New Upper Bounds on the Separating Redundancy of Linear Block Codes

Ngo Minh Tri
Delft University of Technology
Mekelweg 4, 2628 CD Delft
The Netherlands
tringominh@gmail.com

Jos H. Weber
Delft University of Technology
Mekelweg 4, 2628 CD Delft
The Netherlands
j.h.weber@tudelft.nl

Khaled A.S. Abdel-Ghaffar
University of California
Davis, CA 95616
USA
ghaffar@ece.ucdavis.edu

Abstract

For linear block codes correcting both errors and erasures, efficient decoding can be established by using separating parity-check matrices. For a given maximum number of correctable erasures, such matrices yield parity-check equations that do not check any of the erased symbols and which are sufficient to characterize all punctured codes corresponding to this maximum number of erasures. Typically, these parity-check matrices have redundant rows. To reduce decoding complexity, parity-check matrices with small number of rows are preferred. The minimum number of rows in a parity-check matrix separating all erasure sets of size at most \( l \) is called the \( l \)th separating redundancy. In this paper, new upper bounds on the separating redundancy are presented.

1 Introduction

Most decoding algorithms of linear codes, in general, are designed to correct or detect errors. However, many channels cause erasures in addition to errors. In principle, decoding over such channels can be accomplished by deleting the erased symbols and decoding the resulting vector with respect to a punctured code. For any given linear code and any given maximum number of correctable erasures, Abdel-Ghaffar and Weber [1] introduced parity-check matrices yielding parity-check equations that do not check any of the erased symbols and which are sufficient to characterize all punctured codes corresponding to this maximum number of erasures. This allows for the separation of erasures from errors to facilitate decoding. Typically, these parity-check matrices have redundant rows. To reduce decoding complexity, parity-check matrices with small number of rows are preferred.

The decoding technique using separating parity-check matrices is motivated by the interest shown in the last decade in decoding techniques, such as belief propagation especially applied to low-density parity-check (LDPC) codes, that are based on parity-check matrices with a large number of redundant rows. Decoding exploits the redundancy of these matrices to yield good performance. The computational complexity of decoding is reduced at the price of storing parity-check matrices with more rows than necessary to characterize the codes. Actually, decoding techniques based on such parity-check matrices have been introduced already to decode words suffering from erasures only [3]. For this application, the decoder seeks a parity-check equation that checks exactly one erased symbol whose value can be determined directly from the equation. A set of positions is called a stopping set if there is no parity-check equation that checks exactly one symbol in these positions. Erasure decoding fails if and only if erasures fill the positions of a nonempty stopping set. For codes with a Hamming distance \( d \), the separating parity-check matrices do not have nonempty stopping sets of sizes less than or equal to the maximum number of erasures \( l \leq d - 1 \), except in the case of \( l = d - 1 \) and the code is maximum distance separable (MDS). Thus, except for this case, for any pattern of \( l \) or fewer erasures, not only are there enough parity-check equations not checking any of the erased symbols that characterize the
punctured code, but also there is a parity-check equation that checks exactly one of the erased symbols. This greatly facilitates the retrieval of the erased symbols once the errors are corrected. It is not surprising to see that work on separating matrices is related to work on stopping sets, specially to [4],[5],[8],[9]. However, work on stopping sets assumes that the channel does not cause errors, which limits its applicability. On the contrary, separating matrices deal with errors in addition to erasures.

The minimum number of rows in a parity-check matrix separating all erasure sets of size at most \( l \) is called the \( l \)th separating redundancy. In [1], upper and lower bounds on the separating redundancy were presented. In this paper, we give improvements on the upper bounds from [1]. The rest of this paper is organized as follows. In Section 2, the concepts of separating matrices and separating redundancy as introduced in [1] are reviewed. Then, in Section 3, we present upper bounds on the separating redundancy. In Section 4, we focus on bounds on the sizes of parity-check matrices separating a single erasure. Finally, the paper is concluded in Section 5.

### 2 Separating Matrices and Separating Redundancy

Let \( C \) be an \([n, k, d]\) linear block code over \( GF(q) \), where \( n, k, \) and \( d \) denote the code’s length, dimension, and Hamming distance, respectively, and \( q \) is a prime power. Such a code is a \( k \)-dimensional subspace of the space of vectors of length \( n \) over \( GF(q) \), in which any two different vectors differ in at least \( d \) positions. The set of codewords of \( C \) can be defined as the null space of the row space of an \( r \times n \) binary parity-check matrix \( H = (h_{ij}) \) of rank \( n - k \). The row space of \( H \) is the \([n, n - k, d^\perp]\) dual code \( C^\perp \) of \( C \). Since a \( q \)-ary vector \( x \) is a codeword of \( C \) if and only if \( xH^T = 0 \), where the superscript \( T \) denotes transpose, the parity-check matrix \( H \) gives rise to \( r \) parity-check equations, denoted by

\[
PCE_i(x) : \sum_{j=1}^{n} h_{i,j}x_j = 0 \text{ for } i = 1, 2, \ldots, r.
\]

An equation \( PCE_i(x) \) is said to check \( x \) in position \( j \) if and only if \( h_{i,j} \neq 0 \).

In the most general scenario, if the number of erasures, \( t_e \), does not exceed \( d - 1 \), then the decoder can choose two nonnegative integers \( t_\neq \) and \( t_\parallel \) satisfying

\[
t_\parallel + 2t_\neq + t_\parallel \leq d - 1
\]

such that the following is true. If the number of errors does not exceed \( t_\neq \), then the decoder can correct all errors and erasures. Otherwise, if the number of errors is greater than \( t_\neq \) but at most \( t_\neq + t_\parallel \), then the decoder can detect the occurrence of more than \( t_\neq \) errors and, in this case, may request the retransmission of the codeword, see e.g., [7].

Let \( U \) be a subset of \( N = \{1, 2, \ldots, n\} \) and \( T \) be a subset of \( R = \{1, 2, \ldots, r\} \). For any \( H = (h_{ij}) \) of size \( r \times n \), let \( H^T_U = (h_{ij}) \) where \( i \in T \) and \( j \in U \). Then, \( H^T_U \) is a \( |T| \times |U| \) submatrix of \( H \). For simplicity, we write \( H_U \) and \( H^T_U \) to denote \( H^T_U \) in case \( T = R \) and \( U = N \), respectively. We allow for empty matrices, i.e., with no rows or no columns, e.g., if either \( U \) or \( T \) or both are empty. The rank of an empty matrix is defined to be zero. If \( x \) is a vector of length \( n \), then \( x_U \) denotes the vector whose components are indexed by \( U \). Furthermore, for the code \( C \) of length \( n \), define the punctured code

\[
C_U = \{c_U : c \in C\},
\]

i.e., \( C_U \) consists of all codewords in \( C \) in which the components in positions belonging to the set \( U \), defined by \( U = N \setminus \mathcal{U} \), are deleted.

Let \( H = [h_{ij}] \) be an \( r \times n \) matrix over \( GF(q) \) and \( S \) be a subset of \( N \). We define

\[
\tilde{S} = \{i : 1 \leq i \leq r, h_{i,j} = 0 \quad \forall j \in S\}, \tag{2}
\]
Theorem 1 ([1])

1 ≤ E to errors and erasures resulting in a word \( r = (r_1, r_2, \ldots, r_n) \), \( r_i \in \text{GF}(q) \cup \{?\} \) for \( 1 \leq i \leq n \), where ? denotes an erasure. Let \( E_\neq = \{i : r_i \neq c_i\} \) and \( E_? = \{i : r_i = ?\} \) denote the error and erasure patterns, respectively. The decoder picks two nonnegative integers \( t_\neq \) and \( t_? \) satisfying (1) where \( t_? = |E_?| \) is assumed to be at most \( d - 1 \). Then it decodes the word \( r_{E_\neq} \) with respect to the code \( C_{\tilde{E}_\neq} \). If \( |E_\neq| \leq t_\neq \), the decoder succeeds in correcting all the errors and can then retrieve the erasures. If \( t_\neq < |E_\neq| \leq t_\neq + t_?, \) the decoder can detect the occurrence of more than \( t_\neq \) errors.

We consider combined erasure/error decoding of the code \( C \). In this scenario, a transmitted codeword \( c = (c_1, c_2, \ldots, c_n) \), \( c_i \in \text{GF}(q) \) for \( 1 \leq i \leq n \), is subjected to errors and erasures resulting in a word \( r = (r_1, r_2, \ldots, r_n) \), \( r_i \in \text{GF}(q) \cup \{?\} \) for \( 1 \leq i \leq n \), where ? denotes an erasure. Let \( E_\neq = \{i : r_i \neq c_i\} \) and \( E_? = \{i : r_i = ?\} \) denote the error and erasure patterns, respectively. The decoder picks two nonnegative integers \( t_\neq \) and \( t_? \) satisfying (1) where \( t_? = |E_?| \) is assumed to be at most \( d - 1 \). Then it decodes the word \( r_{E_\neq} \) with respect to the code \( C_{\tilde{E}_\neq} \). If \( |E_\neq| \leq t_\neq \), the decoder succeeds in correcting all the errors and can then retrieve the erasures. If \( t_\neq < |E_\neq| \leq t_\neq + t_? \), the decoder can detect the occurrence of more than \( t_\neq \) errors.

We say that a parity-check matrix, \( H \), for the \([n, k, d]\) linear code, \( C \), over \( \text{GF}(q) \) separates \( S \subseteq \{1, 2, \ldots, n\} \) if and only if the submatrix \( H(S) \) is a parity-check matrix of \( C \). If \( |S| \leq d - 1 \), this is the case if and only if \( H(S) \) has rank \( n - k - |S| \) [1]. For \( l = 0, 1, \ldots, d - 1 \), we say that \( H \) is \( l \)-separating for \( C \) if it separates every set \( S \) of size \( |S| = 0, 1, \ldots, l \). It is shown in [1] that if \( H \) separates all sets of size \( l \) for a fixed \( l \leq \min\{d - 1, n - k - 1\} \), then it separates all sets of size \( l \) or less, i.e., \( H \) is \( l \)-separating. Clearly, any parity-check matrix of any linear code is \( 0 \)-separating. Further, for any \([n, k, d]\) code \( C \) over \( \text{GF}(q) \) and any \( l \) with \( 1 \leq l \leq d - 1 \), there exists a parity-check matrix which is \( l \)-separating [1]. The \( l \)th separating redundancy, \( s_l \), of \( C \) is defined to be the minimum number of rows of an \( l \)-separating parity-check matrix of \( C \). In [1], the following lower bound on \( s_l \) was derived:

\[
s_l \geq \frac{n - k - l}{\binom{n - d + l}{l}}. \tag{4}
\]

In the next two sections, we will present upper bounds on \( s_l \).

3 Upper Bounds on the \( l \)th Separating Redundancy

In this section, we provide upper bounds on \( s_l \) for any \( l \leq \min\{d - 1, n - k - 1\} \). In [1], a construction for \( l \)-separating matrices and a consequent upper bound on the \( l \)th separating redundancy were presented, which we repeat here since our improved upper bound is based on these. Let \( H' \) be a full-rank \((n - k) \times n\) parity-check matrix of an \([n, k, d]\) linear code \( C \) over \( \text{GF}(q) \), and let \( S_i \subseteq \{1, 2, \ldots, n\} \), where \( i = 1, 2, \ldots, \binom{n}{l} \), be the distinct subsets of \( \{1, 2, \ldots, n\} \) of size \( l \leq \min\{d - 1, n - k - 1\} \). For each \( i = 1, 2, \ldots, \binom{n}{l} \), \( H'_{S_i} \) has rank \( l \) as \( l \leq d - 1 \). By elementary row operations on \( H' \), we can obtain an \((n - k) \times n\) matrix, \( H_i' \); for each \( i = 1, 2, \ldots, \binom{n}{l} \), of rank \( n - k \) such that its last \( n - k - l \) rows have zeros in the positions indexed by \( S_i \). For example, in case \( S_i = \{1, 2, \ldots, l\} \), the resulting \((n - k) \times n\) matrix has the format

\[
\begin{pmatrix}
0_{n-k-l, l} & \cdots \\
\vdots & \ddots & \ddots \\
\end{pmatrix}, \tag{5}
\]

where \( 0_{i,j} \) is the \( i \times j \) all-zero matrix. Let \( H_i \) denote the matrix whose set of rows is the union of the sets of the last \( n - k - l \) rows in \( H_i' \) for \( i = 1, 2, \ldots, \binom{n}{l} \).

Theorem 1 ([1]) \( H_i \) is an \( l \)-separating parity-check matrix for the code \( C \).
By observing the maximum number of rows in $H_I$, the following upper bound was obtained.

**Corollary 1** ([1]) Let $C$ be an $[n, k, d]$ linear code over GF($q$). Then, for $1 \leq l \leq \min\{d - 1, n - k - 1\}$,

$$s_l \leq \binom{n}{l}(n - k - l).$$

We will now improve upon this bound by constructing the matrices $H'_I$ in such a way that many of these have identical rows among the last $n - k - l$ rows. To this end, we will use covering designs. For $1 \leq t \leq u \leq v$, a $(v, u, t)$ covering design is a collection of $u$-element subsets of $\{1, 2, \ldots, v\}$, called blocks, such that every $t$-element subset of $\{1, 2, \ldots, v\}$ is contained in at least one block. In order to construct an $l$-separating matrix for an $[n, k, d]$ code, we will use an $(n, b, l)$ covering design $B$, where $b$ is an integer such that $l \leq b \leq \min\{d - 1, n - k - 1\}$. We assign to each $l$-element subset of $\mathcal{N}$ a block of $B$ containing this $l$-element subset. For each $j = 1, 2, \ldots, |\mathcal{B}|$, let $I_j$ be the set of indices $i$ for which block $B_j$ is assigned to $S_i$. By elementary row operations on $H'_I$, we can obtain an $(n - k) \times n$ matrix $H''_I$, of rank $n - k$, such that its last $n - k - b$ rows have zeros in the positions indexed by $B_j$. Furthermore, by elementary row operations on the first $b$ rows of $H''_I$, we can obtain, for each $i \in I_j$, an $(n - k) \times n$ matrix $H'_I$, still of rank $n - k$, with rows $l + 1, l + 2, \ldots, b$ having zeros in the positions indexed by $S_i$, and with rows $b + 1, b + 2, \ldots, n - k$ having zeros in the positions indexed by $B_j$. For example, in case $S_i = \{1, 2, \ldots, l\}$ and $B_j = \{1, 2, \ldots, b\}$, the resulting $(n - k) \times n$ matrix has the format

$$
\begin{pmatrix}
\cdots & \cdots & \cdots \\
0_{b-l, l} & \cdots & \cdots \\
0_{n-k-b, l} & \cdots \\
\end{pmatrix}.
$$

Let $H''_I$ denote the matrix whose set of rows is the union of the last $n - k - b$ rows in $H'_I$ for $j = 1, 2, \ldots, |\mathcal{B}|$ and the rows $l + 1, l + 2, \ldots, b$ of $H'_I$ for $i = 1, 2, \ldots, \binom{n}{l}$. Since the matrix $H''_I$ belongs to the class of $H'_I$ matrices, the following result follows from Theorem 1.

**Theorem 2** $H''_I$ is an $l$-separating parity-check matrix for the code $C$.

Let $B(v, u, t)$ denote the minimum size of a $(v, u, t)$ covering design. Then, by observing the size of $H''_I$ when using a minimum-sized covering design, we obtain the following upper bound.

**Corollary 2** Let $C$ be an $[n, k, d]$ linear code over GF($q$). Then, for $1 \leq l \leq b \leq \min\{d - 1, n - k - 1\}$,

$$s_l \leq (n - k - b)B(n, b, l) + \binom{n}{l}(b - l).$$

Hence, we need (upper bounds on) the minimum sizes of covering designs in order to apply this bound. A vast amount of literature and tables regarding covering designs is available, see, e.g., [2], [6]. Here, we restrict ourselves to a simple general upper bound, which suffices to show the superiority of the new bound on the separating redundancy over the old bound as stated in Corollary 1.

**Lemma 1** For $1 \leq t \leq u \leq v$,

$$B(v, u, t) \leq \binom{v - u + t}{t}.$$
Let the matrix rows have zeros in the positions indexed by $H$. Denote the result follows from Theorem 1.

Comparing the bounds from Corollaries 1 and 2, note that

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \leq \binom{n}{k} \binom{n-k}{l} + \binom{n-k}{l} \binom{n}{l}$$

where the first inequality follows from Lemma 1 and the second from the fact that $b \geq l$. Equality holds in the second inequality if and only if $b = l$, in which case equality holds in the first inequality as well. Hence, if $b = l$, the two bounds are the same. However, if $b > l$, the upper bound in Corollary 2 is strictly lower than the one in Corollary 1.

4 Upper Bounds on the 1st Separating Redundancy

For the case $l = 1$, we have the trivial result that $B(n, b, 1) = \lceil n/b \rceil$ and Corollary 2 thus gives the bound

$$s_1 \leq (n-k-b)[n/b] + n(b-1).$$

However, by another construction, we may improve upon this bound. From an $(n-k) \times n$ parity-check matrix $H'$ of $C$, we can always obtain, by elementary row operations, a full-rank $(n-k) \times n$ matrix $H''$ which contains an $(n-k) \times (n-k)$ submatrix $A$ with zeros in all entries outside the main diagonal. Hence, for all $n-k$ sets $S_i = \{i\}$ corresponding to the column indices of $A$, the matrix $H''$ has $n-k-1$ zeros in column $i$. For each of the remaining $k$ sets $S_i = \{i\}$, by elementary row operations on $H'$, we can obtain an $(n-k) \times n$ matrix, $H_i'$ of rank $n-k$ such that its last $n-k-1$ rows have zeros in the positions indexed by $S_i$. Let $H_{11}$ denote the matrix whose set of rows is the union of the last $n-k-1$ rows in these $k$ matrices $H_i'$ and the rows of the matrix $H''$. Since the matrix $H_{11}$ belongs to the class of $H_I$ matrices, the following result follows from Theorem 1.

**Theorem 3** $H_{11}$ is a 1-separating parity-check matrix for the code $C$.

Since the number of rows in $H_{11}$ is at most $k(n-k-1) + (n-k)$, we obtain the following bound.

**Corollary 3** Let $C$ be an $[n, k, d]$ linear code over $GF(q)$ with $d \geq 2$ and $n-k \geq 2$. Then

$$s_1 \leq (k+1)(n-k-1) + 1.$$  

In case the dual code of $C$ contains a codeword $z$ for which all coordinates are non-zero, a further improvement (in case of small alphabet size $q$) can be obtained. Let $H'$ be a full-rank parity-check matrix of $C$ containing $z$ as one of its rows. Let $M$ be the $(n-k-1) \times n$ matrix obtained by removing $z$ from $H'$. For all $\alpha \in GF(q)$, let $M_\alpha$ denote the $(n-k-1) \times n$ matrix obtained by subtracting $\alpha z$ from each row of $M$. Let $H_{q1}$ be the $(q(n-k-1)) \times n$ matrix containing all rows from the $q$ matrices $M_\alpha$.

**Theorem 4** $H_{q1}$ is a 1-separating parity-check matrix for the code $C$. 
Proof. For ease of notation, let \( H = H_{Q1} \). If we subtract the first row of \( M_1 \) from the first row of \( M_0 \), the result is \( z \). Therefore, the matrices \( H \) and \( H' \) have the same row spaces, and consequently the same null spaces, which shows that \( H \) is indeed a parity-check matrix of \( C \). It remains to show that \( H \) is 1-separating. It suffices to prove that \( H(\{j\}) \) has rank \( n-k-1 \) for any given \( j \in \{1, 2, \ldots, n\} \). The matrix \( H(\{j\}) \) consists of the \( n-k-1 \) rows in \( H \) of the format \( m_i - m_{i,j}(z_j)^{-1}z \), where \( m_i \) is the \( i \)th row of \( M \), \( m_{i,j} \) is the \( j \)th coordinate of this row, and \( (z_j)^{-1} \) is the multiplicative inverse of \( z_j \). These rows are linearly independent, and so \( H(\{j\}) \) has rank \( n-k-1 \). Since \( H(\{j\}) \) is obtained by deleting an all-zero column from \( H(\{j\}) \), \( H(\{j\}) \) has also rank \( n-k-1 \). 

Corollary 4 Let \( C \) be an \([n, k, d]\) linear code over \( \text{GF}(q) \) with \( d \geq 2 \) and \( n-k \geq 2 \), for which the dual code contains a codeword all of whose coordinates are non-zero. Then

\[
   s_1 \leq q(n-k-1).
\]

Consequently, for a binary \([n, k, d]\) code for which the redundancy \( n-k \) is at least equal to 2 and in which all codewords have even weight (which implies that the dual code contains the all-one word), we have the upper bound

\[
   s_1 \leq 2(n-k-1).
\]  

Note that the lower bound from (4) gives

\[
   s_1 \geq \frac{n}{n-d^1}(n-k-1).
\]  

Hence, for binary \([n, k, d]\) codes for which the redundancy \( n-k \) is at least equal to 2 and in which all codewords have even weight and for which the Hamming distance of the dual code is \( n/2 \), e.g., for extended Hamming codes, (8) and (9) give

\[
   s_1 = 2(n-k-1).
\]  

Example 1 Let \( C \) be the \([16, 11, 4]\) binary extended Hamming code. The matrix

\[
   H' = \begin{pmatrix}
   1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
   0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
   0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
   0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
   0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1
   \end{pmatrix}
\]  

is a full-rank parity-check matrix of \( C \). Removing the first row and appending the complements of all the other rows give the matrix

\[
   H_{Q1} = \begin{pmatrix}
   0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
   0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
   0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
   0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
   1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
   1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
   1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
   1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0
   \end{pmatrix},
\]
which is a 1-separating parity-check matrix of $C$. For example, the matrix

$$
H_{Q_1}({\{3\}}) = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
\end{pmatrix}, \quad (13)
$$

which is obtained by removing the rows 3, 5, 6, and 8 from $H_{Q_1}$ and then removing the third entry from each of the remaining rows, is indeed a parity-check matrix of the $[15,11,3]$ code obtained by puncturing $C$ in the third position. Note that

$$
H'({\{3\}}) = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
\end{pmatrix}, \quad (14)
$$

which is obtained by removing the rows 1 and 4 from $H'$ and then removing the third entry from each of the remaining rows, is not a parity-check matrix of the $[15,11,3]$ code obtained by puncturing $C$ in the third position. This shows that $H'$ is not a 1-separating parity-check matrix of $C$.

Since the dual code of $C$ is the $[16,5,8]$ first-order Reed-Muller code, it follows from (9) that the matrix in (12) is a 1-separating parity-check matrix of $C$ of smallest size.

5 Conclusion

Separating parity-check matrices are useful for decoding over channels causing errors and erasures. We presented improved upper bounds on the separating redundancy, which is the minimum number of rows in separating matrices. In some cases, such upper bounds are equal or close to the best known lower bound. However, in general, there are still (big) gaps between the best known upper and lower bounds. Hence, more research on bounding techniques for the separating redundancy is required.

Acknowledgment

Khaled Abdel-Ghaffar is supported by the NSF through grant CCF-0727478.
References


