S_{\min}(\boldsymbol{H}') = A_{\min}$.

Proof: By Lemmas 3 and 5, we know that $\boldsymbol{H}'$ does not contain non-empty stopping sets with size less than d. Hence, we have $s(\boldsymbol{H}') \ge g_d$. This, together with $s(\boldsymbol{H}') \le g_d = d$, leads to $s(\boldsymbol{H}') = g_d = d$. We can also conclude from Lemma 5 that the numbers of minimum-size stopping sets of $\boldsymbol{H}$ and $\boldsymbol{H}'$ are equal. By Lemma 3, we have $S_{\min}(\boldsymbol{H}) = S_{\min}(\boldsymbol{H}') = A_{\min}$. □

The following corollary is a direct consequence of Definition 2 and Theorem 1.

Corollary 1: Let C be a binary cycle code constructed from a simple connected graph. Then C has optimal stopping redundancy.

As mentioned in Section 1, there are some binary linear codes in the literature that have been proved to have optimal stopping redundancy. To the best of our knowledge, however, the codes investigated in this letter are the first class of binary linear codes for which a full-rank parity-check matrix $\boldsymbol{H}'$ satisfying $s(\boldsymbol{H}') = d \ge 3$ as well as $S_{\min}(\boldsymbol{H}') = A_{\min}$ can be constructed for each code.

Consider binary Hamming codes, an important class of linear codes invented in the early days of error correction coding. Let m be a positive integer and $m \ge 2$. The binary Hamming code $\mathcal{H}_m$ is a $[2^m-1, 2^m-m-1, 3]$ linear code specified by a full-rank parity-check matrix $\boldsymbol{H}_m$ of size $m \times (2^m-1)$ that contains all the nonzero binary column vectors of length m. By [2, Theorem 3], we conclude that $\mathcal{H}_m$ has optimal stopping redundancy. For $\mathcal{H}_m$, it also holds that [17] $S_{\min}(\boldsymbol{H}_m) = \frac{1}{6}(5^m - 3^{m+1} + 2^{m+1})$ and $A_{\min} = \frac{1}{6}(4^m - 3 \times 2^m + 2)$. Clearly, we have $S_{\min}(\boldsymbol{H}_m) > A_{\min}$ for any $m \ge 3$. (Note that the full-rank parity-check matrix of $\mathcal{H}_m$ is unique up to the equivalence. Note also that the minimum number of rows of a parity-check matrix $\boldsymbol{H}$ of $\mathcal{H}_m$ satisfying $S_{\min}(\boldsymbol{H}) = A_{\min}$ has been considered in [3].) For other binary linear codes in the literature that have been proved to have optimal stopping redundancy, it is unknown whether there exists a full-rank parity-check matrix whose number of minimum-size stopping sets is equal to the number of minimum-weight codewords for each code.

It is known from [3] that a binary linear code C with parity-check matrix $\boldsymbol{H}$ satisfying $s(\boldsymbol{H}) = d$ as well as $S_{\min}(\boldsymbol{H}) = A_{\min}$ indicates that the iterative decoding of C using $\boldsymbol{H}$ is asymptotically optimal over the BEC. Our Theorem 1 suggests that such performance can be achieved through the use of a full-rank parity-check matrix for a binary cycle code constructed from a simple connected graph, which is desirable in terms of the performance and complexity trade-off.[†]

4. Conclusion and Future Work

In this letter, we have constructed a full-rank parity-check matrix for a binary cycle code C from a simple connected graph, where the constructed parity-check matrix contains no stopping set whose size is less than the minimum distance of C. Moreover, the number of minimum-size stopping sets of the constructed parity-check matrix is equal to that of minimum-weight codewords of C. These not only indicate that C has optimal stopping redundancy but also imply that C can achieve asymptotically optimal performance over the BEC under iterative decoding using the constructed parity-check matrix.

As a future work, we will try to find more families of binary linear codes with optimal stopping redundancy. It is also deserved to find binary linear codes with parity-check matrices containing a minimum number of rows such that $s(\boldsymbol{H}) = d$ and $S_{\min}(\boldsymbol{H}) = A_{\min}$.

Acknowledgments

The authors greatly appreciate the reviewer's valuable comments.

References

[1] 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 erasure channel," IEEE Trans. Inf. Theory, vol. 48, no. 6, pp. 1570-1579, Jun. 2002.

[2] M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes," IEEE Trans. Inf. Theory, vol. 52, no. 3, pp. 922-932, Mar. 2006.

[3] J. H. Weber and K. A. S. Abdel-Ghaffar, "Results on parity-check matrices with optimal stopping and/or dead-end set enumerators," IEEE Trans. Inf. Theory, vol. 54, no. 3. pp. 1368-1374, Mar. 2008.

[4] T. Etzion, "On the stopping redundancy of Reed-Muller codes," IEEE Trans. Inf. Theory, vol. 52, no. 11, pp. 4867-4879, Nov. 2006.

[5] M. Hivadi and M. Esmaeili, "On the stopping distance and stopping redundancy of product codes," IEICE Trans. Fundamentals, vol. E91-A, no. 8, pp. 2167-2173, Aug. 2008.

[6] M. Esmaeili and V. Ravanmehr, "Stopping sets of binary parity-check matrices with constant weight columns and stopping redundancy of the associated codes," Utilitas Math., vol. 76, pp. 265-276, Jul. 2008.

[7] M. Esmaeili and V. Ravanmehr, "Two classes of optimal stopping redundancy codes," Ars Combinatoria, vol. 92, pp. 463-471, Jul. 2009.

[8] S. Hakimi and J. Bredeson, "Graph theoretic error-correcting codes," IEEE Trans. Inf. Theory, vol. IT-14, no. 4, pp. 584-591, Jul. 1968.

[9] R. Koetter, W.-C. W. Li, P. O. Vontobel, and J. L. Walker, "Characterizations of pseudo-codewords of (low-density) parity-check codes,"

[†] We mention that the minimum distance of cycle codes constructed from simple connected graphs is at most logarithmic in the code length, see e.g., [15]. This suggests that these codes have relatively modest minimum distance. Nevertheless, our results indicate that these codes can achieve asymptotically optimal performance over the BEC with low complexity.

Adv. in Math., vol. 213, no. 1, pp. 205-229, Aug. 2007.
[10] H. D. Pfister and P. O. Vontobel, "On the relevance of graph covers and zeta functions for the analysis of SPA decoding of cycle codes," in Proc. IEEE Int. Symp. Inf. Theory, Istanbul, Turkey, pp. 3000-3004, Jul. 2013.
[11] N. Axvig and D. Dreher, "Graphical characterizations of linear programming pseudocodewords for cycle codes," IEEE Trans. Inf. Theory, vol. 59, no. 9, pp. 5917-5934, 2013.
[12] H. Liu and L. Ma, "Further results on the separating redundancy of binary linear codes," IEICE Trans. Fundamentals, vol. E102-A, no. 10, pp. 1420-1425, Oct. 2019.
[13] R. J. Wilson. Introduction to Graph Theory, 5th edition. England: Prentice Hall, 2010.
[14] S. Lin and D. J. Costello Jr., Error Correcting Coding: Fundamentals and Applications, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2004.
[15] A. Orlitsky, R. Urbanke, K. Viswanathan, and J. Zhang, "Stopping sets and the girth of Tanner graphs," in Proc. IEEE Int. Symp. Inf. Theory, Lausanne, Switzerland, Jun. 30-Jul. 5, 2002, p. 2.
[16] S.-T. Xia and F.-W. Fu, "Minimum pseudoweight and minimum pseudocodewords of LDPC codes," IEEE Trans. Inf. Theory, vol. 54, no. 1, pp. 480-485, Jan. 2008.
[17] K. A. S. Abdel-Ghaffar and J. H. Weber, "Complete enumeration of stopping sets of full-rank parity-check matrices of Hamming codes," IEEE Trans. Inf. Theory, vol. 53, no. 9. pp. 3196-3201, Sep. 2007.