High Stopping-distance LDPC Product Codes based on Hamming and Finite Geometry Codes

Morteza Hivadi* and Morteza Esmaeili**
*Dept. of Mathematical Sciences
Isfahan University of Technology
84156-83111, Isfahan, Iran
m_hivadi@math.iut.ac.ir, emorteza@cc.iut.ac.ir
*Dept. of Electrical and Computer Engineering
University of Victoria, Victoria, B.C., Canada V8W 3P6
emorteza@ece.uvic.ca

Abstract

High stopping-distance low-density parity-check (LDPC) product codes with finite geometry LDPC and Hamming codes as the constituent codes are constructed. These codes have high stopping distance compared to some well-known LDPC codes. As examples, linear $[511, 180, 30]$, $[945, 407, 27]$, $[2263, 1170, 30]$ and $[4095, 2101, 54]$ LDPC codes are designed with stopping distances 30, 27, 30 and 54, respectively. Due to their good stopping redundancy, they can be considered as low-complexity codes with very good performance when iterative decoding algorithms are used.

Keywords: product code, LDPC code, stopping distance, stopping redundancy, finite geometry.

1 Introduction

The powerful class of product codes, introduced by Elias [1] in 1954, is a subclass of concatenated codes. In this paper we consider only binary linear block codes. By an $[n, k, d]$ code C we mean a binary length n code with

[1] This research was in part supported by a grant from Iran Telecommunication Research Center (ITRC).

ARS COMBINATORIA 99(2011), pp. 97-107

dimension k and minimum distance d. Given binary codes $\mathcal{A}$ and $\mathcal{B}$ with parameters $[n, k, d]$ and $[n', k', d']$, respectively, the $[nn', kk', dd']$ product code $\mathcal{P} = \mathcal{A} \bigotimes \mathcal{B}$ consists of all binary $n' \times n$ matrices whose rows and columns are in $\mathcal{A}$ and $\mathcal{B}$, respectively. $\mathcal{A}$ and $\mathcal{B}$ are referred to as the row and column codes, respectively.

Let C be a binary length n linear code represented by a parity-check matrix $H = (h_{ij})$. The columns of H are indexed by $1, 2, \cdots, n$, and $r(H)$ denotes the number of rows of H. Let S be a subset of $\{1, 2, \cdots, n\}$ and H_S denote the $r(H) \times |S|$ submatrix of H consisting of columns indexed by S. S is called a *stopping set* for H if H_S has no row of weight one. It is known that the performance of C under iterative decoding (belief propagation decoding), over a binary erasure channel (BEC) is determined by the set of stopping sets of H [2]. The size of the smallest stopping set in H, called *the stopping distance* of H and denoted by $s(H)$, has a role on the performance of C under iterative decoding that is very similar to the role of minimum distance of C under maximum-likelihood decoding over the BEC [3]–[9].

It is easily verified that the stopping distance of a parity-check matrix H is upper bounded by the minimum distance d of the corresponding code C. Adding dependent rows to H may increase the stopping distance of the resulting parity-check matrix to the minimum distance of C. Though this process improves the performance of C under iterative decoding, it increases the computational complexity. Therefore, the minimum number of rows of a parity-check matrix H for C satisfying $s(H) = d$, referred to as the *stopping redundancy* of C and denoted by $\rho(C)$ [4], provides a trade-off between the decoding complexity and the performance of C [4]–[9].

There are only a few classes of codes, such as finite geometry (FG) codes and non-LDPC Reed-Muller codes $R(r, m)$ [4], that can be represented by parity-check matrices with known stopping distance (using a recursive construction [4], parity-check matrices with known stopping distance for $RM(r, m)$ can be constructed, but these matrices do not have low-density; for instance the parity-check matrix for the $RM(6, 11)$ code has length 2048 and column weight 330). Some probabilistic algorithms for computing the stopping distance of LDPC codes were introduced in [10], and it was shown in [11] that the problem of determining the stopping distance of a parity-check matrix is an NP-hard problem. Thus, from both the theoretical and practical perspectives, construction of classes of good codes, in particular LDPC codes, represented by parity-check matrices with known stopping distance are of significant interest.

FG codes have relatively large minimum distance and have excellent performance when iterative decoding is employed. Hamming codes are useful for the BEC [12, 13]. These codes have high rate but low minimum distance. Therefore, we use Hamming and FG codes, specifically Type-

I Euclidean geometry (EG) and Type-I projective geometry (PG) LDPC codes [6], as the constituent codes to construct LDPC product codes with good minimum distance and rate. The stopping distance of the resulting parity-check matrices is determined. Among the codes obtained in this paper are $[511, 180, 30]$, $[945, 407, 27]$, $[2263, 1170, 30]$ and $[4095, 2101, 54]$ LDPC codes with stopping distances 30, 27, 30 and 54, respectively, and so are competitive with the best LDPC codes with known stopping distance. It is also shown that the codes presented here have low-complexity and iterative decoding performance close to that with maximum-likelihood decoding. Thus the main contribution of this paper is employing FG and Hamming codes to construct a class of low-complexity product codes having good performance, known stopping distance and a good stopping redundancy bound.

The necessary background on FG and product codes is given in Section 2. The construction of product codes using constituent Hamming and FG-LDPC codes is given in Section 3. The stopping distance of these codes is determined in Subsection 3.1 followed by their stopping redundancy analysis in Subsection 3.2.

2 Stopping distance and stopping redundancy of FG and product codes

2.1 Euclidean and projective geometry LDPC Codes

FG-LDPC codes [14] are an important class of structured LDPC codes constructed from the lines and points of finite Euclidean or projective geometries over finite fields. An FG code, G, has the following basic properties: 1) every line consists of ρ points; 2) any two points are connected by exactly one line; 3) every point is contained by γ lines; 4) any two lines are either parallel or intersect on just one point. A parity-check matrix H_G of a linear FG code G is formed as follows: the rows and columns corresponding to the lines and points of G, respectively, and the entries of H_G are considered according to the incidence structure of G.

Set $q := 2^s$ for some positive integer s, and let $EG(2, q)$ be the Euclidean plane over the q-element field F_q (see e.g. [14, 15]), with $q^2 - 1$ nonorigin points and $q^2 - 1$ lines that do not pass through the origin. Each point lies on q lines and each line contains q points. Consider the Euclidean plane $EG(2, q)$ and the related code $C_{EG(2,q)}$ with parity-check matrix $H_{EG(2,q)}$. It was shown in [14] that $H_{EG(2,q)}$ is a $(q^2 - 1) \times (q^2 - 1)$ circulant matrix. Thus $C_{PG(2,q)}$ is a cyclic code. These codes are called Type-I EG-LDPC codes. It is known that $C_{EG(2,q)}$ has length $n_{EG} = q^2 - 1$, dimension $k_{EG} = n_{EG} - 3^s + 1$, and minimum distance $d_{EG} = q + 1$, and $H_{EG(2,q)}$ has row-weight $\rho = q$ and column-weight $\gamma = q$ [14].

For $q = 2^s$, let $PG(2,q)$ be the projective plane over F_q (see e.g. [14, 15]), with q^2+q+1 points and q^2+q+1 lines. Each point lies on $q+1$ lines and each line contains $q+1$ points. Similarly, the code $C_{PG(2,q)}$ with parity-check matrix $H_{PG(2,q)}$, called a Type-I PG-LDPC code, is constructed from the projective plane $PG(2,q)$. $H_{PG(2,q)}$ is a $(q^2+q+1) \times (q^2+q+1)$ circulant matrix [14]. $C_{PG(2,q)}$ has length $n_{PG} = q^2+q+1$, dimension $k_{PG} = n_{PG} - 3^s - 1$, minimum distance $d_{PG} = q+2$, and the parity-check matrix $H_{PG(2,q)}$ has row-weight $\rho = q+1$ and column-weight $\gamma = q+1$.

2.2 Stopping redundancy of finite geometry codes

It is shown in [3] that the stopping distance of parity-check matrices $H_{EG(2,q)}$ and $H_{PG(2,q)}$ satisfy $s(H_{EG(2,q)}) \geq q+1$ and $s(H_{PG(2,q)}) \geq q+2$. Therefore, we have

$$\begin{cases} s(H_{EG(2,q)}) = q+1 = d_{EG}, \\ s(H_{PG(2,q)}) = q+2 = d_{PG}, \\ \rho(EG(2,q)) \leq q^2-1 = n_{EG(2,q)}, \\ \rho(PG(2,q)) \leq q^2+q+1 = n_{PG(2,q)}. \end{cases} \tag{1}$$

A better upper bound on the stopping redundancy of $EG(2,q)$ and $PG(2,q)$ is given in [6]:

$$\begin{cases} \rho(EG(2,q)) \leq q^2-q = n_{EG(2,q)} - (q-1), \\ \rho(PG(2,q)) \leq q^2+1 = n_{PG(2,q)} - q. \end{cases} \tag{2}$$

2.3 Product codes

Let $H_{\mathcal{A}}$ and $H_{\mathcal{B}}$ be parity-check matrices representing binary linear codes $\mathcal{A}$ and $\mathcal{B}$ with parameters $[n,k,d]$ and $[n',k',d']$, respectively. It is known that the product code $\mathcal{A} \bigotimes \mathcal{B}$ has the following parity-check matrix [16]

$$H_{\mathcal{P}} = \begin{pmatrix} H_{\mathcal{A}} \otimes \mathcal{I}_{n'} \\ \mathcal{I}_n \otimes H_{\mathcal{B}} \end{pmatrix} \tag{3}$$

where $\otimes$ denotes the Kronecker product. Note that the rows of $H_{\mathcal{P}}$ may be linearly dependent.

Theorem 1 [9] Let $\rho(\mathcal{A})$ and $\rho(\mathcal{B})$ be the stopping redundancy of codes $\mathcal{A}$ and $\mathcal{B}$ with parameters $[n,k,d]$ and $[n',k',d']$, respectively. With the matrices $H_{\mathcal{P}}$, $H_{\mathcal{A}}$ and $H_{\mathcal{B}}$, described above, we have $s(H_{\mathcal{P}}) = s(H_{\mathcal{A}})s(H_{\mathcal{B}})$ and $\rho(\mathcal{A} \otimes \mathcal{B}) \leq n'\rho(\mathcal{A}) + n\rho(\mathcal{B})$.

Let $[0_{k\times(n-k)}|\mathcal{I}_k]$ be the $k \times n$ binary matrix where $\mathcal{I}_k$ denotes the $k \times k$ identity matrix and $0_{k\times(n-k)}$ is the $k \times (n-k)$ all-zero matrix. The following matrix $H_{\mathcal{P}1}$, introduced in [17], is a parity-check matrix for $\mathcal{A}\otimes\mathcal{B}$, assuming that the first $n-k$ columns of $H_{\mathcal{A}}$ are linearly independent.

$$H_{\mathcal{P}1} := \begin{pmatrix} H_{\mathcal{A}} \otimes \mathcal{I}_{n'} \\ [0_{k\times(n-k)}|\mathcal{I}_k] \otimes H_{\mathcal{B}} \end{pmatrix} \tag{4}$$

Obviously, $H_{\mathcal{P}1}$ is a submatrix of $H_{\mathcal{P}}$. It has been shown in [9] that

$$s(H_{\mathcal{P}1}) = s(H_{\mathcal{A}})s(H_{\mathcal{B}}) \tag{5}$$

if and only if the first $n-k$ columns of $H_{\mathcal{A}}$, which are assumed to be a set of linearly independent vectors, do not contain a stopping set of size less than $s(H_{\mathcal{A}})s(H_{\mathcal{B}})$.

Theorem 2 [9] Let $H_{\mathcal{A}}$ be a $\rho(\mathcal{A}) \times n$ parity-check matrix for $\mathcal{A}$ with $s(H_{\mathcal{A}}) = d$. Suppose the first $n-k$ columns of $H_{\mathcal{A}}$ are linearly independent and do not contain a stopping set of size less than dd'. Then, using matrix $H_{\mathcal{P}1}$, we obtain

$$\rho(\mathcal{A}\otimes\mathcal{B}) \leq n'\rho(\mathcal{A}) + k\rho(\mathcal{B}). \tag{6}$$

3 Product codes with constituent Hamming and FG codes

For $q' = 2^{s'}$, let $\mathcal{H}(s')$ be the binary $[q'-1, q'-s'-1, 3]$ Hamming code with full-rank parity-check matrix $H(s')$ whose columns are all distinct nonzero binary vectors of length s'. The Hamming codes are useful for the BEC [12, 13]. Product codes with constituent Hamming codes have high rate but low minimum distance. FG-LDPC codes are attractive as their minimum distances are relatively large and have excellent performance under iterative decoding. Accordingly, we use the Hamming and FG codes as constituent codes to construct LDPC product codes with good minimum distance, rate and stopping distance.

3.1 Code construction

Suppose $H(s')$ and $H_{EG(2,q)}$ are parity-check matrices for the Hamming code $\mathcal{H}(s')$ and EG code $C_{PG(2,q)}$, respectively. Using the parity-check matrix $H_{\mathcal{P}}$ in (3), we obtain the following parity-check matrix $H_{P_{H(s')-EG(2,q)}}$ for the product code $\mathcal{H}(s') \otimes C_{EG(2,q)}$:

$$H_{P_{H(s')-EG(2,q)}} = \begin{pmatrix} H(s') \otimes \mathcal{I}_{n_{EG}} \\ \mathcal{I}_{(q'-1)} \otimes H_{EG(2,q)} \end{pmatrix}.$$

The stopping distance of the full-rank matrix $H(s')$ is three. Hence, using (1) and Theorem 1, we obtain $s(H_{P_{H(s')-EG(2,q)}}) = 3(q+1)$. Therefore, for any integers $s' \geq 3$ and $s \geq 2$, the code $\mathcal{H}(s') \otimes \mathcal{C}_{EG(2,q)}$ has parameters:

$$\begin{cases} \text{Length:} & (q'-1)(q^2-1); \\ \text{Dimension:} & (q'-s'-1)(q^2-3^s); \\ \text{Minimum distance:} & 3(q+1); \\ s(H_{P_{H(s')-EG(2,q)}}): & 3(q+1). \end{cases}$$

In a similar way, one can obtain the following parity-check matrix $H_{P_{H(s')-PG(2,q)}}$ for the product code $\mathcal{H}(s') \otimes \mathcal{C}_{PG(2,q)}$.

$$H_{P_{H(s')-PG(2,q)}} = \begin{pmatrix} H(s') \otimes \mathcal{I}_{n_{PG}} \\ \mathcal{I}_{(q'-1)} \otimes H_{PG(2,q)} \end{pmatrix}$$

Using equality $s(H(s')) = 3$, (1) and Theorem 1 we obtain $s(H_{P_{H(s')-PG(2,q)}}) = 3(q+2)$. Thus, for any integers $s' \geq 3$ and $s \geq 2$, the product code $\mathcal{H}(s') \otimes \mathcal{C}_{PG(2,q)}$ has parameters:

$$\begin{cases} \text{Length:} & (q'-1)(q^2+q+1); \\ \text{Dimension:} & (q'-s'-1)(q^2+q-3^s); \\ \text{Minimum distance:} & 3(q+2); \\ s(H_{P_{H(s')-PG(2,q)}}): & 3(q+2). \end{cases}$$

Table 1 provides a list of product codes $\mathcal{H}(s') \otimes \mathcal{C}_{EG(2,q)}$. In this table integers s and s' refer to the parameters of the constituent codes and $q = 2^s$. In addition, several product codes $\mathcal{H}(s') \otimes \mathcal{C}_{PG(2,q)}$ are given in Table 2.

Determining the stopping distance of LDPC codes has been addressed in [10]. Using some probabilistic algorithms, it is shown in [10] that MacKay's [504, 252] and [1008, 504] codes, the [504, 252] progressive edge-growth code and the Ramanujan-Margulis (17, 5) code of length 4896 and dimension 2474 have stopping distances 16, 28, 19, 24, respectively. These codes are comparable with the codes given in Tables 1 and 2, for example, the [511, 180, 30], [945, 407, 27], [2263, 1170, 30] and [4095, 2101, 54] LDPC codes with stopping distances 30, 27, 30 and 54, respectively. Note that the [4095, 2101, 54] code presented here has stopping distance 54 while the Ramanujan-Margulis [4896,2474] code has stopping distance 24. In addition, the [504, 252] progressive edge-growth code has rate 0.5 and stopping distance 19 versus the [511, 180, 30] product code with rate 0.35 and stopping distance 30.

Another interesting property of the codes constructed here is related to their rate. Since the rate of a product code is the product of the rates of its constituent codes, and the rate of the Hamming and FG-LDPC codes tends to 1 as the length increases, the rate of $\mathcal{H}(s') \otimes \mathcal{C}_{EG(2,q)}$ and $\mathcal{H}(s') \otimes \mathcal{C}_{PG(2,q)}$ tends to 1 as q and s' increase.

3.2 Stopping redundancy analysis

In this section, we use Theorem 4 to obtain an upper bound on the stopping redundancy of the product LDPC codes constructed in this paper. This shows that the associated parity-check matrices represent a class of low-complexity codes with good performance.

The redundancy of a length-n code $\mathcal{C}$ is $r(\mathcal{C}) := n - dim(\mathcal{C})$. Theorem 4 in [4] states that

$$\rho(\mathcal{C}) \leq \binom{r(\mathcal{C})}{1} + \binom{r(\mathcal{C})}{2} + \cdots + \binom{r(\mathcal{C})}{d-2}. \tag{7}$$

With $\mathcal{E}_{n,d}(t) := \sum_{i=1}^{d-1} \binom{n}{i}(1 - \frac{i}{2^i})^t$, the following improved bound for $\rho(\mathcal{C})$ [5] is obtained

$$\rho(\mathcal{C}) \leq min\{t \in N : \mathcal{E}_{n,d}(t) < 1\} + (r(\mathcal{C}) - d + 1) \tag{8}$$

Theorem 3 The stopping redundancies of $\mathcal{H}(s') \otimes \mathcal{C}_{EG(2,q)}$ and $\mathcal{H}(s') \otimes \mathcal{C}_{PG(2,q)}$ satisfy:

$$\rho(\mathcal{H}(s') \otimes \mathcal{C}_{EG(2,q)}) \leq (q' + s' - 1)(q^2 - 1), \tag{9}$$

$$\rho(\mathcal{H}(s') \otimes \mathcal{C}_{PG(2,q)}) \leq (q' + s' - 1)(q^2 + q + 1). \tag{10}$$

Proof. The stopping distance of $H(s')$ is equal to the minimum distance of the Hamming code. Hence, $\rho(\mathcal{H}(s')) = s'$. Thus, using (1) and Theorem 1, we obtain

$$\begin{aligned}\rho(\mathcal{H}(s') \otimes \mathcal{C}_{EG(2,q)}) &\leq n_{EG} \times \rho(\mathcal{H}(s')) + (q' - 1) \times \rho(\mathcal{C}_{EG(2,q)}) \\ &\leq (q^2 - 1)s' + (q' - 1)(q^2 - 1) \\ &= (q' + s' - 1)(q^2 - 1).\end{aligned}$$

Equation (10) can be deduced using a similar argument. ■

Example 1 Let $\mathcal{C}_{PG(2,2)}$ be the [7, 3, 4] code with parity-check matrix $H_{PG(2,2)}$ [14]:

$$H_{PG(2,2)} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The product code $\mathcal{H}(3) \otimes \mathcal{C}_{PG(2,2)}$ is a $[49, 12, 12]$ code. The matrix $H_{P_{H(3)-PG(2,2)}}$ is a parity-check matrix for the product code $\mathcal{H}(3) \otimes \mathcal{C}_{PG(2,2)}$:

$$H_{P_{H(3)-PG(2,2)}} = \begin{pmatrix} H(3) \otimes \mathcal{I}_7 \\ \mathcal{I}_7 \otimes H_{PG(2,2)} \end{pmatrix}.$$

The stopping distance of $H_{P_{H(3)-PG(2,2)}}$ is 12. According to (7) and (8) we have $\rho(\mathcal{A}\otimes\mathcal{B}) \leq 5.2\times 10^8$ and $\rho(\mathcal{A}\otimes\mathcal{B}) \leq 4501$, respectively. However, the upper bound given by (10) implies $\rho(\mathcal{H}(3)\otimes\mathcal{C}_{PG(2,2)}) \leq 70$.

A motivation for introducing a better upper bound on the stopping redundancy of a code $\mathcal{C}$ is the fact that removing dependent rows decreases the complexity of iterative decoding. The codes $EG(2,q)$ and $PG(2,q)$ have been represented in [6] by the parity-check matrices $H'_{EG(2,q)}$ and $H'_{PG(2,q)}$, respectively, which have fewer rows than $H_{EG(2,q)}$ and $H_{PG(2,q)}$, respectively. Thus, using matrices $H'_{EG(2,q)}$ and $H'_{PG(2,q)}$ for $H_{\mathcal{B}}$ in (4), we obtain the following parity-check matrices $H'_{P1_{H(s')-EG(2,q)}}$ and $H'_{P1_{H(s')-PG(2,q)}}$ for $\mathcal{H}(s')\otimes\mathcal{C}_{EG(2,q)}$ and $\mathcal{H}(s')\otimes\mathcal{C}_{PG(2,q)}$, respectively.

$$H'_{P1_{H(s')-EG(2,q)}} = \begin{pmatrix} H(s')\otimes\mathcal{I}_{n_{EG}} \\ [\mathbf{0}_{(q'-s'-1)\times(s')}|\mathcal{I}_{(q'-s'-1)}]\otimes H'_{EG(2,q)} \end{pmatrix},$$

$$H'_{P1_{H(s')-PG(2,q)}} = \begin{pmatrix} H(s')\otimes\mathcal{I}_{n_{PG}} \\ [\mathbf{0}_{(q'-s'-1)\times(s')}|\mathcal{I}_{(q'-s'-1)}]\otimes H'_{PG(2,q)} \end{pmatrix}.$$

These matrices improve the upper bounds given in (9) and (10).

Theorem 4 (a) The matrices $H'_{P1_{H(s')-EG(2,q)}}$ and $H'_{P1_{H(s')-PG(2,q)}}$ have stopping distance $3(q+1)$ and $3(q+2)$, respectively; (b) The stopping redundancies of $\mathcal{H}(s')\otimes\mathcal{C}_{EG(2,q)}$ and $\mathcal{H}(s')\otimes\mathcal{C}_{PG(2,q)}$ satisfy the following constraints.

$$\begin{cases} \rho(\mathcal{H}(s')\otimes\mathcal{C}_{EG(2,q)}) \leq (q'-1)(q^2-1)-(q'-s'-1)(q-1), \\ \rho(\mathcal{H}(s')\otimes\mathcal{C}_{PG(2,q)}) \leq (q'-1)(q^2+q+1)-(q'-s'-1)q. \end{cases} \tag{11}$$

Proof. (a) All the length s' weight-one vectors are among the columns of $H(s')$. There is no stopping set for the associated s' column submatrix of $H(s')$. Hence the conditions in (5) hold. It is shown in [6] that $s(H'_{EG(2,q)}) = q+1$ and $s(H'_{PG(2,q)}) = q+2$. Therefore, using this and (5), we obtain $s(H'_{P1_{H(s')-EG(2,q)}}) = 3(q+1)$ and $s(H'_{P1_{H(s')-PG(2,q)}}) = 3(q+2)$. For statement (b), the stopping redundancy of $\mathcal{H}(s')$ is s'. Since the conditions in (5) hold, using (2) in (6), we obtain

$$\begin{aligned}\rho(\mathcal{H}(s')\otimes\mathcal{C}_{EG(2,q)}) &\leq n_{EG}\times\rho(\mathcal{H}(s')) + (q'-s'-1)\times\rho(\mathcal{C}_{EG(2,q)})) \\ &\leq (q^2-1)s' + (q'-s'-1)(q^2-q) \\ &= (q^2-1)s' + (q'-s'-1)((q^2-1)-(q-1)) \\ &= (q'-1)(q^2-1)-(q'-s'-1)(q-1).\end{aligned}$$

Equation (11) is proved in a similar way. ■

Example 2 Consider the $[49, 12, 12]$ code $\mathcal{H}(3) \otimes \mathcal{C}_{PG(2,2)}$ introduced in Example 1. Applying column permutation $\sigma_c = (12)(34)(67)$ and row permutation $\sigma_r = (36)(47)$ on matrix $H_{PG(2,2)}$ we obtain the following matrix.

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Using the process introduced in [6], we remove the second and third rows of this matrix followed by the column permutation σ_c to obtain the following matrix $H'_{PG(2,2)}$.

$$H'_{PG(2,2)} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

The following matrix $H'_{P1_{H(3)-PG(2,2)}}$ is a parity-check matrix for $\mathcal{H}(3) \otimes \mathcal{C}_{PG(2,2)}$.

$$H'_{P_{H(3)-PG(2,2)}} = \begin{pmatrix} H(3) \otimes \mathcal{I}_7 \\ [0_{4\times 3}|\mathcal{I}_4] \otimes H'_{PG(2,2)} \end{pmatrix}$$

Theorem 4 implies that $s(H'_{P1_{H(3)-PG(2,2)}}) = 12$. According to the upper bound given by (11) we have $\rho(H(2,3) \otimes \mathcal{C}_{PG(2,2)}) \leq 41$.

Table 3 illustrates the stopping redundancy bounds given by (7), (8), Theorem 3 and Theorem 4 applied to some of the medium-length LDPC product codes given here. As shown in the table, the first two bounds for these codes are very large and hence useless. Compared to these two bounds, the other two bounds, in particular the fourth one, are much better. Denoting the fourth bound by b_4 and the codes considered in Table 3, top to bottom, by C_i, $1 \leq i \leq 5$, we have $b_4(C_1) = 1.447r(C_1)$, $b_4(C_2) = 1.613r(C_2)$, $b_4(C_3) = 1.787r(C_3)$, $b_4(C_4) = 1.88r(C_4)$, $b_4(C_5) = 2.077r(C_5)$. To see the growth rate of this relation, consider the $[66591, 46341, 102]$ code given in Table 2. For this code we have $b_4(C) = 3.198r(C)$.

The parity-check matrices given in Theorem 4 satisfy $s(H) = d$, and hence the iterative decoding performance of the associated codes is close to that with ML decoding [4]. Therefore, considering the fact that the number of redundant rows of these matrices, compared to the redundancy, is not large, these matrices provide low-complexity codes with very good performance under iterative decoding.

Table 1: Parameters for product codes $\mathcal{H}(s') \otimes C_{EG(2,q)}$.

s'	s	length	dimension	min dist.	$s(H_{P_{H(s')-EG(2,q)}})$
3	2	105	28	15	15
4	2	225	77	15	15
5	2	465	182	15	15
3	3	441	148	27	27
4	3	945	407	27	27
5	3	1953	962	27	27
3	4	1785	700	51	51
4	4	3825	1925	51	51
5	4	7905	4550	51	51
6	4	16065	9975	51	51
3	5	7161	3124	99	99
4	5	15345	8591	99	99
5	5	31713	20306	99	99
6	5	64449	44517	99	99
3	6	28665	13468	195	195
4	6	61425	37037	195	195

Table 2: Parameters for product codes $\mathcal{H}(s') \otimes C_{PG(2,q)}$.

s'	s	length	dimension	min dist.	$s(H_{P_{H(s')-PG(2,q)}})$
3	2	147	44	18	18
4	2	315	121	18	18
5	2	651	286	18	18
3	3	511	180	30	30
4	3	1095	495	30	30
5	3	2263	1170	30	30
3	4	1911	764	54	54
4	4	4095	2101	54	54
5	4	8463	4966	54	54
6	4	17199	10887	54	54
3	5	7399	3252	102	102
4	5	15855	8943	102	102
5	5	32767	21138	102	102
6	5	66591	46341	102	102
3	6	29127	13724	198	198
4	6	62415	37741	198	198

Table 3: Upper bounds on the stopping redundancy of some LDPC product codes.

code	Bound (7)	Bound (8)	Theorem 3	Theorem 4
$[511, 180, 30]$	4.00×10^{40}	2.01×10^{9}	730	479
$[945, 407, 27]$	7.15×10^{42}	3.00×10^{8}	1197	868
$[1953, 962, 27]$	3.89×10^{49}	3.50×10^{8}	2268	1771
$[2263, 1170, 30]$	2.87×10^{55}	2.83×10^{9}	2628	2055
$[4095, 2101, 54]$	2.51×10^{103}	4.76×10^{16}	5037	4143

References

[1] P. Elias, "Error-free coding," *IRE Trans. Inform. Theory*, vol. 9, pp. 29–37, Jan. 1954.

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

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

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

[5] J. Han and P.H. Siegel, " Improved upper bounds on stopping redundancy," *IEEE Trans. Inform. Theory*, vol. 53, no. 1, pp. 90–104, Jan. 2007.

[6] H.-y. Liu, X.-y. Lin, L.-r. Ma and J. Chen, "On the stopping distance and stopping redundancy of finite geometry LDPC codes," *IEICE Trans. Fundamentals*, vol. E91A, no. 8, pp. 2159–2166, Aug. 2008.

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

[8] M. Esmaeili and M.J. Amoshahi, "On the Stopping distance of Array Code Parity-check Matrices," *IEEE Trans. Inform. Theory*, Vol. 55, No. 8, pp. 3488–3493, AUGUST 2009.

[9] M. Hivadi and M. Esmaeili, "On the stopping distance and stopping redundancy of product codes," *IEICE Trans. Fundamentals*, vol. E91A, no. 8, pp. 2167–2173, Aug. 2008.

[10] M. Hirotomo, Y. Konishi and M. Morii, "A probabilistic algorithm for finding the minimum-size stopping sets of LDPC codes," *Proc. IEEE Inform. Theory Workshop*, pp. 66-70, May 2008.

[11] K.M. Krishnan and P. Shankar, " Computing the stopping distance of a Tanner graph is NP-hard," *IEEE Trans. Inform. Theory*, vol. 53, no. 6, pp. 22782280, June 2007.

[12] R.J. McEliece,"Are there turbo-codes on Mars?," Shannon Lecture, *IEEE Int. Symp. Inform. Theory*, June - July, 2004. http://www.systems.caltech.edu/EE/Faculty/rjm/.

[13] J.H. Weber and K.A. Abdel-Ghaffar," Stopping set analysis for Hamming codes," *Proc. IEEE Inform. Theory Workshop*, pp. 244-247, Aug.-Sept. 2005.

[14] Y. Kou, S. Lin, and M. Fossorier, "Low-density parity-check codes based on finite geometries: A rediscovery and more,"*IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2711-2736, Nov. 2001.

[15] S. Lin and D.J. Costello, Jr., Error Control Coding: Fundamentals and Applications, 2nd Ed., *Prentice-Hall, Upper Saddle River, NJ*, 2004.

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

[17] M. Esmaeili,"On full-rank parity-check matrices of product codes," *Utilitas Mathematica*, vol. 76, pp. 3–10, July 2008.