Trapping Set Structure of LDPC Codes on Finite Geometries

Qiuju Diao, Ying Yu Tai, Shu Lin, Khaled Abdel-Ghaffar
Department of Electrical and Computer Engineering University of California, Davis, CA 95616, USA
Email: {qdiao, yytai, shulin, kaghaffar}@ucdavis.edu

***Abstract*—The trapping set structure of LDPC codes constructed based on finite geometries, called finite geometry (FG) LDPC codes, is analyzed using a geometric approach. In this approach, trapping sets in the Tanner graph of an FG-LDPC code are represented by subgeometries of the geometry based on which the code is constructed. Using this geometrical representation, bounds and configurations of trapping sets of an FG-LDPC code can be derived and analyzed.**

I. Introduction

LDPC codes [1] are currently the most promising coding technique to achieve the Shannon capacities for a wide range of channels. They perform very well with iterative decoding based on belief propagation. However, with iterative decoding, most LDPC codes have a common severe weakness, known as *error-floor* [2]. Error-floor may preclude LDPC codes from applications where very low error rates are required. For the AWGN channel, the error-floor is mostly caused by an undesirable structure, known as a *trapping set* [3], of the Tanner graph of the code.

A trapping set in the Tanner graph $\mathcal{G}$ of an LDPC code is a set Λ of variable-nodes (VNs) in $\mathcal{G}$ which induces a subgraph $\mathcal{G}[\Lambda]$ of $\mathcal{G}$ with check-nodes (CNs) of odd degrees [3]. The cardinality $|\Lambda|$ of Λ, is called the size of the trapping set. In the transmission of a codeword, if errors occur at the locations of the VNs of a trapping set, then there will be some parity-check failures. In this case, if an iterative algorithm is used to decode the LDPC code, the decoder must perform another decoding iteration based on the messages passed to it from the previous decoding iteration. If messages passed to the decoder contain *highly unreliable information*, the next decoding iteration is very likely to fail again and another decoding iteration is needed. As decoding iterations continue, the unreliable information passed from one decoding iteration to another may be accumulated to a degree which prevents the decoder to converge. In this case, the decoder is trapped and decoding fails. Extensive studies and simulation results show that the trapping sets that result in high decoding failure rates and contribute significantly to a high error-floor are those with small sizes which contain small numbers of odd-degree CNs in their induced subgraphs of the Tanner graph of the code.

For the AWGN channel, the error-floor of an LDPC code decoded with an iterative decoding algorithm, such as the sum-product algorithm (SPA) or the min-sum algorithm (MSA), is primarily dominated by small *harmful* trapping sets in its Tanner graph and its minimum distance. If the Tanner graph of an LDPC code has no small harmful trapping sets of sizes smaller than the minimum distance of the code, then the error-floor of the code is dominated by the minimum distance of the code. In this case, if the minimum distance of the code is relatively large, the error-floor of the code is expected to be low. To design or construct LDPC codes with larges minimum distances and no small harmful trapping sets in their Tanner graphs is, in general, combinatorially hard, but is a challenging problem.

LDPC codes constructed based on finite geometries, such as Euclidean and projective geometries, are known to have large minimum distances [4]-[7]. These codes are commonly referred to as finite geometry (FG) LDPC codes. Codes constructed based on Euclidean geometries are called EG-LDPC codes and the codes constructed based on projective geometries are called PG-LDPC codes. It was proved in [8] that the Tanner graph of a PG-LDPC code contains no small trapping sets with sizes smaller than its minimum distance. In two recent papers [9], [10], we proved that the Tanner graph of an EG-LDPC code contains no small trapping sets with sizes smaller than its minimum distance. Since the Tanner graphs of both EG- and PG-LDPC codes contain no small trapping sets with sizes smaller than their minimum distance, their error-floors are primarily dominated by their minimum distances. Since their minimum distances are relatively large, their error-floors are expected to be very low.

In this paper, we analyze the general trapping set structure of FG-LDPC codes using a *geometric approach*. In this approach, trapping sets in the Tanner graph of an FG-LDPC code are represented by subgeometries of the geometry based on which the code is constructed. Using this geometrical representation, the size and configuration of a trapping set of a given size can be analyzed and determinced.

The rest of this paper is organized as follows. Section II gives relevant definitions and concepts of trapping sets of an LDPC codes. Section III gives a brief introduction of finite geometries and develops some structural properties that are pertinent for analyzing the general trapping set structures of FG-LDPC codes. In Sections IV and V, we consider specifically the trapping set structures of EG- and PG-LDPC codes. Section VI concludes the paper with some remarks.

II. Trapping Sets: Definitions and Concepts

As pointed out in the introduction, the performances of iterative decoding of most LDPC codes suffer from error-floors, which are mainly caused by harmful small trapping sets in the Tanner graph of the parity-check matrix based on which the decoding is carried out. In this section, we briefly review the relevant definitions and concepts of trapping sets of an LDPC code.

First, we define trapping sets and some subclasses of harmful trapping sets and follow this with a motivation of these definitions.

Definition 1. Let $\mathcal{G}$ be the Tanner graph of a binary LDPC code $\mathcal{C}$ given by the null space of an $m \times n$ matrix $\mathbf{H}$ over GF(2). For $1 \leq \kappa \leq n$ and $0 \leq \tau \leq m$, we have following definitions [3],[8],[11]:

1) A (κ, τ) *trapping set* is a set,Λ, of κ VNs in $\mathcal{G}$ which induces a subgraph, denoted by $\mathcal{G}[\Lambda]$, of $\mathcal{G}$ with exactly τ odd-degree CNs and an arbitrary number of even-degree CNs.
2) A (κ, τ) trapping set is *elementary* if all the CNs in the induced subgraph $\mathcal{G}[\Lambda]$ have degree one or degree two, and there are exactly τ degree-one CNs.
3) A (κ, τ) trapping set is small if $\kappa \leq \sqrt{n}$ and $\frac{\tau}{\kappa} \leq 4$.
4) A (κ, τ) trapping set is *absorbing* if every VN in the trapping set is connected in $\mathcal{G}[\Lambda]$ to fewer CNs of odd degree than CNs of even degree. If in addition, every VN not in the trapping set is connected to fewer CNs of odd degree in $\mathcal{G}[\Lambda]$ than other CNs, i.e., CNs not in $\mathcal{G}[\Lambda]$ or in $\mathcal{G}[\Lambda]$ but of even degree, then the trapping set is *fully absorbing*[11].

Suppose, in transmission of a codeword in $\mathcal{C}$, an error pattern **e** with κ errors at the locations of the κ VNs of a (κ, τ) trapping set occurs. This error pattern will cause τ parity-check failures. In this case, for iterative decoding, another decoding iteration must be carried out to correct the failed check-sums. Iterative decoding, such as the SPA and MSA, is very *susceptible* to trapping sets of a code because it works locally in a distributed-processing manner. Each CN has a local processor unit to process the messages received from the VNs connected to it and each VN has a local processor unit to process the messages received from the CNs connected to it. Hopefully, these local processor units through iterations and message exchanges collect enough information to make a global optimum decision of the transmitted code bits.

In each decoding iteration, we call a CN a *satisfied* CN if it satisfies its corresponding check-sum constraint (i.e., its corresponding check-sum is equal to zero), otherwise, we call it an *unsatisfied* CN. During the decoding process, the decoder undergoes *state transitions* from one state to another until all the CNs satisfy their corresponding check-sum constraints or a predetermined maximum number of iterations is reached. The i-th state of an iterative decoder is represented by the hard-decision decoded sequence obtained at the end of the i-th iteration. In the process of a decoding iteration, the messages from the satisfied CNs try to *reinforce* the current decoder state, while the messages from the unsatisfied CNs try to *change* some of the bit decisions to satisfy their check-sum constraints. If errors affect the κ code bits (or the κ VNs) of a (κ, τ) trapping set Λ, the τ odd-degree CNs, each connected to an odd number of VNs in Λ, will not be satisfied while all other CNs will be satisfied. The decoder will succeed in correcting the errors in Λ if the messages coming from the unsatisfied CNs connected to the VNs in Λ are strong enough to overcome the messages coming from the satisfied CNs. However, this may not be the case if τ is small. As a result, the decoder may not converge to a valid codeword even if more decoding iterations are performed and this non-convergence of decoding results in an error-floor. In this case, the decoder is said to be trapped.

For the AWGN channel, error patterns with small number of errors are more probable to occur than error patterns with larger number of errors. Consequently, in message-passing decoding algorithms, the most harmful (κ, τ) trapping sets are usually those with small values of κ and τ. Extensive studies and simulation results show that the trapping sets that result in high decoding failure rates and contribute significantly to high error-floors are those with small values κ and small ratios $\frac{\tau}{\kappa}$ (especial $\frac{\tau}{\kappa} \leq 1$). These conclusions are captured by the notions of elementary trapping sets and small trapping sets, see Definition 1, parts 2) and 3). In general, trapping sets for which τ is relatively large compared to κ result in relatively small decoding failure rates and contribute little to error-floor.

The notion of absorbing sets is motivated by the fact that for the *binary symmetric channel* (BSC), if the channel causes errors in the VNs of an absorbing set, then a Gallager type-B decoder [1] (or a one-step majority-logic [12] decoder) will fail. With soft-decision iterative decoding, such as the SPA or the MSA, if most of the soft messages become saturated, i.e., their magnitudes are clipped to some finite values to avoid numerical overflow [13] (which is usually true in the error-floor region), then the decoder will behave like a Gallager type-B decoder and will fail.

As all check-sums of a codeword in the code are satisfied, the positions of the nonzero bits in a codeword forms a $(\kappa, 0)$ trapping set, where κ is the weight of the codeword. If an error pattern determined by these positions occurs, the decoder converges to an incorrect codeword and commits an undetected error. In this case, the decoder is permanently trapped. If there are no harmful trapping sets of sizes smaller than the minimum distance of an LDPC code, then the error-floor of the code decoded with iterative decoding is primarily dominated by the minimum distance. If the minimum distance of the code is large enough, its error-floor will be low. LDPC codes constructed from finite geometries, such as Euclidean and projective geometries, are classes of such codes.

III. Finite Geometries and Finite Geometry LDPC Codes

First, we give a brief discussion of finite geometries that include both Euclidean and projective geometries as subclasses. We develop some of the structural properties of finite geometries which are pertinent for constructing LDPC codes and analyzing their trapping set structures. Excellent presentation and coverage of finite geometries can be found in

[14]-[17], especially [17] which is an outstanding introductory book to finite geometries in general form).

Consider the finite geometry, **FG**, consisting of a set, $\mathcal{N}$, of n points and a set, $\mathcal{M}$, of m lines, where each line is a nonempty set of q points. If a line $\mathcal{L}$ contains a point $\mathbf{a}$, we say that $\mathbf{a}$ is on $\mathcal{L}$ and that $\mathcal{L}$ passes through $\mathbf{a}$. We require that any two distinct points are on exactly one line. For every point $\mathbf{a}$ in **FG**, there are exactly γ lines 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 **FG** 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 n points of **FG** are on the intersecting lines in $\Delta(\mathbf{a})$. Two intersecting bundles $\Delta(\mathbf{a})$ and $\Delta(\mathbf{b})$ at two distinct points $\mathbf{a}$ and $\mathbf{b}$ have one and only one line in common, namely the line connecting the two points $\mathbf{a}$ and $\mathbf{b}$. Let Λ be a set of points in **FG**. Then

$$\Phi(\Lambda) = \bigcup_{\mathbf{a}\in\Lambda} \Delta(\mathbf{a}) \tag{1}$$

is the union of intersecting bundles at points in Λ, i.e., $\Phi(\Lambda)$ is the set of lines in **FG** such that each line passes through *at least one point* in Λ.

For a set $\Lambda \subsetneqq \mathcal{N}$ of points and a line $\mathcal{L} \in \mathcal{M}$ in **FG**, the *restriction* of $\mathcal{L}$ to Λ is $\mathcal{L} \bigcap \Lambda$ consisting of the points in Λ that are on $\mathcal{L}$. The subgeometry induced by Λ in **FG**, denoted by **FG**$[\Lambda]$, consists of Λ as the set of its points and the restrictions of the lines in $\mathcal{L} \in \Phi(\Lambda)$ as its lines. Notice that the subgeometry **FG**$[\Lambda]$ has $|\Lambda|$ points and $|\Phi(\Lambda)|$ lines. Any two points in **FG**$[\Lambda]$ are on a unique line.

A matrix, $\mathbf{H}_{FG}$, can be constructed from the finite geometry **FG** as follows. The rows of $\mathbf{H}_{FG}$ are labeled by the m lines and the columns are labeled by the n points. The entry at the column labeled by a point $\mathbf{a}$ and the row labeled by a line $\mathcal{L}$ is 1 if and only if $\mathcal{L}$ passes through $\mathbf{a}$. The matrix $\mathbf{H}_{FG}$ is the incidence matrix of **FG** and each row is the incidence vector of the line labeling that row. It follows that the matrix $\mathbf{H}_{FG}$ has m rows and n columns with constant column weight γ and constant row weight q. If γ is small compared to m, then $\mathbf{H}_{FG}$ is a sparse matrix. In this case, the null space of $\mathbf{H}_{FG}$ gives a (γ, q)-regular FG-LDPC code, $\mathcal{C}_{FG}$, of length n. Since any two distinct points in **FG** are connected by a unique line, for any two distinct columns of $\mathbf{H}_{FG}$ there is exactly one row that has ones in the two columns. This implies that no two rows (or two columns) in $\mathbf{H}_{FG}$ have more than one place where they both have non-zero components. This structural property of $\mathbf{H}_{FG}$ is referred to as the *row-column (RC)-constraint*. [5], [12]. The RC-constraint on $\mathbf{H}_{FG}$ ensures that the minimum distance $\mathcal{C}_{FG}$ is at least $\gamma+1$ and the girth of its Tanner graph is 6 [5]. The matrix $\mathbf{H}_{FG}$ is then a parity-check matrix for $\mathcal{C}_{FG}$ which is called the *basic* FG-LDPC code.

The Tanner graph, $\mathcal{G}_{FG}$, associated with the matrix $\mathbf{H}_{FG}$ is a bipartite graph composed of two sets of nodes, the set of variable nodes (VNs) labeled by the points in **FG** or, equivalently, the columns of $\mathbf{H}_{FG}$, and the set of check nodes (CNs) labeled by the lines in **FG** or, equivalently, the rows of $\mathbf{H}_{FG}$. Edges in $\mathcal{G}_{FG}$ connect only VNs to CNs. The VN labeled by a point $\mathbf{a}$ is connected to the CN labeled by a line $\mathcal{L}$ by an edge if and only if $\mathcal{L}$ passes through $\mathbf{a}$, i.e., if and only if the entry in $\mathbf{H}_{FG}$ at the corresponding row and column is one. In this case, we say that this VN and this CN are adjacent. Hence, $\mathcal{G}_{FG}$ is a bipartite graph that has n VNs, m CNs, and each VN has degree γ. Furthermore, any two distinct VNs are connected to exactly one CN as any two points in **FG** are connected by a unique line. This implies that the girth of $\mathcal{G}_{FG}$, which is the shortest length of a cycle in the bipartite graph, is six. The Tanner graph $\mathcal{G}_{EG}$ is a graphical representation of the finite geometry **FG**.

If Λ is a set of points in the finite geometry **FG**, then the VNs in $\mathcal{G}_{FG}$ labeled by the points in Λ are adjacent to the CNs labeled by the lines in $\Phi(\Lambda)$. The pair $(\Lambda, \Phi(\Lambda))$ forms a subgraph of the Tanner graph $\mathcal{G}_{FG}$, which is denoted by $\mathcal{G}_{FG}[\Lambda]$. We say that the subgraph $\mathcal{G}_{FG}[\Lambda]$ is induced by the set Λ. This subgraph is the graphical representation of the subgeometry **FG**$[\Lambda]$ of **FG** induced by Λ. This subgraph has $|\Lambda|$ VNs and $|\Phi(\Lambda)|$ CNs.

Let *rank*$(\mathbf{H}_{FG})$ denote the rank of $\mathbf{H}_{FG}$. If $m > rank(\mathbf{H}_{FG})$, then $\mathbf{H}_{FG}$ has $m-rank(\mathbf{H}_{FG})$ redundant rows. We define the ratio $\xi_{EG} = (m - rank(\mathbf{H}_{FG}))/m$ as the *row-redundancy* of the parity-check matrix $\mathbf{H}_{FG}$. In general, the parity-check matrix of an FG-LDPC code has a large row-redundancy (i.e., a large number of redundant rows), particularly the parity-check matrices of EG- and PG-LDPC codes). Many studies and simulation results show that row-redundancy of a parity-check matrix helps the decoding of an LDPC code to converge fast and also pushes the error-floor of the code down.

IV. Trapping Set Structure of FG-LDPC Codes

A. Geometrical Interpretation of a Trapping Set

The Tanner graph $\mathcal{G}_{FG}$ associated with **FG**, as described in Section III, consists of n VNs and m CNs. Each VN has degree γ and any two VNs are adjacent to a unique CN. A (κ, τ) trapping set in $\mathcal{G}_{FG}$ is defined by the subgraph $\mathcal{G}_{FG}[\Lambda]$ of $\mathcal{G}_{FG}$ induced by a set Λ of κ VNs that has exactly τ odd-degree CNs. The κ VNs in this induced subgraph $\mathcal{G}_{FG}[\Lambda]$ are labeled by κ points in **FG**. The CNs adjacent to the κ VNs in the induced subgraph $\mathcal{G}_{FG}[\Lambda]$ are labeled by the lines in **FG** that pass through at least one of the κ points labeling the VNs. The subgraph $\mathcal{G}_{FG}[\Lambda]$ of the Tanner graph $\mathcal{G}_{FG}$ has exactly τ CNs of odd degree if and only if there are exactly τ lines, each passing through an odd number of the κ points in Λ. These points and the lines that pass through them form a subgeometry **FG**$[\Lambda]$ of **FG**. Therefore, a (κ, τ) trapping set can be represented by a subgeometry of **FG** induced by κ points such that this subgeometry has exactly τ lines, each passing through an odd number of the points in Λ. With this interpretation of a trapping set from a geometrical point of view, we can analyze the trapping set structure of the Tanner graph of a basic FG-LDPC code based on the structure of points and lines in the finite geometry **FG**.

B. General Bounds on Trapping Sets of Basic EG-LDPC Codes

Let Λ be a set of κ points whose corresponding VNs induce a (κ, τ) trapping set. Recall that $\Phi(\Lambda)$ (defined by (1)) is the set of lines in **FG**, each passing through at least one point in Λ. Then, Λ induces a subgeometry **FG**$[\Lambda]$ in **FG** whose lines are obtained by restricting the lines in $\Phi(\Lambda)$ to the set Λ. Among the $|\Phi(\Lambda)|$ lines in **FG**$[\Lambda]$, there are exactly τ lines, each passing through an odd number of points in Λ. Hence, if m_i is the number of lines **FG**$[\Lambda]$, or equivalently in $\Phi(\Lambda)$, each passing through exactly i points in Λ, where $1 \leq i \leq \kappa$, then τ is the sum of m_i over all odd integers i such that $1 \leq i \leq \kappa$. Since $2\lfloor(\kappa+1)/2\rfloor - 1$ is the largest odd integer not exceeding κ, we have

$$\tau = m_1 + m_3 + m_5 + \ldots + m_{2\lfloor(\kappa+1)/2\rfloor-1}. \qquad (2)$$

Since the minimum distance of the basic FG-LDPC code $\mathcal{C}_{FG}$ is lower bounded by $\gamma+1$, we are only concerned with trapping sets with sizes smaller than $\gamma+1$. Let $\mathbf{a}$ be a point in Λ and $\mathcal{L}$ be a line in $\Phi(\Lambda)$ passing through $\mathbf{a}$. The pair $(\mathbf{a}, \mathcal{L})$ is called a *point-line pair* in the subgeometry **FG**$[\Lambda]$ $= (\Lambda, \Phi(\Lambda))$. Such a point-line pair in $(\Lambda, \Phi(\Lambda))$ represents a pair of adjacent VN and CN in the trapping set $\mathcal{T}(\kappa, \tau)$. There are two ways of counting the total number of such point-line pairs. Since each line in $\Phi(\Lambda)$ containing i points in Λ gives i point-line pairs in $(\Lambda, \Phi(\Lambda))$, the total number of point-line pairs in $(\Lambda, \Phi(\Lambda))$ is $m_1 + 2m_2 + \ldots + \kappa m_\kappa$. Since each of the κ points in Λ is intersected by γ lines, the total number of point-line pairs in $(\Lambda, \Phi(\Lambda))$ is also equal to $\kappa\gamma$. Based on the above two ways of counting of the total number of point-line pairs in $(\Lambda, \Phi(\Lambda))$, we have the following equality:

$$m_1 + 2m_2 + \ldots + \kappa m_\kappa = \kappa\gamma. \qquad (3)$$

Next, we count the number of pairs of points in Λ. Since Λ consists of κ points, there are $\binom{\kappa}{2}$ pairs of points in Λ. 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, then we must have the following equality:

$$\binom{2}{2}m_2 + \binom{3}{2}m_3 + \cdots + \binom{\kappa}{2}m_\kappa = \binom{\kappa}{2}. \qquad (4)$$

Multiplying both sides in (4) by 2 and subtracting them from the corresponding sides in (3), we have

$$m_1 - \sum_{i=3}^{\kappa} i(i-2)m_i = \kappa\gamma - \kappa(\kappa-1). \qquad (5)$$

With some algebraic manipulations of (5), we obtain the following expression for the number of lines in $\Phi(\Lambda)$, each containing an odd number of points in Λ:

$$\begin{aligned} \tau &= \sum_{i=1,3,5} m_i \\ &= (\gamma+1-\kappa)\kappa + \sum_{i=3,5\ldots}(i-1)^2 m_i + \sum_{i=4,6\ldots} i(i-2)m_i. \end{aligned} \qquad (6)$$

If we know the distribution of the points in Λ over the lines in $\Phi(\Lambda)$, τ can be enumerated using (5). In fact, we can even determine the configuration the trapping set corresponding to the subgeometry $(\Lambda, \Phi(\Lambda))$. By configuration, we mean the degree distributions of the VNs and CNs of the trapping set.

Since the two sums in the right side of (6) are non-negative, we have the following lower bound on the number τ of odd-degree CNs in a (κ, τ) trapping set of the Tanner graph $\mathcal{G}_{FG}$ of the basic FG-LDPC code $\mathcal{C}_{FG}$:

$$\tau \geq (\gamma+1-\kappa)\kappa. \qquad (7)$$

For $\kappa < \gamma$, τ can be many times larger than κ. It follows from Definition 1 part 3 that the Tanner graph $\mathcal{G}_{FG}$ of the FG-LDPC code $\mathcal{C}_{FG}$ contains no small trapping set with size $\kappa < \gamma - 3$. For $\kappa < \gamma - 3$, τ is at least 5 times larger than κ, i.e., $\frac{\tau}{\kappa} \geq 5$. Recall that the minimum distance of the FG-LDPC code $\mathcal{C}_{FG}$ is at least $\gamma + 1$. The above says that the Tanner graph $\mathcal{G}_{FG}$ of an FG-LDPC code $\mathcal{C}_{EG}$ contains no small trapping set with size κ less than the lower bound on the minimum distance of $\mathcal{C}_{EG}$ minus 3.

If $1 \leq \kappa \leq \gamma$, then $(\gamma+1-\kappa)\kappa \geq \gamma$. This follows from the fact that $(\gamma+1-\kappa)\kappa$ is a *concave function* in κ which equals γ for $\kappa = 1$ and γ. We conclude that the number of CNs of odd degree in any trapping set of size at most γ is at least γ. Since the ratio of the number of CNs of odd degree to the number κ of VNs is at least $\gamma+1-\kappa$, it follows, from Definition 1 part 3, that the Tanner graph $\mathcal{G}_{FG}$ associated with the parity-check matrix $\mathbf{H}_{FG}$ contains no small trapping set of size $\kappa \leq \gamma - 4$ as $\frac{\tau}{\kappa} \geq \gamma + 1 - \kappa > 4$ in this case.

Equality holds in (7) if and only if $m_3 = m_4 = \ldots = m_\kappa = 0$, i.e., each line in $\Phi(\Lambda)$ passes through at most two points in Λ. This is the same as saying that no three points in Λ are collinear [17]. In this case, we say that the points in Λ have a *uniform pair-wise distribution*. If this condition holds and $\kappa \leq \gamma$, then Λ forms a $(\kappa, (\gamma+1-\kappa)\kappa)$ elementary trapping set. Any other distribution of points will result in a trapping set with a larger number of CNs of odd degrees. From (4), we find that the number of degree-2 CNs is equal to $\kappa(\kappa-1)/2$. Therefore, a trapping set of size $\kappa \leq \gamma$ in the Tanner graph $\mathcal{G}_{FG}$ of a basic FG-LDPC code for which the κ point-VNs has a uniform pair-wise distribution induces a subgraph $\mathcal{G}_{FG}[\Lambda]$ with $(\gamma+1-\kappa)\kappa$ CNs of degree-1 and $\kappa(\kappa-1)/2$ CNs of degree-2. It can be readily shown that for $\kappa < \lfloor(2\gamma+3)/3\rfloor$, the number of CNs of degree-1 is greater than the number of CNs of degree-2. Any distribution of points in Λ other than the uniform pair-wise distribution will result in a trapping set with a larger number of CNs of odd degrees.

As another special case, we consider the extreme opposite case in which all the points in Λ are collinear. Then, $m_2 = m_3 = \ldots = m_{\kappa-1} = 0$ and $m_\kappa = 1$. Substituting in (3), it follows that $m_1 = (\gamma-1)\kappa$, i.e., the trapping set has $(\gamma-1)\kappa$ CNs of degree 1 in addition to a CN of degree κ. Hence, Λ forms a $(\kappa, (\gamma-1)\kappa)$ trapping set if κ is even and a $(\kappa, (\gamma-1)\kappa+1)$ trapping set if κ is odd. Typically, such trapping sets do not trap the iterative decoder since they have large numbers of CNs of odd degree.

Next we show that the Tanner graph $\mathcal{G}_{FG}$ does not have an absorbing trapping set of size $\kappa \leq \lfloor\gamma/2\rfloor + 1$. To prove this, we use the intersecting structure that each point a in the finite geometry **FG** is intersected by γ lines. Let $\mathbf{a}$ be a point in a set Λ of κ points in **FG**. Any point in Λ other than $\mathbf{a}$ is on a unique line passing through $\mathbf{a}$. Hence, there are at most $\kappa - 1$ lines, each passing through $\mathbf{a}$ and a point in Λ other than $\mathbf{a}$. Since there are in total γ lines passing through $\mathbf{a}$, there are at least $\gamma - (\kappa - 1)$ of them that do not pass through any point in Λ other than $\mathbf{a}$. This implies that the VN corresponding to $\mathbf{a}$ in the Tanner graph $\mathcal{G}_{FG}$ is connected to at least $\gamma - (\kappa - 1)$ CNs in the induced graph $\mathcal{G}_{FG}[\Lambda]$ of degree one, which is odd. In particular, if $\kappa \leq \lfloor\gamma/2\rfloor + 1$, then, in $\mathcal{G}_{FG}[\Lambda]$, the number of CNs of odd degree connected to the VN labeled by $\mathbf{a}$ is at least equal to the number of CNs of even degree connected to it. This implies that the Tanner graph $\mathcal{G}_{FG}$ does not contain any absorbing set of size less than or equal to $\lfloor\gamma/2\rfloor + 1$. We readily see that the smallest size of an absorbing set in $\mathcal{G}_{EG}$ is $\lfloor\gamma/2\rfloor + 2$.

V. Applications to Euclidean Geometries

In last section, we have developed the trapping set structure of LDPC codes constructed using finite geometries defined in a general manner. General finite geometries contain Euclidean and projective geometries as special subclasses. Consequently, the results on trapping set structure developed in Section III apply for LDPC codes constructed using these two special subclasses of finite geometries. In this section, we focus only on a special subclass of Euclidean geometries.

A. Two-Dimensional Euclidean Geometries

A two-dimensional Euclidean geometry $\text{EG}(2, q)$ over $\text{GF}(q)$ consists of q^2 points and $q^2 + q$ lines [14], [15]. Each line consists of q points. Two lines are either parallel or they intersect at one and only one point. For every point $\mathbf{a}$ in $\text{EG}(2, q)$, there are $q + 1$ lines intersecting at it. For every line in $\text{EG}(2, q)$, there are $q - 1$ lines parallel to it. These q parallel lines form a parallel bundle. The $q^2 + q$ lines can be partitioned into $q + 1$ parallel bundles. The field $\text{GF}(q^2)$ is a realization of the geometry $\text{EG}(2, q)$. Let α be a primitive element of $\text{GF}(q^2)$. Then, the elements, $\alpha^{-\infty} = 0$, $\alpha^0 = 1$, α,…, α^{q^2-2}, represent the q^2 points of $\text{EG}(2, q)$ where $\alpha^{-\infty}$ represents the origin of $\text{EG}(2, q)$.

B. Basic EG-LDPC Code and Its Trapping Set Structure

Let $\mathcal{G}_{EG}$ be the Tanner graph of $\text{EG}(2, q)$ and let $\mathbf{H}_{EG}$ be the incidence matrix of $\mathcal{G}_{EG}$. $\mathbf{H}_{EG}$ is a $(q^2 + q) \times q^2$ matrix over $\text{GF}(2)$ with column and row weights $q + 1$ and q, respectively. We can arrange columns and row of $\mathbf{H}_{EG}$ as follows. The first column of $\mathbf{H}_{EG}$ correspond to the origin point $\alpha^{-\infty}$ of $\text{EG}(2, q)$ and other $q^2 - 1$ columns correspond to the non-origin points, $\alpha^0 = 1$, α, …, α^{q^2-2}. The first $q+1$ rows correspond to the lines of $\text{EG}(2, q)$ that intersecting at the origin point $\alpha^{-\infty}$ and other $q^2 - 1$ rows correspond to the line in $\text{EG}(2, q)$ not containing the origin point. The null space of $\mathbf{H}_{EG}$ gives an extended cyclic EG-LDPC code $\mathcal{C}_{EG}$, called a basic EG-LDPC code, of length $n = q^2$ and minimum distance at least $q + 2$. In extended cyclic form, encoding of $\mathcal{C}_{EG}$ can be implemented with a simple feedback shift-register with modulo-2 adder to form the overall parity check symbol.

With n, m, and γ replaced by q^2, $q^2 + q$ and $q + 1$. Then, it follows from (6) and (7) that for $1 \leq \kappa \leq q + 1$, the number τ of odd-degree CNs in any (κ, τ) trapping satisfies the following equality and bound:

$$\begin{aligned}\tau &= \sum_{i=1,3,5} m_i \\ &= (q + 2 - \kappa)\kappa + \sum_{i=3,5\ldots} (i-1)^2 m_i + \sum_{i=4,6\ldots} i(i-2) m_i.\end{aligned} \tag{8}$$

$$\tau \geq (q + 2 - \kappa)\kappa. \tag{9}$$

Consider the special case for which $q = 2^s$, the rank of the parity-check matrix $\mathbf{H}_{EG}$ of the basic EG-LDPC code $\mathcal{C}_{EG}$ is 3^s [5], [12]. Then the basic EG-EDPC code $\mathcal{C}_{EG}$ has the following parameters: 1) length $n = 4^s$; 2) dimension $k = 4^s - 3^s$; 3) minimum distance $d_{min} = 2^s + 2$; and 4) number of redundant rows $\delta = 4^s - 3^s + 2^s$. The Tanner graph $\mathcal{G}_{EG}$ of the EG-LDPC code $\mathcal{C}_{EG}$ has no small trapping set with size $\kappa < 2^s - 2$ (Definition 1, part 3) and no absorbing set of size smaller than or equal to $2^{s-1} + 1$. Notice that the parity-check matrix $\mathbf{H}_{EG}$ has large number of redundant row. This large row redundancy of the parity-check matrix $\mathbf{H}_{EG}$ not only helps to lower the error-floor of the code but also makes the decoding of the code to converge fast.

C. An Improve Bound on the Trapping Sets of the Basic EG-LDPC Codes

In the following, we show that the bound given by (9) can be improved by considering the detailed structure of the geometry $\text{EG}(2, q)$ and the configuration of lines passing through the points corresponding to the trapping set. The approach is based on the lines of a parallel bundle passing through the points labeling the VNs of a trapping set. Based on the geometrical interpretation presented above, to characterize the subgraph induced by a trapping set of κ VNs, labeled α^{j_1} , α^{j_2}, …, α^{j_κ}, in the Tanner graph of an EG-LDPC code, we consider the set $\Lambda = \{\alpha^{j_1}, \alpha^{j_2}, \ldots, \alpha^{j_\kappa}\}$ of κ points in $\text{EG}(2, q)$ and the set of lines, $\Phi(\Lambda)$, that pass through the points in Λ. Notice that the set of lines passing through α^{j_l}, for $1 \leq l \leq \kappa$, is the intersecting bundle at $\Delta(\alpha^{j_l})$ at α^{j_l}. Hence, $\Phi(\Lambda) = \Delta(\alpha^{j_1}) \bigcup \Delta(\alpha^{j_2}) \bigcup \ldots \bigcup \Delta(\alpha^{j_\kappa})$. A CN of degree 1 corresponds to a line passing through one and only one point in Λ, i.e., the line belongs to one and only one of the intersecting bundles $\Delta(\alpha^{j_1})$, $\Delta(\alpha^{j_1})$, …, $\Delta(\alpha^{j_\kappa})$. In the following, we lower bound the number of such lines.

Recall that each parallel bundle, of q lines, contains all the points in $\text{EG}(2, q)$ and, in particular, all the points in $\Lambda = \{\alpha^{j_1}, \alpha^{j_2}, \ldots, \alpha^{j_\kappa}\}$. Let $\mathcal{P}$ be a parallel bundle of lines and $\mathcal{L}_{i_1}$,$\mathcal{L}_{i_2}$, …,$\mathcal{L}_{i_b}$ be the lines in $\mathcal{P}$, each passing through at least one point in Λ. We call these b lines center lines. Thus, in total we have b center lines and all other lines in $\Phi(\Lambda)$

are non-center lines. For $1 \leq l \leq b$, let Λ_l be the set of points in Λ that are on the center line $\mathcal{L}_{i_l}$ and let κ_l be the number of such points. Since the center lines $\mathcal{L}_{i_1}$,$\mathcal{L}_{i_2}$, ...,$\mathcal{L}_{i_b}$ are parallel, each point in Λ is on one and only one of these lines. Hence, Λ_1, Λ_2, ..., Λ_b are disjoint sets whose union is Λ and $\kappa_1 + \kappa_2 + \ldots + \kappa_b = \kappa$. We denote by $m_1^{'}$ the number of center lines $\mathcal{L}_{i_l}$, $1 \leq l \leq b$, for which $\kappa_l = 1$, i.e., $m_1^{'} = |\{l : 1 \leq l \leq b, \kappa_l = 1\}|$. For $1 \leq i \leq \kappa$, let $m_i^{''}$ denote the number of non-center lines, each passing through i points in Λ. Since any two points in κ_l are connected by a center line, they cannot be on the same non-center line. Hence, the points on any non-center line belong to different sets Λ_1, Λ_2, ..., Λ_b. This implies that

$$m_i^{''} = 0 \text{ for } i > b. \tag{10}$$

We are interested in lower bounding $m_1 = m_1^{'} + m_1^{''}$, the total number of lines in $\Phi(\Lambda)$ that pass through exactly one point in Λ.

Since each of the κ points in Λ is on $q+1$ lines, including the center line, each point is on exactly q non-center lines. Hence, by counting, in two different ways, the number of point-line pairs consisting of a point in Λ and a non-center line in $\Phi(\Lambda)$ passing through the point, we obtain

$$m_1^{''} + 2m_2^{''} + \ldots + bm_b^{''} = q\kappa. \tag{11}$$

For $1 \leq r < t \leq b$, there are $\kappa_r\kappa_t$ pairs of points, one belonging to Λ_r and the other to Λ_t. Hence, the number of pairs of points in Λ that do not belong to the same set Λ_l for $1 \leq l \leq b$, is given by

$$\begin{aligned} \rho &= \sum_{1 \leq r < t \leq b} \kappa_r\kappa_t \\ &= \frac{(\sum_{l=1}^{b} \kappa_l)^2 - \sum_{l=1}^{b} \kappa_l^2}{2} \\ &= \frac{\kappa^2 - \sum_{l=1}^{b} \kappa_l^2}{2}. \end{aligned} \tag{12}$$

Since the two points in every such pair are connected by a non-center line, and a non-center line passing through i points in Λ connects $\binom{i}{2}$ such pairs, we have

$$\binom{2}{2} m_2^{''} + \binom{3}{2} m_3^{''} + \ldots + \binom{b}{2} m_b^{''} = \rho. \tag{13}$$

From (11) and (13) and following the same argument leading to (6), we obtain

$$m_1^{''} \geq q\kappa - 2\rho = q\kappa - \kappa^2 + \sum_{l=1}^{b} \kappa_l^2. \tag{14}$$

Since the number of lines in $\Phi(\Lambda)$ passing through a single point in Λ is $m_1 = m_1^{'} + m_1^{''}$, which is a lower bound on the number τ of odd-degree CNs in $\mathcal{G}[\Lambda]$, we obtain

$$\tau \geq m_1 \geq q\kappa - \kappa^2 + \sum_{l=1}^{b} \kappa_l^2 + |\{l : 1 \leq l \leq b, \kappa_l = 1\}|. \tag{15}$$

This gives a lower bound on the number of CNs of odd degree and in particular, degree one in a trapping set of size κ. We notice that this lower bound agrees with the lower bound in (9) whenever $\kappa_l \leq 2$ for all $1 \leq l \leq b$ and improves upon it in all other cases.

Inequality (14) can be applied easily once the points in the geometry corresponding to the VNs of the trapping set are given. The inequality depends on the numbers κ_1, κ_2, ..., κ_b, which in turn depend on the set Λ of points as well as on the choice of the parallel bundle $\mathcal{P}$. For example, if each point is represented by a two-tuple (a_0, a_1) over GF(q), then $\{(a_0, a_1) : a_0 \in GF(q)\}$ for some $a_1 \in GF(q)$ is a line associated with this value of a_1. The q lines associated with the q values of $a_1 \in GF(q)$ form a parallel bundle. (This parallel bundle can be viewed as the set of the q horizontal lines in a two-dimensional plane where each point in the Euclidean geometry is represented by its cartesian coordinates.) The number of points in Λ on the line associated with a_1 is the number of points $(a_0, a_1) \in \Lambda$. From this, it is easy to compute κ_1, κ_2, ..., κ_b which can be used in (15) to obtain a lower bound on the number of CNs of degree one in the trapping set.

D. Trapping Set Structure of Other EG-LDPC Codes

If we delete the first column of the parity-check matrix $\mathbf{H}_{EG}$ in extended cyclic form, we obtain a $(q^2+q) \times (q^2-1)$ matrix $\mathbf{H}_{EG,cyc,0}$ in cyclic form for which the cyclic shift of a row in $\mathbf{H}_{EG,cyc,0}$ one place to the right is another row in $\mathbf{H}_{EG,cyc,0}$. The columns of $\mathbf{H}_{EG,cyc,0}$ correspond to the non-origin points of EG$(2, q)$. $\mathbf{H}_{EG,cyc,0}$ has constant column weight $q + 1$ but two different row weights, $q - 1$ and q. The rows with weight $q - 1$ correspond to the $q + 1$ lines in EG$(2, q)$ that intersect at the origin. The null space of $\mathbf{H}_{EG,cyc,0}$ gives a cyclic EG-LDPC code $\mathcal{C}_{EG,cyc,0}$, called a type-0 cyclic EG-LDPC code, of length $n = q^2 - 1$ and minimum distance at least $q + 2$.

The Tanner graph of $\mathbf{H}_{EG,cyc,0}$, denoted by $\mathcal{G}_{EG,cyc,0}$, is a subgraph of the Tanner graph $\mathcal{G}_{EG}$ of the basic EG-LDPC code $\mathcal{C}_{EG}$ with the removal of the VN corresponding the origin point $\alpha^{-\infty}$ of EG$(2, q)$ and the $q + 1$ edges connecting to it. Hence $\mathbf{H}_{EG,cyc,0}$ is an incidence matrix of the subgraph $\mathcal{G}_{EG,cyc,0}$ of $\mathcal{G}_{EG}$. For $1 \leq \kappa \leq q + 1$, the number τ of odd-degree CNs in a (κ, τ) trapping set of the Tanner graph of $\mathcal{C}_{EG,cyc,0}$ satisfies both the equality given (8) and the bound given by (9). Its Tanner graph $\mathcal{G}_{EG,cyc,0}$ contains no small trapping set with size $\kappa < q - 2$.

If we remove the first column and the first $q + 1$ rows from the parity-check matrix $\mathbf{H}_{EG}$ of the basic EG-LDPC code $\mathcal{C}_{EG}$, we obtain a $(q^2 - 1) \times (q^2 - 1)$ matrix $\mathbf{H}_{EG,cyc,1}$ which is a circulant with both column and row weights equal to q. The null space of $\mathbf{H}_{EG,cyc,1}$ gives a cyclic EG-LDPC code $\mathcal{C}_{EG,cyc,1}$, called a type-1 cyclic EG-LDPC code, with minimum distance at least $q + 1$ [4], [5]. The Tanner graph $\mathcal{G}_{EG,cyc,1}$ of $\mathcal{C}_{EG,cyc,1}$ is a subgraph of the Tanner graph $\mathcal{G}_{EG}$ of the basic EG-LDPC code $\mathcal{C}_{EG}$ with the removal of the VN labeled by the origin point of EG$(2, q)$ and all the $q + 1$ CNs adjacent to it. $\mathcal{G}_{EG,cyc,1}$ consists of $q^2 - 1$ VNs and $q^2 - 1$ CNs. For $1 \leq \kappa \leq q$, the number τ of odd-degree CNs in a (κ, τ)

trapping set satisfies the equality given by (8) and the bound given by (9) with q replaced by $q-1$. For $1 \leq \kappa \leq q-4$, $\mathcal{G}_{EG,cyc,1}$ contains no small trapping set with size $\kappa < q-3$. In this case, $\tau/\kappa \geq 5$.

With appropriate column and row permutations [9], [18], the circulant matrix $\mathbf{H}_{EG,cyc,1}$ can be decomposed as a $(q+1) \times (q+1)$ array $\mathbf{H}_{EG,qc,1}$ of circulant permutation matrices (CPMs) and zero matrices (ZMs) of size $(q-1)\times(q-1)$. The null space of $\mathbf{H}_{EG,qc,1}$ give a QC-EG-LDPC code, denoted by $\mathcal{C}_{EG,qc,1}$, of length $n = q^2-1$. The QC-EG-LDPC code $\mathcal{C}_{EG,qc,1}$ and the type-1 cyclic EG-LDPC code $\mathcal{C}_{EG,cyc,1}$ are combinatorially equivalent. The trapping set structure of $\mathcal{C}_{EG,qc,1}$ is identical to that of $\mathcal{C}_{EG,cyc,1}$.

For $1 \leq \mu, \rho \leq q$, let $\mathbf{H}_{EG,qc,1}(\mu,\rho)$ be a $\mu\times\rho$ sub-array of $\mathbf{H}_{EG,qc,1}$. The null space of $\mathbf{H}_{EG,qc,1}(\mu,\rho)$ gives a QC-LDPC code of length $\rho(q-1)$.

As an example, we consider the type-1 cyclic code $\mathcal{C}_{EG,cyc,1}$ constructed based on the two-dimensional Euclidean geometry EG$(2,2^6)$ over GF(2^6). The code is a $(4095, 3367)$ cyclic LDPC code with rate 0.8222 and minimum distance exactly 65, whose parity-check matrix $\mathbf{H}_{EG,cyc,1}$ is a 4095×4095 circulant over GF(2) with both column and row weights 64, and rank 728. $\mathbf{H}_{EG,cyc,1}$ has 3367 redundant rows and row redundancy $\xi = 0.8222$. The Tanner graph $\mathcal{G}_{EG,cyc,1}$ of the code contains no (κ,τ) trapping set with size κ smaller than 64 with the ratio $\tau/\kappa \leq 1$, no small (κ,τ) trapping set with size smaller than 61 with the ratio $\tau/\kappa \leq 4$ and no absorbing set with size smaller than 32. For $\kappa = 32$, the number τ of odd-degree CNs contained in a trapping set of size κ is at least 34 times larger than κ. This is to say that any trapping set of size 32 contains at least 1088 CNs of odd degrees. Hence, the error-floor of this code is expected be very low.

VI. Two-Dimensional Projective Geometries and Their Trapping Set Structures

Since projective geometries [14], [17] form another subclass of finite geometries, the analysis of the trapping set structure of LDPC codes on finite geometries given in Section IV can be applied to analyze the trapping set structure of LDPC codes constructed based on projective geometries. For illustration, we consider the LDPC code constructed based on the two-dimensional projective geometry PG$(2,q)$ with q as a power of a prime.

The two-dimensional projective geometry PG$(2,q)$ has $n = q^2+q+1$ points and $m = q^2+q+1$ lines. Each line passes through $q+1$ points and each point is on $q+1$ lines. Any two distinct points are on a unique line. The lines in the projective geometries have the same intersecting structure as in the Euclidean geometries. However, unlike an Euclidean geometry, the lines in a projective geometry do not have the parallel structure since any two lines in a projective geometry intersect at a point, i.e., there are no parallel lines. The incidence matrix of the projective geometry PG$(2,q)$, denoted by $\mathbf{H}_{PG}$, is a $(q^2+q+1)\times(q^2+q+1)$ RC-constrained matrix of column and row weights equal to $q+1$. With proper ordering of the rows and the columns, $\mathbf{H}_{PG}$ can be put in a circulant form [12]. In this form, the null space of $\mathbf{H}_{PG}$ gives a cyclic PG-LDPC code, denoted by $\mathcal{C}_{PG}$, of length q^2+q+1 and minimum distance at least $q+2$. It is interesting to notice that if we delete from the projective geometry, PG$(2,q)$, a line $\mathcal{L}$ and all $q+1$ points on that line, then we obtain the Euclidean geometry EG$(2,q)$ [5].

The trapping set structures given by (7) and (8) hold for a two-dimensional PG-LDPC codes. For the special case $q = 2^s$, the cyclic PG-LDPC code $\mathcal{C}_{PG}$ has the following parameters [5], [8], [12] : 1) length $n = 4^s+2^s+1$; 2) dimension $4^s - 3^s + 2^s$, i.e., $\mathbf{H}_{PG}$ has rank 3^s+1; and 3) minimum distance 2^s+2. The circulant parity-check matrix $\mathbf{H}_{PG}$ has $4^s-3^s+2^s$ redundant rows and hence its row redundancy is $(4^s-3^s+2^s)/(4^s+2^s+1)$ which is close to 1 for $s \geq 4$. For this special case, the bound given by (8) on τ of a (κ,τ) trapping set with $1 \leq \kappa \leq q+1$ was first proved by Ländner and Milenkovic [8]. Consequently, the Tanner graph of the parity-check matrix $\mathbf{H}_{PG}$ of the cyclic PG-LDPC code does not have harmful trapping sets of sizes smaller than its minimum distance 2^s+2 and the same result was recently reproved in [9] based on the simple RC-constraint satisfied by $\mathbf{H}_{PG}$.

VII. Conclusions and Remarks

In this paper, we have analyzed the general trapping set structure of FG-LDPC codes that include EG-LDPC codes and PG- LDPC codes as subclasses. Our approach to the analysis is a geometric approach. In this approach, trapping sets in the Tanner graph of an FG-LDPC code are represented by subgeometries of the geometry based on which the code is constructed. Using this geometrical representation, the size and configuration of a trapping set of a given size can be analyzed. It was shown that the Tanner graph of an FG-LDPC code contains no small trapping sets with size κ less than its minimum distance minus 3. Since the minimum distances of FG-LDPC codes are relatively large, these codes basically has no harmful small trapping sets. As a consequence, they have very low error-floors. FG-LDPC codes that can achieve a BER below 10^{-15} have been reported recently [19], [20].

The techniques developed can be modified to analyze the trapping set structure of several classes of QC-LDPC codes constructed based on finite field and experimental designs, such as Latin squares. The Tanner graphs of these codes can be modeled as the Tanner graphs of partial geometries. Consequently, their trapping set structure can be analyzed using the geometrical approach proposed in this paper.

Acknowledgment

This research was supported by NSF under the Grant CCF 1015548 and gift grants from Northrop Grumman Space Technology, Intel, LSI Corporation and Cadence.

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] D. J. C. MacKay and M. S. Postol, “Weaknesses of Margulis and Ramanujan-Margulis low-density parity-check codes,” *Electronic Notes in Theoretical Computer Science*, vol. 74, pp. 97–104, 2003.

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

[4] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low density parity check codes based on finite geometries: a rediscovery," *Proc. IEEE 2000 International Symposium on Information Theory (ISIT)*, Sorrento, Italy, June 25-30, 2000, p.200.

[5] 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. Inform. Theory*, vol. 47, no. 7, pp. 2711–2736, Nov. 2001.

[6] H. Tang, J. Xu, S. Lin, and K. A. S. Abdel-Ghaffar, "Codes on finite geometries," *IEEE Trans. Inf. Theory*, vol. 51, no. 2, pp. 572-596, Feb. 2005.

[7] J. Xu, L. Chen, I. Djurdjevic, S. Lin, and K. Abdel-Ghaffar, "Construction of regular and irregular LDPC codes: Geometry decomposition and masking," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 121–134, Jan. 2007.

[8] S. Ländner and O. Milenkovic, "Algorithmic and combinatorial analysis of trapping sets in structured LDPC codes," *Proc. Int. Conf. Wireless Networks, Communications and Mobile Computing*, Maui, HI, pp. 630–635, Jun. 2005.

[9] Q. Huang, Q. Diao, S. Lin, and K. Abdel-Ghaffar, "Cyclic and quasi-cyclic LDPC codes on constrained parity-check matrices and their trapping sets," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2648-2671, May 2012.

[10] Q. Diao, Y. Y. Tai, S. Lin and K. Abdel-Ghaffar, "Trapping Set Structure of Finite Geometry LDPC Codes," *Proc. IEEE 2012 Int. Symp. Inform. Theory (ISIT)*, Boston, Ma. July 1-6, 2012.

[11] L. Dolecek, Z. Zhang, V. Anantharam, M. J. Wainwright, and B. Nikolic, "Analysis of absorbing sets and fully absorbing sets of array-based LDPC codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 181-201, Jan. 2010.

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

[13] B. K. Butler and P. H. Siegel, "Error floor approximation for LDPC codes in the AWGN channel," arXiv:1202.2826v1[cs.IT], Feb 2012.

[14] H. Mann, *Analysis and Design of Experiments*. New York, NY: Dover, 1949.

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

[16] A. P. Street and D. J. Street, *Combinatorics of Experimental Designs*, New York, NY: Oxford, Clarendon Press, 1987.

[17] L. M. Batten, *Combinatorics of Finite Geometries*, Cambridge, UK, Cambridge University Press, 2nd edition, 1997.

[18] N. Kamiya, "High-rate quasi-cyclic low-density parity-check codes derived from finite affine planes," *IEEE Trans. Inf. Theory*, vol. 53, no. 4, pp. 1444-1459, Apr. 2007.

[19] Q. Huang, Q. Diao, S. Lin, and K. Abdel-Ghaffar, "Cyclic and Quasi-Cyclic Codes: New Development," *Information Theory and Applications (ITA) Workshop*, UCSD, San Diego, Feb. 7-10, 2011.

[20] S. Lin and Q. Diao, "Algebraic LDPC Codes: Error-Floor, Trapping Set Structure, and The Rate of Decoding Convergence," *IEEE 2012 ICC Workshop on Data Storage Technology*, Ottawa, Canada June 10-15 2012. (committees.comsoc.org/spfs/icc2012/slides/slides.part3.pdf)