www.combinatorics.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. 7 No. 4 (2018), pp. 1-6.

www.ui.ac.ir

ON THE MINIMUM STOPPING SETS OF PRODUCT CODES

MORTEZA HIVADI* AND AKBAR ZARE CHAVOSHI

Communicated by Dianhua Wu

Abstract. It is shown that the certain combinatorial structures called stopping sets have the important role in analysis of iterative decoding. In this paper, the number of minimum stopping sets of a product code is determined by the number of the minimum stopping sets of the corresponding component codes. As an example, the number of minimum stopping sets of the $r-$dimensional SPC product code is computed.

1. Introduction

Let F_2 be the field of 2 elements. A binary linear $[n, k]$ code C is a k-dimensional vector subspace of the vector space F_2^n, where $F_2^n = \{ (x_0, x_1, \ldots, x_{n-1}) \mid x_i \in F_2 \}$. The elements of C are called codewords and the Hamming weight of a codeword is the number of non-zero coordinates. An $[n, k, d]$ code is an $[n, k]$ code with minimum (non-zero) Hamming weight d. A generator matrix for a code C is any $k \times n$ matrix G whose rows form a basis for C. The dual code $C^{\perp}$ of C is defined as $C^{\perp} = \{ x \in F_2^n \mid x \,.\, c = 0 \; for \; all \; c \in C \}$. An $(n-k) \times n$ generator matrix H of $C^{\perp}$ is called a parity check matrix of C.

Recently, it has shown that the performance of linear codes under iterative decoding over the BEC is determined by certain combinatorial structures called stopping sets [8]. Let us define the concept of a stopping set in the next section. The size of the smallest non-empty stopping set in a parity-check

MSC(2010): Primary: 94B25; Secondary: 94B35.
Keywords: Stopping set, Stopping distance, Product code.
Received: 21 December 2016, Accepted: 23 December 2017.
*Corresponding author.

DOI: http://dx.doi.org/10.22108/toc.2017.101199.1465

.

matrix H of C is called the stopping distance of H. This later concept is denoted by $s(H)$. It was shown that the problem of determining the stopping distance of a parity-check matrix is a NP-hard problem [3]. The number of stopping sets of H of size i is denoted by $S_i(H)$.

One method for constructing powerful codes from other codes is the product coding technique. Product codes were introduced by Elias [2] in 1954. These codes are a subclass of concatenated codes. Consider two binary linear codes R and C with parameters $[n, k, d]$ and $[n', k', d']$, respectively. The product code $P = R \bigotimes C$ consists of all the matrices with all rows in the code R and all columns in the code C. The component codes R and C are called the row code and the column code, respectively. The product code P is a binary linear $[nn', kk', dd']$ code. The minimum codewords of the product code $R \bigotimes C$ are determined by the minimum codewords of the component codes R and C [5]. The number of the minimum stopping sets has a crucial role in performance of C under iterative decoding akin to the role of number of the minimum codewords of C under maximum-likelihood decoding over BEC when the erasure probability is small [10, 11]. In this paper the number of minimum stopping sets of the product code $R \bigotimes C$ is determined by the number of the minimum stopping sets of the corresponding component codes.

The paper is organized as follows. The number of minimum stopping sets of a product code is determined in Section 2. Computing of the number of minimum stopping sets of the $r-$dimensional SPC product code, is given in Section 3.

2. Minimum Stopping Sets of product codes

Let C be a binary linear $[n, k, d]$ code and let $H = (h_{ij})$ be a parity-check matrix of C. We index the columns of H by $1, 2, \ldots, n$ and consider S as a subset of $\{1, 2, \ldots, n\}$. Let $N_r(H)$ denote the number of rows of H and H_S denote the $N_r(H) \times |S|$ submatrix of H consisting of columns indexed by S.

A set S is the support of a codeword if and only if all rows in H_S have even weight, i.e.

$$|\{j \in S \ : \ h_{ij} = 1\}| = 0 \ (mod\ 2) \ \forall \ i = 1, 2, \ldots, N_r(H).$$

Definition 2.1. For a given parity-check matrix H of C, a subset S of column indices of H is called a *stopping set* in H if H_S has no row of weight one, i.e.

$$|\{j \in S \ : \ h_{ij} = 1\}| \neq 1 \ \forall \ i = 1, 2, \ldots, N_r(H).$$

The size of a stopping set S is equal to the number of elements in S. A stopping set of the smallest size is called a *minimum stopping set*. It follows from definition that the support of any codeword is a stopping set. Hence $s(H) \leq d$.

In this paper H_R and H_C stand for parity-check matrices of two binary linear codes R and C with parameters $[n, k, d]$ and $[n', k', d']$, respectively. It is known that the product code $R \bigotimes C$ has the following parity-check matrix H_P [9] wherein "$\otimes$" stands for the Kronecker product operation. Note

DOI: http://dx.doi.org/10.22108/toc.2017.101199.1465

that the rows of H_P may be linearly dependent.

$$H_P = \begin{pmatrix} H_R \otimes I_{n'} \\ I_n \otimes H_C \end{pmatrix} \tag{2.1}$$

Definition 2.2. Consider the product code $R \otimes C$ defined by two given codes R and C of lengths n and n', respectively. The set $B_i := \{i, i+n', \ldots, i+(n-1)n'\}$, $1 \leq i \leq n'$, is called the ith *row-set* and the set $B'_j := \{(j-1)n'+1, (j-1)n'+2, \cdots, (j-1)n'+n'\}$, $1 \leq j \leq n$, is called the jth *column-set*. Let E be a subset of $\{1, 2, \ldots, nn'\}$. For each row-set B_i and column-set B'_j we set $E_i := \{(a-i)/n'+1 \ : a \in B_i \cap E\ \}$ and $E'_j := \{a-(j-1)n' \ : a \in B'_j \cap E\ \}$; note that $(a-i)/n'$ is a nonnegative integer.

The stopping sets in the parity-check matrix H_P of the product code $R \bigotimes C$ are determined by stopping sets in the parity-check matrices H_R and H_C of the corresponding component code R and C, respectively [6].

Lemma 2.3. [6] A subset E of $\{1, 2, \ldots, nn'\}$ is a stopping set in H_P, given by (2.1), if and only if for each row-set B_i with $B_i \cap E \neq \emptyset$, E_i is a stopping set in H_R and for each column-set B'_j satisfying $B'_j \cap E \neq \emptyset$, E'_j is a stopping set in H_C.

Lemma 2.4. [6] Let $S_R = \{i_1, i_2, \ldots, i_r\}$ and $S_C = \{j_1, j_2, \ldots, j_c\}$ be two stopping sets in the parity-check matrices H_R and H_C, respectively. Then the set S_{RC} defined by (2.2) is a stopping set in H_P.

$$\begin{aligned} S_{RC} = \{&(i_1-1)n'+j_1, (i_1-1)n'+j_2, \ldots, (i_1-1)n'+j_c, \\ &(i_2-1)n'+j_1, (i_2-1)n'+j_2, \ldots, (i_2-1)n'+j_c, \\ &\ldots, (i_r-1)n'+j_1, (i_r-1)n'+j_2, \ldots, (i_r-1)n'+j_c\}. \end{aligned} \tag{2.2}$$

The stopping set in form (2.2) is called the *obvious stopping set* of the product code. The size of S_{RC} is equal to the product of the size of stopping sets S_R and S_C.

Example 2.5. Let R be the $[2, 1, 2]$ binary code and C be the $[8, 4, 4]$ Reed-Muller code with parity-check matrix H_C:

$$H_C = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}. \tag{2.3}$$

Then

$$H_P = \begin{pmatrix} I_8 & I_8 \\ H_C & \mathbf{0} \\ \mathbf{0} & H_C \end{pmatrix}.$$

Setting $E = \{1, 3, 4, 9, 11, 12\}$, we have

$$\begin{gathered} E_1 = E_3 = E_4 = \{1, 2\}, \\ E_2 = E_5 = E_6 = E_7 = E_8 = \emptyset, \\ E'_1 = E'_2 = \{1, 3, 4\}. \end{gathered}$$

DOI: http://dx.doi.org/10.22108/toc.2017.101199.1465

The set $\{1,2\}$ is a stopping set in H_R and the set $\{1,3,4\}$ is a stopping set in H_C. Hence Lemma 2.3 implies that $\{1,3,4,9,11,12\}$ is a stopping set in H_P. This stopping set is a obvious stopping set.

Lemma 2.6. Let the stopping distance of parity-check matrices H_R and H_C be $s(H_R)$ and $s(H_C)$, respectively. Let E be a stopping set in H_P.

(i) If the size of $\cup_{i=1}^{n'} E_i$ is equal to $s(H_R)$. Then E is the obvious stopping set.

(ii) If the size of $\cup_{j=1}^{n} E'_j$ is equal to $s(H_C)$. Then E is the obvious stopping set.

Proof. Consider case (i). Suppose that the size of $\cup_{i=1}^{n'} E_i$ is equal to $s(H_R)$. Since E is a stopping set in H_P, Lemma 2.3 implies that for each row-set B_i with $B_i \cap E \neq \emptyset$, E_i is a stopping set in H_R. Hence the size of E_i where $B_i \cap E \neq \emptyset$, is at least $s(H_R)$. Thus if $E_i \neq \emptyset$, $1 \leq i \leq n'$, the size of E_i is equal to $s(H_R)$. Therefore for each row-set B_i with $B_i \cap E \neq \emptyset$, we have $E_i = \cup_{i=1}^{n'} E_i$. Hence for i, $1 \leq i \leq n'$, the set E_i is empty or the constant set $\cup_{i=1}^{n'} E_i$. Therefore E is an obvious stopping set. Statement (ii) is proved in a similar way. □

It is shown that the stopping distance of the parity-check matrix H_P of the product code $R \bigotimes C$ is equal to the product of the stopping distances of parity-check matrices H_R and H_C of component codes R and C [6].

Lemma 2.7. [6] Let the stopping distance of parity-check matrices H_R and H_C be $s(H_R)$ and $s(H_C)$, respectively. Then the stopping distance of H_P is $s(H_R)s(H_C)$.

It is well known that the performance under iterative decoding over the BEC is computed by the number of minimum stopping sets when the erasure probability is small [10, 11].

Theorem 2.8. Let the number stopping sets of size $s(H_R)$ and $s(H_C)$ in parity-check matrices H_R and H_C be $S_{s(H_R)}$ and $S_{s(H_C)}$, respectively. Then the number of stopping sets of size $s(H_P)$ in H_P is $S_{s(H_R)}S_{s(H_C)}$.

Proof. Suppose $E \subseteq \{1,2,\ldots,nn'\}$ is a stopping set of size $s(H_R)s(H_C)$ in H_P. In the first, we show that the size of $\cup_{i=1}^{n'} E_i$ is equal to $s(H_R)$. Hence Lemma 2.6 implies that E is a obvious stopping set.

Lemma 2.3 implies that for each row-set B_i with $B_i \cap E \neq \emptyset$, E_i is a stopping set in H_R. Hence $\cup_{i=1}^{n'} E_i$ is a stopping set in H_R. Thus $|\cup_{i=1}^{n'} E_i| \geq s(H_R)$. The size of $\cup_{i=1}^{n'} E_i$ is equal to the number of column-sets B'_j satisfying $B'_j \cap E \neq \emptyset$. Hence the number of column-sets B'_j for which $B'_j \cap E \neq \emptyset$, is at least $s(H_R)$. The size of $B'_j \cap E$ is equal to the size of E'_j. Theorem 2.3 implies that for each column-set B'_j with $B'_j \cap E \neq \emptyset$, the set E'_j is a stopping set in H_C. Hence for each B'_j satisfying $B'_j \cap E \neq \emptyset$, the size of $B'_j \cap E$ is at least $s(H_C)$. Hence $|E| \geq s(H_R)s(H_C)$. Since $|E| = s(H_R)s(H_C)$, we have $|\cup_{i=1}^{n'} E_i| = s(H_R)$.

Now suppose E is a obvious stopping set of size $s(H_R)s(H_C)$. Hence there exist two stopping sets S_R and S_C in parity-check matrices H_R and H_C, respectively, such that $E = S_{RC}$. It follows from $|S_R| \geq s(H_R)$, $|S_C| \geq s(H_C)$ and $|S_{RC}| = s(H_R)s(H_C)$ that $|S_R| = s(H_R)$ and $|S_C| = s(H_C)$. Therefore the number stopping set of size $s(H_R)s(H_C)$ in H_P is $S_{s(H_R)}S_{s(H_C)}$. □

DOI: http://dx.doi.org/10.22108/toc.2017.101199.1465

Example 2.9. Let R be the linear $[3,2,2]$ code and let C be the $[8,4,4]$ Reed-Muller code with parity-check matrix H_C given in (2.3). Then we have

$$s(H_R) = 2,\ s(H_C) = 3,$$

$$S_2(H_R) = 3,\ S_3(H_C) = 2$$

Hence Theorem 2.8 implies that $S_6(H_P) = 6$.

3. Minimum Stopping Sets of SPC Product Codes

Let C_i, $1 \leq i \leq r$, be a binary linear code with parameters $[n_i, k_i, d_i]$. Then the corresponding r-dimensional product code can be constructed in the following way [7]. The data to be transmitted are arranged in a hypercube of dimension r with the length in each dimension defined by $\{k_1, k_2, \ldots, k_r\}$. The ith dimension is encoded with C_i, and this is repeated for all $i = 1, 2, \ldots, r$ dimensions. The resulting $r-$dimensional product code has length $\prod_{i=1}^{r} n_i$, minimum distance $\prod_{i=1}^{r} d_i$ and rate $\prod_{i=1}^{r} R_i$, where R_i is the rate of C_i. If component codes C_i, $1 \leq i \leq r$, are the SPC codes with same length n, then the $r-$dimensional product code has the length n^r and the minimum distance 2^r and the rate $(\frac{n-1}{n})^r$. This code is called an r-dimensional SPC product code. Product codes based on SPC codes have been introduced by Battial [1].

By recursive construction, we constructed a parity-check matrix H^r_{SPC} for the $r-$dimensional SPC product code. Let $H_{SPC} = [11\cdots1]$ be the parity-check matrix of the SPC code. The 1-dimensional SPC product code is the SPC code. Thus, $H^1_{SPC} = H_{SPC}$. Using the construction (2.1), the matrix

$$H^r_{SPC} = \begin{pmatrix} H^{(r-1)}_{SPC} \otimes I_n \\ I_n \otimes H_{SPC} \end{pmatrix} \tag{3.1}$$

is a parity-check matrix of the $r-$dimensional SPC product code.

In the following theorem, the stopping distance of H^r_{SPC} and the number of minimum stopping sets in H^r_{SPC} is computed.

Theorem 3.1. The stopping distance of parity-check matrix H^r_{SPC} of the $r-$dimensional SPC product code is 2^r and the number of minimum stopping sets in H^r_{SPC} is equal to $\binom{n}{2}^r$.

Proof. The proof is by induction on r. The 1-dimensional SPC product code is the SPC code of length n. The stopping distance of H^1_{SPC} is two and the number of stopping sets of size two is $\binom{n}{2}$. Thus the theorem holds for $r = 1$.

We now assume that the theorem holds for dimension $(r-1)$. Then $s(H^{(r-1)}_{SPC}) = 2^{(r-1)}$ and $S_{2^{(r-1)}}(H^{(r-1)}_{SPC}) = \binom{n}{2}^{(r-1)}$. Lemma 2.7 implies that $s(H^r_{SPC}) = s(H^{(r-1)}_{SPC})s(H^1_{SPC}) = 2^r$. Using Theorem 2.8, we have

$$\begin{aligned} S_{2^r}(H^r_{SPC}) &= S_{2^{(r-1)}}(H^{(r-1)}_{SPC})S_2(H^1_{SPC}) \\ &= \tbinom{n}{2}^{(r-1)} \times \tbinom{n}{2} = \tbinom{n}{2}^r. \end{aligned}$$

□

DOI: http://dx.doi.org/10.22108/toc.2017.101199.1465

References

[1] G. Battail, *Building long codes by combination of simple ones*, thanks to weighted-output decoding, in Proc. URSI ISSSE Erlangen Germany, 1989.

[2] P. Elias, Error-free coding, *IRE Trans. Inform. Theory*, 29–37 (1954).

[3] K. M. Krishnan and P. Shankar, Computing the stopping distance of a Tanner graph is NP-hard, *IEEE Trans. Inform. Theory*, **53** (2007) 2278–2280.

[4] R. J. McEliece, *Are there turbo-codes on Mars?*, Shannon Lecture, Proc. IEEE Int. Symp. Inform. Theory, Chicago, IL, USA, 2004.

[5] R. L. Miller, Number of minimum-weight code words in a product code, *Electronics Letters*, **14** (1978) 642–643.

[6] M. Hivadi and M. Esmaeili, On the Stopping Distance and Stopping Redundancy of Product Codes, *IEICE Trans.*, **E91-A** (2008) 2167–2173.

[7] W. W. Peterson and E. J. Weldon, *Error Correcting Codes*, 2nd Ed., MIT Press, 1972.

[8] C. Di, D. Proietti, I. E. Telatar, T. J. Richardson and R. L. Urbanke, Finitelength analysis of low-density parity-check codes on the binary erasure channel, *IEEE Trans. Inform. Theory*, **48** 1570–1579 (2002).

[9] R. M. Roth, *Introduction to Coding Theory*, Cambridge University Press, 2006.

[10] 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. Inform. Theory*, **54** (2008) 1368–1374 .

[11] S.-T. Xia and F.-W. Fu, *Stopping Set Distributions of Some Linear Codes*, Proc. IEEE Information Theory Workshop, 2006.

M. Hivadi

Department of Mathematics, Institute for Advanced Studies in Basic Sciences, zanjan, Iran

Email: m.hivadi@iasbs.ac.ir

A. Zare Chavoshi

Department of Mathematics, Malek ashtar university of technology Tehran, Iran

Email: nonemail@gmail.com

DOI: http://dx.doi.org/10.22108/toc.2017.101199.1465