Correcting Combinations of Errors and Erasures with Euclidean Geometry LDPC Codes

Qiuju Diao[1], Ying Yu Tai[2], Shu Lin[1] and Khaled Abdel-Ghaffar[1]
[1] Dept. of Electrical and Computer Engineering University of California, Davis, CA 95616
[2] SanDisk Corporation, Milpitas, CA 95035
Email: {judiao, yytai, shulin, ghaffar}@ucdavis.edu

***Abstract*—It is shown that Euclidean geometry LDPC codes in conjunction with their shortened codes obtained by puncturing their parity-check matrices are effective in correcting combinations of errors and erasures with a two-phase decoding scheme. This is due to the large row redundancies of the parity-check matrices of these codes which are given by the incidence matrices of Euclidean geometries.**

I. Introduction

LDPC codes [1] are so far mostly constructed or designed for correcting errors caused by an AWGN channel or correcting erasures caused by an erasure channel. Rarely, they are constructed or designed for correcting *combinations* of errors and erasures caused by an *erasure/error channel*.

In this paper, we explore using Euclidean geometry (EG) LDPC codes in conjunction with their shortened codes for correcting combinations of errors and erasures. Let $\mathbf{H}_{\mathrm{EG}}$ be the parity-check matrix of an EG-LDPC code $\mathcal{C}_{\mathrm{EG}}$. The parity-check matrix of a shortened code of $\mathcal{C}_{\mathrm{EG}}$ is a submatrix of $\mathbf{H}_{\mathrm{EG}}$ obtained by deleting a set of chosen columns and the rows that have 1-entries in the locations corresponding to the deleted columns. Since $\mathbf{H}_{\mathrm{EG}}$ is a low-density parity-check matrix, the parity-check matrix of a shortened code of $\mathcal{C}_{\mathrm{EG}}$ is also a low-density matrix. In correcting errors and erasures, decoding consists of two phases. First, the erasures are removed from the received vector resulting in a shortened received vector. This shortened received vector is then decoded based on its corresponding parity-check matrix to correct the errors (if any) using an iterative message-passing algorithm. After this error correction phase, the removed erasures are re-inserted back in their original positions. Then, the erasures are corrected using a simple algebraic method based on the parity-check matrix $\mathbf{H}_{\mathrm{EG}}$ of the original code $\mathcal{C}_{\mathrm{EG}}$.

The most important aspect in this approach is that the parity-check matrices used for decoding the shortened codes are submatrices of the original parity-check matrix. Hence, no extra memory or computations are needed to determine these matrices. Practically, this allows for using the same decoder hardware of $\mathcal{C}_{\mathrm{EG}}$ to decode the shortened codes simply by disabling the processing units corresponding to the deleted columns and rows of its parity-check matrix. However, for this approach to be feasible, it is necessary that the parity-check matrix of the original code has a large number of redundant rows in order to contain the parity-check matrices of the shortened codes as submatrices. This is exactly the case for the parity-check matrices of EG-LDPC codes [2]–[4].

The shortening of an EG-LDPC code is based on the structural properties of the Euclidean geometry based on which the code is constructed. For the ease of presentation of the code shortening method, we focus on EG-LDPC codes constructed using two-dimensional Euclidean geometries over finite fields. The concepts and techniques developed for this subclass of EG-LDPC codes can be applied in a straightforward manner to EG-LDPC codes constructed using Euclidean geometries of higher dimension, projective geometries, finite fields and combinatorial designs. (Throughout this paper we follow the traditional coding literature which uses Euclidean geometry to refer to affine geometry.)

The rest of this paper is organized as follows. Section II gives a brief review of two-dimensional Euclidean geometries and their structural properties that are pertinent for shortening EG-LDPC codes. Section III gives a basic construction of EG-LDPC codes. Section IV presents a method for shortening a basic EG-LDPC code to obtain shortened LDPC codes and shows that the shortened LDPC codes perform close to the original code. Section V describes a two-phase decoding method for correcting combinations of errors and erasures. Section VI concludes the paper with some remarks.

II. Two-dimensional Euclidean geometries

A two-dimensional Euclidean geometry $\mathrm{EG}(2,q)=[\mathcal{N},\mathcal{M}]$ over the finite field $\mathrm{GF}(q)$ consists of a set $\mathcal{N}$ of q^2 points and a set $\mathcal{M}$ of $q(q+1)$ lines [3]–[5]. A point in $\mathcal{N}$ is a two-tuple $\mathbf{a}=(a_0,a_1)$ over $\mathrm{GF}(q)$ and the zero two-tuple $(0,0)$ is called the *origin* of $\mathrm{EG}(2,q)$. A line in $\mathcal{M}$ is a one-dimensional subspace, or its coset, of the vector space of all the q^2 two-tuples over $\mathrm{GF}(q)$. A line in $\mathcal{M}$ consists of q points and any two distinct points in $\mathcal{N}$ are connected by one and only one line in $\mathcal{M}$.

For every point $\mathbf{a}$ in $\mathcal{N}$, there are exactly $q+1$ lines in $\mathcal{M}$ that intersect at $\mathbf{a}$, i.e., all of them pass through $\mathbf{a}$. These lines are said to form an *intersecting bundle* at $\mathbf{a}$, denoted by $\Delta(\mathbf{a})$. Any point in $\mathcal{N}$ other than $\mathbf{a}$ is on one and only one line in $\Delta(\mathbf{a})$ while the point $\mathbf{a}$ is on every line in $\Delta(\mathbf{a})$. Therefore, all the q^2 points in $\mathcal{N}$ are on the lines in $\Delta(\mathbf{a})$. Two intersecting bundles at two distinct points have one and only one line in common, namely the line connecting the two points. *The intersecting structure of lines plays the key role in constructing shortened EG-LDPC codes from a basic EG-LDPC code.*

The field GF(q^2), as an extension field of GF(q), is a realization of EG$(2,q)$. Let α be a primitive element of GF(q^2). Then, $\alpha^{-\infty} \triangleq 0$, $\alpha^0 = 1$, α, α^2,..., α^{q^2-2} give all the q^2 elements of GF(q^2) and they represent the q^2 points of $\mathcal{N}$. The origin of EG$(2,q)$ is represented by $\alpha^{-\infty}$. The set $\mathcal{L}_{-\infty} = \{\alpha^{-\infty} = 0, \alpha^0 = 1, \alpha^{q+1}, \ldots, \alpha^{(q-2)(q+1)}\}$ of the q elements in GF(q^2), which represent q points in $\mathcal{N}$, forms a line passing through the origin of EG$(2,q)$. For $0 \leqslant j \leqslant q$, the set $\alpha^j\mathcal{L}_{-\infty} = \{0, \alpha^j, \alpha^{(q+1)+j}, \ldots, \alpha^{(q-2)(q+1)+j}\}$ of q points also forms a line passing through the origin of EG$(2,q)$. Hence, $\mathcal{L}_{-\infty}, \alpha\mathcal{L}_{-\infty}, \ldots, \alpha^q\mathcal{L}_{-\infty}$ form the set $\Delta(\alpha^{-\infty})$ of the $q+1$ lines that intersect at the origin of EG$(2,q)$. Let $\mathcal{L} = \{\alpha^{j_1}, \alpha^{j_2}, \ldots, \alpha^{j_q}\}$ be a line in $\mathcal{M}$ not passing through the origin of EG$(2,q)$ with α^{j_1}, α^{j_2}, ..., α^{j_q} as its q points where $0 \leq j_1, j_2, \ldots, j_q < q^2 - 1$. For $0 \leq i < q^2 - 1$, let $\alpha^i\mathcal{L} = \{\alpha^{j_1+i}, \alpha^{j_2+i}, \ldots, \alpha^{j_q+i}\}$. Then, the set $\alpha^i\mathcal{L}$ of q points in $\mathcal{N}$ also forms a line in $\mathcal{M}$ not passing through the origin and $\mathcal{L}$, $\alpha\mathcal{L}$, ..., $\alpha^{q^2-2}\mathcal{L}$ give all the q^2-1 lines in $\mathcal{M}$ not passing through the origin of EG$(2,q)$ [3], [4]. The structure of lines in $\mathcal{M}$ developed above is called the *cyclic structure*.

III. Basic EG-LDPC codes

Let $\mathcal{L}$ be a line in $\mathcal{M}$. Based on $\mathcal{L}$, we define the following q^2-tuple over GF(2), $\mathbf{v}_{\mathcal{L}} = (v_{-\infty}, v_0, v_1, \ldots, v_{q^2-2})$, whose components correspond to the q^2 points $\alpha^{-\infty}, \alpha^0, \alpha, \alpha^2, \ldots, \alpha^{q^2-2}$ in $\mathcal{N}$, where $v_j = 1$ if and only if α^j is a point on $\mathcal{L}$ and $v_j = 0$ otherwise. This q^2-tuple $\mathbf{v}_{\mathcal{L}}$ is called the *incidence vector* of the line $\mathcal{L}$. Form a $q(q+1) \times q^2$ matrix $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$, which is called the *incidence matrix* of EG$(2,q) = [\mathcal{N},\mathcal{M}]$ over GF(2), with the incidence vectors of the lines in $\mathcal{M}$ as rows arranged in a specific way. Let $\mathcal{L}_{-\infty}$ be a line in $\Delta(\alpha^{-\infty})$ and $\mathcal{L}$ be a line in $\Delta(\alpha^{-\infty})^c = \mathcal{M} \setminus \Delta(\alpha^{-\infty})$. We arrange the rows of $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ in such a way that the incidence vectors of the lines $\mathcal{L}_{-\infty}, \alpha\mathcal{L}_{-\infty}, \ldots, \alpha^q\mathcal{L}_{-\infty}$, in this order, are the first $q+1$ rows of $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ and the incidence vectors of the lines $\mathcal{L}, \alpha\mathcal{L}, \ldots, \alpha^{q^2-2}\mathcal{L}$, in this order, are the last q^2-1 rows of $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$. We label the rows of $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ using the lines in $\mathcal{M}$ in this specified order and we label the columns using the points $\alpha^{-\infty}, \alpha^0, \alpha, \ldots, \alpha^{q^2-2}$, in this order. Hence, $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ has the form:

$$\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M}) = \begin{bmatrix} \mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \Delta(\alpha^{-\infty})) \\ \mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \Delta(\alpha^{-\infty})^c) \end{bmatrix}, \quad (1)$$

which consists of two submatrices. It follows from the cyclic structure of the lines in $\mathcal{M}$ that: 1) the top submatrix $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \Delta(\alpha^{-\infty}))$ of $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$, which is of size $(q+1) \times q^2$, has a column of ones of length $q+1$ followed by $q-1$ identity matrices of size $(q+1) \times (q+1)$; and 2) the bottom submatrix $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \Delta(\alpha^{-\infty})^c)$ of $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ has a column of zeros of length q^2-1 followed by a $(q^2-1) \times (q^2-1)$ circulant matrix.

The matrix $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ is an incidence matrix of the geometry EG$(2,q)$ with columns and rows corresponding to the points and lines of EG$(2,q)$, respectively. The column and row weights of $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ are $q+1$ and q, respectively. Since two lines in EG$(2,q)$ has at most one point in common, no two rows (or two columns) have more than one position where they both have 1-entries. This structural property is referred to as the row-column (RC) constraint [2], [3]. From the intersecting structure of lines in $\mathcal{M}$, it is clear that, for each column of $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ labeled by a point α^j in $\mathcal{N}$, there are $q+1$ rows with 1-components at the position j for $j = -\infty, 0, 1, \ldots, q^2-2$. These $q+1$ rows are said to be *attached to the column labeled* α^j. These rows simply correspond to the lines in $\mathcal{M}$ that intersect at the point α^j.

The null space of $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ gives a $(q+1,q)$-regular EG-LDPC code of length q^2, denoted by $\mathcal{C}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ and called a basic EG-LDPC code. The RC-constraint on the rows and columns of $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ ensures that: (1) the minimum distance of $\mathcal{C}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ is at least $q+2$ [2]; and (2) the girth of the Tanner graph of $\mathcal{C}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ is at least 6 [2]. In a recent paper [6], we proved that the Tanner graph of $\mathcal{C}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ contains no trapping set [7] of size smaller than $q+1$ with the number of odd-degree CNs less than $q+1$. For large q, the minimum distance of $\mathcal{C}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ is relatively large. Since it has no harmful trapping sets with size smaller than its minimum distance, the error-floor of $\mathcal{C}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ is dominated by its minimum distance and is expected to be very low.

Consider the special case for which $q = 2^s$ where s is a positive integer. For this case, it can be proved that the rank of $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ is 3^s [8]. Consequently, $\mathcal{C}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ is a $(4^s, 4^s - 3^s)$ code with minimum distance exactly $2^s + 2$. For $s > 3$, the parity-check matrix of this code has a large number of redundant rows which is $4^s - 3^s$.

Since the parity-check matrix $\mathbf{H}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ of a basic EG-LDPC code $\mathcal{C}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ satisfies the RC-constraint, it is one-step majority-logic decodable [3], [4]. For each code symbol of a codeword in $\mathcal{C}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$, $q+1$ *orthogonal check-sums* [3], [4] can be formed such that the code symbol is contained in each of these check-sums and any other code symbol is contained in at most one of these check-sums. For a binary symmetric channel, this orthogonal structure ensures that the basic EG-LDPC code $\mathcal{C}_{\mathrm{EG}}(\mathcal{N},\mathcal{M})$ is capable of correcting $\lfloor (q+1)/2 \rfloor$ or fewer errors. For a binary erasure channel, if a received word contains $q+1$ or fewer erasures, there is at least one orthogonal check-sum containing only one erasure and no other [4]. From this check-sum, the erased symbol can be recovered.

IV. Shortened EG-LDPC codes

Let Λ be a set of κ points in $\mathcal{N}$. Assume that $\kappa \leqslant q$. This assumption will be clarified later. Let $\Phi(\Lambda) = \cup_{\mathbf{a}\in\Lambda}\Delta(\mathbf{a})$ which is the union of the intersecting bundles of lines in $\mathcal{M}$ intersecting at the points in Λ. $\Phi(\Lambda)$ is the set of lines in $\mathcal{M}$, each passing through at least one point in Λ. Let $\Lambda^c = \mathcal{N} \setminus \Lambda$ and $\Phi(\Lambda)^c = \mathcal{M} \setminus \Phi(\Lambda)$. If we delete all the points in Λ

and all the lines in $\Phi(\Lambda)$ from $\mathrm{EG}(2,q)$, we obtain a residual geometry, denoted $(\Lambda^c, \Phi(\Lambda)^c)$. The incidence matrix of this residual geometry is the matrix, denoted by $\mathbf{H}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$, which can be obtained from the basic matrix $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \mathcal{M})$ by deleting all the columns labeled by points in Λ and all the rows attached to these columns. The matrix $\mathbf{H}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$ is a $(q^2+q-|\Phi(\Lambda)|) \times (q^2-\kappa)$ submatrix of the basic matrix $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \mathcal{M})$. It follows from the intersecting structure of lines in $\mathcal{M}$ that, deleting a column that corresponds to a point $\mathbf{a}$ in Λ and the $q+1$ rows attached to it from $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \mathcal{M})$ reduces the weight of each column of $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \mathcal{M})$ that corresponds to a point in Λ^c by one. Since the intersecting bundles at the points in Λ have common lines, the reductions of weights for the columns in $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \mathcal{M})$ corresponding to the $q^2-\kappa$ points in Λ^c may be different. However, the maximum column weight reduction is κ. Hence, the minimum column weight of the punctured matrix $\mathbf{H}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$ is $q+1-\kappa$.

The null space of the punctured matrix $\mathbf{H}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$ gives a shortened EG-LDPC code, denoted by $\mathcal{C}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$, of length $q^2-\kappa$ with minimum distance at least $q+2-\kappa$. For $\kappa = 1, 2, \ldots, q$, we can construct a sequence of shortened codes of $\mathcal{C}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$ with different rates and minimum distances. For the case that $\Lambda = \{\alpha^{-\infty}\}$, the punctured matrix $\mathbf{H}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$ is a $(q^2-1) \times (q^2-1)$ circulant matrix obtained by deleting from the basic matrix $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \mathcal{M})$ the column labeled by the origin point $\alpha^{-\infty}$ of $\mathrm{EG}(2,q)$ and the $q+1$ rows attached to it. The column and row weights of this circulant matrix are both equal to q. The null space of $\mathbf{H}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$ gives a cyclic EG-LDPC code, denoted $\mathcal{C}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$, with minimum distance at least $q+1$. Cyclic EG codes were first proposed as LDPC codes in 2001 [2].

To determine the exact number of rows in $\mathbf{H}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$, denoted by $\mathcal{R}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$, we must determine $|\Phi(\Lambda)|$, which is a difficult problem since $|\Phi(\Lambda)|$ depends on the distribution of the points in Λ and the size of this set. However, a lower bound on $\mathcal{R}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$ can be derived. From this bound, we can bound the largest number κ of columns that we can delete without resulting in a null punctured matrix.

For $i = 1, 2, \ldots, \kappa$, let m_i be the number of lines in $\Phi(\Lambda)$ each passing through exactly i points in Λ. Then, $|\Phi(\Lambda)| = \sum_{i=1}^{\kappa} m_i$. Let $(\mathbf{a}, \mathcal{L})$ be a pair that consists of a point $\mathbf{a}$ in Λ and a $\mathcal{L}$ line in $\Phi(\Lambda)$ passing through the point $\mathbf{a}$. Such a pair is called a *point-line pair* in the subgeometry $(\Lambda, \Phi(\Lambda))$. There are two different ways of counting the number of point-line pairs in $(\Lambda, \Phi(\Lambda))$. Since each of the κ points in Λ is on $q+1$ lines, the total number of such pairs is $\kappa(q+1)$. Alternatively, since a line passing through i points in Λ contributes i such pairs, the total number of point-line pairs is $m_1 + 2m_2 + \cdots + \kappa m_\kappa$. Hence,

$$m_1 + 2m_2 + \cdots + \kappa m_\kappa = \kappa(q+1). \tag{2}$$

Next, we count, also in two different ways, the number of unordered pairs of points in Λ. Since Λ consists of κ points, there are $\binom{\kappa}{2}$ such pairs. Alternatively, since every pair of points in Λ is on a unique line in $\Phi(\Lambda)$ and a line passing through i points in Λ connects $\binom{i}{2}$ pairs of points, the total number of pairs of points in Λ is $\sum_{i=1}^{\kappa} \binom{i}{2} m_i$. Hence,

$$\binom{2}{2} m_2 + \binom{3}{2} m_3 + \cdots + \binom{\kappa}{2} m_\kappa = \binom{\kappa}{2}. \tag{3}$$

As $\binom{i}{2} = i(i-1)/2 \leqslant \kappa(i-1)/2$ for $i \leqslant \kappa$, it follows from (3) that

$$\sum_{i=2}^{\kappa} (i-1) m_i \geq \kappa - 1. \tag{4}$$

Combining (2) and (4), and using $|\Phi(\Lambda)| = \sum_{i=1}^{\kappa} m_i$, we get $|\Phi(\Lambda)| \leqslant \kappa q + 1$ with equality if the κ points in Λ are collinear, i.e. they are on the same line. Hence,

$$\mathcal{R}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c) \geq q^2 - (\kappa-1)q - 1. \tag{5}$$

For $\kappa = q+1$, $\mathbf{H}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$ may be a null matrix. That is why we restrict the size of Λ to be no greater than q at the beginning of this section. However, it should be stated that, depending on the distribution of points in Λ, it is possible that $\mathcal{R}_{\mathrm{EG}}(\Lambda^c, \Phi(\Lambda)^c)$ is positive even if $\kappa > q$.

Example 1. Let $\mathrm{EG}(2,2^5)$ be the code construction geometry. This geometry consists of 1024 points and 1056 lines, each line passing through 32 points. The incidence matrix $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \mathcal{M})$ of this geometry is a 1056×1024 matrix with column and row weights 33 and 32, respectively. The rank of this matrix is $3^5 = 243$. Hence, $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \mathcal{M})$ has 813 redundant rows. Its null space gives the (1024,781) basic EG-LDPC code, $\mathcal{C}_{\mathrm{EG}}(\mathcal{N}, \mathcal{M})$, with minimum distance exactly 34. The Tanner graph of this code contains no harmful trapping set with size smaller than 30 [6], [8]. Puncturing the matrix $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \mathcal{M})$ by deleting various columns and their attached rows, we obtain various punctured matrices whose null spaces give various shortened EG-LDPC codes. Table I gives the parameters of the punctured matrices and their resulting codes if $\kappa = 4, 8, 12, 16, 32, 34$ *randomly chosen* columns and their attached rows are deleted from $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \mathcal{M})$. We see that all the shortened codes have the *same dimension* (even for $\kappa = 34$ which exceeds $q = 32$) and the rank of each punctured matrix is κ less than the rank of $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \mathcal{M})$. The BER performances of these shortened EG-LDPC codes over the AWGN channel decoded using the SPA with 50 iterations are shown in Fig. 1. We see that, for $\kappa = 2, 4, 8, 16$, the performance curves of the shortened codes cluster together and are very close to the performance of the basic (1024,781) code.

Next, we examine the decoding convergence rate and the effect of the distribution of punctured bits on the performance of the shortened codes. The entries in Table I corresponding to 16 punctured bits are generated by randomly selecting a set Λ_1 of 16 points in $\mathrm{EG}(2,2^5)$ and deleting from $\mathbf{H}_{\mathrm{EG}}(\mathcal{N}, \mathcal{M})$ the 16 columns labelled by the points in Λ_1 and their attached rows. The number of rows attached to these 16 columns is 431. The resultant matrix is the 625×1008 matrix, $\mathbf{H}_{\mathrm{EG}}(\Lambda_1^c, \Phi(\Lambda_1)^c)$, with constant row weight 32 and minimum column weight

17. The rank of this matrix is 227 which is 16 less than the rank of $\mathbf{H}_{\rm EG}(\mathcal{N},\mathcal{M})$ and it still has 398 redundant rows. The null space given by $\mathbf{H}_{\rm EG}(\Lambda_1^c,\Phi(\Lambda_1)^c)$ is a (1008,781) shortened EG-LDPC code, $\mathcal{C}_{\rm EG}(\Lambda_1^c,\Phi(\Lambda_1)^c)$, of rate 0.7748 and minimum distance at least 18. The Tanner graph of this shortened code contains no harmful trapping set with size smaller than 14. The bit performances of this code with 5, 10, and 50 iterations of the SPA are shown in Fig.2. We see that the decoding of this code converges fast due to the large row redundancy of its parity-check matrix.

Let Λ_2 be a set of 16 collinear points in EG$(2,2^5)$. In this case, the number of rows attached to the 16 columns labeled by points in Λ_2 is $16\times 32+1=513$. Removing these columns and their attached rows, we obtain a 543×1008 punctured matrix, $\mathbf{H}_{\rm EG}(\Lambda_2^c,\Phi(\Lambda_2)^c)$, with minimum column weight 17. The rank of this punctured matrix is still 227 but it has a smaller number of redundant rows, 316, compared to the 398 redundant rows of the above punctured matrix obtained by deleting the 16 columns corresponding to the randomly selected Λ_1 and their attached rows. The null space of the 543×1008 punctured matrix, $\mathbf{H}_{\rm EG}(\Lambda_2^c,\Phi(\Lambda_2)^c)$, again gives the (1008,781) EG-LDPC code $\mathcal{C}_{\rm EG}(\Lambda_2^c,\Phi(\Lambda_2)^c)$. The code $\mathcal{C}_{\rm EG}(\Lambda_2^c,\Phi(\Lambda_2)^c)$ performs almost the same as the code $\mathcal{C}_{\rm EG}(\Lambda_1^c,\Phi(\Lambda_1)^c)$. △△

From the above example, we have an important observation that the rank reduction of a punctured matrix is the same as the number of columns being deleted from $\mathbf{H}_{\rm EG}(\mathcal{N},\mathcal{M})$. We have the same observation for puncturing the basic matrices constructed based on other two-dimensional Euclidean geometries, say EG$(2,2^q)$ for $q=4,6$, and 7, no matter which columns are deleted as long as their number is small. Actually, depending on which columns are deleted, this is true even if the number of deleted columns exceeds q.

V. Two-phase decoding for correcting random errors and erasures

The basic EG-LDPC code $\mathcal{C}_{\rm EG}(\mathcal{N},\mathcal{M})$ in conjunction with its shortened codes can be used for correcting combinations of errors and erasures with a two-phase decoding scheme. Set the maximum number of erasures to be corrected to $\kappa_{max}\le q$.

Let $\mathbf{v}=(v_{-\infty},v_0,v_1,\ldots,v_{q^2-2})$ be a codeword in $\mathcal{C}_{\rm EG}(\mathcal{N},\mathcal{M})$ whose components are labeled by the points $\alpha^{-\infty},\alpha^0,\alpha^1,\ldots,\alpha^{q^2-2}$ in EG$(2,q)$. If we delete all the code bits in $\mathbf{v}$ with indices labeled by the points in Λ, we obtain a punctured vector, denoted by $\mathbf{v}'(\Lambda)$, of length $q^2-\kappa$. Before we discuss the two-phase decoding for correcting combinations of errors and erasures, we need to show that the punctured vector $\mathbf{v}'(\Lambda)$ is a codeword in the shortened code $\mathcal{C}_{\rm EG}(\Lambda^c,\Phi(\Lambda)^c)$. Since $\mathbf{v}$ is in the null space of $\mathbf{H}_{\rm EG}(\mathcal{N},\mathcal{M})$, it is orthogonal to every row in $\mathbf{H}_{\rm EG}(\mathcal{N},\Phi(\Lambda)^c)$ which is the submatrix of $\mathbf{H}_{\rm EG}(\mathcal{N},\mathcal{M})$ obtained by removing the rows in $\mathbf{H}_{\rm EG}(\mathcal{N},\mathcal{M})$ that correspond to the lines in $\Phi(\Lambda)$. The rows in $\mathbf{H}_{\rm EG}(\mathcal{N},\Phi(\Lambda)^c)$ correspond to all the lines in EG$(2,q)=(\mathcal{N},\mathcal{M})$ which do not pass through any of the points in Λ. Hence, every row in $\mathbf{H}_{\rm EG}(\mathcal{N},\Phi(\Lambda)^c)$ has zeros in the positions labeled by the points in Λ. These are precisely the positions of bits deleted from $\mathbf{v}$ to obtain $\mathbf{v}'(\Lambda)$. Furthermore, by deleting these positions from the rows in $\mathbf{H}_{\rm EG}(\mathcal{N},\Phi(\Lambda)^c)$, we obtain the rows in $\mathbf{H}_{\rm EG}(\Lambda^c,\Phi(\Lambda)^c)$ which is the parity-check matrix of the shortened code $\mathcal{C}_{\rm EG}(\Lambda^c,\Phi(\Lambda)^c)$. Therefore, the punctured vector $\mathbf{v}'(\Lambda)$ is orthogonal to the rows in $\mathbf{H}_{\rm EG}(\Lambda^c,\Phi(\Lambda)^c)$ and is a codeword in the shortened code $\mathcal{C}_{\rm EG}(\Lambda^c,\Phi(\Lambda)^c)$.

Suppose a codeword $\mathbf{v}$ in $\mathcal{C}_{\rm EG}(\mathcal{N},\mathcal{M})$ is transmitted over a binary symmetric error/erasure channel. Let $\mathbf{r}$ be the received sequence which contains the κ erasures at the positions labeled by a set Λ of κ points with $\kappa\leqslant\kappa_{max}$. In the first phase of decoding, the decoder deletes the κ erasures from the received sequence $\mathbf{r}$. Let $\mathbf{r}(\Lambda)$ be the resulting vector of length $q^2-\kappa$. The decoder decodes $\mathbf{r}(\Lambda)$ using the punctured matrix $\mathbf{H}(\Lambda^c,\Phi(\Lambda)^c)$ as a parity-check matrix. Decoding can be accomplished using an iterative message-passing algorithm, say the SPA or the MSA. If decoding is successful, it produces a codeword in $\mathcal{C}_{\rm EG}(\Lambda^c,\Phi(\Lambda)^c)$ which we denote by $\mathbf{u}$, then the decoder proceeds to the second phase of decoding. If decoding of $\mathbf{r}(\Lambda)$ fails, we stop the decoding process and declare a decoding failure.

In the second phase of decoding, the decoder inserts the erased symbols in $\mathbf{u}$ in their proper positions to produce the sequence $\mathbf{u}'$ of length q^2. This sequence contains κ erasures in the positions labeled by points in Λ. The decoder's task now is to find a codeword $\mathbf{v}'$ in $\mathcal{C}_{\rm EG}(\mathcal{N},\mathcal{M})$ that agrees with $\mathbf{u}'$ in all positions labeled by the points in Λ^c. To accomplish this, the decoder searches for a row in the parity-check matrix $\mathbf{H}_{\rm EG}(\mathcal{N},\mathcal{M})$ that has zeros in all positions labeled by points in Λ except for exactly one position, i.e., a row labeled by a line passing through exactly one point in Λ. Since $\kappa\leqslant\kappa_{max}\leqslant q$, such a row exists due to the orthogonal structure of $\mathbf{H}(\mathcal{N},\mathcal{M})$. Let $\mathbf{h}$ be such a row and $\mathbf{h}(\mathbf{a})$ be the bit in $\mathbf{h}$ labeled by the point $\mathbf{a}$ in EG$(2,q)$. Then, $\mathbf{h}(\mathbf{a}^*)=1$ for a unique $\mathbf{a}^*\in\Lambda$ and $\mathbf{h}(\mathbf{a})=0$ for all $\mathbf{a}\in\Lambda$ and $\mathbf{a}\neq\mathbf{a}^*$. Since $\mathbf{v}'$ is selected to be in $\mathcal{C}_{\rm EG}(\mathcal{N},\mathcal{M})$, it is orthogonal to $\mathbf{h}$ over GF(2). Hence, $\sum_{\mathbf{a}\in\mathcal{N}}\mathbf{h}(\mathbf{a})\mathbf{v}'(\mathbf{a})=0$ in GF(2), where $\mathbf{v}'(\mathbf{a})$ is the bit in $\mathbf{v}'$ labeled by the point $\mathbf{a}$. This equation implies that $\mathbf{v}'(\mathbf{a}^*)=\sum_{\mathbf{a}\in\mathcal{N}\setminus\Lambda}\mathbf{h}(\mathbf{a})\mathbf{v}'(\mathbf{a})$, from which the bit $\mathbf{v}'(\mathbf{a}^*)$ can be determined. By doing this, all the erasures can be recovered. At the completion of the second decoding phase, a vector $\mathbf{v}'$ is obtained. Then, the decoder checks if $\mathbf{v}'\cdot\mathbf{H}(\mathcal{N},\mathcal{M})^T=0$. If so, $\mathbf{v}'$ is the final decoder output, otherwise decoding fails.

The two-phase decoder succeeds in retrieving the transmitted codeword $\mathbf{v}$ if the first phase is successful in retrieving $\mathbf{v}(\Lambda)$. In other words, the block error rate of the two-phase decoder equals that of the first phase. Typically, over AWGN channels, it is the decoder that decides which of the received bits to erase based on their reliabilities. The maximum number κ_{max} of erasures introduced by the decoder should be chosen to optimize the error performance of the decoding.

Example 2. As an illustration of the concepts enunciated in this section, we use the (1024,781) basic EG-LDPC code constructed in Example 1 for correcting combinations of random errors and erasures. The column weight of the parity-check matrix $\mathbf{H}(\mathcal{N},\mathcal{M})$ of this code is 33. Suppose the channel causes $\kappa = 16$ erasures whose positions are labeled by the points in Λ_1 given Example 1. Then, in the first phase of decoding, all erasures are deleted from the received sequence and the resulting vector is decoded with respect to the shortened code $\mathcal{C}_{\mathrm{EG}}(\Lambda_1^c, \Phi(\Lambda_1)^c)$ based on its parity-check matrix $\mathbf{H}_{\mathrm{EG}}(\Lambda_1^c, \Phi(\Lambda_1)^c)$. Once this phase is accomplished, the decoder retrieves all the erased bits in the second phase. In a different scenario, suppose that the channel causes $\kappa = 16$ erasures whose positions are labeled by the points in Λ_2, rather than Λ_1. Then, decoding in the first phase is performed based on the parity-check matrix $\mathbf{H}_{\mathrm{EG}}(\Lambda_2^c, \Phi(\Lambda_2)^c)$ of the punctured code $\mathcal{C}_{\mathrm{EG}}(\Lambda_2^c, \Phi(\Lambda_2)^c)$. In both scenarios, the decoder succeeds in retrieving the erased bits correctly in the second phase if it is successful in the first phase. $\triangle\triangle$

VI. Conclusion and Remarks

We have shown that basic EG-LDPC codes and their shortened codes constructed based on two-dimensional Euclidean geometries are effective in correcting combinations of errors and erasures using a two-phase decoding scheme. The basic ingredients of the approach we developed here can be applied to finite geometry LDPC codes constructed based on Euclidean geometries of dimensions higher than two and projective geometries. All these finite geometry LDPC codes have large redundant rows in their parity-check matrices. Several classes of structured LDPC codes constructed based on finite fields and combinatorial designs, [4], [9], have similar structural properties as the basic EG-LDPC codes, especially large row redundancy. These codes and their shortened codes can be used for correcting combinations of errors and erasures.

References

[1] R. G. Gallager, "Low density parity-check codes," *IRE Trans. Inf. Theory*, vol. IT-8, no. 1, pp. 21–28, Jan. 1962.

[2] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: A rediscovery and new results," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2711–2736, Nov. 2001.

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

[4] W. E. Ryan and S. Lin, *Channel Codes: Classical and Modern*. New York, NY: Cambridge Univ. Press, 2009.

[5] R. D. Carmichael, *Introduction to the Theory of Groups of Finite Orders*. New York, NY: Dover, 1956.

[6] Q. Diao, Y. Y. Tai, S. Lin, and K. Abdel-Ghaffar, "Trapping set structure of finite geometry LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Cambridge, MA, Jul. 1–6 2012, pp. 3088 –3092.

[7] T. Richardson, "Error floors of LDPC codes," in *Proc. 41st Annual Allerton Conf. Commun., Control and Comp.*, Monticello, IL, Oct. 2003, pp. 1426–1435.

[8] Q. Diao, Y. Y. Tai, S. Lin, and K. Abdel-Ghaffar, "LDPC codes on partial geometries: Trapping set structure, puncturing, and correction of combinations of errors and erasures," *IEEE Trans. Inf. Theory*, submitted, 2012.

[9] L. Zhang, Q. Huang, S. Lin, K. Abdel-Ghaffar, and I. F. Blake, "Quasi-cyclic LDPC codes: An algebraic construction, rank analysis, and codes on Latin squares," *IEEE Trans. Commun.*, vol. 58, no. 11, pp. 3126 –3139, Nov. 2010.

TABLE I
THE PARAMETERS OF THE PUNCTURED MATRICES OF THE PARITY-CHECK MATRIX $\mathbf{H}_{EG}$ OF THE BASIC (1024,781) EG-LDPC CODE AND THE CORRESPONDING EG-LDPC CODES GIVEN IN EXAMPLE 1

No. of Punctured Bits	No. of Columns	No. of Rows	Rank	EG-LDPC Codes
0	1024	1056	243	(1024,781)
4	1020	930	239	(1020,781)
8	1016	816	235	(1016,781)
12	1012	714	231	(1012,781)
16	1008	625	227	(1008,781)
32	992	347	211	(992,781)
34	990	320	209	(990,781)

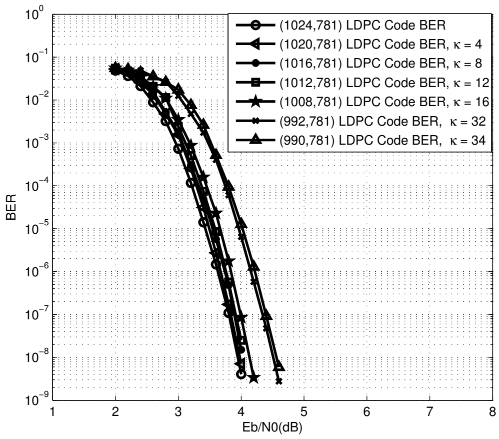

Fig. 1. The error performances of the (1024,781) basic EG-LDPC code and its punctured codes.

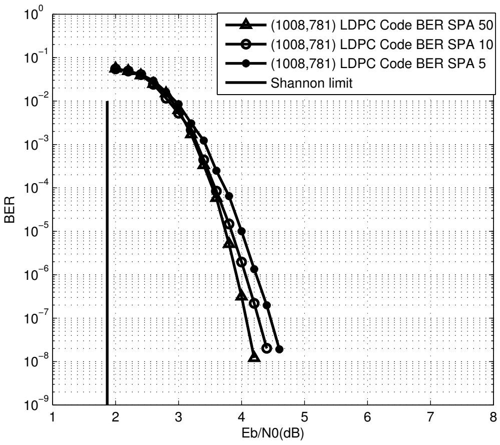

Fig. 2. The error performance of the (1008,781) punctured EG-LDPC code $\mathcal{C}_{\mathrm{EG}}(\Lambda_1^c, \Phi(\Lambda_1)^c)$ decoded with 5, 10, 50 iterations of the SPA.