On the Stopping Redundancy of Reed–Muller Codes

Tuvi Etzion, *Fellow, IEEE*

***Abstract*—The stopping redundancy of the code is an important parameter which arises from analyzing the performance of a linear code under iterative decoding on a binary erasure channel. In this paper, we will consider the stopping redundancy of Reed–Muller codes and related codes. Let $\mathcal{R}(\ell, m)$ be the Reed–Muller code of length 2^m and order ℓ. Schwartz and Vardy gave a recursive construction of parity-check matrices for the Reed–Muller codes, and asked whether the number of rows in those parity-check matrices is the stopping redundancy of the codes. We prove that the stopping redundancy of $\mathcal{R}(m-2, m)$, which is also the extended Hamming code of length 2^m, is $2m-1$ and thus show that the recursive bound is tight in this case. We prove that the stopping redundancy of the simplex code equals its redundancy. Several constructions of codes for which the stopping redundancy equals the redundancy are discussed. We prove an upper bound on the stopping redundancy of $\mathcal{R}(1, m)$. This bound is better than the known recursive bound and thus gives a negative answer to the question of Schwartz and Vardy.**

***Index Terms*—Iterative decoding on binary erasure channel, Reed–Muller codes, simplex codes, stopping distance, stopping redundancy, stopping sets.**

I. Introduction

THE performance of iterative decoding algorithms on low-density parity-check codes can be analyzed precisely on the binary erasure channel. Di, Proietti, Telatar, Richardson, and Urbanke[1] have shown that this performance is completely determined by *stopping sets* in a Tanner graph of the code. A stopping set $\mathcal{S}$ in a code $\mathcal{C}$ is a subset of the variable nodes of a Tanner graph for $\mathcal{C}$ such that each neighbor of $\mathcal{S}$ is connected to at least two members of $\mathcal{S}$. The *stopping distance* of $\mathcal{C}$ is the size of the smallest stopping set. The role of the stopping distance in iterative decoding is akin to the role of minimum Hamming distance in maximum-likelihood decoding. Therefore, the aim is to try and maximize the stopping distance as one tries to maximize the minimum Hamming distance. However, there is an important difference between the stopping distance of $\mathcal{C}$ and the minimum distance of $\mathcal{C}$. While the minimum distance is a property of the code $\mathcal{C}$, the stopping distance is determined by the specific choice of a Tanner graph for the code, or equivalently, the specific choice of a parity-check matrix for $\mathcal{C}$. The stopping distance was discussed in several papers [4], [7], [8]. Similar definitions with different terminology are given in [2], [3], [9].

Manuscript received September 20, 2005; revised July 5, 2006.

The author is with the Department of Computer Science, Technion–Israel Institute of Technology, Technion City, Haifa 32000, Israel (e-mail: etzion@cs.technion.ac.il).

Communicated by G. Zémor, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2006.883542

Let $\boldsymbol{F}_2^n$ be the vector space of binary words of length n. An (n, k, d) binary linear code is a linear subspace of F_2^n with dimension k and minimum Hamming distance d. Let $\mathcal{C}$ be an (n, k, d) code. $\mathcal{C}$ has a $k \times n$ *generator matrix* $\mathcal{G}$. $\mathcal{C}$ is the linear span of the rows of $\mathcal{G}$. $\mathcal{C}$ has a $\rho \times n$ *parity-check matrix* $\mathcal{H}$. The rows of $\mathcal{H}$ span the orthogonal space of $\mathcal{C}$. Usually, when we consider error-correcting codes we choose ρ to be $n-k$. $n-k$ is called the *redundancy* of $\mathcal{C}$ and it will be denoted by $r(\mathcal{C})$. We will number the rows of the matrices from top to bottom, where row 0 in a matrix is the top row. We will number the columns of the matrices from left to right, where column 0 in a matrix is the leftmost column. Given a code $\mathcal{C}$ with a parity-check matrix $\mathcal{H}$, the *stopping distance* of $\mathcal{H}$ is defined as the largest integer $s(\mathcal{H})$ such that each nonempty set of $s(\mathcal{H})-1$ or less columns of $\mathcal{H}$ contains a row with weight one. The *stopping redundancy* of an (n, k, d) code $\mathcal{C}$, $\rho(\mathcal{C})$, is defined as the smallest number of rows in a parity-check matrix $\mathcal{H}$ of $\mathcal{C}$, such that $s(\mathcal{H}) = d(\mathcal{C})$, where $d(\mathcal{C})$ is the minimum distance of $\mathcal{C}$.

In this paper we consider the Reed–Muller codes and related codes. Reed–Muller codes can be defined in terms of Boolean functions. For a code of length 2^m, we have m variables $v_0, \cdots, v_{m-1}$, which can have values of 0 or 1. A Boolean function is a function $f(v_0, \cdots, v_{m-1})$ which can have the values 0 or 1. Such a function can be specified by a truth table that gives a value of f for each of its 2^m arguments. Each function f can be represented as sum of products of variables. The degree of a function f is the largest number of distinct variables in a product of variables. Note that given a product and a variable v_i, either v_i or $\bar{v}_i$ can appear in the product, but not both. The ℓth order Reed–Muller code $\mathcal{R}(\ell, m)$ is the set of functions with degree at most ℓ. For more information about the representation of a Reed–Muller code as sets of boolean functions, the reader is referred to [5, pp. 370-377]. To find the stopping redundancy of $\mathcal{R}(\ell, m)$, we first have to know the minimum distance of the code. This distance is well known.

Lemma 1: The minimum Hamming distance of $\mathcal{R}(\ell, m)$ is $2^{m-\ell}$.

It was proved in [8] that the matrix

$$\mathcal{H}(\ell, m) = \begin{bmatrix} \mathcal{H}(\ell-1, m-1) & \mathcal{H}(\ell-1, m-1) \\ 0 & \mathcal{H}(\ell, m-1) \\ \mathcal{H}(\ell, m-1) & 0 \end{bmatrix} \quad (1)$$

where

$$\mathcal{H}(m-1, m) = [1 \ \cdots \ 1], \quad \mathcal{H}(0, m) = [\,\mathbf{1} \quad I_{2^m-1}\,]$$

$\mathbf{1}$ is the all-one column vector, and I_k is the $k \times k$ identity matrix, is a parity-check matrix for $\mathcal{R}(\ell, m)$, for which $s(\mathcal{H}(\ell, m)) = 2^{m-\ell}$. Schwartz and Vardy [8] asked whether the number of

rows in $\mathcal{H}(\ell, m)$ is the stopping redundancy of $\mathcal{R}(\ell, m)$, i.e., whether this recursive construction is optimal.

In Section II, we discuss the stopping redundancy of the extended Hamming code of length 2^m, which is the Reed–Muller code of length 2^m and order $m-2$. Schwartz and Vardy [8] have proved that $\rho(\mathcal{R}(m-2,m)) \leq 2m-1$. We will prove that this bound is tight, i.e., $\rho(\mathcal{R}(m-2,m)) = 2m-1$. The proof is done by showing first that the parity-check matrix must include all rows of the classic parity-check matrix of $\mathcal{R}(m-2,m)$. The linear combinations of these rows in the other rows of the parity-chick matrix are translated into another matrix, and properties of this new matrix which implies stopping distance 4 are examined.

We continue in Section III to examine the stopping redundancy of other codes with minimum distance 4. A general bound on the stopping redundancy of these codes is given.

In Section IV, we examine the stopping redundancy of the $(2^m-1, m, 2^{m-1})$ simplex code. This code is closely related to the $(2^m, m+1, 2^{m-1})$ first-order Reed–Muller code. c is a codeword in the simplex code if and only if $c0$ and $\bar{c}1$ are codewords in the first-order Reed–Muller code. The method for proving the stopping redundancy of the simplex code is the basis for the technique used for the first-order Reed–Muller code. We prove that the stopping redundancy of the simplex code is equal to its redundancy. We present a few constructions for other codes whose stopping redundancies are equal to their redundancies.

In Section V, we prove that the general bound for Reed–Muller codes given in [8] is not tight. We show that

$$\rho(\mathcal{R}(1,m)) \leq \frac{(6m-7)2^{m-1} + (-1)^{m-1}}{9}.$$

This bound is better than the previous bound ($\rho(\mathcal{R}(1,m)) \leq (m-2)2^{m-1}+1$) obtained by the recursive construction of Schwartz and Vardy and thus provides a negative answer to their question. The proof is done by constructing a parity-check matrix for $\mathcal{R}(1,m)$. Several matrices are used and defined recursively, where each one uses some of the other matrices of smaller length.

In Section VI, we conclude with a discussion and a list of open problems.

II. The Extended Hamming Codes

For two given integers i, m, $0 \leq i < m$, let $v_{i,m}$ be the binary row vector of length 2^m consisting of 2^{m-i-1} periods of 2^i *zeroes* followed by 2^i *ones*. Let $v_{m,m}$ be the all-ones binary vector of length 2^m.

Example:

$$\begin{aligned} v_{0,4} &= 0101010101010101 \\ v_{1,4} &= 0011001100110011 \\ v_{2,4} &= 0000111100001111 \\ v_{3,4} &= 0000000011111111 \\ v_{4,4} &= 1111111111111111. \end{aligned}$$

Let $\mathcal{V}[m]$ be the $(m+1) \times 2^m$ matrix whose ith row is $v_{i,m}$, $0 \leq i \leq m$. By definition we have (see [5]) the following.

Lemma 2: $\mathcal{V}[m]$ is a parity-check matrix for $\mathcal{R}(m-2,m)$.

The first result is due to [8].

Lemma 3: For $m \geq 2$, $\rho(\mathcal{R}(m-2,m)) \leq 2m-1$

Schwartz and Vardy [8] have shown that the matrix $\mathcal{P}_m$, $m \geq 2$, whose definition is given below, is a parity-check matrix of $\mathcal{R}(m-2,m)$ with stopping distance 4 and redundancy $2m-1$

$$\mathcal{P}_2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$$\mathcal{P}_m = \begin{bmatrix} 00\cdots0 & 11\cdots1 \\ 11\cdots1 & 00\cdots0 \\ \mathcal{P}_{m-1} & \mathcal{P}_{m-1} \end{bmatrix}, \qquad m \geq 3.$$

In this section, we will prove that the upper bound of Schwartz and Vardy is tight, i.e., the stopping redundancy of $\mathcal{R}(m-2,m)$ is $2m-1$.

Let $\mathcal{A}$ be a $t \times n$ matrix with t distinct rows. A $q \times n$ matrix $\mathcal{B}$, with q distinct rows, is a *submatrix* of $\mathcal{A}$ if the q rows of $\mathcal{B}$ are also rows of $\mathcal{A}$. Let $\mathcal{A}$ an $\mathcal{B}$ be two $t \times n$ matrices. $\mathcal{A}$ and $\mathcal{B}$ are called *isomorphic* matrices if $\mathcal{B}$ can be obtained from $\mathcal{A}$ by a permutation on the rows of $\mathcal{A}$ and a permutation on the columns of $\mathcal{A}$. Note that two matrices $\mathcal{A}$ and $\mathcal{B}$ are isomorphic if and only if their corresponding Tanner graphs are isomorphic. In the sequel, throughout the paper we will sometimes abuse definitions when we sometimes say "column" and we really mean "column number." The real meaning will be always understood from the context.

Lemma 4: If $\mathcal{H}$ is a parity-check matrix for $\mathcal{R}(m-2,m)$, then there exists a submatrix of $\mathcal{H}$ isomorphic to the submatrix obtained from the first m rows of $\mathcal{V}[m]$.

Proof: Since $\mathcal{H}$ is spanned by $\mathcal{V}[m]$, it follows that $\mathcal{H}$ has m linearly independent rows which are spanned by vectors $u_0, u_1, \ldots, u_{m-1}$, where for each i, $0 \leq i \leq m-1$, either $u_i = v_{i,m}$ or $u_i = v_{i,m} + v_{m,m}$. Let $w_1, w_2, \ldots, w_m$ be such a set of m linearly independent rows of $\mathcal{H}$. One can easily verify that the $m \times 2^m$ matrix defined by these m rows has each element of $\boldsymbol{F}_2^m$ appearing exactly once as a column. Therefore, we can permute the columns of this matrix to obtain the order of the 2^m columns of $\mathcal{V}[m]$.

Thus, there exists a submatrix of $\mathcal{H}$ isomorphic to the submatrix obtained from the first m rows of $\mathcal{V}[m]$. □

Let $\mathcal{H}$ be an $(m+k) \times 2^m$ parity-check matrix of $\mathcal{R}(m-2,m)$ whose first m rows are the first m rows of $\mathcal{V}[m]$ and its stopping distance is 4. The stopping distance of $\mathcal{V}[m]$ is 3 and therefore $k > 0$. Let h_i be row $m+i$, $0 \leq i \leq k-1$, of $\mathcal{H}$. We can write h_i as a linear combination of the rows of $\mathcal{V}[m]$, i.e., $h_i = \sum_{j=0}^{m} b_{i,j} v_{j,m}$, $b_{i,j} \in \{0,1\}$. We define a $k \times (m+1)$ *translation matrix* $\mathcal{B}[\mathcal{H}]$ whose entry in row i, column j is $b_{i,j}$, $0 \leq i \leq k-1$, $0 \leq j \leq m$.

Let $\mathbb{Z}_{m+1} = \{0, 1, \ldots, m\}$ be the set of columns of $\mathcal{B}[\mathcal{H}]$. Let Π_1, Π_2, Π_3, be three disjoint nonempty subsets of $\mathbb{Z}_{m+1}$ such that $m \in \Pi_3$. If for any such three subsets, there exists a row of $\mathcal{B}[\mathcal{H}]$ in which

- the number of *ones* in the columns of Π_3 is odd;

- the number of *ones* in the columns of Π_1 is odd or the number of *ones* in the columns of Π_2 is odd;

then the matrix $\mathcal{B}[\mathcal{H}]$ will be called **stopping free**.

Let $\mathcal{A}$ be an $r \times n$ binary matrix and let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be t distinct integers between 0 and $n-1$. $\mathcal{A}(\alpha_1, \alpha_2, \ldots, \alpha_t)$ is the projection of $\mathcal{A}$ onto the columns $\alpha_1, \alpha_2, \ldots, \alpha_t$. For a set of columns S, we denote by $\mathcal{A}(S)$ the projection of $\mathcal{A}$ onto the set of columns S. The set of $b-a+1$ consecutive integers $\{a, a+1, \ldots, b\}$ will be denoted by $[a..b]$.

Lemma 5: Let $\mathcal{H}$ be an $(m+k) \times 2^m$ parity-check matrix of $\mathcal{R}(m-2, m)$ whose first m rows are the first m rows of $\mathcal{V}[m]$. $\mathcal{H}$ has stopping distance 4 if and only if $\mathcal{B}[\mathcal{H}]$ is stopping free.

Proof: The first m rows of $\mathcal{H}$ are the first m rows of $\mathcal{V}[m]$. Hence, we can consider each of these rows as a Boolean variable and a column in these m rows as an assignment of Boolean values to these m variables. There are 2^m distinct columns. Each one has one of the 2^m different assignments of boolean values to these m variables. Consider now three different columns α, ξ, and γ of $\mathcal{H}$. If $\mathcal{H}$ has stopping distance 4 then $\mathcal{H}(\alpha, \xi, \gamma)$ must have a row of weight one. If the first m rows of $\mathcal{H}(\alpha, \xi, \gamma)$ do not have such a row of weight one then each one of these m rows has one of the values $000, 111, 011, 101$, or 110. Note, that at least two of the three patterns $011, 101, 110$, must appear as a row since otherwise there will be two identical columns in the first m rows of $\mathcal{H}(\alpha, \xi, \gamma)$. The last k rows of $\mathcal{H}$ (and hence also of $\mathcal{H}(\alpha, \xi, \gamma)$) are linear combinations of the first m rows and the all-ones vector. We distinguish between the following two cases.

Case 1: Exactly two of these three patterns appear (without loss of generality (w.l.o.g.) we assume that 011 and 101 are these patterns). As in the last k rows of $\mathcal{H}(\alpha, \xi, \gamma)$, we must have a row of weight one and this row is a linear combination of the $m+1$ rows of $\mathcal{V}[m](\alpha, \xi, \gamma)$ we must have in this combination the following set of conditions fulfilled.

- An odd number of vectors which correspond to the pattern 011 or an odd number of vectors which correspond to the pattern 101.
- An odd number of vectors which correspond to the pattern 111 (including the all-ones row of $\mathcal{V}[m]$).
- Each one of the vectors which corresponds to the pattern 000 can appear in the combination (but also can be omitted).

Let

$$\Pi_1 = \{i : v_{i,m}(\alpha, \xi, \gamma) = 011,\ 0 \le i \le m-1\}$$
$$\Pi_2 = \{i : v_{i,m}(\alpha, \xi, \gamma) = 101,\ 0 \le i \le m-1\}$$
$$\Pi_3 = \{i : v_{i,m}(\alpha, \xi, \gamma) = 111,\ 0 \le i \le m\}.$$

Note, that each of these sets is nonempty, but otherwise can contain any element between 0 to $m-1$ provided they are all disjoint. It can be verified now that the set of conditions is satisfied for any α, ξ, and γ, if and only if $\mathcal{B}[\mathcal{H}]$ is stopping free.

Case 2: All three patterns appear. Similarly, in the last k rows of $\mathcal{H}(\alpha, \xi, \gamma)$, we must have a row of weight one and this row is linear combination of the $m+1$ rows of $\mathcal{V}[m](\alpha, \xi, \gamma)$, so we must have in this combination the following set of conditions fulfilled.

- An odd number of vectors which correspond to the pattern 011 or an odd number of vectors which correspond to the pattern 101, or an odd number of vectors which correspond to the pattern 110, but not an odd number of vectors for all the three patterns.
- An odd number of vectors which correspond to the pattern 111 (including the all-ones row of $\mathcal{V}[m]$).
- Each one of the vectors which correspond to the pattern 000 can appear in the combination (but also can be omitted).

This case is resolved similarly to Case 1. We need to give a slightly different definitions for Π_1 and Π_2 from those given in Case 1. We leave the definitions to the reader.

Thus, $\mathcal{H}$ has stopping distance 4 if and only if $\mathcal{B}[\mathcal{H}]$ is stopping free. □

Let $\mathcal{H}$ be an $(m+k) \times 2^m$, $0 < k < m-1$, parity-check matrix of $\mathcal{R}(m-2, m)$ whose first m rows are the first m rows of $\mathcal{V}[m]$ and let $\mathcal{B}[\mathcal{H}] = [\beta_0, \beta_1, \ldots, \beta_m]$ be its translation matrix. Assume further that the last column of $\mathcal{B}[\mathcal{H}]$ is the all-ones column vector. Assume that the maximum number of linearly independent columns from the first m columns of $\mathcal{B}[\mathcal{H}]$ is τ. Let Δ be a set of such τ linearly independent columns. We distinguish between two cases.

Case 1: Column m of $\mathcal{B}[\mathcal{H}]$ is linearly dependent in the columns of Δ. Let $\Delta_1 \subseteq \Delta$ be the set of columns from Δ which sums to all-ones column vector. Clearly, $\tau \le m-2$, since $k < m-1$, and hence there are at least two columns, except for column m, which are not in Δ_1. Let Π_1 be a set with one of these columns, Π_2 a set with a second column, and $\Pi_3 = \Delta_1 \cup \{m\}$. Since the sum of the columns of Π_3 is the all-zeroes column vector, it follows that all the rows of $\mathcal{B}[\mathcal{H}](\Pi_3)$ have even weight and hence $\mathcal{B}[\mathcal{H}]$ is not stopping free.

Case 2: Column m and the columns of Δ are linearly independent. Therefore, $\tau < k$, and there are at least three columns in the first m columns of $\mathcal{B}[\mathcal{H}]$ which are not in Δ. Let β_x and β_y be two of these three column vectors. Since Δ is a maximal set of independent columns it follows that β_x and β_y are linear combinations of columns from Δ. Hence, we can write

$$\beta_x = \sum_{z \in \Delta_1} \beta_z + \sum_{z \in \Delta_3} \beta_z$$

and

$$\beta_y = \sum_{z \in \Delta_2} \beta_z + \sum_{z \in \Delta_3} \beta_z$$

where $\Delta_i \subset \Delta$, $i \in \{1,2,3\}$, and for $i \ne j$, $\Delta_i \cap \Delta_j = \emptyset$, $i, j \in \{1,2,3\}$. Now, let $\Pi_1 = \Delta_1 \cup \{x\}$, $\Pi_2 = \Delta_2 \cup \{y\}$, and $\Pi_3 = \Delta_3 \cup \{m\}$. Note that the number of *ones* in each row of $\mathcal{B}[\mathcal{H}](\Pi_1 \cup \Delta_3)$ is even, and the number of *ones* in each row of $\mathcal{B}[\mathcal{H}](\Pi_2 \cup \Delta_3)$ is even. Consider a row ζ in $\mathcal{B}[\mathcal{H}]$, we distinguish between two subcases.

Case 2.1: The number of *ones* in row ζ of $\mathcal{B}[\mathcal{H}](\Delta_3)$ is odd. It follows that the number of *ones* in row ζ of $\mathcal{B}[\mathcal{H}](\Pi_3)$ is even.

Case 2.2: The number of *ones* in row ζ of $\mathcal{B}[\mathcal{H}](\Delta_3)$ is even. It follows that the number of *ones* in row ζ of $\mathcal{B}[\mathcal{H}](\Pi_1)$ is even and the number of *ones* in row ζ of $\mathcal{B}[\mathcal{H}](\Pi_2)$ is even.

Both subcases imply that $\mathcal{B}[\mathcal{H}]$ is not stopping free.

This analysis of the matrix $\mathcal{B}[\mathcal{H}]$ in which the last column is the all-ones vector is generalized to a general matrix $\mathcal{B}[\mathcal{H}]$ in the following lemma. In fact, the case in which the last column is the all-ones vector is covered by this lemma. We have given it as it clarifies in a simple way the more general and complicated case.

Lemma 6: If $\mathcal{H}$ is an $(m+k)\times 2^m$, $0<k<m-1$, parity-check matrix of $\mathcal{R}(m-2,m)$, whose first m rows are the first m rows of $\mathcal{V}[m]$, then $\mathcal{B}[\mathcal{H}]$ is not stopping free.

Proof: From the discussion preceding the lemma we have that $\mathcal{B}[\mathcal{H}]=[\beta_0,\beta_1,\ldots,\beta_m]$ is not stopping free if its last column is the all-ones vector. By definition it is not stopping free if the last column is the all-zeroes vector. Hence, we can assume that the last column of $\mathcal{B}[\mathcal{H}]$ has exactly t *ones*, where $0<t<k$. Again, w.l.o.g. we assume that the t *ones* are in the first t rows of $\mathcal{B}[\mathcal{H}]$. Let $\mathcal{B}'[\mathcal{H}]=[\beta'_0,\beta'_1,\ldots,\beta'_m]$ be the $t\times(m+1)$ matrix obtained from the first t rows of $\mathcal{B}[\mathcal{H}]$ and let $\mathcal{B}''[\mathcal{H}]=[\beta''_0,\beta''_1,\ldots,\beta''_m]$ be the $(k-t)\times(m+1)$ matrix obtained from the last $k-t$ rows of $\mathcal{B}[\mathcal{H}]$. Let τ be the maximum number of linearly independent columns from the first m columns of $\mathcal{B}'[\mathcal{H}]$ and let Δ be a corresponding set with τ columns indices. Let x be a column index, $0\le x\le m-1$, which is not in Δ. We write β'_x as a linear combination of columns from $\mathcal{B}'[\mathcal{H}](\Delta)$, i.e., $\beta'_x=\sum_{z\in\Delta_1}\beta'_z$, where $\Delta_1\subseteq\Delta$. Let Δ_2 be the set of columns indices which are not in Δ and does not include both x and m. One can easily verify that $\tau=|\Delta|\le t$ and $|\Delta_2|=m-\tau-1$. Δ_2 has $2^{m-\tau-1}-1$ nonempty subsets. Let Y be a nonempty subset of Δ_2 and let $\Gamma_1(Y),\Gamma_2(Y),\Gamma_3(Y)$ be three disjoint subsets of Δ such that

$$\Delta_1=\Gamma_1(Y)\cup\Gamma_3(Y) \tag{2}$$

$$\beta'_x=\sum_{z\in\Gamma_1(Y)}\beta'_z+\sum_{z\in\Gamma_3(Y)}\beta'_z \tag{3}$$

$$\sum_{z\in Y}\beta'_z=\sum_{z\in\Gamma_2(Y)}\beta'_z+\sum_{z\in\Gamma_3(Y)}\beta'_z \tag{4}$$

and let

$$\mathcal{L}(Y,x)=\sum_{z\in\Gamma_3(Y)}\beta''_z \tag{5}$$

i.e., $\Gamma_3(Y)$ refers to the set of columns from Δ which appears in the linear combination which sums to β'_x and also appears in the linear combination which sums to $\sum_{z\in Y}\beta'_z$. $\mathcal{L}(Y,x)$ is the sum of the corresponding columns in $\mathcal{B}''[\mathcal{H}]$.

$\mathcal{L}(Y,x)$ is a column vector of length $k-t$ and hence there are 2^{k-t} possible values for $\mathcal{L}(Y,x)$. Since $k<m-1$ and $\tau\le t$, it follows that $2^{k-t}<2^{m-\tau-1}-1$ and hence there exist two different nonempty subsets Y_1, Y_2, of Δ_2, such that $\mathcal{L}(Y_1,x)=\mathcal{L}(Y_2,x)$.

Let Λ_i, $1\le i\le 7$, be the unique seven disjoint subsets of Δ which fulfill the following set of nine conditions, which are an extension of (2)–(4).

$$\begin{aligned}
\Gamma_1(Y_1)&=\Lambda_1\cup\Lambda_5.\\
\Gamma_2(Y_1)&=\Lambda_2\cup\Lambda_6\\
\Gamma_3(Y_1)&=\Lambda_4\cup\Lambda_7\\
\Gamma_1(Y_2)&=\Lambda_1\cup\Lambda_4\\
\Gamma_2(Y_2)&=\Lambda_3\cup\Lambda_6\\
\Gamma_3(Y_2)&=\Lambda_5\cup\Lambda_7
\end{aligned} \tag{6,7}$$

$$\beta'_x=\sum_{z\in\Lambda_1}\beta'_z+\sum_{z\in\Lambda_4}\beta'_z+\sum_{z\in\Lambda_5}\beta'_z+\sum_{z\in\Lambda_7}\beta'_z \tag{8}$$

$$\sum_{z\in Y_1}\beta'_z=\sum_{z\in\Lambda_2}\beta'_z+\sum_{z\in\Lambda_4}\beta'_z+\sum_{z\in\Lambda_6}\beta'_z+\sum_{z\in\Lambda_7}\beta'_z \tag{9}$$

$$\sum_{z\in Y_2}\beta'_z=\sum_{z\in\Lambda_3}\beta'_z+\sum_{z\in\Lambda_5}\beta'_z+\sum_{z\in\Lambda_6}\beta'_z+\sum_{z\in\Lambda_7}\beta'_z. \tag{10}$$

From (5) and (6) we have

$$\mathcal{L}(Y_1,x)=\sum_{z\in\Lambda_4}\beta''_z+\sum_{z\in\Lambda_7}\beta''_z. \tag{11}$$

From (5) and (7) we have

$$\mathcal{L}(Y_2,x)=\sum_{z\in\Lambda_5}\beta''_z+\sum_{z\in\Lambda_7}\beta''_z. \tag{12}$$

Consider now the subset Y_3 of Δ_2 defined by $Y_3=Y_1\cup Y_2\setminus(Y_1\cap Y_2)$. By (9) and (10) we have

$$\sum_{z\in Y_3}\beta'_z=\sum_{z\in\Lambda_2}\beta'_z+\sum_{z\in\Lambda_3}\beta'_z+\sum_{z\in\Lambda_4}\beta'_z+\sum_{z\in\Lambda_5}\beta'_z. \tag{13}$$

By (3), (4), (8), and (13)

$$\Gamma_3(Y_3)=\Lambda_4\cup\Lambda_5 \tag{14}$$

and by (5) and (14) we have

$$\mathcal{L}(Y_3,x)=\sum_{z\in\Lambda_4}\beta''_z+\sum_{z\in\Lambda_5}\beta''_z\,.$$

By (11), (12), and since $\mathcal{L}(Y_1,x)=\mathcal{L}(Y_2,x)$ we have

$$\mathcal{L}(Y_3,x)=\sum_{z\in\Lambda_4}\beta''_z+\sum_{z\in\Lambda_5}\beta''_z=\mathbf{0} \tag{15}$$

where $\mathbf{0}$ is the all-zeroes column vector.

Now, we want to show that $\mathcal{B}[\mathcal{H}]$ is not stopping free. We define the following three subsets of $\mathbb{Z}_{m+1}$: $\Pi_1=\{x\}\cup\Lambda_1\cup\Lambda_7$, $\Pi_2=Y_3\cup\Lambda_2\cup\Lambda_3$, $\Pi_3=\Lambda_4\cup\Lambda_5\cup\{m\}$.

First, we have to show that Π_1, Π_2, and Π_3 are nonempty. This is easy to verify since $x\in\Pi_1$; $Y_1\ne Y_2$ implies that $Y_3=Y_1\cup Y_2\setminus(Y_1\cap Y_2)\ne\emptyset$, i.e., Π_2 is nonempty; and $m\in\Pi_3$.

Next, we have to show that for each row of $\mathcal{B}[\mathcal{H}]$ one of the following holds:

- the number of *ones* in the columns of Π_3 is even;
- the number of *ones* in the columns of Π_1 is even and the number of *ones* in the columns of Π_2 is even.

Consider row j of $\mathcal{B}[\mathcal{H}]$. We distinguish between three cases.

Case 1: $0\le j\le t-1$ and the number of *ones* in row j of $\mathcal{B}[\mathcal{H}](\Lambda_4\cup\Lambda_5)$ is odd. Since column m of row j has a *one*, it follows that the number of *ones* in row j of $\mathcal{B}[\mathcal{H}](\Pi_3)$ is even.

Case 2: $0\le j\le t-1$ and the number of *ones* in row j of $\mathcal{B}[\mathcal{H}](\Lambda_4\cup\Lambda_5)$ is even. Since by (8) in row j the number of *ones* in $\mathcal{B}[\mathcal{H}](\{x\}\cup\Lambda_1\cup\Lambda_4\cup\Lambda_5\cup\Lambda_7)$ is even (note that $\{x\}$, Λ_1, Λ_4, Λ_5, Λ_7, are disjoint subsets), and by (13) the number of *ones* in row j of $\mathcal{B}[\mathcal{H}](Y_3\cup\Lambda_2\cup\Lambda_3\cup\Lambda_4\cup\Lambda_5)$ is even (note that Y_3, Λ_2, Λ_3, Λ_4, Λ_5, are disjoint subsets), it follows that in

row j the number of *ones* in $\mathcal{B}[\mathcal{H}](\Pi_1)$ is even and the number of *ones* in $\mathcal{B}[\mathcal{H}](\Pi_2)$ is even.

Case 3: $t \leq j \leq k-1$. By (15) we have that the number of *ones* in row j of $\mathcal{B}[\mathcal{H}](\Lambda_4 \cup \Lambda_5)$ is even. Since column m of row j has a *zero*, it follows that the number of *ones* in row j of $\mathcal{B}[\mathcal{H}](\Pi_3)$ is even.

Thus, $\mathcal{B}[\mathcal{H}]$ is not stopping free. □

As a consequence of Lemmas 1 and 3–6, we have the following.

Theorem 1: The stopping redundancy of the extended Hamming code ($\mathcal{R}(m-2,m)$) is $2m-1$.

Corollary 1: The following matrix is a parity-check matrix of $\mathcal{R}(m-2,m)$ with $2m-1$ rows and stopping distance 4:

$$\begin{bmatrix} v_{0,m} \\ v_{1,m} \\ v_{2,m} \\ \vdots \\ v_{m-1,m} \\ \bar{v}_{0,m} \\ \bar{v}_{1,m} \\ \vdots \\ \bar{v}_{m-2,m} \end{bmatrix}$$

where $\bar{v}_{i,m} = v_{i,m} + v_{m,m}$.

How many nonisomorphic parity-check matrices of $\mathcal{R}(m-2,m)$ with stopping distance 4 have redundancy $2m-1$? We conjecture that there are exactly two nonisomorphic parity-check matrices. The first one is $\mathcal{P}_m$ and the second one is defined recursively by

$$\mathcal{P}'_2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$\mathcal{P}'_m = \begin{bmatrix} 00\cdots0 & 11\cdots1 \\ 11\cdots1 & 00\cdots0 \\ \mathcal{P}'_{m-1} & \mathcal{P}'_{m-1} \end{bmatrix}, \qquad m \geq 3.$$

III. Codes With Minimum Distance 4

The extended Hamming code is only one of the linear codes with minimum distance 4. The stopping redundancy of all codes with minimum distance less than 4 is known [8].

Theorem 2: Let $\mathcal{C}$ be a binary linear code with minimum distance $d(\mathcal{C}) \leq 3$. Then **any** parity-check matrix H of $\mathcal{C}$ satisfies $s(H) = d(\mathcal{C})$, and therefore $\rho(\mathcal{C}) = r(\mathcal{C})$.

Theorem 2 implies that the first distance d for which the stopping redundancy of codes with minimum distance d is unknown is 4. Schwartz and Vardy [8] also provide an upper bound on the stopping redundancy of linear codes with minimum distance 4.

Theorem 3: Let $\mathcal{C}$ be an $(n,k,3)$ binary linear code. Then the extended code $\mathcal{C}_e$ is an $(n+1,k,4)$ code with

$$\rho(\mathcal{C}_e) \leq 2\rho(\mathcal{C}) = 2r(\mathcal{C}) - 2.$$

Theorem 3 can be slightly improved.

Theorem 4: Let $\mathcal{C}$ be an $(n,k,3)$ binary linear code. Then the extended code $\mathcal{C}_e$ is an $(n+1,k,4)$ code with

$$\rho(\mathcal{C}_e) \leq 2\rho(\mathcal{C}) - 1 = 2r(\mathcal{C}) - 3.$$

Proof: Let H be and arbitrary $r(\mathcal{C}) \times n$ parity-check matrix for $\mathcal{C}$. Assume that

$$H = \begin{bmatrix} H' \\ a_0 a_1 \cdots a_{n-1} \end{bmatrix}$$

where H' is an $(r(\mathcal{C})-1) \times n$ matrix. We construct a parity-check matrix H_e as follows:

$$H_e = \begin{bmatrix} H & \mathbf{0} \\ \bar{H}' & \mathbf{1} \end{bmatrix}$$

where $\bar{T}$ is the bitwise complement of T, and $\mathbf{0}$, $\mathbf{1}$ are the all-zeroes and all-ones column vectors, respectively. Obviously the matrix

$$\begin{bmatrix} H & \mathbf{0} \\ 11\cdots1 & 1 \end{bmatrix}$$

is a parity-check matrix of $\mathcal{C}_e$. It is easy to verify that this matrix and H_e span the same vector space and hence H_e is a parity-check matrix for $\mathcal{C}_e$.

Let $\mathcal{I}$, $|\mathcal{I}| \leq 3$, be a subset of $\mathbb{Z}_{n+1}$. We have to show that $H_e(\mathcal{I})$ has a row with weight one. By Theorem 2, we have to consider only subsets for which $|\mathcal{I}| = 3$. If $n \in \mathcal{I}$ then the claim follows from the fact that any two columns of $\mathcal{H}$ are distinct. Assume $\mathcal{I} = \{\alpha, \xi, \gamma\}$, $n \notin \mathcal{I}$; each one of the matrices $\mathcal{H}_e(\alpha,\xi)$, $\mathcal{H}_e(\alpha,\gamma)$, $\mathcal{H}_e(\xi,\gamma)$, must have a row with weight one. Hence, in $\mathcal{H}(\alpha,\xi,\gamma)$ there are at least two rows with weights one or two. If one of them has weight one then the claim is proved. If they both have weight two then their complements have weight one and at least one of them appears in $\bar{\mathcal{H}}'(\alpha,\xi,\gamma)$.

Thus, $\rho(\mathcal{C}_e) \leq 2\rho(\mathcal{C}) - 1 = 2r(\mathcal{C}) - 3$. □

It is interesting to note that the bound of Theorem 4 is attained by the extended Hamming code as a consequence of Theorem 1.

IV. The Simplex Code

As noted in the Introduction, there is a tight connection between the first-order Reed–Muller codes and the simplex codes. The $(2^m, m+1, 2^{m-1})$ first-order Reed–Muller code is the dual code of the $(2^m, 2^m-m-1, 4)$ extended Hamming code; the $(2^m-1, m, 2^{m-1})$ simplex code is the dual of the $(2^m-1, 2^m-m-1, 3)$ Hamming code. We start to examine first the stopping redundancy of the $(2^m-1, m, 2^{m-1})$ simplex code $\mathcal{S}_m$. Consider the following generator matrix $\mathcal{G}_m$ of the simplex code:

$$\mathcal{G}_m = [g_1\ g_2\ \cdots\ g_{2^m-1}]$$

where the g_i's are the 2^m-1 different nonzero column vectors of length m.

The matrix $\mathcal{G}_m$ can be defined recursively as follows:

$$\mathcal{G}_2 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$\mathcal{G}_m = \begin{bmatrix} \mathcal{G}_{m-1} & \mathcal{G}_{m-1} & \mathbf{0} \\ 00\cdots0 & 11\cdots1 & 1 \end{bmatrix}, \qquad m \geq 3.$$

For each $m \geq 2$ we define a matrix $\mathcal{H}_m$ as follows:

$$\mathcal{H}_2 = [1 \quad 1 \quad 1]$$
$$\mathcal{H}_m = \begin{bmatrix} I_{2^{m-1}-1} & I_{2^{m-1}-1} & \mathbf{1} \\ \mathcal{H}_{m-1} & \mathbf{0}\cdots\mathbf{0} & \mathbf{0} \end{bmatrix}, \qquad m \geq 3.$$

The following lemma is a trivial observation.

Lemma 7: $\mathcal{H}_m$, $m \geq 2$, is the parity-check matrix for the simplex code of order m.

Lemma 8: The stopping distance of $\mathcal{H}_m$ is 2^{m-1}.

Proof: The proof is be induction on m. For $m = 2$ it is trivial that $s(\mathcal{H}_2) = 2$. For the induction step let $\mathcal{I} \subset \mathbb{Z}_{2^m}$, $|\mathcal{I}| \leq 2^{m-1} - 1$. We distinguish between three cases.

Case 1: $2^m - 2 \in \mathcal{I}$.

By the pigeon-hole principle, there is a pair $\{j, j+2^{m-1}-1\}$, $0 \leq j \leq 2^{m-1} - 2$, such that $\mathcal{I} \cap \{j, j + 2^{m-1} - 1\} = \emptyset$. Therefore, row j of $\mathcal{H}_m(\mathcal{I})$ has weight one.

Case 2: $2^m - 2 \notin \mathcal{I}$ and there exists a j, $0 \leq j \leq 2^{m-1} - 2$, such that $\left|\mathcal{I} \cap \{j, j + 2^{m-1} - 1\}\right| = 1$.

Row j of $\mathcal{H}_m(\mathcal{I})$ has weight one.

Case 3: $2^m - 2 \notin \mathcal{I}$ and for each j, $0 \leq j \leq 2^{m-1} - 2$, we have $\left|\mathcal{I} \cap \{j, j + 2^{m-1} - 1\}\right| \in \{0, 2\}$.

The size of $\mathcal{I}$ is even, $\left|\mathcal{I} \cap [0..2^{m-1} - 2]\right| = \left|\mathcal{I} \cap [2^{m-1} - 1..2^m - 2]\right| \leq 2^{m-2} - 1$. Therefore, by the induction hypothesis the projection of the $2^{m-1} - m$ bottom rows of $\mathcal{H}_m$ onto $\mathcal{I}$ contains a row with weight one

Thus, the stopping distance of $\mathcal{H}_m$ is 2^{m-1}. □

Theorem 5: The stopping redundancy of the $(2^m - 1, m, 2^{m-1})$ simplex code is $2^m - m - 1$.

Proof: By Lemma 8, the stopping distance of $\mathcal{H}_m$ is 2^{m-1} which is the minimum Hamming distance of the simplex code. Since the redundancy of the simplex code is $2^m - m - 1$ which is also the number of rows in $\mathcal{H}_m$, it follows that the stopping redundancy of the $(2^m-1, m, 2^{m-1})$ simplex code is 2^m-m-1. □

The simplex codes are a family of codes with the property that the redundancy of the codes in the family equals their stopping redundancy. Schwartz and Vardy [8] gave two recursive constructions which obtain other families of codes with this property. Their constructions are summarized in the following two theorems.

Theorem 6: Let $\mathcal{C}_1$, $\mathcal{C}_2$ be (n_1, k_1, d_1), (n_2, k_2, d_2) binary linear codes with $\rho(\mathcal{C}_1) = r(\mathcal{C}_1) = n_1 - k_1$, $\rho(\mathcal{C}_2) = r(\mathcal{C}_2) = n_2 - k_2$, respectively. Then $\mathcal{C}_3 = \{(u, v) : u \in \mathcal{C}_1, v \in \mathcal{C}_2\}$ is an $(n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\})$ code with $\rho(\mathcal{C}_3) = r(\mathcal{C}_3) = n_1 + n_2 - (k_1 + k_2)$. If $\mathcal{H}_1$ and $\mathcal{H}_2$ are the corresponding parity-check matrices of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, then

$$\mathcal{H}_3 = \begin{bmatrix} \mathcal{H}_1 & \mathbf{0} \\ \mathbf{0} & \mathcal{H}_2 \end{bmatrix}$$

is the corresponding parity-check matrix of $\mathcal{C}_3$.

Theorem 7: Let $\mathcal{C}_1$ be an (n, k, d) binary linear code with $\rho(\mathcal{C}_1) = r(\mathcal{C}_1) = n - k$. Then the code $\mathcal{C}_2 = \{(u, u) : u \in \mathcal{C}_1\}$ is a $(2n, k, 2d)$ code with $\rho(\mathcal{C}_2) = r(\mathcal{C}_2) = 2n - k$. If $\mathcal{H}_1$ is the corresponding parity-check matrix of $\mathcal{C}_1$ then

$$\mathcal{H}_2 = \begin{bmatrix} I_n & I_n \\ \mathcal{H}_1 & \mathbf{0} \end{bmatrix}$$

is the corresponding parity-check matrix of $\mathcal{C}_2$.

The proof that the stopping redundancy of the simplex code equals its redundancy is a special case of the following theorems which are proved similarly to Theorem 5.

Theorem 8: Let $\mathcal{C}_1$ be an (n, k, d) binary linear code with $\rho(\mathcal{C}_1) = r(\mathcal{C}_1) = n - k$. Then the code
$$\mathcal{C}_2 = \{(u, u, 0) : u \in \mathcal{C}_1\} \cup \{(u, \bar{u}, 1) : u \in \mathcal{C}_1\}$$
is a $(2n+1, k+1, \min\{n+1, 2d\})$ code with $\rho(\mathcal{C}_2) = r(\mathcal{C}_2) = 2n-k$. If $\mathcal{H}_1$ is the corresponding parity-check matrix of $\mathcal{C}_1$ then

$$\mathcal{H}_2 = \begin{bmatrix} I_n & I_n & \mathbf{1} \\ \mathcal{H}_1 & \mathbf{0}\cdots\mathbf{0} & \mathbf{0} \end{bmatrix}$$

is the corresponding parity-check matrix of $\mathcal{C}_2$.

Theorem 9: Let $\mathcal{C}_1$ be an (n, k, d) binary linear code with $\rho(\mathcal{C}_1) = r(\mathcal{C}_1) = n - k$. Then the code
$$\mathcal{C}_2 = \{(u, v, u, 0) : (u, v) \in \mathcal{C}_1\} \cup \{(u, v, \bar{u}, 1) : (u, v) \in \mathcal{C}_1\}$$
where the length of v is ℓ, is a $(2n - \ell + 1, k + 1, \min\{n - \ell + 1, 2d - \ell\})$ code with $\rho(\mathcal{C}_2) = r(\mathcal{C}_2) = 2n - \ell - k$. If $\mathcal{H}_1$ is the corresponding parity-check matrix of $\mathcal{C}_1$ then

$$\mathcal{H}_2 = \begin{bmatrix} I_{n-\ell}\tilde{\mathbf{0}} & I_{n-\ell} & \mathbf{1} \\ \mathcal{H}_1 & \mathbf{0}\cdots\mathbf{0} & \mathbf{0} \end{bmatrix}$$

where $\tilde{\mathbf{0}}$ is an $(n-\ell) \times \ell$ all-zeroes matrix, is the corresponding parity-check matrix of $\mathcal{C}_2$.

The combination of Theorems 6 through 9 can be used to obtain various codes for which the stopping redundancy is equal to the redundancy. Some of these codes can be proved to have the largest dimension, given their length and minimum distance. For many others we suspect this is the case too.

V. First-Order Reed–Muller Codes

The first-order Reed–Muller code can be obtained easily from the simplex code. Let $\mathcal{S}_m$ be the $(2^m - 1, m, 2^{m-1})$ simplex code. The $(2^m, m + 1, 2^{m-1})$ first-order Reed–Muller code $\mathcal{R}(1, m)$ can be defined by $\{(u, 0) : u \in \mathcal{S}_m\} \cup \{(\bar{u}, 1) : u \in \mathcal{S}_m\}$.

The following matrix is a generator matrix of $\mathcal{R}(1, 3)$:

$$\mathcal{G}(1,3) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

We define now the generator matrix $\mathcal{G}(1, m)$ of $\mathcal{R}(1, m)$ recursively from $\mathcal{G}(1, 3)$

$$\mathcal{G}(1, m) = \begin{bmatrix} \mathcal{G}(1, m-1) & \mathcal{G}(1, m-1) \\ 00\cdots0 & 11\cdots1 \end{bmatrix}.$$

It was asked in [8] whether $\rho(\mathcal{R}(1,m))$ is equal to the number of rows in the parity-check matrix obtained via (1) starting with the parity-check matrix

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \tag{16}$$

for $\mathcal{R}(1,3)$. Indeed, $\rho(\mathcal{R}(1,3)) = 5$, while for larger lengths the construction yields $\rho(\mathcal{R}(1,4)) \leq 17$, $\rho(\mathcal{R}(1,5)) \leq 49$, and $\rho(\mathcal{R}(1,6)) \leq 129$, and generally $\rho(\mathcal{R}(1,m)) \leq (m-2)2^{m-1}+1$. We will prove that $\rho(\mathcal{R}(1,4)) \leq 15$, $\rho(\mathcal{R}(1,5)) \leq 41$, and $\rho(\mathcal{R}(1,6)) \leq 103$. In general our main result in this section is as follows.

Theorem 10: For $m \geq 2$

$$\rho(\mathcal{R}(1,m)) \leq \frac{(6m-7)2^{m-1} + (-1)^{m-1}}{9}.$$

This result reduces the number of rows in a parity-check matrix with no stopping sets of size $2^{m-1}-1$ or less by one third compared to the recursive construction of [8]. The proof of Theorem 10 is by constructing a parity-check matrix for $\mathcal{R}(1,m)$. This matrix will consist of a few submatrices of the parity-check matrices of $\mathcal{R}(1,n)$, $n < m$. We will first present these submatrices with their properties. The first lemma presents one of the main ideas for reducing the number of rows in our parity-check matrix. The proof is trivial and hence it is omitted. We will say that a subset $\mathcal{I}$ of columns are covered by a matrix $\mathcal{A}$ if $\mathcal{A}(\mathcal{I})$ contains a row with weight one. In this case, we also say that $\mathcal{A}$ covers the subset $\mathcal{I}$.

Lemma 9: Assume $\mathcal{I} = \{\ell_1, \ell_2, \ldots, \ell_k\} \subset \mathbb{Z}_{2^{n-1}}$, $k \leq 2^{n-2}-1$ is covered by the $r \times 2^{n-1}$ matrix

$$\begin{bmatrix} \mathcal{A}_{n-1} \\ \mathcal{B}_{n-1} \end{bmatrix}.$$

Then the subset $\{\ell_1, \ell_2, \ldots, \ell_k, 2^{n-1}+\ell_1, 2^{n-1}+\ell_2, \ldots, 2^{n-1}+\ell_k\}$ is covered by the matrix

$$\begin{bmatrix} \mathcal{A}_{n-1} & \mathbf{0} \\ \mathbf{0} & \mathcal{B}_{n-1} \end{bmatrix}.$$

We will present now a few types of matrices which will be used in the recursion for the proof of Theorem 10. For any given matrix $\mathcal{A}$, let $\mathcal{A}^i$ be the right cyclic shift of $\mathcal{A}$ by i positions. Note that $\mathcal{A} = \mathcal{A}^0$.

For the first type of matrices we want to form a parity-check matrix for $\mathcal{R}(1,n)$, $n \geq 2$, called Ψ_n, such that given a subset $\mathcal{I} \subset \mathbb{Z}_{2^n}$, $0 \in \mathcal{I}$, $|\mathcal{I}| \leq 2^{n-1}-1$, of the columns, $\Psi_n(\mathcal{I})$ has a row of weight one. We first present the matrices Ψ_2 and Ψ_3, which are the basis for the recursive construction

$$\Psi_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\Psi_3 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

For a given integer $\ell \geq 1$ and $0 \leq i \leq 2^\ell - 1$, let Λ_ℓ^i be the following $(2^\ell - 1) \times 2^\ell$ matrix:

$$\Lambda_\ell^i = \begin{bmatrix} \mathbf{0} & \mathbf{1} & I_{2^\ell - 1 - i} \\ I_i & \mathbf{1} & \mathbf{0} \end{bmatrix}.$$

Ψ_n, $n \geq 4$, is defined by

$$\Psi_n = \begin{bmatrix} \Lambda_{n-1}^{2^{n-2}} & \Lambda_{n-1}^{2^{n-2}} \\ \Theta_{n-1} & \mathbf{0} \\ \mathbf{0} & \Psi_{n-1}^{2^{n-2}} \end{bmatrix}$$

$$\text{where} \qquad \Theta_{n-1} = \begin{bmatrix} \Psi_{n-2} & \mathbf{0} \\ \mathbf{0} & \Psi_{n-2} \end{bmatrix}. \tag{17}$$

Lemma 10: For a given n', assume that for all $3 \leq n \leq n'$, Ψ_n covers any subset $\mathcal{I} \subset \mathbb{Z}_{2^n}$ such that $|\mathcal{I}| \leq 2^{n-1}-1$ and $0 \in \mathcal{I}$. Then the matrix Δ_n defined by

$$\Delta_n = \begin{bmatrix} \Psi_n \\ \Theta_n \end{bmatrix} = \begin{bmatrix} \Lambda_{n-1}^{2^{n-2}} & \Lambda_{n-1}^{2^{n-2}} \\ \Theta_{n-1} & \mathbf{0} \\ \mathbf{0} & \Psi_{n-1}^{2^{n-2}} \\ \Psi_{n-1} & 0 \\ 0 & \Psi_{n-1} \end{bmatrix}, \qquad n \geq 4,$$

$$\Delta_3 = \begin{bmatrix} \Psi_3 \\ \Theta_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{18}$$

covers any subset $\mathcal{I}$ such that $|\mathcal{I}| \leq 2^{n-1}-1$, $0 \notin \mathcal{I}$, and $2^{n-1} \in \mathcal{I}$.

Proof: The proof is by induction on n. The basis of the induction is Δ_3. For the induction step let $n \geq 4$ and $\mathcal{I} \subset \mathbb{Z}_{2^n}$, such that $|\mathcal{I}| \leq 2^{n-1}-1$, $0 \notin \mathcal{I}$, and $2^{n-1} \in \mathcal{I}$. Let $\mathcal{I}_1 = \mathcal{I} \cap [0..2^{n-1}-1]$ and $\mathcal{I}_2 = \mathcal{I} \cap [2^{n-1}..2^n-1]$. We distinguish between four cases.

Case 1: $\left|\{2^{n-2}, 2^{n-1}+2^{n-2}\} \cap \mathcal{I}\right| = 0$.

The projection of $\begin{bmatrix} \Lambda_{n-1}^{2^{n-2}} & \Lambda_{n-1}^{2^{n-2}} \end{bmatrix}$ onto $\mathcal{I}$ has a row with weight one.

Case 2: $\left|\{2^{n-2}, 2^{n-1}+2^{n-2}\} \cap \mathcal{I}\right| = 1$.

By the pigeon-hole principle there exist at least one j, $0 \leq j \leq 2^{n-1}-1$, $j \neq 2^{n-2}$, such that $\left|\{j, 2^{n-1}+j\} \cap \mathcal{I}\right| = 0$. Hence, the projection of $\begin{bmatrix} \Lambda_{n-1}^{2^{n-2}} & \Lambda_{n-1}^{2^{n-2}} \end{bmatrix}$ onto $\mathcal{I}$ has a row with weight one

Case 3: $\left|\{2^{n-2}, 2^{n-1}+2^{n-2}\} \cap \mathcal{I}\right| = 2$ and $|\mathcal{I}_2| \leq 2^{n-2}-1$.

The third row of (18) implies that $\Delta_n(\mathcal{I})$ contains a row with weight one.

Case 4: $\left|\{2^{n-2}, 2^{n-1}+2^{n-2}\} \cap \mathcal{I}\right| = 2$ and $|\mathcal{I}_1| \leq 2^{n-2}-1$.

Since $0 \notin \mathcal{I}$, $2^{n-2} \in \mathcal{I}$, and the projection of the second and fourth rows of (18) onto $\mathbb{Z}_{2^{n-1}}$ is Δ_{n-1}, it follows by the induction hypothesis that $\Delta_n(\mathcal{I})$ contains a row with weight one. □

It is important to note at this point that by permuting columns of Δ_n, the resulting matrix will cover corresponding subsets to the permutation taken. This property will be trivially true of other matrices that we use, and we will use it quite often without mentioning it.

Lemma 11: The matrix Ψ_n, $n \geq 4$, is a parity-check matrix of $\mathcal{R}(1,n)$ which covers each subset $\mathcal{I} \subset \mathbb{Z}_{2^n}$ such that $|\mathcal{I}| \leq 2^{n-1}-1$ and $0 \in \mathcal{I}$.

Proof: The proof has two parts. First, we will prove that given any subset $\mathcal{I}, 0 \in \mathcal{I}, |\mathcal{I}| \leq 2^{n-1}-1$, $\Psi_n(\mathcal{I})$ has a row with weight one. After that we will prove that Ψ_n is a parity-check matrix of $\mathcal{R}(1,n)$.

The proof of the first part is by induction on n. We will use Ψ_2 and Ψ_3 as the induction basis. For the induction step let $\mathcal{I} \subset \mathbb{Z}_{2^n}, 0 \in \mathcal{I}, |\mathcal{I}| \leq 2^{n-1}-1$. Let $\mathcal{I}_1 = \mathcal{I} \cap [0..2^{n-1}-1]$ and $\mathcal{I}_2 = \mathcal{I} \cap [2^{n-1}..2^n-1]$. We distinguish between four cases.

Case 1: $\left|\{2^{n-2}, 2^{n-1}+2^{n-2}\} \cap \mathcal{I}\right| = 2$ and $|\mathcal{I}_2| \leq 2^{n-2}-1$.

Since $2^{n-1}+2^{n-2} \in \mathcal{I}_2$, it follows by the induction hypothesis on the bottom row of (17) that $\Psi_n(\mathcal{I})$ contains a row with weight one.

Case 2: $\left|\{2^{n-2}, 2^{n-1}+2^{n-2}\} \cap \mathcal{I}\right| = 2$ and $|\mathcal{I}_1| \leq 2^{n-2}-1$.

Let $\mathcal{I}'_1 = \mathcal{I} \cap [0..2^{n-2}-1]$ and $\mathcal{I}'_2 = \mathcal{I} \cap [2^{n-2}..2^{n-1}-1]$. Clearly, one of the following two holds: $0 \in \mathcal{I}'_1$ and $|\mathcal{I}'_1| \leq 2^{n-3}-1$, or $2^{n-2} \in \mathcal{I}'_2$ and $|\mathcal{I}'_2| \leq 2^{n-3}-1$. Therefore, by the induction hypothesis, the second row of (17) implies that $\Psi_n(\mathcal{I})$ contains a row with weight one.

Case 3: $\left|\{2^{n-2}, 2^{n-1}+2^{n-2}\} \cap \mathcal{I}\right| = 1$.

Since $|\mathcal{I}| \leq 2^{n-1}-1$ it follows by the pigeon-hole principle that there exist an integer $\ell \in \mathbb{Z}_{2^{n-1}}$ such that $\ell, 2^{n-1}+\ell \notin \mathcal{I}$. Therefore, the top row of (17) implies that $\Psi_n(\mathcal{I})$ contains a row with weight one.

Case 4: $\left|\{2^{n-2}, 2^{n-1}+2^{n-2}\} \cap \mathcal{I}\right| = 0$, and there exist an integer ℓ, $\ell \in \mathbb{Z}_{2^{n-1}}$ such that $\left|\{\ell, 2^{n-1}+\ell\} \cap \mathcal{I}\right| = 1$.

The top row of (17) implies that $\Psi_n(\mathcal{I})$ contains a row with weight one.

By examining the four cases, we infer that the only case which was not considered is $\left|\{2^{n-2}, 2^{n-1}+2^{n-2}\} \cap \mathcal{I}\right| = 0$, and there is no integer ℓ, $\ell \in \mathbb{Z}_{2^{n-1}}$ such that $\left|\{\ell, 2^{n-1}+\ell\} \cap \mathcal{I}\right| = 1$. Hence, $|\mathcal{I}| = 2k$, $1 \leq k \leq 2^{n-2}-1$, $\mathcal{I} = \{\ell_1, \ell_2, \ldots, \ell_k, 2^{n-1}+\ell_1, 2^{n-1}+\ell_2, \ldots, 2^{n-1}+\ell_k\}$, $\left|\{2^{n-2}, 2^{n-1}+2^{n-2}\} \cap \mathcal{I}\right| = 0$, and $\left|\{0, 2^{n-1}\} \cap \mathcal{I}\right| = 2$.

By the induction hypothesis the claim is proved for Ψ_μ, $\mu < n$. Therefore, by Lemma 10 the subset $\mathcal{I}' = \{\ell_1, \ell_2, \ldots, \ell_k\} \subset \mathbb{Z}_{2^{n-1}}$, $2^{n-2} \notin \mathcal{I}'$, is covered by the matrix

$$\begin{bmatrix} \Theta_{n-1} \\ \Psi_{n-1}^{2^{n-2}} \end{bmatrix} = \begin{bmatrix} \Psi_{n-2} & \mathbf{0} \\ \mathbf{0} & \Psi_{n-2} \\ \Lambda_{n-2}^{2^{n-3}} & \Lambda_{n-2}^{2^{n-3}} \\ \mathbf{0} & \Theta_{n-2} \\ \Psi_{n-2}^{2^{n-3}} & \mathbf{0} \end{bmatrix}.$$

Thus, by Lemma 9, the subset $\mathcal{I}$ is covered by the matrix

$$\begin{bmatrix} \Theta_{n-1} & \mathbf{0} \\ \mathbf{0} & \Psi_{n-1}^{2^{n-2}} \end{bmatrix}.$$

Hence, $\Psi_n(\mathcal{I})$ has a row with weight one.

Now, we have to prove that Ψ_n is a parity-check matrix of $\mathcal{R}(1,n)$, $n \geq 2$. The claim is proved again by induction. The induction basis is $n = 2$ and $n = 3$ for which the claim can be easily verified. The rows of $\begin{bmatrix} \Lambda_{n-1}^{2^{n-2}} & \Lambda_{n-1}^{2^{n-2}} \end{bmatrix}$ are linearly independent and belong to the orthogonal subspace of $\mathcal{G}(1,n)$. Clearly, these rows are linearly independent with any other linear combination of rows from $\begin{bmatrix} \mathbf{0} & \Psi_{n-1}^{2^{n-2}} \end{bmatrix}$. By using the induction hypothesis, we obtain that these rows of Ψ_n belong to the orthogonal subspace of $\mathcal{G}(1,n)$ and include $2^{n-1}-n$ linearly independent rows. Hence, the total number of linearly independent rows in Ψ_n is $2^{n-1}-1+2^{n-1}-n = 2^n-(n+1)$ and hence, Ψ_n is a parity-check matrix of $\mathcal{R}(1,n)$. □

Corollary 2: If h_n is the number of rows in Ψ_n then for $n \geq 4$, $h_n = 2^{n-1}-1+2h_{n-2}+h_{n-1}$.

Lemma 12:

$$h_n = \frac{(3n-5)2^{n+1}+9+(-1)^n}{18}$$

for $n \geq 2$.

Proof: The proof is by induction with the basis $h_2 = 1$ and $h_3 = 4$. □

It is interesting to note that the sequence $\{h_i\}_{i=2}^{\infty}$ appears in the on-line encyclopedia of integer sequences [6]. But, we couldn't find any connection between the two problems which generate these sequences.

The second type of submatrices of $\mathcal{R}(1,n)$ will be denoted by Π_n. A subset $\mathcal{I} \subset \mathbb{Z}_{2^{n-2}} \cup [2^{n-1}..2^{n-1}+2^{n-2}-1]$, $|\mathcal{I}| \leq 2^{n-2}-1$, should be covered by Π_n if one of the following holds:

- $\left|\mathcal{I} \cap [0..2^{n-2}-1]\right| \leq 2^{n-3}-1$ and $0, 2^{n-3} \in \mathcal{I}$;
- $\left|\mathcal{I} \cap [2^{n-1}..2^{2-1}+2^{n-2}-1]\right| \leq 2^{n-3}-1$ and 2^{n-1}, $2^{n-1}+2^{n-3}+2^{n-4} \in \mathcal{I}$;
- $|\mathcal{I}| = 2k$, $k \leq 2^{n-3}-1$, $\mathcal{I} = \{\ell_1, \ell_2, \ldots, \ell_k, 2^{n-1}+\ell_1, 2^{n-1}+\ell_2, \ldots, 2^{n-1}+\ell_k\}$, $0 \notin \mathcal{I}$, and $2^{n-3}, 2^{n-3}+2^{n-4} \in \mathcal{I}$.

Subsets of this type will be called triple uncovered subsets of order n.

We define

$$\Pi_n = \begin{bmatrix} \Phi_{n-2} & \tilde{\mathbf{0}} & \mathbf{0} & \tilde{\mathbf{0}} \\ \mathbf{0} & \tilde{\mathbf{0}} & \Gamma_{n-2} & \tilde{\mathbf{0}} \end{bmatrix} \tag{19}$$

where

$$\Phi_{n-2} = \begin{bmatrix} \Lambda_{n-4}^{2^{n-5}+2^{n-6}} & \mathbf{0} & \mathbf{0} & \Lambda_{n-4}^{2^{n-5}+2^{n-6}} \\ \Gamma_{n-4} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \Psi_{n-4}^{2^{n-5}+2^{n-6}} \\ \mathbf{0} & \Lambda_{n-4}^{2^{n-5}} & \Lambda_{n-4}^{2^{n-5}} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \Theta_{n-4} & \mathbf{0} \\ \mathbf{0} & \Psi_{n-4}^{2^{n-5}} & \mathbf{0} & \mathbf{0} \end{bmatrix} \tag{20}$$

$$\Gamma_{n-2} = \begin{bmatrix} \Lambda_{n-4}^{2^{n-5}} & \mathbf{0} & \Lambda_{n-4}^{2^{n-5}} & \mathbf{0} \\ \Phi_{n-4} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \Psi_{n-4}^{2^{n-5}} & \mathbf{0} \\ \mathbf{0} & \Lambda_{n-4}^{2^{n-5}} & \mathbf{0} & \Lambda_{n-4}^{2^{n-5}} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \Theta_{n-4} \\ \mathbf{0} & \Psi_{n-4}^{2^{n-5}} & \mathbf{0} & \mathbf{0} \end{bmatrix} \tag{21}$$

and $\tilde{\mathbf{0}}$ is a zero matrix with 2^{m-2} columns.

The following lemma is proved similarly to Lemma 11.

Lemma 13:

- Assume the matrix Φ_{n-2} covers each subset $\mathcal{I} \subset \mathbb{Z}_{2^{n-2}}$ such that $2 \leq |\mathcal{I}| \leq 2^{n-3}-1$ and $0, 2^{n-3} \in \mathcal{I}$. Then the matrix

$$\begin{bmatrix} \Lambda_{n-2}^{2^{n-3}} & \Lambda_{n-2}^{2^{n-3}} \\ \Phi_{n-2} & \mathbf{0} \\ \mathbf{0} & \Psi_{n-2}^{2^{n-3}} \end{bmatrix}$$

covers any subset $\mathcal{I} \subset \mathbb{Z}_{2^{n-1}}$ such that $|\mathcal{I}| \leq 2^{n-2}-1$ and $0 \in \mathcal{I}$.

- Assume the matrix Γ_{n-2} covers each subset $\mathcal{I}$ such that $2 \leq |\mathcal{I}| \leq 2^{n-3}-1$ and $0, 2^{n-3}+2^{n-4} \in \mathcal{I}$. Then the matrix

$$\begin{bmatrix} \Lambda_{n-2}^{2^{n-3}+2^{n-4}} & \Lambda_{n-2}^{2^{n-3}+2^{n-4}} \\ \Gamma_{n-2} & \mathbf{0} \\ \mathbf{0} & \Psi_{n-2}^{2^{n-3}+2^{n-4}} \end{bmatrix}$$

covers any subset $\mathcal{I}$ such that $|\mathcal{I}| \leq 2^{n-2}-1$ and $0 \in \mathcal{I}$.

Lemma 14: The matrix Φ_{n-2} covers each subset $\mathcal{I} \subset \mathbb{Z}_{2^{n-2}}$ such that $2 \leq |\mathcal{I}| \leq 2^{n-3}-1$ and $0, 2^{n-3} \in \mathcal{I}$. The matrix Γ_{n-2} covers each subset $\mathcal{I} \subset \mathbb{Z}_{2^{n-2}}$ such that $2 \leq |\mathcal{I}| \leq 2^{n-3}-1$ and $0, 2^{n-3}+2^{n-4} \in \mathcal{I}$.

Proof: The proof is by induction on n. The basis of the induction are the following four matrices, shown at the bottom of the page.

For the induction step, let $\mathcal{I} \subset \mathbb{Z}_{2^{n-2}}$, and we define the following eight subsets of $\mathcal{I}$:

- $\tilde{\mathcal{I}}_1 = \mathcal{I} \cap [0..2^{n-4}-1]$.
- $\tilde{\mathcal{I}}_2 = \mathcal{I} \cap [2^{n-4}..2^{n-3}-1]$.
- $\tilde{\mathcal{I}}_3 = \mathcal{I} \cap [2^{n-3}..2^{n-3}+2^{n-4}-1]$.
- $\tilde{\mathcal{I}}_4 = \mathcal{I} \cap [2^{n-3}+2^{n-4}..2^{n-2}-1]$.
- $\mathcal{I}_1 = \tilde{\mathcal{I}}_2 \cup \tilde{\mathcal{I}}_3$.
- $\mathcal{I}_2 = \tilde{\mathcal{I}}_2 \cup \tilde{\mathcal{I}}_4$.
- $\mathcal{I}_3 = \tilde{\mathcal{I}}_1 \cup \tilde{\mathcal{I}}_3$.
- $\mathcal{I}_4 = \tilde{\mathcal{I}}_1 \cup \tilde{\mathcal{I}}_4$.

We distinguish between two cases.

Case 1: $0, 2^{n-3} \in \mathcal{I}$.

This case has two subcases:

Case 1.1: $|\mathcal{I}_4| \leq 2^{n-4}-1$.

By Lemma 13 and by the induction hypothesis on Γ_{n-4} the first three rows of (20) cover $\mathcal{I}$.

Case 1.2: $|\mathcal{I}_1| \leq 2^{n-4}-1$.

By Lemma 11, the bottom three rows of (20) cover $\mathcal{I}$.

Case 2: $0, 2^{n-3}+2^{n-4} \in \mathcal{I}$.

This case has two subcases:

Case 2.1: $|\mathcal{I}_3| \leq 2^{n-4}-1$.

By Lemma 13 and by the induction hypothesis on Φ_{n-4}, the first three rows of (21) cover $\mathcal{I}$.

Case 2.2: $|\mathcal{I}_2| \leq 2^{n-4}-1$.

By Lemma 11, the bottom three rows of (21) cover $\mathcal{I}$. □

Lemma 15: The matrix Π_n covers all triple uncovered subsets of order n.

Proof: The proof is by induction on n. We claim that Π_n covers all triple uncovered subsets of order n. The basis for the induction are the matrices Π_5 and Π_6 as defined by (19).

For the remainder of our discussion we define again the following eight subsets of $\mathcal{I}$:

- $\tilde{\mathcal{I}}_1 = \mathcal{I} \cap [0..2^{n-4}-1]$.
- $\tilde{\mathcal{I}}_2 = \mathcal{I} \cap [2^{n-4}..2^{n-3}-1]$.
- $\tilde{\mathcal{I}}_3 = \mathcal{I} \cap [2^{n-3}..2^{n-3}+2^{n-4}-1]$.
- $\tilde{\mathcal{I}}_4 = \mathcal{I} \cap [2^{n-3}+2^{n-4}..2^{n-2}-1]$.
- $\mathcal{I}_1 = \tilde{\mathcal{I}}_2 \cup \tilde{\mathcal{I}}_3$.
- $\mathcal{I}_2 = \tilde{\mathcal{I}}_2 \cup \tilde{\mathcal{I}}_4$.
- $\mathcal{I}_3 = \tilde{\mathcal{I}}_1 \cup \tilde{\mathcal{I}}_3$.
- $\mathcal{I}_4 = \tilde{\mathcal{I}}_1 \cup \tilde{\mathcal{I}}_4$.

For the induction step, let $\mathcal{I}$ be a triple uncovered subset of order n. We distinguish between three cases.

Case 1: $\left|\mathcal{I} \cap [0..2^{n-2}-1]\right| \leq 2^{n-3}-1$ and $0, 2^{n-3} \in \mathcal{I}$. By Lemma 14, these subsets are covered by Φ_{n-2} (in Π_n).

Case 2: $\left|\mathcal{I} \cap [2^{n-1}..2^{n-1}+2^{n-2}-1]\right| \leq 2^{n-3}-1$ and $2^{n-1}, 2^{n-1}+2^{n-3}+2^{n-4} \in \mathcal{I}$. By Lemma 14, these subsets are covered by Γ_{n-2} (in Π_n).

Case 3: $|\mathcal{I}| = 2k$, $k \leq 2^{n-3}-1$, $\mathcal{I} = \{\ell_1, \ell_2, \ldots, \ell_k, 2^{n-1}+\ell_1, 2^{n-1}+\ell_2, \ldots, 2^{n-1}+\ell_k\}, 2^{n-3}, 2^{n-3}+2^{n-4} \in \mathcal{I}$, and $0 \notin \mathcal{I}$.

$$\Phi_3 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

$$\Gamma_3 = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$$\Phi_4 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\Gamma_4 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

We distinguish between four subcases.

Case 3.1: $|\mathcal{I}_1| \leq 2^{n-4} - 1$.

The third and the second columns of (20) consist of Ψ_{n-3} and since $2^{n-3} \in \mathcal{I}$, it follows from Lemma 11 that $\Pi_n(\mathcal{I})$ contains a row with weight one.

Case 3.2: $|\mathcal{I}_2| \leq 2^{n-4} - 1$.

This case is solved exactly as Case 3.1 with the fourth and second columns of (21).

Case 3.3: $|\mathcal{I}_3| \leq 2^{n-4} - 1$.

By considering the projection of the first row of (21) the only uncovered subsets are those in which $0 \notin \mathcal{I}_3$ and 2^{n-5}, $2^{n-3}, 2^{n-3} + 2^{n-5} \in \mathcal{I}_3$. If $\left|\tilde{\mathcal{I}}_3\right| \leq 2^{n-5} - 1$, then these subsets are covered by the top third row of (21). Thus, the only uncovered subsets are those in which $\left|\tilde{\mathcal{I}}_1\right| \leq 2^{n-5} - 1$, $0 \notin \tilde{\mathcal{I}}_1$, $2^{n-5} \in \tilde{\mathcal{I}}_1$.

Case 3.4: $|\mathcal{I}_4| \leq 2^{n-4} - 1$.

This case is dealt with as Case 3.3 by using the top first and third rows of (20). The only uncovered subsets are those in which $\left|\tilde{\mathcal{I}}_1\right| \leq 2^{n-5} - 1$, $0 \notin \tilde{\mathcal{I}}_1$, $2^{n-5} + 2^{n-6} \in \tilde{\mathcal{I}}_1$.

If either Case 3.1 or Case 3.2 holds then the subset $\mathcal{I}$ is covered. Clearly, Case 3.1 or Case 3.4 must hold; also Case 3.2 or Case 3.3 must hold. Thus, uncovered subsets remain if both Cases 3.3 and 3.4 hold. Thus, the only uncovered subsets are those in which $\left|\tilde{\mathcal{I}}_1\right| \leq 2^{n-5} - 1$, $0 \notin \tilde{\mathcal{I}}_1$, and $2^{n-5}, 2^{n-5} + 2^{n-6} \in \tilde{\mathcal{I}}_1$. Now, we can use the induction hypothesis on Π_{n-2}, on the second row in both (20) and (21), and Lemma 9, to conclude the proof that all subsets are covered. □

We are now in a position to define our parity-check matrix of $\mathcal{R}(1, m)$. The construction of this matrix $\mathcal{H}(m)$ is in three steps.

Step 1: The first $2^{m-1} - 1$ rows of $\mathcal{H}(m)$ are the rows of the following matrix:

$$\Omega_m = [\, \Lambda_{m-1} \quad \Lambda_{m-1} \,].$$

As before, the key to understanding the remaining construction is to understand which subsets are covered, which subsets are uncovered, and which subsets we will cover such that all the uncovered subsets will be covered. Let $\mathcal{I}$ be a subset of $\mathbb{Z}_{2^m}$ such that $|\mathcal{I}| \leq 2^{m-1} - 1$. We distinguish between three cases.

Case 1: $\left|\{0, 2^{m-1}\} \cap \mathcal{I}\right| = 1$.

By the pigeon-hole principle there exist at least one j, $1 \leq j \leq 2^{m-1} - 1$, such that $\left|\{j, 2^{m-1} + j\} \cap \mathcal{I}\right| = 0$. Hence, $\Omega_m(\mathcal{I})$ has a row with weight one.

Case 2: $\left|\{0, 2^{m-1}\} \cap \mathcal{I}\right| = 0$.

If there exist at least one j, $1 \leq j \leq 2^{m-1} - 1$, such that $\left|\{j, 2^{m-1} + j\} \cap \mathcal{I}\right| = 1$ then $\Omega_m(\mathcal{I})$ has a row with weight one. If such j does not exist then $|\mathcal{I}| = 2k$, $k \leq 2^{m-2} - 1$, and $\mathcal{I} = \{\ell_1, \ell_2, \ldots, \ell_k, 2^{m-1} + \ell_1, 2^{m-1} + \ell_2, \ldots, 2^{m-1} + \ell_k\}$.

Case 3: $\left|\{0, 2^{m-1}\} \cap \mathcal{I}\right| = 2$.

All the rows of $\Omega_m(\mathcal{I})$ have at least weight two.

Step 2: Let $\Omega_{\ell,1}$ and $\Omega_{\ell,2}$ be the following $(2^{\ell-1} - 1) \times 2^\ell$ matrices:

$$\Omega_{\ell,1} = \left[\, \Lambda_{\ell-1}^{2^{\ell-2}} \quad \Lambda_{\ell-1}^{2^{l-2}} \,\right]$$
$$\Omega_{\ell,2} = \left[\, \Lambda_{\ell-1}^{2^{\ell-2}+2^{\ell-3}} \quad \Lambda_{\ell-1}^{2^{l-2}+2^{\ell-3}} \,\right].$$

The next $2^{m-1} - 2$ rows of $\mathcal{H}(m)$ are the rows of the matrix

$$\begin{bmatrix} \Omega_{m-1,1} & \mathbf{0} \\ \mathbf{0} & \Omega_{m-1,2} \end{bmatrix}.$$

It is important to note that $\Omega_{m-1,1}$ and $\Omega_{m-1,2}$ are isomorphic to Ω_{m-1} and the analysis of Cases 1 through 3 holds for $\Omega_{m-1,1}$ and $\Omega_{m-1,2}$ by using the corresponding permutations of columns. Therefore, we can easily find the subsets of $\mathbb{Z}_{2^m}$ which are not covered by the $2^m - 3$ rows defined in Steps 1 and 2. Given a subset $\mathcal{I} = \mathcal{I}_1 \cup \mathcal{I}_2$, where $\mathcal{I}_1 = \mathcal{I} \cap \{0, 1, \ldots, 2^{m-1} - 1\}$, $\mathcal{I}_2 = \mathcal{I} \cap \{2^{m-1}, 2^{m-1} + 1, \ldots, 2^m - 1\}$, and $|\mathcal{I}| \leq 2^{m-1} - 1$, $\mathcal{I}$ is not covered by the first $2^m - 3$ rows of $\mathcal{H}(m)$ if it is of one of the following four types.

Type 1: $\{0, 2^{m-3}, 2^{m-2} + 2^{m-3}, 2^{m-1}\} \subset \mathcal{I}$ and $|\mathcal{I}_1| \leq 2^{m-2} - 1$; or $\{0, 2^{m-1}, 2^{m-1} + 2^{m-3} + 2^{m-4}, 2^{m-1} + 2^{m-2} + 2^{m-3} + 2^{m-4}\} \subset \mathcal{I}$ and $|\mathcal{I}_2| \leq 2^{m-2} - 1$ (see Case 3 for Ω_m and Case 3 for Ω_{m-1}).

Type 2: $\{0, 2^{m-1}\} \subset \mathcal{I}$, $\left|\{2^{m-3}, 2^{m-2} + 2^{m-3}\} \cap \mathcal{I}\right| = 0$, $|\mathcal{I}_1| = 2k$, $k \leq 2^{m-3} - 1$, and $\mathcal{I}_1 = \{\ell_1, \ell_2, \ldots, \ell_k, 2^{m-2} + \ell_1, 2^{m-2} + \ell_2, \ldots, 2^{m-2} + \ell_k\}$; or $\{0, 2^{m-1}\} \subset \mathcal{I}$, $\left|\{2^{m-1} + 2^{m-3} + 2^{m-4}, 2^{m-1} + 2^{m-2} + 2^{m-3} + 2^{m-4}\} \cap \mathcal{I}\right| = 0$, $|\mathcal{I}_2| = 2k$, $k \leq 2^{m-3} - 1$, and $\mathcal{I}_2 = \{\ell_1, \ell_2, \ldots, \ell_k, 2^{m-2} + \ell_1, 2^{m-2} + \ell_2, \ldots, 2^{m-2} + \ell_k\}$ (see Case 3 for Ω_m and Case 2 for Ω_{m-1}).

Type 3: $0, 2^{m-3} \notin \mathcal{I}$, $|\mathcal{I}| = 4k$, $k \leq 2^{m-3} - 1$, $\mathcal{I} = \{\ell_1, \ell_2, \ldots, \ell_k, 2^{m-2} + \ell_1, 2^{m-2} + \ell_2, \ldots, 2^{m-2} + \ell_k, 2^{m-1} + \ell_1, 2^{m-1} + \ell_2, \ldots, 2^{m-1} + \ell_k, 2^{m-1} + 2^{m-2} + \ell_1, 2^{m-1} + 2^{m-2} + \ell_2, \ldots, 2^{m-1} + 2^{m-2} + \ell_k\}$, or $0, 2^{m-3} + 2^{m-4} \notin \mathcal{I}$, $|\mathcal{I}| = 4k$, $k \leq 2^{m-3} - 1$, $\mathcal{I} = \{\ell_1, \ell_2, \ldots, \ell_k, 2^{m-2} + \ell_1, 2^{m-2} + \ell_2, \ldots, 2^{m-2} + \ell_k, 2^{m-1} + \ell_1, 2^{m-1} + \ell_2, \ldots, 2^{m-1} + \ell_k, 2^{m-1} + 2^{m-2} + \ell_1, 2^{m-1} + 2^{m-2} + \ell_2, \ldots, 2^{m-1} + 2^{m-2} + \ell_k\}$ (see Case 2 for Ω_m and Case 2 for Ω_{m-1}).

Type 4: $0 \notin \mathcal{I}$, $2^{m-3}, 2^{m-3} + 2^{m-4}, 2^{m-2} + 2^{m-3}, 2^{m-2} + 2^{m-3} + 2^{m-4} \in \mathcal{I}$, $|\mathcal{I}| = 2k$, $k \leq 2^{m-2} - 1$, and $\mathcal{I} = \{\ell_1, \ell_2, \ldots, \ell_k, 2^{m-1} + \ell_1, 2^{m-1} + \ell_2, \ldots, 2^{m-1} + \ell_k\}$ (see Case 2 for Ω_m and Case 3 for Ω_{m-1}).

This analysis implies the following lemma.

Lemma 16: If the uncovered subsets of Types 1 through 4 will be covered then all subsets of size $2^{m-1} - 1$ or less will be covered.

Step 3: The remaining rows of $\mathcal{H}(m)$ are composed from the matrix

$$\Upsilon_m = \begin{bmatrix} \Phi_{m-2} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \Upsilon_{m-2,1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \Gamma_{m-2} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \Upsilon_{m-2,2} \end{bmatrix}$$

where

$$\Upsilon_{m-2,1} = \begin{bmatrix} \Lambda_{m-3}^{2^{m-4}} & & & \Lambda_{m-3}^{2^{m-4}} \\ \mathbf{0} & \Psi_{m-4} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \Psi_{m-4} & \mathbf{0} \\ \Lambda_{m-4}^{2^{m-5}+2^{m-6}} & \mathbf{0} & \mathbf{0} & \Lambda_{m-4}^{2^{m-5}+2^{m-6}} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \Theta_{m-4}^{2^{m-6}} \\ \Upsilon_{m-4,2} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}$$

$$\Upsilon_{3,1} = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\Upsilon_{3,2} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\Upsilon_{4,1} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\Upsilon_{4,1} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$ □

---

and

$$\Upsilon_{m-2,2} = \begin{bmatrix} \Lambda_{m-3}^{2^{m-4}} & & \Lambda_{m-3} & \\ \mathbf{0} & \Psi_{m-4} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \Psi_{m-4} \\ \Lambda_{m-4}^{2^{m-5}} & \mathbf{0} & \Lambda_{m-4}^{2^{m-5}} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \Theta_{m-4} & \mathbf{0} \\ \Upsilon_{m-4,1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}.$$

Lemma 17: Let $\mathcal{I} \subset \mathbb{Z}_{2^{m-2}}$ and $|\mathcal{I}| \leq 2^{m-3} - 1$.

- If $2^{m-3} \in \mathcal{I}$, then $\Upsilon_{m-2,1}$ covers $\mathcal{I}$.
- If $2^{m-3} + 2^{m-4} \in \mathcal{I}$, then $\Upsilon_{m-2,2}$ covers $\mathcal{I}$.

Proof: The proof is by induction and very similar to the proof of Lemma 11. Note that $\Upsilon_{m-2,1}$ and $\Upsilon_{m-2,2}$ have the same structure as Ψ_{m-2}. We omit the proof and just mention that the basis of the induction are the matrices shown at the top of the page.

Lemma 18: $\mathcal{H}(m)$ is a parity-check matrix of $\mathcal{R}(1, m)$.

Proof: It is easy to verify that the $2^{m-1} + 2^{m-2} - 2$ rows of Ω_m and $[\,\Omega_{m-1,1} \quad \mathbf{0}\,]$ are linearly independent. These $2^{m-1} + 2^{m-2} - 2$ rows are linearly independent with any linear combination of rows from $[\mathbf{0} \quad \Upsilon_{m-2,1} \quad \mathbf{0} \quad \mathbf{0}]$. As $\Upsilon_{m-2,1}$ is isomorphic to Ψ_{m-2} we have by Lemma 11 that $[\mathbf{0} \quad \Upsilon_{m-2,1} \quad \mathbf{0} \quad \mathbf{0}]$ includes $2^{m-2} - m + 1$ linearly independent rows. Therefore, $\mathcal{H}(m)$ has $2^m - m - 1$ linearly independent rows. It is also easy to verify (e.g., by use of induction again) that all rows used in $\mathcal{H}(m)$ belong to the orthogonal subspace of $\mathcal{G}(1, m)$. Thus, $\mathcal{H}(m)$ is a parity-check matrix of $\mathcal{R}(1, m)$. □

Lemma 19: The stopping distance of $\mathcal{H}(m)$ is 2^{m-1}.

Proof: By Lemma 16, we only have to show that Υ_m covers the uncovered subsets of Types 1 through 4. We distinguish between four cases; a case for each type.

1) The uncovered subsets of Type 1 are covered as follows:

- $\left|\mathcal{I}\cap[0..2^{m-2}-1]\right| \leq 2^{m-3}-1$ and $0, 2^{m-3} \in \mathcal{I}$. These subsets are covered by Φ_{m-2} as proved in Lemma 15 (Case 1).
- $\left|\mathcal{I}\cap[2^{m-2}..2^{m-1}-1]\right| \leq 2^{m-3}-1$ and $2^{m-2}+2^{m-3} \in \mathcal{I}$. These subsets are covered by $\Upsilon_{m-2,1}$ as proved in Lemma 17.
- $\left|\mathcal{I}\cap[2^{m-1}..2^{m-1}+2^{m-2}-1]\right| \leq 2^{m-3}-1$ and $2^{m-1}, 2^{m-1}+2^{m-3}+2^{n-4} \in \mathcal{I}$. These subsets are covered by Γ_{m-2} as proved in Lemma 15 (Case 2).
- $\left|\mathcal{I}\cap[2^{m-1}+2^{m-2}..2^m-1]\right| \leq 2^{m-3}-1$ and $2^{m-1}+2^{m-2}+2^{m-3}+2^{m-4} \in \mathcal{I}$. These subsets are covered by $\Upsilon_{m-2,2}$ as proved in Lemma 17.

2) The uncovered subsets of Type 2 are covered as follows:
- $\left|\mathcal{I}\cap[0..2^{m-2}-1]\right| \leq 2^{m-3}$, $0 \in \mathcal{I}$, and $2^{m-3} \notin \mathcal{I}$. These subsets are covered by $\Upsilon_{m-2,1}$ and Φ_{m-2} by using the observation that the matrix $\begin{bmatrix}\Upsilon_{m-2,1}\\ \Phi_{m-2}\end{bmatrix}$ is isomorphic to Δ_{m-2} and using Lemmas 9 and 10.
- $\left|\mathcal{I}\cap[2^{m-1}..2^{m-1}+2^{m-2}-1]\right| \leq 2^{m-3}$, $2^{m-1} \in \mathcal{I}$, and $2^{m-1}+2^{m-3}+2^{m-4} \notin \mathcal{I}$. These subsets are covered by $\Upsilon_{m-2,1}$ and Γ_{m-2} by using the observation that the matrix $\begin{bmatrix}\Upsilon_{m-2,2}\\ \Gamma_{m-2}\end{bmatrix}$ is isomorphic to Δ_{m-2} and using Lemmas 9 and 10.

3) To show that uncovered subsets of Type 3 are covered it is sufficient to prove that the matrix

$$\begin{bmatrix}\Phi_n\\ \Gamma_n\\ \Upsilon_{n,1}\\ \Upsilon_{n,2}\end{bmatrix}, \qquad n \geq 3$$

covers any subset $\mathcal{I} \subset \mathbb{Z}_{2^n}$, such that $1 \leq |\mathcal{I}| \leq 2^{n-1}-1$. This is done with induction by using similar arguments as for the discussion in this section. We omit the proof and leave it to the readers.

4) The uncovered subsets of Type 4 are covered as follows:
- $\left|\mathcal{I}\cap[0..2^{m-2}-1]\right| \leq 2^{m-3}$, $2^{m-3}, 2^{m-3}+2^{m-4} \in \mathcal{I}$, and $0 \notin \mathcal{I}$. These subsets are covered by Φ_{m-2} and Γ_{m-2} as proved in Lemma 15 (Case 3).
- $\left|\mathcal{I}\cap[2^{m-2}..2^{m-1}-1]\right| \leq 2^{m-3}$ and $2^{m-2}+2^{m-3} \in \mathcal{I}$. These subsets are covered by $\Upsilon_{m-2,1}$ as proved in Lemma 17. □

Lemma 20: Let f_m be the number of rows in $\mathcal{H}(m)$.

$$f_m = \frac{(6m-7)2^{m-1}+(-1)^{m-1}}{9}, \qquad m \geq 5.$$

Proof: f_m is determined by Steps 1 through 3. One can easily verify that
- the number of rows in Φ_{m-2} is $2h_{m-3}$;
- the number of rows in Γ_{m-2} is $2h_{m-3}$;
- the number of rows in $\Upsilon_{m-2,1}$ is h_{m-2};
- the number of rows in $\Upsilon_{m-2,2}$ is h_{m-2}.

Hence, $f_m = 2^m-3+4h_{m-3}+2h_{m-2} = 2^{m-1}-1+2h_{m-1}$. The lemma follows immediately from Lemma 12. □

Theorem 11: $\rho(\mathcal{R}(1,m)) \leq F_m$, $m \geq 2$.

Proof: The theorem is trivial for $m = 2$, and is verified for $m = 3$ from (16). For $m = 4$, we use the following parity-check matrix for $\mathcal{R}(1,4)$ with stopping redundancy 15:

$$\begin{bmatrix}
1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0\\
1&0&0&1&0&0&0&0&1&0&0&1&0&0&0&0\\
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
1&0&0&0&0&1&0&0&1&0&0&0&0&1&0&0\\
1&0&0&0&0&0&1&0&1&0&0&0&0&0&1&0\\
1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1\\
0&0&1&1&0&0&1&1&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&1&1&0&0&1\\
0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1\\
0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1
\end{bmatrix}.$$

For $m \geq 5$ the theorem follows from Lemmas 18–20. □

The proof of Theorem 10 is an immediate consequence from Lemma 20 and Theorem 11.

VI. Conclusion and Open Problems

We have proved that the stopping redundancy of the extended Hamming code of length 2^m is $2m-1$. We have shown that the stopping redundancy of the simplex code is equal to its redundancy. An upper bound on the stopping redundancy of the first-order Reed–Muller code is given. The stopping redundancy of related codes, such as codes with minimum distance 4 and codes whose stopping redundancies is equal to their redundancies, was also discussed.

Many interesting open problems remain in finding the stopping redundancies of codes. Several problems are related to the codes which are discussed in this paper.

- Characterize all codes for which the stopping redundancy equals the redundancy.
- Our upper bound on the stopping redundancy of $\mathcal{R}(1,m)$ implies new upper bounds for $\mathcal{R}(\ell,m)$ if $\ell \geq 1$ and $m-\ell \geq 3$ by using (1). Can better bounds than the ones obtained by (1) be given?
- Is the upper bound on the stopping redundancy of $\mathcal{R}(1,m)$ tight?

Finally, in [9], a similar stopping redundancy of a code $\mathcal{C}$, in which the only stopping sets of size $d(\mathcal{C})$ are codewords, is discussed. In [3], this was generalized and stopping redundancies of a code, in which all stopping sets of size $m \leq r(\mathcal{C})$ contain codewords, is considered. This leads to hierarchy of stopping redundancies. The values of these redundancies are interesting for all codes, including the ones discussed in this paper.

Acknowledgment

The author would like to thank Alexander Vardy and Moshe Schwartz for presenting the problem to him and many valuable discussions. He also is indebted to two anonymous referees who read the paper carefully to provide many useful comments.

REFERENCES

[1] C. Di, D. Proietti, İ.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] J. Han and P. H. Siegel, "Improved upper bounds on stopping redundancy," *IEEE Trans. Inf. Theory*, submitted for publication.

[3] H. D. L. Hollmann and L. M. G. M. Tolhuizen, "On parity check collections for iterative erasure decoding that correct all correctable erasure patterns of a given size," *IEEE Trans. Inf. Theory*, submitted for publication.

[4] N. Kashyap and A. Vardy, "Stopping sets in codes from designs," in *Proc. IEEE Int. Symp. Information Theory*, Yokohama, Japan, Jun./Jul. 2003, p. 122.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[6] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences Sequence A102301 [Online]. Available: http://www.research.att.com/njas/sequences/

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

[8] 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.

[9] J. H. Weber and K. A. S. Abdel-Ghaffar, "Stopping set analysis for Hamming codes," in *Proc. IEEE IT Soc. Information Theory Workshop on Coding and Complexity*, Rotorua, New Zealand, Aug./Sep. 2005, pp. 244–247.