Low-Density Parity-Check Codes on Partial Geometries

Shu Lin
(Co-authors: Qiuju Diao, Ying-yu Tai and Khaled Abdel-Ghaffar)

Department of Electrical and Computer Engineering
University of California, Davis
Davis, CA 95616, U.S.A.
Abstract

Many known algebraic constructions of low-density parity-check (LDPC) codes can be placed in a general framework using the notion of partial geometries. Based on this notion, the structure of such LDPC codes can be analyzed using a geometric approach that illuminates important properties of their parity-check matrices. In this approach, trapping sets are represented by sub-geometries of the geometry used to construct the code. Based on the incidence relations between lines and points in this geometry, the structure of trapping sets is investigated. On the other hand, it is shown that removing a sub-geometry corresponding to a trapping set gives a punctured matrix which can be used as a parity-check matrix of an LDPC code. This relates trapping sets, represented by sub-geometries, and punctured matrices, represented by the residual geometries. The null spaces of these punctured matrices are LDPC codes which inherit many of the good structural properties of the original code. Hence, new LDPC codes, with various lengths and rates, can be obtained by puncturing an LDPC code constructed based on a partial geometry. Furthermore, these punctured matrices and codes can be used in a two-phase decoding scheme to correct combinations of random errors and erasures.
I. Introduction

- Partial geometries generalize both Euclidean and projective geometries which were used to construct the first classes of algebraic LDPC codes ever reported in the literature and which were shown to have excellent performance [1]-[2].

- LDPC Codes constructed based on the more general partial geometries were considered in [3]-[8].

- Diverse classes of algebraic LDPC codes that appear in the literature are actually partial geometry codes although their construction methods do not seem to have any geometrical notion.
Coverage of this presentation:

1. Partial geometries and their structural properties;
2. Code construction;
3. Trapping set structure;
4. Punctured codes;
5. Correction of combinations of random errors and erasures
Partial geometries were first introduced by Bose in 1963 [9]. An excellent coverage of partial geometries can be found in Batten [10]-[14].

Consider a system composed of a set $N$ of $n$ points and a set $M$ of $m$ lines where each line is a set of points. If a line $L$ contains a point $p$, we say that $p$ is on $L$ and that $L$ passes through $p$.

If two points are on a line, then we say that the two points are adjacent and if two lines pass through the same point, then we say that the two lines intersect, otherwise they are parallel.
The system composed of the sets $N$ and $M$ is a *partial geometry* if the following conditions are satisfied for some fixed integers $\rho \geq 2$, $\gamma \geq 2$, and $\delta \geq 1$ [9], [10]:

1. Any two points are on at most one line,
2. Each point is on $\gamma$ lines,
3. Each line passes through $\rho$ points,
4. If a point $p$ is not on a line $L$, then there are exactly $\delta$ lines, each passing through $p$ and a point on $L$. 
Such a partial geometry will be denoted by $\text{PaG}(\gamma, \rho, \delta)$, or $\text{PaG}$ for short, and $\gamma$, $\rho$, and $\delta$ are called the parameters of the partial geometry.

A simple counting argument shows that the partial geometry $\text{PaG}(\gamma, \rho, \delta)$ has exactly

$$n = \rho((\rho - 1)(\gamma - 1) + \delta)/\delta$$

points and

$$m = \gamma((\gamma - 1)(\rho - 1) + \delta)/\delta$$

lines.
If \( p \) and \( p' \) are two adjacent points, then there are exactly 
\( \gamma \delta + \rho - \gamma - \delta - 1 \) points, such that each of these points is 
adjacent to both \( p \) and \( p' \).

On the other hand, if \( p \) and \( p' \) are not adjacent, then there are 
exactly \( \gamma \delta \) points, such that each of these points is adjacent to 
both \( p \) and \( p' \).

Well known examples of partial geometries are Euclidean and 
projective geometries over finite fields [12]-[14].
If $\delta = \gamma - 1$, the partial geometry $\text{PaG}(\gamma, \rho, \gamma - 1)$ is called a net [9] which consists of $n = \rho^2$ points and $m = \gamma \rho$ lines.

Each point $p$ not on a line $L$ is on a unique line which is parallel to $L$.

The set of $m = \gamma \rho$ lines in $\text{PaG}(\gamma, \rho, \gamma - 1)$ can be partitioned into $\gamma$ classes, each consisting of $\rho$ lines, such that all the lines in each class are parallel, any two lines in two different classes intersect, and each of the $n = \rho^2$ points is on a unique line in each class.

These classes of lines are called parallel bundles.

A two-dimensional Euclidean geometry (or affine geometry) is a net.
For every point $p$ in $\text{PaG}(\gamma, \rho, \delta)$ there are exactly $\gamma$ lines that intersect at $p$, i.e., all of them pass through $p$. These lines are said to form an intersecting bundle at $p$, denoted by $\Delta(p)$.

Notice that $p$ is on every line in $\Delta(p)$, there are exactly $\gamma(\rho - 1)$ points, each is on a unique line in $\Delta(p)$, and all the other $n - \gamma(\rho - 1) - 1$ points in $\text{PaG}(\gamma, \rho, \delta)$ are not on any line in $\Delta(p)$.

If $\delta = \rho$, then every point in $\text{PaG}(\gamma, \rho, \rho)$ is adjacent to $p$ since every point is on a line in $\Delta(p)$. In this case, any two points in $\text{PaG}(\gamma, \rho, \rho)$ are connected by a line.

Examples for which $\delta = \rho$ are two-dimensional Euclidean and projective geometries.
Let $\Lambda$ be a set of points in $\text{PaG}(\gamma, \rho, \delta)$. Then $\Phi(\Lambda) = \bigcup_{p \in \Lambda} \Delta(p)$ is the union of intersecting bundles at points in $\Lambda$, i.e., $\Phi(\Lambda)$ is the set of lines in $\text{PaG}(\gamma, \rho, \delta)$ such that each line passes through at least one point in $\Lambda$.

For a set $\Lambda \subseteq N$ of points and a line $L \in M$ in $\text{PaG}(\gamma, \rho, \delta)$, the restriction of $L$ to $\Lambda$ is $L \cap \Lambda$ which consists of the points in $\Lambda$ that are on $L$.

The subgeometry induced by $\Lambda$ in $\text{PaG}(\gamma, \rho, \delta)$, denoted by $\text{PaG}[\Lambda]$, consists of $\Lambda$ as the set of its points and the restrictions of the lines in $L \in \Phi(\Lambda)$ as its lines.

Notice that the subgeometry $\text{PaG}[\Lambda]$ has $|\Lambda|$ points and $|\Phi(\Lambda)|$ restricted lines.
Construct an $m \times n$ matrix, $H_{PaG}$, based on the partial geometry $PaG(\gamma, \rho, \delta)$ as follows. The rows of $H_{PaG}$ are labeled by the $m$ lines and the columns are labeled by the $n$ points. The entry at the column labeled by a point $p$ and the row labeled by a line $L$ is 1 if and only if $L$ passes through $p$.

In this case, we say that this row in $H_{PaG}$ labeled by $L$ is attached to that column labeled by $p$. Since there are $\gamma$ lines pass the point $p$, there are $\gamma$ rows attached to the column labeled by $p$. 
The matrix $H_{PaG}$ is called the *incidence matrix* of the partial geometry $PaG(\gamma, \rho, \delta)$ and each row is the *incidence vector* of the line labeling that row.

Since each line consists of $\rho$ points, the incidence vector of a line in $PaG(\gamma, \rho, \delta)$ has weight $\rho$.

It follows that the matrix $H_{PaG}$ has constant column weight $\gamma$ and constant row weight $\rho$.

Since any two distinct points are connected by at most one line, for any two distinct columns there is at most one row that has ones in the two columns, $H_{PaG}$ is said to satisfy the Row-Column (RC)-constraint.
If $\gamma$ is small compared to $m$, then $H_{PaG}$ is sparse. In this case, the null space of $H_{PaG}$ gives an RC-constrained $(\gamma, \rho)$-regular LDPC code, $C_{PaG}$, of length $n$. The matrix $H_{PaG}$ is then a parity-check matrix for $C_{PaG}$ which is called a PaG-LDPC code.

It was shown in [13] that the rank of $H_{PaG}$ is upper bounded by

$$rank(H_{PaG}) \leq \gamma \rho (\gamma - 1)(\rho - 1)/(\rho (\gamma + \rho - \delta - 1)) + 1.$$ 

Furthermore, if $\gamma + \rho + \delta$ is even, then

$$rank(H_{PaG}) \geq \gamma \rho (\gamma - 1)(\rho - 1)/((\delta (\gamma + \rho - \delta - 1)).$$
The minimum distance, $d_{\text{min}}$, of the PaG-LDPC code $C_{\text{PaG}}$ is lower bounded by

$$d_{\text{min}} \geq \max\{\gamma + 1, \gamma(\rho - \gamma + \delta + 1)/\delta, 2(\rho + \delta - 1)/\delta\}.$$  

The transpose, $H_{\text{PaG}}^T$, of the matrix $H_{\text{PaG}}$ is the incidence matrix of a partial geometry PaG($\rho, \gamma, \delta$), called the dual of PaG($\gamma, \rho, \delta$) obtained by identifying the points of PaG($\gamma, \rho, \delta$) with the lines of PaG($\rho, \gamma, \delta$) and vice versa. A point $p$ is on a line $L$ in PaG($\rho, \gamma, \delta$) if and only if the line in PaG($\gamma, \rho, \delta$) identified with $p$ passes through the point in PaG($\gamma, \rho, \delta$) identified with $L$.

The null space of $H_{\text{PaG}}^T$ also gives a PaG-LDPC code, denoted by $C_{\text{PaG,d}}$. 
The **Tanner graph**, $G_{PaG}$, associated with the matrix $H_{PaG}$ is a bipartite graph composed of two sets of nodes, the set of variable nodes (VNs) labeled by the points in the partial geometry $PaG(\gamma, \rho, \delta)$ or, equivalently, the columns of $H_{PaG}$, and the set of check nodes (CNs) labeled by the lines in $PaG(\gamma, \rho, \delta)$ or, equivalently, the rows of $H_{PaG}$. Edges in $G_{PaG}$ connect only VNs to CNs.

The VN labeled by a point $p$ is connected to the CN labeled by a line $L$ by an edge if and only if $L$ passes through $p$, i.e., if and only if the entry in $H_{PaG}$ at the corresponding row and column is 1. In this case, we say that this VN and this CN are adjacent.
Hence, $G_{PaG}$ is a bipartite graph that has $n$ VNs, $m$ CNs, each VN has degree $\gamma$, and each CN has degree $\rho$. Furthermore, any two distinct VNs are connected to at most one CN as any two points in $PaG(\gamma, \rho, \delta)$ are connected by at most one line. This implies that the girth of $G_{PaG}$, which is the shortest length of a cycle in the bipartite graph, is at least six.

$G_{PaG}$ contains $n\gamma(\gamma - 1)(\rho - 1)(\delta - 1)/6$ cycles of length 6.

As each such cycle contains three VNs, each VN is on $\gamma(\gamma - 1)(\rho - 1)(\delta - 1)/2$ cycles of length six.

Such a large number of short cycles causes correlation in the messages passed during iterative decoding (after three iterations).
However, the Tanner graph has a **high-degree** of connectivity as each pair of VNs is connected by a **path of length at most four** in $G_{PaG}$, as any two points in $PaG(\gamma, \rho, \delta)$ are either adjacent or both adjacent to a common point.

With iterative message-passing decoding, this high-degree connectivity allows **rapid and large amount of information exchanges** between all the VNs which offsets the effect of short cycles.

This high-degree of connectivity results in **fast decoding convergence**.
The major disadvantage of this high-degree connectivity is the decoder complexity, in both hardware and computation, and memory required to store messages for information exchanges between processing units.

This decoder complexity issue can be overcome for PaG-LDPC codes whose parity-check matrices has block cyclic structure.
V. SUBGRAPHS AND PUNCTURED CODES

- The Tanner graph $G_{PaG}$ of a PaG-LDPC code is actually a graphical representation of the partial geometry $PaG(\gamma, \rho, \delta)$ with the VNs and CNs representing the points and lines of $PaG(\gamma, \rho, \delta)$ and the edges connecting the VNs to a CN representing the points labeling the VNs lying on the line labeling the CN.

- Let $\Lambda$ be a set of points in $PaG(\gamma, \rho, \delta)$ and $\Phi(\Lambda)$ be the set of lines in $PaG(\gamma, \rho, \delta)$ such that each line passes through at least one point in $\Lambda$.

- The VNs in $G_{PaG}$ labeled by the points in $\Lambda$ are adjacent to the CNs labeled by the lines in $\Phi(\Lambda)$. Then, the VNs labeled by the points in $\Lambda$ and the CNs labelled by the lines in $\Phi(\Lambda)$ form a subgraph of $G_{PaG}$, denoted by $G_{PaG}[\Lambda]$. 
This subgraph $G_{PaG}[\Lambda]$ consists of $|\Lambda|$ VNs and $|\Phi(\Lambda)|$ CNs.

We say that this subgraph $G_{PaG}[\Lambda]$ is induced by the set $\Lambda$ of VNs in $G_{PaG}$.

$G_{PaG}[\Lambda]$ is the graphical representation of the subgeometry $PaG[\Lambda]$ of the $PaG(\gamma, \rho, \delta)$ induced by $\Lambda$.

The correspondence $G_{PaG}[\Lambda] \leftrightarrow PaG[\Lambda]$ is one-to-one.
Let $H_{PaG}(\Lambda, \Phi(\Lambda))$ be the incidence matrix of the subgraph $G_{PaG}[\Lambda]$ of the Tanner graph $G_{PaG}$ of the partial geometry $PaG(\gamma, \rho, \delta)$ (or the incidence matrix of the subgeometry $PaG[\Lambda]$ of $PaG(\gamma, \rho, \delta)$).

$H_{PaG}(\Lambda, \Phi(\Lambda))$ is a submatrix of the incidence matrix $H_{PaG}$ (or a punctured matrix of $H_{PaG}$ obtained by deleting the columns labeled by the points in $\Lambda^c$ and the rows labeled by the lines in $\Phi(\Lambda)^c$).

Then the null space of $H_{PaG}(\Lambda, \Phi(\Lambda))$ also gives a PaG-LDPC code, denoted by $C_{PaG}(\Lambda, \Phi(\Lambda))$, which may be considered as a punctured code of PaG-LDPC code $C_{PaG}$. 
Let $\text{PaG}(\Lambda^c, \Phi(\Lambda)^c)$ denote the residue geometry of $\text{PaG}(\gamma, \rho, \delta)$ obtained by deleting the points and lines in $\text{PaG}(\Lambda)$ from $\text{PaG}(\gamma, \rho, \delta)$.

Let $H_{\text{PaG}}(\Lambda^c, \Phi(\Lambda)^c)$ denote the incidence matrix of the residue geometry $\text{PaG}(\Lambda^c, \Phi(\Lambda)^c)$.

The null space of $H_{\text{PaG}}(\Lambda^c, \Phi(\Lambda)^c)$ also gives a PaG-LDPC code.

Given a partial geometry $\text{PaG}(\gamma, \rho, \delta)$, a family of PaG-LDPC codes can be constructed.

There are many types of partial geometries. From these types of partial geometries, different families of PaG-LDPC codes can be constructed.
There are many types of partial geometries that appear in textbooks and can be used to construct LDPC codes. Here, we give present five different types, three classical and two new types.

The two new types were initially developed without any geometric notion.

The LDPC codes constructed from these five types of partial geometries are mostly quasi-cyclic (QC) or cyclic codes.
The $s$-dimensional Euclidean geometry, $\text{EG}(s,q)$, where $q$ is a prime or a power of a prime, consists of $q^s$ points and $q^{s-1}(q^s - 1)/(q - 1)$ lines [10]-[13].

Each point is represented by an $s$-tuple over $\text{GF}(q)$. The point represented by the all-zero $s$-tuple is called the origin.

A line in $\text{EG}(s,q)$ contains $q$ points. A line is either a one-dimensional subspace or its coset of the vector space of all the $q^s$ $s$-tuples over $\text{GF}(q)$.

A point is on $(q^s - 1)/(q - 1)$ lines. Any two distinct points in $\text{EG}(s,q)$ are connected by one and only one line.
Hence, $\text{EG}(s, q)$ is a partial geometry with parameters $\gamma = (q^s - 1)/(q - 1)$ and $\rho = \delta = q$, i.e., $\text{EG}(s, q) = \text{PaG}((q^s - 1)/(q - 1), q, q)$. $\text{GF}(q^s)$ as an extension field of $\text{GF}(q)$ is a realization of $\text{EG}(s, q)$ and hence, the points of $\text{EG}(s, q)$ can be represented by the $q^s$ elements of $\text{GF}(q^s)$. Based on $\text{EG}(s, q)$, a large class of Euclidean geometry (EG) LDPC codes can be constructed [1]-[5], including cyclic and QC-LDPC codes as subclasses.
The $s$-dimensional projective geometry, $\text{PG}(s, q)$, where $q$ is a prime or a power of a prime, has $n = (q^{s+1} - 1)/(q - 1)$ points and $m = (q^s - 1)(q^{s+1} - 1)/(q - 1)(q^2 - 1)$ lines. Each line passes through $q + 1$ points and each point is on $(q^s - 1)/(q - 1)$ lines [12] - [14]. Any two distinct points are on a unique line.

Hence, $\text{PG}(s, q)$ is a partial geometry with parameters $\gamma = (q^s - 1)/(q - 1)$ and $\rho = \delta = q + 1$.

Based on lines and points of $\text{PG}(s, q)$, families of cyclic and quasi cyclic $\text{PG}$-LDPC codes can be constructed.
A balanced incomplete block design (BIBD) consists of a set of $n$ points and distinct subsets, called blocks, each consisting of $\rho$ points, such that each point is in exactly $\gamma$ blocks and each pair of distinct points is in exactly $\lambda$ blocks. By viewing the blocks as lines, a BIBD with $\lambda = 1$ is a partial geometry PaG($\gamma$, $\rho$, $\rho$).

Numerous constructions of BIBDs appear in [15] and the references therein.

Constructions of LDPC codes based on BIBDs with $\lambda = 1$ can be found in [16] - [18]. These codes are called BIBD-LDPC codes and they perform well with iterative decoding.
Let $H$ be an RC-constrained matrix of size $m \times n$ with row weight $\rho$ and column weight $\gamma$, where $n = (\rho - 1)\gamma + 1$.

Then, it can be shown that $H$ is the incidence matrix of a partial geometry $\text{PaG}(\gamma, \rho, \rho)$. The partial geometry has $n$ points corresponding to the columns of $H$ and $m$ lines corresponding to the rows of $H$.

The RC-constraint implies that any two points are on at most one line. Furthermore, since each row has weight $\rho$ and each column has weight $\gamma$, each line passes through $\rho$ points and each point is on $\gamma$ lines.
Next, we will argue that if a point $p$ is not on a line $L$ then there are exactly $\rho$ lines, each passing through $p$ and a point on $L$ in case $n = (\rho - 1)\gamma + 1$.

Since every row has $\rho$ ones, then by adding all the $\gamma$ rows attached to the column corresponding to the point $p$, where the sum is over the integers rather than over GF(2), we obtain a vector, $z$, of length $n$ whose components as integers add up to $\gamma \rho$.

Notice that the entry in the column corresponding to the point $p$ in $z$ is $\gamma$. Hence, all other $(\rho - 1)\gamma$ components in $z$ add up to $(\rho - 1)\gamma$. 
Because of the RC-constraint, all these components are at most equal to 1 and, hence, all of them equal 1. Therefore, every column other than the one corresponding to $p$ is attached to a unique row corresponding to a line passing through $p$.

Since $L$ is a line not passing through the point $p$ that passes through exactly $\rho$ points, each one of these points is on a line passing through $p$. This completes the proof that $H$ is the incidence matrix of a partial geometry $\text{PaG}(\gamma, \rho, \rho)$.

Notice that the projective geometry, $\text{PG}(s, q)$, which is a partial geometry $\text{PaG}((q^s - 1)/(q - 1), q + 1, q + 1)$, is a special case of this construction.
Let $H$ be an $m \times n$ RC-constrained matrix which is a $\gamma \times \rho$ array of $\gamma \times \gamma$ circulant permutation matrices (CPMs), where $m = \gamma^2$ and $n = \gamma \rho$.

Then $H$ is the incidence matrix of a partial geometry $\mathrm{PaG}(\gamma, \rho, \rho - 1)$. The partial geometry has $n = \gamma \rho$ points corresponding to the columns of $H$ and $m = \gamma^2$ lines corresponding to the rows of $H$. Each point is on $\gamma$ lines and each line passes through $\rho$ points. The RC-constraint implies that any two points are on at most one line.
• The code constructed based on this partial geometry, i.e., whose parity-check matrix is $H$, is quasi cyclic.

• There are many constructions of a matrix $H$ which is an $m \times n$ RC-constrained matrix in the form of a $\gamma \times \rho$ array of $\gamma \times \gamma$ CPMs based on finite fields and Latin squares, see e.g., [19] - [25].

• If $\gamma = \rho$, then the partial geometry $\text{PaG}(\gamma, \rho, \rho - 1)$ constructed in this way is actually a net where each parallel bundle of lines in this net corresponds to the rows comprising a row of CPMs in $H$. 
The above two cases shows that many algebraic constructions of LDPC codes can be unified under the framework of partial geometries.

Consequently, the structure of these finite field LDPC codes can be studied based on a geometrical approach, especially the trapping set structure and connectivity of the VNs in the Tanner graph of such a code.
V. TRAPPING SETS OF LDPC CODES

Introduction

- LDPC codes perform well with iterative decoding based on belief propagation, such as the \textit{sum-product algorithm} (SPA) or the \textit{min-sum algorithm} (MSA) [20], [26].

- However, with iterative decoding, most LDPC codes have a common severe weakness, known as the \textit{error-floor}. The error-floor of an LDPC code is characterized by the phenomenon that as the SNR continues to increase, the error probability suddenly drops at a rate much slower than that in the region of low to moderate SNR.

- The error-floor may preclude LDPC codes from applications where very low error rates are required, such as high-speed satellite communications, optical communications, hard-disk drives and flash memories.
High error-floors most commonly occur for unstructured random or pseudo-random LDPC codes constructed using computer-based methods or algorithms. Structured LDPC codes constructed based on finite geometries, finite field and combinatorial designs [2], [19]-[25], [27], in general, have much lower error-floors.

Ever since the phenomenon of the error-floors of LDPC codes with iterative decoding became known [28], a great deal of research effort has been expended in finding its causes and methods to resolve or mitigate the error-floor problem [20], [24], [28]-[54].

For the AWGN channel, the error-floor of an LDPC code is mostly caused by an undesirable structure, known as a trapping set [28], in the Tanner graph of the code based on which the decoding is carried out.
Extensive studies and simulation results show that most trapping sets that cause high error-floors of LDPC codes are the trapping sets of small size.

In a very recent paper [24], we investigated trapping set structure of RC-constrained regular LDPC codes and showed that, for an RC-constrained $(\gamma, \rho)$-regular LDPC code, its Tanner graph contains no trapping set of size at most equal to $\gamma$ with the number $\tau$ of odd-degree CNs smaller than $\gamma$.

The second part of this presentation is on trapping set structure of the PaG-LDPC codes.
For the AWGN channel, we adopt from literature definitions of trapping sets and related structures as combinatorial objects that capture the failing mechanisms of iterative decoding algorithms in general and which are independent of the particular decoder used.

After we briefly review these definitions and concepts of trapping sets of an LDPC code, we give bounds on the sizes of these trapping sets for PaG-LDPC codes.

First, we define trapping sets and some subclasses of trapping sets and follow this with a motivation of these definitions.
Definition 1. Let $G$ be the Tanner graph of a binary LDPC code, $C$, of length $n$ given by the null space of an $m \times n$ matrix $H$ over GF(2). For $1 \leq \kappa \leq n$ and $0 \leq \tau \leq m$, we have the following definitions [28], [29]:

1. A $(\kappa, \tau)$ trapping set is a set, $\Lambda$, of $\kappa$ VNs in $G$ which induces a subgraph, $G[\Lambda]$, of $G$ with exactly $\tau$ odd-degree CNs and an arbitrary number of even-degree CNs.

2. A $(\kappa, \tau)$ trapping set is elementary if all the CNs in the induced subgraph $G[\Lambda]$ have degree one or degree two, and there are exactly $\tau$ degree-one CNs.
A $(\kappa, \tau)$ trapping set is small if $\kappa \leq \sqrt{n}$ and $\tau / \kappa \leq 4$.

A $(\kappa, \tau)$ trapping set is absorbing if every VN in the trapping set is connected in $G[\Lambda]$ 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 $G[\Lambda]$ than other CNs, i.e., CNs not in $G[\Lambda]$ or in $G[\Lambda]$ but of even degree, then the trapping set is fully absorbing [48]
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 $\kappa$ code bits (or the $\kappa$ VNs) of a $(\kappa, \tau)$ trapping set $\Lambda$, the $\tau$ odd-degree CNs, each connected to an odd number of VNs in $\Lambda$, will not be satisfied while all other CNs will be satisfied.

The decoder will succeed in correcting the errors in $\Lambda$ if the messages coming from the $\tau$ unsatisfied CNs connected to the VNs in $\Lambda$ are strong enough to overcome the messages coming from the satisfied CNs. However, this may not be the case if $\tau$ 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 \((\kappa, \tau)\) trapping sets are usually those with small values of \(\kappa\) and \(\tau\).

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 \(\kappa\) and small ratios \(\tau/\kappa\).

These conclusions are captured by the notions of elementary trapping sets and small trapping sets, see Definition 1, parts 2 and 3.
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 (or a one-step majority-logic) 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 [77] (which is usually true in the error-floor region), then the decoder will behave like a Gallager type-B decoder and will fail.

Absorbing sets characterize the non-codeword states to which the decoder converges when it fails.
As all check-sums of a codeword in the code are satisfied, the VNs corresponding to the nonzero bits in a codeword forms a \((\kappa, 0)\) trapping set, where \(\kappa\) 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.

An LDPC code with relative large minimum distance whose Tanner graph does not contain harmful trapping set with size smaller than its minimum distance is said to have a **good trapping set structure**.
VI. GEOMETRICAL INTERPRETATION OF TRAPPING SETS OF PARTIAL GEOMETRY LDPC CODES

Geometrical Interpretation of a Trapping Set

- Consider the PaG-LDPC code $C_{PaG}$ constructed based on the partial geometry PaG($\gamma, \rho, \delta$).

- A $(\kappa, \tau)$ trapping set in the Tanner graph $G_{PaG}$ of $C_{PaG}$ is defined by the subgraph $G_{PaG}[\Lambda]$ induced by the VNs labeled by the points in a set $\Lambda$ of size $\kappa$ in the partial geometry PaG($\gamma, \rho, \delta$) such that $G_{PaG}[\Lambda]$ has exactly $\tau$ odd-degree CNs. The CNs adjacent to the $\kappa$ VNs in the induced subgraph are labeled by the lines in PaG($\gamma, \rho, \delta$), each passing through at least one of the $\kappa$ points labeling the VNs, i.e., the lines in $\Phi(\Lambda)$. 
Recall that the subgraph $G_{PaG}[\Lambda]$ of $G_{PaG}$ is the graphical representation of the subgeometry $PaG[\Lambda]$ of $PaG(\gamma, \rho, \delta)$ induced by $\Lambda$ which consists of the points in $\Lambda$ and the restricted lines in $\Phi(\Lambda)$.

Since the correspondence $G_{PaG}[\Lambda] \leftrightarrow PaG[\Lambda]$ is one-to-one. The subgraph $G_{PaG}[\Lambda]$ has exactly $\tau$ CNs of odd degree if and only if there are exactly $\tau$ lines in $\Phi(\Lambda)$ that pass through an odd number of points in $\Lambda$.

The above says that a trapping set in the Tanner graph $G_{PaG}$ can be represented by a subgeometry in $PaG(\gamma, \rho, \delta)$. 
Based on the geometrical representation of trapping sets given above, we can analyze the trapping set structure of a PaG-LDPC code.

Let $m_i$ be the number of lines in $\Phi(\Lambda)$, each passing through exactly $i$ points in $\Lambda$, where $1 \leq i \leq \kappa$.

Then, $\tau$ 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 $\kappa$, we have

$$\tau = m_1 + m_3 + m_5 + \cdots + m_{2\lfloor (\kappa + 1)/2 \rfloor - 1}. \quad (1)$$
Let the subgeometry $\text{PaG}[\Lambda]$ represented by $(\Lambda, \Phi(\Lambda))$

Let $p$ be a point in $\Lambda$ and $L$ be a line in $\Phi(\Lambda)$ passing through $p$. The pair $(p, L)$ is called a point-line pair in the subgeometry $(\Lambda, \Phi(\Lambda))$. Such a point-line pair in $(\Lambda, \Phi(\Lambda))$ represents a pair of adjacent VN and CN in a $(\kappa, \tau)$ trapping set.

There are two ways of counting the total number of such point-line pairs.
Since each line in $\Phi(\Lambda)$ containing $i$ points in $\Lambda$ gives $i$ point-line pairs in $(\Lambda, \Phi(\Lambda))$, the total number of point-line pairs in $(\Lambda, \Phi(\Lambda))$ is

$$m_1 + 2m_2 + \cdots + \kappa m_\kappa.$$  

(2)

Since each of the $\kappa$ points in $\Lambda$ is on $\gamma$ lines, the total number of such pairs in $(\Lambda, \Phi(\Lambda))$ is also equal to $\kappa \gamma$. Consequently, we have the following equality:

$$m_1 + 2m_2 + \cdots + \kappa m_\kappa = \kappa \gamma.$$  

(3)
Next, we count, also in two different ways, the number of pairs of adjacent points in $\Lambda$. (Throughout this paper, by a pair of points we mean an unordered pair of distinct points.)

Since $\Lambda$ consists of $\kappa$ points, there are at most $\binom{\kappa}{2}$ such pairs.

Alternatively, since every pair of adjacent points in $\Lambda$ is on a unique line in $\Phi(\Lambda)$ and a line passing through $i$ points in $\Lambda$ connects $\binom{i}{2}$ pairs of points, the total number of pairs of adjacent points in $\Lambda$ is

$$\binom{2}{2} m_2 + \binom{3}{2} m_3 + \ldots + \binom{\kappa}{2} m_{\kappa}.$$
Hence, we have the following inequality:

\[
\binom{2}{2} m_2 + \binom{3}{2} m_3 + \ldots + \binom{\kappa}{2} m_\kappa \leq \binom{\kappa}{2}.
\] (4)

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

\[
m_1 - \sum_{i=3}^{\kappa} i(i - 2)m_i \geq \gamma \kappa - \kappa(\kappa - 1)
\] (5)
From (5) with some algebraic manipulations, we obtain the following lower bound on for the number \( \tau \) of lines in the subgeometry \( \text{PaG}[\Lambda] = (\Lambda, \Phi(\Lambda)) \), each containing an odd number of points in \( \Lambda \):

\[
\tau \geq \sum_{i=1,3,5,...} m_i = (\gamma + 1 - \kappa) \kappa + \sum_{i=3,5,...} (i-1)^2 m_i + \sum_{4,6,...} i(i-2)m_i.
\]  

(6)

Equality in the above lower bound on \( \tau \) holds if \( \delta = \rho \), i.e., every pair of points in the partial geometry \( \text{PaG}(\gamma, \rho, \delta) \) are adjacent. This is the case for the first 4 types of partial geometries mentioned earlier.
For this case, if we know the distribution of points in \( \Lambda \) over the lines in \( \Phi(\Lambda) \), we can enumerate \( \tau \) exactly. In fact, we can even determine the configuration the trapping set corresponding to the subgeometry \( \text{PaG}[\Lambda] = (\Lambda, \Phi(\Lambda)) \). 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 \( \tau \):

\[
\tau \geq (\gamma + 1 - \kappa)\kappa. \tag{7}
\]

For \( \kappa < \gamma \), \( \tau \) can be many times larger than \( \kappa \). It follows from Definition 1-3 that the Tanner graph \( G_{\text{PaG}} \) of the PaG-LDPC code \( C_{\text{PaG}} \) contains no small trapping set with size \( \kappa < \gamma - 3 \). For \( \kappa < \gamma - 3 \), \( \tau \) is at least 5 time larger than \( \kappa \), i.e., \( \tau/\kappa \geq 5 \).
There are two special cases for which the equality of (6) holds.

The first case is that each line in $\Phi(\Lambda)$ passes through at most two points in $\Lambda$ is that equality (4) holds and no three points in $\Lambda$ are collinear.

In this case, $m_3 = m_4 = \ldots = m_\kappa = 0$ and the subgeometry $PaG(\Lambda)$ of $PaG(\gamma, \rho, \delta)$ induced by the set $\Lambda$ of points represents a $(\kappa, (\gamma + 1 - \kappa)\kappa)$ elementary trapping set with $(\gamma + 1 - \kappa)\kappa$ CNs of degree-1 and $\kappa(\kappa - 1)/2$ CNs of degree-2.

It can be 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.
As another special case is that all the points in \( \Lambda \) are collinear. In this case, \( m_2 = \ldots = m_{\kappa - 1} = 0 \) and \( m_\kappa = 1 \). Then, the equalities of (4) and (6) hold.

It follows from (6) that: if \( \kappa \) is even, \( \text{PaG}(\Lambda) \) represents a \((\kappa, (\gamma - 1)\kappa)\) trapping set with \((\gamma - 1)\kappa\) CNs of degree-1 and one CN of degree-\(\kappa\); and (2) if \( \kappa \) is odd, \( \text{PaG}(\Lambda) \) represents a \((\kappa, (\gamma - 1)\kappa + 1)\) trapping set with \((\gamma - 1)\kappa\) CNs of degree-1 and one CN of degree-\(\kappa\) (all CNs have odd degree).
Based on the intersecting structure of lines in a partial geometry $\text{PaG}(\gamma, \rho, \delta)$, it can be easily prove that the Tanner graph $G_{\text{PaG}}$ of the PaG-LDPC code $C_{\text{PaG}}$ does not have any absorbing set of size $\kappa \leq \lfloor \gamma/2 \rfloor + 1$.

The smallest size of an absorbing set is $\lceil \gamma/2 \rceil + 2$. 
Recall that the partial geometry $\text{PaG}(\gamma, \rho, \delta)$ is a net if $\delta = \gamma - 1$ in which case the lines can be partitioned into $\gamma$ parallel bundles, each consisting of $\rho$ parallel lines, and each point is on a unique line in each parallel bundle.

Examples of nets are two-dimensional Euclidean geometries and partial geometries corresponding certain arrays of CPMs constructed based on finite fields and Latin squares.

In case of a net, we can improve upon the bound in (6) by considering the distribution of points labeling the VNIs in a trapping set over the lines in a parallel bundle.

Recall that each parallel bundle of $\rho$ lines contains all the points in $\text{PaG}(\gamma, \rho, \gamma - 1)$ and, in particular, all the points in $\Lambda$. 

Let $P$ be a parallel bundle of lines and $L_1, L_2, ..., L_\rho$ be the lines in $P$.

For $1 \leq l \leq \rho$, let $\Lambda_l$ be the (possibly empty) set of points in $\Lambda$ that are on the line $L_l$ and let $\kappa_l$ be the number of such points.

Since the lines $L_1, L_2, ..., L_\rho$ are parallel, each point in $\Lambda$ is on one and only one of these lines. Hence, $\Lambda_1, \Lambda_2, ..., \Lambda_\rho$ are disjoint sets whose union is $\Lambda$ and $\kappa_1 + \kappa_2 + \cdots + \kappa_\rho = \kappa$. 
Then, the number $\tau$ of odd-degree CNs is a $(\kappa, \tau)$ trapping set of a net-LDPC code is lower bounded as below:

$$\tau \geq (\gamma - 1)\kappa - \kappa^2 + \sum_{l=1}^{\rho} \kappa_l^2 + |l : 1 \leq l \leq b, \kappa_l \text{ is odd}|. \quad (8)$$

This bound agrees with (7) whenever $\kappa_l \leq 2$ for all $1 \leq l \leq \rho$ and improves upon it in all the other cases.
The bound on $\tau$ given in (8) can be applied easily once the distribution of the set of points $\Lambda$ corresponding to the VNs of the trapping set over the lines in a parallel bundle is given without the need to explicitly determine $\Phi(\Lambda)$.

The bound depends on the numbers $\kappa_1, \kappa_2, \ldots, \kappa_{\rho}$, which in turn depend on the set of points $\Lambda$ as well as on the choice of the parallel bundle $P$.

For example, if the net is the two-dimensional Euclidean geometry $\text{EG}(2, q)$, where $q$ is a prime or a power of a prime, then each point can be represented by a two-tuple $(a_0, a_1)$ over $\text{GF}(q)$ and $\{(a_0, a_1) : a_0 \in \text{GF}(q)\}$ for some $a_1 \in \text{GF}(q)$ is a line associated with this value of $a_1$. The $q$ lines associated with the $q$ values of $a_1 \in \text{GF}(q)$ 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 $\Lambda$ on the line associated with $a_1$ is the number of points $(a_0, a_1) \in \Lambda$. This gives the numbers $\kappa_1, \kappa_2, \ldots, \kappa_\rho$ which can be used in (8) to obtain a lower bound on $\tau$ in a $(\kappa, \tau)$ trapping set.
A Bound on Average Number of Odd-Degree CNs of a Trapping Set

- The bound $\tau \geq (\gamma + 1 - \kappa)\kappa$ given by (7) gives a rather skewed picture of trapping sets since it bounds the smallest $\tau$ of a $(\kappa, \tau)$ trapping set.

- For a given $\kappa$, it is possible that there are numerous $(\kappa, \tau)$ trapping sets in the Tanner graph with $\tau$ significantly larger than this lower bound.

- Actually, by averaging the sharper lower bound given in (8) for nets over all configurations of the distribution of the $\kappa$ points on the $\rho$ lines composing a parallel bundle, assuming that all configurations are equally probable, we obtain the following lower bound on the average value, $\bar{\tau}$, of $\tau$ in a $(\kappa, \tau)$ trapping set:

$$\bar{\tau} \geq (\gamma + 1 - \kappa)\kappa + \kappa(\kappa - 1)/\rho + (\rho/2)[1 - (1 - 2/\rho)^{\kappa}] - \kappa.$$ (9)
VII. TWO-DIMENSIONAL EUCLIDEAN GEOMETRIES

- The two-dimensional Euclidean geometry $\text{EG}(2, q)$ over $\text{GF}(q)$ is a partial geometry $\text{PaG}(q + 1, q, q)$ with $\gamma = q + 1$, $\rho = q$ and $\delta = \gamma - 1 = q$. Hence it is a net.

- $\text{EG}(2, q)$ consists of a set $N$ of $q^2$ points and a set $M$ of $q^2 + q$ lines. Each line consists of $q$ points. Each point is on $q + 1$ lines. Any two points are connected by a unique line. The $q^2 + q$ lines can be partitioned into $q + 1$ parallel bundles, each consisting of $q$ parallel lines.

- A point in $N$ is a two-tuple $a = (a_0, a_1)$ over $\text{GF}(q)$ and the zero two-tuple $(0, 0)$ is called the origin of $\text{EG}(2, q)$. A line in $M$ is a one-dimensional subspace, or its coset, of the vector space of all the $q^2$ two-tuples over $\text{GF}(q)$. 
The field \( GF(q^2) \), as an extension field of \( GF(q) \), is a realization of \( EG(2, q) \) [12], [13], [20].

Let \( \alpha \) be a primitive element of \( GF(q^2) \). Then, the powers of \( \alpha \),

\[
\alpha^{-\infty} = 0, \alpha^0 = 1, \alpha, \alpha^2, ..., \alpha^{q^2-2},
\]

give all the \( q^2 \) elements of \( GF(q^2) \) and they represent the \( q^2 \) points of \( N \). The origin of \( EG(2, q) \) is represented by \( \alpha^{-\infty} \).

Factor \( q^2 - 1 \) as the product of \( q - 1 \) and \( q + 1 \), i.e., \( q^2 - 1 = (q + 1)(q - 1) \). Then the order of the element \( \beta = \alpha^{q+1} \) is \( q - 1 \), i.e., \( \beta^{q-1} = 1 \).
The set

\[ L_{-\infty} = \{ \alpha^{-\infty} = 0, \alpha^0 = 1, \alpha^{q+1}, ..., \alpha^{(q-2)(q+1)} \} \]

of the \( q \) elements in \( \text{GF}(q^2) \), which represent \( q \) points in \( N \), forms a line passing through the origin of \( EG(2, q) \).

For \( 0 \leq j \leq q \), the set

\[ \alpha^j L_{-\infty} = \{ 0, \alpha^j, \alpha^{(q+1)+j}, ..., \alpha^{(q-2)(q+1)+j} \} \]

of \( q \) points also forms a line passing through the origin of \( EG(2, q) \).

Note that \( \alpha^{q+1} L_{-\infty} = L_{-\infty} \). Hence, \( L_{-\infty}, \alpha L_{-\infty}, ..., \alpha^q L_{-\infty} \) form the set \( \Delta(\alpha^{-\infty}) \) of the \( q + 1 \) lines that intersect at the origin of \( EG(2, q) \).
Let $L = \{\alpha^{j_1}, \alpha^{j_2}, \ldots, \alpha^{j_q}\}$ be a line in $M$ not passing through the origin of $\text{EG}(2, q)$ with $\alpha^{j_1}, \alpha^{j_2}, \ldots, \alpha^{j_q}$ 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 $\alpha^i L = \{\alpha^{j_1+i}, \alpha^{j_2+i}, \ldots, \alpha^{j_q+i}\}$. Then, the set $\alpha^i L$ of $q$ points in $N$ also forms a line in $M$ not passing through the origin.

The lines $L, \alpha L, \ldots, \alpha^{q^2-2} L$ give all the $q^2 - 1$ lines in $M$ not passing through the origin of $\text{EG}(2, q)$.
The structure of lines in $M$ developed above is called the *cyclic structure*.

This cyclic structure allows us to construct all the lines in $M$ from two lines, one passing through the origin of $\text{EG}(2, q)$ and the other not passing through the origin.
Let $L$ be a line in $M$. Based on $L$, we define the following $q^2$-tuple over $\mathbb{GF}(2)$,

$$
\mathbf{v}_L = (v_{-\infty}, v_0, v_1, \ldots, v_{q^2-2})
$$

whose components correspond to the $q^2$ points $\alpha^{-\infty}, \alpha^0, \alpha, \alpha^2, \ldots, \alpha^{q^2-2}$ in $N$, where $v_j = 1$ if and only if $\alpha^j$ is a point on $L$ and $v_j = 0$ otherwise.

The weight of $\mathbf{v}_L$ is $q$. This $q^2$-tuple $\mathbf{v}_L$ is called the *incidence vector* of the line $L$. 

Form a $q(q + 1) \times q^2$ matrix $H_{EG}(N, M)$ over GF(2) with the incidence vectors of the lines in $M$ as rows which are arranged in a specific way.

Let $L_{-\infty}$ be a line in $\Delta(\alpha^{-\infty})$ and $L$ be a line in $\Delta(\alpha^{-\infty})^c = M \setminus \Delta(\alpha^{-\infty})$.

We arrange the rows of $H_{EG}(N, M)$ in such a way that the incidence vectors of the lines $L_{-\infty}, \alpha L_{-\infty}, \ldots, \alpha^q L_{-\infty}$, in this order, are the first $q + 1$ rows of $H_{EG}(N, M)$ and the incidence vectors of the lines $L, \alpha L, \ldots, \alpha^{q^2-2} L$, in this order, are the last $q^2 - 1$ rows of $H_{EG}(N, M)$. We label the rows of $H_{EG}(N, M)$ using the lines in $M$ in this specified order.
We label the columns using the points $\alpha^{-\infty}, \alpha^0, \alpha, ..., \alpha^{q^2-2}$ in $N$ in this order. Hence, $H_{EG}(N, M)$ has the form:

$$H_{EG}(N, M) = \begin{bmatrix} H_{EG}(N, \Delta(\alpha^{-\infty})) \\ H_{EG}(N, \Delta(\alpha^{-\infty})^c) \end{bmatrix}. \quad (10)$$

which consists of two submatrices.

It follows from the cyclic structure of the lines in $M$ that: 1) the top submatrix $H_{EG}(N, \Delta(\alpha^{-\infty}))$ 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 $H_{EG}(N, \Delta(\alpha^{-\infty})^c)$ has a column of zeros of length $q^2 - 1$ followed by a $(q^2 - 1) \times (q^2 - 1)$ circulant matrix with both column and row weight equal to $q$. 
The matrix $H_{EG}(N, M)$ 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 $H_{EG}(N, M)$ 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 ensures that $H_{EG}(N, M)$ satisfies the RC-constraint.

From the intersecting structure of lines in $M$, it is clear that, for each column of $H_{EG}(N, M)$ labeled by a point $\alpha^j$ in $N$, there are $q + 1$ rows with 1-component at the position $j$ with $j = -\infty, 0, 1, ..., q^2 - 2$. These $q + 1$ rows are said to be attached to the column labeled $\alpha^j$. These rows simply correspond to the lines in $M$ that intersect at the point $\alpha^j$, i.e., $\Delta(\alpha^j)$.
The null space of $H_{EG}(N, M)$ gives a $(q + 1, q)$-regular EG-LDPC code, denoted by $C_{EG}(N, M)$, of length $q^2$ with minimum distance at least $q + 2$. This code is called a basic EG-LDPC code.

The Tanner graph $G_{EG}$ of $C_{EG}(N, M)$ consists of $q^2$ VNs, each with degree $q + 1$, and $q^2 + q$ CNs, each with degree $q$.

Any two VNs are connected by a path of length 2. Each VN is on $q(q - 1)(q^2 - 1)/2$ cycles of length 6. Hence, the VNs are highly connected. With iterative decoding, this high degree of connectivity provides fast exchange of information between VNs. This fast exchange of information results in fast decoding convergence.
It follows from the bound given by (7) that for a \((\kappa, \tau)\) trapping set in \(G_{EG}\), the number of odd-degree CNs is lower bounded as follows:

\[ \tau \geq (q + 2 - \kappa)\kappa \]  \hspace{1cm} (11)

For \(\kappa < q - 2\), the ratio \(\tau/\kappa \geq 5\). Since \(\sqrt{n} = q\), it follows from Definition 1-3 that the Tanner graph \(G_{EG}\) contains no small trapping set of size less than \(q - 2\) (minimum distance minus 4).

In fact, \(G_{EG}\) contains no trapping set of size at most \(q + 1\) with \(\tau/\kappa < 1\). The trapping set with small \(\kappa\) and \(\tau/\kappa < 1\) are the most probable and harmful ones for iterative decoding.
Since the parity-check matrix $H_{EG}(N, M)$ of a basic EG-LDPC code $C_{EG}(N, M)$ satisfies the RC-constraint, it is one-step majority-logic decodable [55].

For each code symbol of a codeword in $C_{EG}(N, M)$, $q + 1$ orthogonal check-sums 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 $C_{EG}(N, M)$ 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 [55].

From this check-sum, the erased symbol can be recovered. However, if a received word contains more than $q + 1$ erasures, the code may not be able to correct them.

This implies that the size of a smallest stopping set is at least $q + 1$. 
Consider the special case for which $q = 2^s$ where $s$ is a positive integer.

For this case, the rank of $\mathbf{H}_{EG}(N, M)$ is $3^s$ [56], [57].

Consequently, the basic EG-LDPC code $C_{EG}(N, M)$ is a $(4^s, 4^s - 3^s)$ code with minimum distance exactly $2^s + 2$ [58].

For $s > 3$, the parity-check matrix of this code has a large number of redundant rows which is $4^s - 3^s$. This large row redundancy makes iterative decoding of $C_{EG}(N, M)$ converge very fast.
Consider the basic EG-LDPC code constructed based on EG(2, $2^6$).

It is a (65, 64)-regular (4160, 3367) LDPC code with minimum distance exactly 66 whose parity-check matrix $H_{EG}$ is a $4160 \times 4096$ matrix over GF(2) with both column and row weights 65 and 64, respectively.

It follows from (11) that the Tanner graph of this code has no small trapping set of size less than 62.

For $\kappa = 62$, $\tau$ is lower bounded by 248. However, it follows from (9) that the average number of CN’s of odd-degree of a trapping set of size $\kappa = 62$ is 272.62.
The rank of the parity-check matrix $H_{EG}$ of this code is $3^6 = 729$. HEG has 3367 redundant rows.

It has 3431 redundant rows and hence has a very large row redundancy.

This large row redundancy makes the iterative decoding of this code using either the SPA or the MSA converge very fast as shown in Figure 1.

Since the code has a quite large minimum distance and no small trapping sets, its error-floor is expected to be very low.
IX. SHORTENED EG-LDPC CODES

Let $\Lambda$ be a set of $\kappa$ points in $N$. Assume that $\kappa \leq q + 1$. This assumption will be clarified later.

Let $\Phi(\Lambda) = \bigcup_{a \in \Lambda} \Delta(a)$ which is the union of the intersecting bundles of lines in $M$ intersecting at the points in $\Lambda$. $\Phi(\Lambda)$ is the set of lines in $M$, each passing through at least one point in $\Lambda$. If the lines in $\Phi(\Lambda)$ are restricted with respect to $\Lambda$, then $(\Lambda, \Phi(\Lambda))$ form a subgeometry of $\text{EG}(2, q)$ induced by $\Lambda$. If the number of lines in $\Phi(\Lambda)$ that contain odd number of points in $\Lambda$ is $\tau$. Then $(\Lambda, \Phi(\Lambda))$ is a geometrical representation of a $(\kappa, \tau)$ trapping set in the Tanner graph $G_{EG}$ of basic EG-LDPC code $C_{EG}(N, M)$. 
Let $\Lambda^c = N \setminus \Lambda$ and $\Phi(\Lambda)^c = M \setminus \Phi(\Lambda)$.

If we delete all the points in $\Lambda$ and all lines in $\Phi(\Lambda)$ from $\text{EG}(2, q)$, we obtain a residual geometry, denoted $(\Lambda^c, \Phi(\Lambda)^c)$.

The incidence matrix of this residual geometry is the matrix, denoted by $H_{EG}(\Lambda^c, \Phi(\Lambda)^c)$, which can be obtained from the basic matrix $H_{EG}(N, M)$ by deleting all the columns labeled by points in $\Lambda$ and all the rows attached to these columns, i.e., labeled by lines in $\Phi(\Lambda)$.

The matrix $H_{EG}(\Lambda^c, \Phi(\Lambda)^c)$ is a $(q^2 + q - |\Phi(\Lambda)|) \times (q^2 - \kappa)$ submatrix of the basic EG-matrix $H_{EG}(N, M)$. It satisfies the RC-constraint.
It follows from the intersecting structure of lines in $M$ that, deleting a column that corresponds to a point $a$ in $\Lambda$ and the $q + 1$ rows attached to it from $H_{EG}(N, M)$ reduces the weight of each column of $H_{EG}(N, M)$ that corresponds to a point in $\Lambda^c$ by one.

Since the intersecting bundles at the points in $\Lambda$ have common lines, the reductions of weights for the columns in $H_{EG}(N, M)$ corresponding to the $q^2 - \kappa$ points in $\Lambda^c$ may be different. However, the maximum column weight reduction is $\kappa$. Hence, the minimum column weight of the punctured matrix $H_{EG}(\Lambda^c, \Phi(\Lambda)^c)$ is $q + 1 - \kappa$. 
The null space of the punctured matrix $H_{EG}(\Lambda^c, \Phi(\Lambda)^c)$ gives a shortened EG-LDPC code, denoted by $C_{EG}(\Lambda^c, \Phi(\Lambda)^c)$, of length $q^2 - \kappa$ with minimum distance at least $q + 2 - \kappa$.

For $\kappa = 1, 2, \ldots, q + 1$, we can construct a sequence of shortened codes of $C_{EG}(\Lambda^c, \Phi(\Lambda)^c)$ with different rates and minimum distances.

Let $R_{EG}(\Lambda^c, \Phi(\Lambda)^c)$ denote the number of rows in the punctured matrix $H_{EG}(\Lambda^c, \Phi(\Lambda)^c)$. It can be proved that $R_{EG}(\Lambda^c, \Phi(\Lambda)^c)$ is lower bounded as following:

$$R_{EG}(\Lambda^c, \Phi(\Lambda)^c) \geq q^2 - (\kappa - 1)q - 1. \quad (12)$$
The equality of (12) holds if the $\kappa$ points in $\Lambda$ are collinear. In this case, $H_{EG}(\Lambda^c, \Phi(\Lambda)^c)$ has the smallest number of rows.

If $\kappa = q$ and the $q$ points in $\Lambda$ form a line in $EG(2, q)$, then $R_{EG}(\Lambda^c, \Phi(\Lambda)^c) = q - 1$.

For $\kappa = q + 1$, $H_{EG}(\Lambda^c, \Phi(\Lambda)^c)$ may be a null matrix. That is why we restrict the size of $\Lambda$ no greater than $q + 1$ at the beginning of this section.

Shortened EG-LDPC codes also perform well with various iterative decoding algorithms.
A basic EG-LDPC code together with its shortened codes can be used to correct combinations of random errors and erasures using a two-phase decoding algorithm.
Cyclic EG-LDPC codes

For the case that \( \Lambda = \{\alpha^{-\infty}\} \), the punctured matrix \( H_{EG}(\{\alpha^{-\infty}\}^c, \Delta(\alpha^{-\infty})^c) \) is a \((q^2 - 1) \times (q^2 - 1)\) circulant matrix obtained by deleting from the basic matrix \( H_{EG}(N, M) \) the column labeled by the origin point \( \alpha^{-\infty} \) of \( \text{EG}(2, q) \) and the rows attached to it. The column and row weights of this circulant matrix are both equal to \( q \).

The null space of \( H_{EG}(\{\alpha^{-\infty}\}^c, \Delta(\alpha^{-\infty})^c) \) gives a cyclic EG-LDPC code, denoted \( C_{EG}(\{\alpha^{-\infty}\}^c, \Delta(\alpha^{-\infty})^c) \), with minimum distance at least \( q + 1 \).

Cyclic EG-LDPC codes were discovered by Kou, Lin and Fossorier in 2001 [2].
The circulant parity-check matrix \( H_{EG}(\{\alpha^{-\infty}\}^c, \Delta(\alpha^{-\infty})^c) \) of the cyclic EG-LDPC code \( C_{EG}(\{\alpha^{-\infty}\}^c, \Delta(\alpha^{-\infty})^c) \) can be put into a \((q + 1) \times (q + 1)\) array of circulant permutation matrices (CPMs) and zero matrices (ZMs) of size \((q - 1) \times (q - 1)\), denoted by \( H_{EG,qc}(\{\alpha^{-\infty}\}^c, \Delta(\alpha^{-\infty})^c) \), where the second subscript ”qc” of \( H_{EG,qc}(\{\alpha^{-\infty}\}^c, \Delta(\alpha^{-\infty})^c) \) stands for ”quasi-cyclic”.

Each row (or column) block of \( H_{EG,qc}(\{\alpha^{-\infty}\}^c, \Delta(\alpha^{-\infty})^c) \) consists of \( q \) CPMs and one ZM.

The null space of \( H_{EG,qc}(\{\alpha^{-\infty}\}^c, \Delta(\alpha^{-\infty})^c) \) gives a quasi-cyclic (QC) EG-LDPC code \( C_{EG,qc}(\alpha^{-\infty}^c, \Delta(\alpha^{-\infty})^c) \) which is combinatorially equivalent to the cyclic EG-LDPC Code \( C_{EG,qc}(\alpha^{-\infty}^c, \Delta(\alpha^{-\infty})^c) \).
Let $t$ and $u$ be two positive integers such that $1 \leq t, u \leq q + 1$. Let $H_{EG, qc}(t, u)$ be a $t \times u$ subarray of $H_{EG, qc}(\{\alpha^{-\infty}\}^c, \Delta(\alpha^{-\infty})^c)$.

$H_{EG, qc}(t, u)$ is a $t(q - 1) \times u(q - 1)$ matrix.

The null space of $H_{EG, qc}(t, u)$ gives a QC-EG-LDPC code of length $u(q - 1)$.

Different choices of $t$ and $u$ result in QC-EG-LDPC codes of various lengths and rates.
These decoding algorithms provide a wide spectrum of trade-off between error performance and decoding complexity.

Cyclic and QC-EG-LDPC codes not only can achieve very low error rates close to the Shannon limit with the SPA, the MSA and the RID but also have encoding and decoding implementation advantages.
IX. Remarks

- Many constructions of LDPC codes based on finite fields and combinatorial designs can be viewed from geometrical point of view. Consequently, their trapping set structure can be analyzed geometrically.

- Algebraic LDPC codes constructed based on finite fields and combinatorial designs can be shortened in a similar way as that for the basic EG-LDPC codes. These codes and their shortened codes can be used for correcting combinations of random errors and erasures.

- A generalized quadrangle is a special case of partial geometry. Hence, it can be used for construction of LDPC codes.
REFERENCES


