Two Classes of Optimal Stopping Redundancy Codes

M. Esmaeili and V. Ravanmehr
Department of Mathematical Sciences
Isfahan University of Technology
84156-83111, Isfahan, Iran
Email: emorteza@cc.iut.ac.ir

Abstract

The binary linear code $\mathcal{H}_{m,2}^{\perp}$, $m > 2$, of length $\binom{m}{2}$ represented by the generator matrix $H_{m,2}$ consisting of all distinct column strings of length m and Hamming weight 2 is considered. A parity-check matrix $H_{m,2}^{\perp}$ is assigned to the code $\mathcal{H}_{m,2}^{\perp}$. The code $\mathcal{H}_{m,2.3}$, $m > 3$, of length $\binom{m}{2} + \binom{m}{3}$ represented by the parity-check matrix $H_{m,2.3}$ consisting of all distinct column strings of length m and Hamming weight two or three is also considered. It is shown that $\mathcal{H}_{m,2}^{\perp}$ and $\mathcal{H}_{m,2.3}$ are *optimal stopping redundancy* codes, that is for each of these codes *the stopping distance* of the associated parity-check matrix is equal to the minimum Hamming distance of the code, and the rows of the parity-check matrix are linearly independent. Explicit formulas determining the number of stopping sets of arbitrary size for these codes are given.

Keywords: Stopping set, stopping distance, stopping redundancy.

1 Introduction

The performance of a low-density parity-check code on the binary erasure channel is determined by a type of combinatorial structure on the parity-check matrix H referred to as *stopping set* [2]. Let $\mathcal{C}$ be a linear block code of length n, dimension k and minimum distance d represented by a $r \times n$ parity-check matrix H with $r \geq n - k$. An l-subset $T \subset \{1, 2, \cdots, n\}$ is called a stopping set of size l for H if the $r \times l$ submatrix of H consisting of columns with coordinate indexes in T has no row of Hamming weight one. Accordingly, stopping distance is a parameter assigned to H while the minimum distance is a fixed parameter assigned to $\mathcal{C}$.

The size of the smallest non-empty stopping sets for H is called the *stopping distance* of H and is denoted by $s(H)$ [4],[5],[6],[7],[9],[12],[13]. The stopping distance $s(H)$ has a role on the performance of iterative decoding of $\mathcal{C}$ on the binary erasure channel that is very similar to that of minimum distance of $\mathcal{C}$ under maximum likelihood decoding.

A related concept is *stopping redundancy*. The number of rows of H effects the complexity of iterative decoding algorithms applied on graphs representing H, such as the Tanner graph of H [11]. Accordingly, Schwartz and Vardy [10] introduced the concept of *stopping redundancy*. The stopping redundancy $\rho(\mathcal{C})$ of $\mathcal{C}$ is the minimum number of rows of a parity-check matrix H satisfying $s(H) = d(\mathcal{C})$. A code $\mathcal{C}$ has *optimal stopping redundancy*, or just *optimal redundancy* if it satisfies $\rho(\mathcal{C}) = r(\mathcal{C})$ where $r(\mathcal{C})$ is the redundancy of $\mathcal{C}$, that is $r(\mathcal{C}) = n - k$.

The role of multiplicity of stopping sets is similar to that of the number of codewords in the weight distribution. Therefore, enumeration of the stopping sets of a given parity-check matrix H is of great importance. McEliece [8] determined the number of stopping sets of size three for a full-rank parity-check matrix of the Hamming codes, and a formula giving the number of stopping sets of any size in this matrix was given in [1].

In this paper, matrices $H_{m,2}$ and $H_{m,2.3}$, $m > 3$, are considered where $H_{m,2}$ consists of all distinct length-m weight-two column strings and $H_{m,2.3}$ contains all distinct length-m weight-two and weight-three column stings. A stopping set analysis of the code with parity-check matrix $H_{m,2}$ is given in [4]. Here we consider the codes $\mathcal{H}_{m,2}^{\perp}$ and $\mathcal{H}_{m,2.3}$ with generator matrix $H_{m,2}$ and parity-check matrix $H_{m,2.3}$, respectively. $\mathcal{H}_{m,2}^{\perp}$ is analyzed using a parity-check matrix $H_{m,2}^{\perp}$ derived from $H_{m,2}$.

In Section 2, we show that the code $\mathcal{H}_{m,2}^{\perp}$ is an optimal redundancy code with $s(H_{m,2}^{\perp}) = d(\mathcal{H}_{m,2}^{\perp}) = m - 1$, and provide a formula enumerating the stopping sets of arbitrary size l in the parity-check matrix $H_{m,2}^{\perp}$. Section 3 is devoted to studying $\mathcal{H}_{m,2.3}$ and $H_{m,2.3}$. It is shown that $\mathcal{H}_{m,2.3}$, $m \geq 3$, is an optimal redundancy code with $d(\mathcal{H}_{m,2.3}) = s(H_{m,2.3}) = 3$ and $\rho(\mathcal{H}_{m,2.3}) = r(\mathcal{H}_{m,2.3}) = m$. A formula enumerating the stopping sets of arbitrary size l for the parity-check matrix $H_{m,2.3}$ is provided.

2 Complete weight-2 generator matrices

Let $\mathcal{H}_{m,2}$ be the binary code with parity-check matrix $H_{m,2}$ consisting of all distinct binary weight-two length-m column-strings. The dual-code $\mathcal{H}_{m,2}^{\perp}$ with generator matrix $H_{m,2}$ is considered.

It is easy to verify the following recursive relation for $H_{m,2}$ up to column permutation

$$H_{2,2} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \text{and} \quad H_{m+1,2} = \begin{pmatrix} 1 & 0 \\ I_m & H_{m,2} \end{pmatrix}, \quad m \geq 2;$$

where I_m is the $m \times m$ identity matrix, and $\mathbf{1}$ and $\mathbf{0}$ are the all-one and all-zero strings of lengths m and $\binom{m}{2}$, respectively.

Since each column of $H_{m,2}$ has Hamming weight two, the rows of this matrix add to zero. This together with the existence of the identity matrix I_{m-1} in $H_{m,2}$ implies that the rank of $H_{m,2}$ is $m-1$. In fact to obtain a generator matrix for $\mathcal{H}_{m,2}^{\perp}$ it suffices to delete the first row of $H_{m,2}$. Accordingly, the matrix $H_{m,2}^{\perp}$, given by (1), is a parity-check matrix for $\mathcal{H}_{m,2}^{\perp}$ where 'tr' denotes transpose

$$H_{m,2}^{\perp} := \left(H_{m-1,2}^{tr}\ \mathcal{I}_{\binom{m-1}{2}}\right). \tag{1}$$

For example, we have

$$H_{5,2} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$

$$H_{6,2}^{\perp} = (H_{5,2}^{tr}\ \ \mathcal{I}_{10}) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Theorem 1 For the code $\mathcal{H}_{m,2}^{\perp}$, $m \geq 3$, with parity-check matrix $H_{m,2}^{\perp}$, we have $s(H_{m,2}^{\perp}) = d(\mathcal{H}_{m,2}^{\perp}) = m-1$.

Proof. Applying the recursive structure of matrix $H_{m,2}$ one can easily show that $d(\mathcal{H}_{m,2}^{\perp}) = m-1$ (see Proposition 1 in [3]).

Given a code $\mathcal{C}$ with parity-check matrix H we have $s(H) \leq d(\mathcal{C})$. Thus to show $s(H_{m,2}^{\perp}) = m-1$ for $m \geq 3$, we need to prove that there is no stopping set of size $m-2$ or less for $H_{m,2}^{\perp}$. We refer to the matrices $H_{m-1,2}^{tr}$ and $\mathcal{I}_{\binom{m-1}{2}}$ as the right and left parts of $H_{m,2}^{\perp}$. It is obvious that each row of $H_{m-1,2}^{tr}$ has Hamming weight two.

Let $S \subseteq \{1, 2, \cdots, \binom{m}{2}\}$ be an arbitrary set of column indexes of $H_{m,2}^{\perp}$ with $|S| \leq m-2$. We show that S is not a stopping set for $H_{m,2}^{\perp}$. Three cases are considered.

Case 1. If $S \cap \{m, m+1, \cdots, \binom{m}{2}\} = \emptyset$, then $S \subseteq \{1, 2, \cdots, m-1\}$. Since any matrix consisting of less than $m-1$ columns of the left side of $H_{m,2}^{\perp}$ has at least one row of weight one, the set S is not a stopping set.

Case 2. As the right side of $H_{m,2}^{\perp}$ is the identity matrix $\mathcal{I}_{\binom{m-1}{2}}$, obviously a stopping set cannot be a subset of $\{m, m+1, \cdots, \binom{m}{2}\}$.

Case 3. Suppose $|S \cap \{1, 2, \cdots, m-1\}| = k$ with $0 < k < m-2$. This implies that $0 < |S \cap \{m, m+1, \cdots, \binom{m}{2}\}| \leq m-2-k$.

Any k columns, $1 \leq k \leq m-1$, of the left side of $H_{m,2}^{\perp}$ add to a binary string of weight $k(m-1-k)$ (Theorem 2 in [3]). In other words, any k-column submatrix of the right side of $H_{m,2}^{\perp}$ has $k(m-1-k)$ rows of weight one. On the other hand, for $1 \leq k \leq m-3$ we have $k(m-1-k) > m-2-k$. Therefore, the set S cannot be a stopping set for $H_{m,2}^{\perp}$, implying that $s(H_{m,2}^{\perp}) = m-1$. ■

Corollary 1 (Optimality of $\mathcal{H}_{m,2}^{\perp}$) The binary code $\mathcal{H}_{m,2}^{\perp}$, $m \geq 3$, is an optimal redundancy code.

Proof. The rows of $H_{m,2}^{\perp}$ are linearly independent and according to Theorem 1 the number of rows of $H_{m,2}^{\perp}$ is an upper bound for the stopping redundancy of $\mathcal{H}_{m,2}^{\perp}$. ■

Theorem 2 The number of stopping sets of size l, $l \geq m-1$, denoted s_l, in the parity-check matrix $H_{m,2}^{\perp}$, $m \geq 3$, is

$$s_l := \sum_{i=1}^{m-1} \binom{m-1}{i} \binom{\frac{i(i-1)}{2}}{l-i(m-i)}, \quad 0 \leq l - i(m-i) \leq \frac{i(i-1)}{2}. \qquad (2)$$

Proof. As $s(H_{m,2}^{\perp}) = m-1$, the number of stopping sets of size less than $m-1$ is zero. The right side of $H_{m,2}^{\perp}$ is an identity matrix and does not contain a stopping set. Hence, to have a stopping set we must choose at least one column from the left side. The number of ways for choosing i columns from the left side is $\binom{m-1}{i}$. Any i columns of the left side form $i(m-1-i)$ rows of weight one and $\binom{i}{2} = \frac{i(i-1)}{2}$ rows of weight two.

Let S be a stopping set of size l containing i column-indices from the left side. From among the columns associated with the remaining $l-i$ column-indices chosen from the right side, we need $i(m-1-i)$ columns to be matched with the weight-one rows formed in the left side, while the nonzero entry of each of the remaining $l-i-i(m-1-i) = l-i(m-i)$ right-side columns needs to be matched with one of the weight-two rows formed in the left side. This gives relation (2). ■

3 Combined weight-2 & weight-3 parity-check matrices

For a given positive integer m, let $H_{m,2,3}$ denote the matrix consisting of all distinct length-m binary column-strings of weight two or three.

Table 1: The number of stopping sets for $H^{\perp}_{m,2}$, $3 \leq m \leq 7$.

	$H^{\perp}_{3,2}$	$H^{\perp}_{4,2}$	$H^{\perp}_{5,2}$	$H^{\perp}_{6,2}$	$H^{\perp}_{7,2}$
s_3	1	4	0	0	0
s_4	0	6	5	0	0
s_5	0	6	6	6	0
s_6	0	1	25	10	7
s_7	0	0	38	45	15
s_8	0	0	27	135	105
s_9	0	0	10	260	455
s_{10}	0	0	1	357	1385
s_{11}	0	0	0	340	3087
s_{12}	0	0	0	205	5310
s_{13}	0	0	0	75	7305
s_{14}	0	0	0	15	7980
s_{15}	0	0	0	1	6837
s_{16}	0	0	0	0	4488
s_{17}	0	0	0	0	2175
s_{18}	0	0	0	0	740
s_{19}	0	0	0	0	165
s_{20}	0	0	0	0	21
s_{21}	0	0	0	0	1

The linear code represented by $H_{m,2.3}$ is denoted by $\mathcal{H}_{m,2.3}$. Thus the code $\mathcal{H}_{m,2.3}$ has length $\binom{m}{2} + \binom{m}{3}$. Relation (3) gives a recursive construction for $H_{m,2.3}$ wherein $H_{m,1.2}$ consists of all distinct length-m column-strings of weight one or two.

$$H_{m+1,2.3} = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ H_{m,1.2} & H_{m,2.3} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{0} \\ H_{m,2} & \mathcal{I}_m & H_{m,2.3} \end{pmatrix} \qquad (3)$$

As an example, for $m = 3$ and $m = 4$ we have

$$H_{3,2.3} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \quad H_{4,2.3} = \left(\begin{array}{ccc|ccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ \hline 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{array}\right).$$

It follows from relation (3) and the existence of $\mathcal{I}_m$ in $H_{m+1,2.3}$ that the last m rows of $H_{m+1,2.3}$ are linearly independent. This together with the weight-three submatrix $\begin{pmatrix} \mathbf{1} \\ H_{m,2} \end{pmatrix}$ implies that the rank of $H_{m,2.3}$ is m.

Theorem 3 (Optimality of $\mathcal{H}_{m,2.3}$) For the code $\mathcal{H}_{m,2.3}$, $m \geq 3$, of length $\binom{m}{2} + \binom{m}{3}$ and its parity-check matrix $H_{m,2.3}$, we have $d(\mathcal{H}_{m,2.3}) = s(H_{m,2.3}) = 3$ and $\rho(\mathcal{H}_{m,2.3}) = r(\mathcal{H}_{m,2.3}) = m$.

Proof. The parity-check matrix $H_{m,2.3}$ consists of distinct nonzero columns and its last three columns are linearly dependent, implying that the minimum Hamming distance of $\mathcal{H}_{m,2.3}$ is three. According to Theorem 3 in [10], for a code C with minimum distance at most three and parity-check matrix H representing C, we have $s(H) = d(C)$ and $\rho(C) = r(C)$. Therefore, $s(H_{m,2.3}) = 3$ and $\rho(\mathcal{H}_{m,2.3}) = r(\mathcal{H}_{m,2.3}) = m$. ∎

The rest of this section is devoted to enumerating stopping sets of size l in these matrices. Let C be a binary linear $[n,k,d]$ block code with an $r \times n$, $n-k \leq r \leq 2^{n-k}$, parity-check matrix H. Assume that S is a subset of the coordinate set $\{1,2,...,n\}$ and T is a subset of the row-index set $\{1,2,...,r\}$. The restriction of matrix H to S and T is denoted by H_S^T. Thus H_S^T is a $|T| \times |S|$ sub-matrix of H. We denote H_S^T by H_S or H^T depending on $T = \{1,2,...,r\}$ or $S = \{1,2,...,n\}$. Given a subset T of $\{1,2,...,r\}$, we denote by z_T the number of all-zero columns in H^T. If $T = \phi$ then $z_T = n$.

A p-subset Y of $\{1,2,...,n\}$ is said to be of type p with respect to T, a subset of $\{1,2,...,r\}$, if H_Y^T has no all-zero column and its rows have Hamming weight one. The number of subsets of $\{1,2,...,n\}$ which are of type p with respect to T is denoted by $y(T,p)$. By definition we have

$$y(T,p) = \begin{cases} 0 & \text{if } T = \phi \ \& \ p \geq 1 \ \text{ or } \ T \neq \phi \ \& \ p = 0, \\ 1 & \text{if } T = \phi \ \& \ p = 0. \end{cases}$$

It is known [1] that s_l, the number of stopping sets of size l, $0 \leq l \leq n$, in a given $r \times n$ parity-check matrix H is determined by the following relation

$$s_l = \sum_{T \subseteq \{1,2,...,r\}} (-1)^{|T|} \sum_{p=0}^{l} y(T,p) \binom{z_T}{l-p}. \tag{4}$$

Lemma 1 Let T be a t-subset of the row-index set $\{1,2,\cdots,m\}$. Each weight-one length-t column vector appears exactly $m-t+1$ times in $H_{m,1.2}^T$ for all $T \subseteq \{1,2,\cdots,m\}$.

Proof. The proof is by induction on m. It is easily verified that each weight-one length-t column vector appears exactly $3-t$ times in $H_{2,1.2}^T$ for $T \subseteq \{1,2\}$. Suppose the result holds for $H_{m,1.2}$ and consider $H_{m+1,1.2}$. We have the following recursive relation

$$H_{m+1,1.2} = \begin{pmatrix} 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ & & & 0 & & & \\ & H_{m,1.2} & & \vdots & & H_{m,1} & \\ & & & 0 & & & \end{pmatrix}.$$

Suppose $T \subseteq \{1,2,\cdots,m+1\}$ and $1 \notin T$. By the induction hypothesis, each weight-one length-t column vector appears $m-t+1$ times in $H_{m,1.2}^T$. Also, each weight-one length-t vector appears just once in $H_{m,1}^T$. Therefore, each weight-one length-t vector appears $(m-t+1)+1 = m-t+2$ times in $H_{m+1,1.2}^T$.

Assume that $1 \in T$. If $T = \{1\}$ then the statement is trivial. Thus suppose $1 \in T \neq \{1\}$. Consider a weight-one length-t vector in $H_{m+1,1.2}^T$.

If the nonzero bit of the vector is in the first row then we are limited to the right side of the matrix given above. In this case, due to the matrix $H_{m,1}$, one can easily verify that the number of times the given weight-one length-t vector appears is $1 + m - (t-1) = m - t + 2$. On the other hand, if the nonzero component of the considered vector is in a row different from the first one we are limited to the left side of the matrix and by the induction hypothesis, the vector appears $m - (t-1) + 1 = m - t + 2$ times in $H^T_{m,1.2}$ and hence $m - (t-1) + 1 = m - t + 2$ times in $H^T_{m+1,1.2}$. ■

Lemma 2 For any t-element set $T \subseteq \{1, 2, \cdots, m\}$, each weight-one length-t column vector appears $\binom{m-t+1}{2}$ times in $H^T_{m,2.3}$, while the number of times each weight-two length-t column vector occurs is $m - t + 1$.

Proof. We apply induction on m. It is easy to see that the statements hold for $m \leq 3$. Assume that the statements are true for $H_{m,2.3}$ and consider the recursive relation

$$H_{m+1,2.3} = \begin{pmatrix} 0 & \cdots & 0 & 1 & \cdots & 1 \\ & H_{m,2.3} & & & H_{m,1.2} & \end{pmatrix}.$$

Let $T \subseteq \{1, 2, \cdots, m+1\}$ be a t-element set and suppose $1 \notin T$. By the induction hypothesis any weight-one length-t vector $\mathbf{v}$ appears $\binom{m-t+1}{2}$ times in $H^T_{m,2.3}$. According to Lemma 1, the number of times $\mathbf{v}$ appears in $H^T_{m,1.2}$ is $m - t + 1$. Thus, the number of times vector $\mathbf{v}$ is replicated in $H^T_{m+1,2.3}$ is $\binom{m-t+1}{2} + (m - t + 1) = \binom{m-t+2}{2}$.

If $T = \{1\}$ then obviously the number of times the unique weight-one length-one vector is replicated in $H^T_{m+1,2.3}$ is $\binom{m}{1} + \binom{m}{2} = \binom{m+1}{2} = \binom{m-t+2}{2}$. Suppose $1 \in T \neq \{1\}$. Consider a weight-one length-t vector $\mathbf{v}$ in $H^T_{m+1,2.3}$ and assume that the first component of $\mathbf{v}$ is 1. Then we are limited to the right side of $H_{m+1,2.3}$, and the number of weight-zero vectors in $H^{T-\{1\}}_{m,1.2}$ is $\binom{m+1}{2} - \binom{t-1}{2} - (m - t + 2)(t-1) = \binom{m-t+2}{2}$. On the other hand, if the first component of $\mathbf{v}$ is 0 then we have to just consider the left side of $H_{m+1,2.3}$, and by the induction hypothesis the number of occurrences of the weight-one length-$(t-1)$ vector $\mathbf{v}'$, obtained from $\mathbf{v}$ by deleting its first component, in $H^{T-\{1\}}_{m,2.3}$ is $\binom{m-(t-1)+1}{2} = \binom{m-t+2}{2}$.

The same approach and arguments apply to the weight-two column vectors and hence is omitted. ■

Theorem 4 For parity-check matrix $H_{m,2.3}$, $m \geq 3$, and a t-element set $T \subseteq \{1, 2, \cdots, m\}$, we have

$$z_T = \binom{m-t}{2} + \binom{m-t}{3} \tag{5}$$

and $Y(T,p)$ is given by

$$Y(T,p) = \begin{cases} \sum_{x_1,x_2,x_3} \frac{t!}{x_1!\ x_2!\ x_3!\ \ 2^{x_2}\ 6^{x_3}} \binom{m-t+1}{1}^{x_2} \binom{m-t+1}{2}^{x_1}, \\ \qquad\qquad \text{if} \quad p \le t \le 3p, \\ 0, \qquad\qquad \text{otherwise;} \end{cases} \tag{6}$$

where x_1, x_2, x_3 satisfy the following

$$\begin{aligned} x_1 + 2x_2 + 3x_3 &= t, \\ x_1 + x_2 + x_3 &= p, \\ x_1, x_2, x_3 &\ge 0. \end{aligned}$$

The number of stopping sets of size l is obtained using relations (4), (5) and (6).

Proof. Consider a t-subset T of $\{1, 2, \cdots, m\}$. The complement of T, denoted T^c, has $m-t$ elements and the number of weight-two columns having their nonzero components in the rows with index in T^c is $\binom{m-t}{2}$. Also, the number of weight-three columns having their nonzero components in the rows with index in T^c is $\binom{m-t}{3}$. Therefore, $z_T = \binom{m-t}{2} + \binom{m-t}{3}$.

Obviously, for $p > t$ we have $y(T,p) = 0$ since any matrix M with p nonzero columns has at least p nonzero entries, and hence the number of rows in M, that is t, must be at least p if each row needs to have precisely one nonzero element. The same argument shows that if $t > 3p$ then $y(T,p) = 0$ since each column of $H_{m,2.3}$ has Hamming weight two or three. Therefore, we need to determine $y(T,p)$ for $p \le t \le 3p$.

Consider a $t \times p$ submatrix M of $H^T_{m,2.3}$ whose rows have Hamming weight one and has no all-zero column. Denote the number of columns in M with weight i by x_i, $1 \le i \le 3$. Thus $x_1+x_2+x_3 = p$ and $x_1+2x_2+3x_3 = t$.

Let (x_1, x_2, x_3) be a solution of this system. The number of p-subsets of type p with respect to T associated with (x_1, x_2, x_3) is computed as follows. The number of ways of choosing x_1 distinct length-t weight-one strings is $\binom{t}{x_1}$ and each of these weight-one columns is replicated $\binom{m-t+1}{2}$ times, giving $\binom{t}{x_1}\binom{m-t+1}{2}^{x_1}$. For the x_2 weight-two columns, we need to choose $2x_2$ positions of the remaining $t - x_1$ row indices, a problem with $\binom{t-x_1}{2x_2}$ solutions. A given set of $2x_2$ positions can be partitioned into 2-element sets in $\frac{(2x_2)!}{x_2!2^{x_2}}$ different ways. This together with the number of times each weight-two column is replicated, that is $m - t + 1$, gives $\binom{t-x_1}{2x_2}\frac{(2x_2)!}{x_2!2^{x_2}}(m - t + 1)^{x_2}$. The remaining $t - x_1 - 2x_2 = 3x_3$ positions are partitioned into 3-element sets in $\frac{(3x_3)!}{x_3!6^{x_3}}$ different ways and each weight-three column is replicated only once.

Thus the number of p-subsets associated with a solution (x_1, x_2, x_3) is

$$\binom{t}{x_1}\binom{m-t+1}{2}^{x_1}\binom{t-x_1}{2x_2}\frac{(2x_2)!}{x_2!2^{x_2}}(m-t+1)^{x_2}\frac{(3x_3)!}{x_3!6^{x_3}}$$

$$= \frac{t!}{x_1!\ x_2!\ x_3!\ \ 2^{x_2}\ 6^{x_3}}\binom{m-t+1}{1}^{x_2}\binom{m-t+1}{2}^{x_1}. \qquad \blacksquare$$

References

[1] 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. Inform. Theory*, vol. 53, no. 9, pp. 3196–3201, Sept. 2007.

[2] C. Di, D. Proietty, I.E. Telater, T.J. Richardson and R.L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1570–1579, June 2002.

[3] M. Esmaeili and A. Zaghian, "On the combinatorial structure of a class of $[\binom{m}{2}, \binom{m-1}{2}, 3]$ shortened Hamming codes and their dual-codes," *Discrete Applied Math.*, vol. 157, pp. 356–363, Jan. 2009.

[4] 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, July 2008.

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

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

[7] N. Kashyap and A. Vardy, "Stopping sets in codes from designs," *Proc. IEEE Int. Symp. Inform. Theory*, p. 122, June-July, 2003.

[8] R.J. McEliece, "Are there turbo codes on Mars?," *Shannon Lecture, IEEE Int. Symp. Inform. theory*, June-July, 2004.

[9] A. Orlitsky, K. Viswanathan and J. Zhang, "Stopping set distribution of LDPC code ensembles," *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 929–953, Mar. 2005.

[10] M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 3, pp. 922–932, March 2006.

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

[12] J.H. Weber and K.A.S. Abdel-Ghaffar, "Results on parity-check matrices with optimal stopping and/or dead-end set enumerators," *Submitted to IEEE Trans. Inform. Theory*, July 7, 2006. arXiv:cs.IT/0607024. [Online].

[13] S.-T. Xia and F.-W. Fu, "On the stopping distance of finite geometry LDPC codes," *IEEE Commun. Letters*, vol. 10, no. 5, pp. 381–383, May 2006.