A Finite Field Construction of QC-LDPC Codes Free of Small Size Elementary Trapping Sets

Daniel Panario
School of Mathematics and Statistics
Carleton University
daniel@math.carleton.ca

Joint work with Farzane Amirzade (Shahrood University of Technology) and Mohammad-Reza Sadeghi (Amirkabir University of Technology)

30th CCC – Feb 14, 2019

Introduction

LDPC codes

A low-density parity-check (LDPC) code is a linear code whose parity-check matrix is sparse.

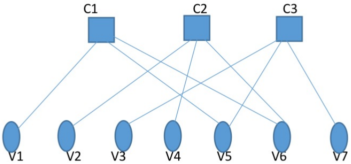
Quasi-cyclic low-density parity-check codes (QC-LDPC codes) are an essential category of LDPC codes that have simple implementation and favorable performance.

Tanner graph

A Tanner graph is a bipartite graph with vertex sets formed by the set of variable nodes (VNs) and the set of check nodes (CNs). The adjacency matrix of the Tanner graph is the parity-check matrix of the code.

Example

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$



Tanner graph

A Tanner graph is an important representation of a code. The girth, that is, the length of the shortest cycles of the Tanner graph, has been known (experimentally) to influence the code performance.

Since Tanner graphs with short cycles do not produce good results, constructions which lead to the existence of 4-cycles in their Tanner graphs are avoided. Indeed, in almost all of the algebraic-based constructions known the Tanner graph has girth at least 6.

If for each variable node v and each check node c we have $\deg(v) = m$ and $\deg(c) = n$, then the Tanner graph gives an (m, n)-regular LDPC code.

We are interested in sparse regular QC-LDPC codes with girth at least 6.

Trapping sets

Another phenomenon that significantly influences the performance of LDPC codes are trapping sets.

Trapping set

An (a, b) trapping set of size a is an induced subgraph of the Tanner graph on a variable nodes and b check nodes of odd degrees, called the unsatisfied check nodes. The even degree check nodes are satisfied check nodes.

Empirical results in the literature show that among all trapping sets, the most harmful ones are those with check nodes of degree 1 or 2. These are called elementary trapping set (ETS)

Elementary trapping sets

Elementary trapping set

A trapping set with check nodes of degree 1 or 2 is called an elementary trapping set (ETS).

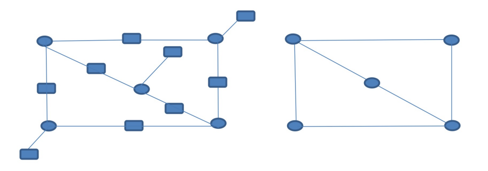
All unsatisfied check nodes in an ETS have degree 1.

Variable Node graph

In an (a, b) ETS, by removing all 1-degree check nodes and replacing every 2-degree check node with an edge, we obtain a graph with a vertices: the Variable Node (VN) graph.

Example

Suppose $m = 3$. We denote variable nodes with circles and check nodes with squares. We depict a (5,3) ETS and its corresponding VN graph:



In a Tanner graph with girth at least 8, the VN graph of each ETS is a triangle-free graph. For example, in the above example the ETS contains no 6-cycles and its corresponding VN graph is triangle-free.

Quasi-cyclic LDPC codes

Quasi-cyclic LDPC codes

Let N be a positive integer. Consider the following exponent matrix $B = [b_{ij}]$, where $b_{ij} \in \{0, 1, \ldots, N-1\}$ or $b_{ij} = \infty$,

$$B = \begin{bmatrix} b_{\mathbf{00}} & b_{\mathbf{01}} & \cdots & b_{\mathbf{0}(n-\mathbf{1})} \\ b_{\mathbf{10}} & b_{\mathbf{11}} & \cdots & b_{\mathbf{1}(n-\mathbf{1})} \\ \vdots & \vdots & \ddots & \vdots \\ b_{(m-\mathbf{1})\mathbf{0}} & b_{(m-\mathbf{1})\mathbf{1}} & \cdots & b_{(m-\mathbf{1})(n-\mathbf{1})} \end{bmatrix}. \tag{1}$$

We replace $b_{ij} \neq \infty$ by the $N \times N$ circulant permutation matrix (CPM) such that the nonzero 1-component of the top row is in the b_{ij}-th position. Elements $b_{ij} = \infty$ are replaced by the $N \times N$ zero matrix.

The null space of this parity-check matrix gives a QC-LDPC code.
If B contains no ∞, then we have a fully connected QC-LDPC code.

Our results

We give an algebraic construction of QC-LDPC codes with column weight 3 and girth 6 whose Tanner graphs are free of small ETSs.

First, we present a new construction for the exponent matrix of QC-LDPC codes with girth at least 6 based on multiplicative cyclic subgroups of the finite field $\mathbb{F}_q$.

Then, we give a submatrix of the exponent matrix where we can prove that its Tanner graph is free of $(4, 0)$ and $(4, 2)$ ETSs.

Finally, we show that the Tanner graph of a fully connected $(3, n)$-regular QC-LDPC code with girth 6 has no $(5, 1)$ ETS.

Consider a fully connected QC-LDPC code with column weight 3.

Every vertex of a VN graph corresponds to a column of B and each edge of a VN graph corresponds to a row of B.

Example

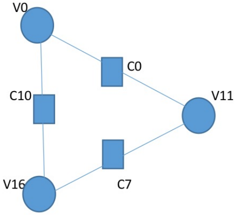
Let an exponent matrix B with $N = 5$ and row indices u, v, w:

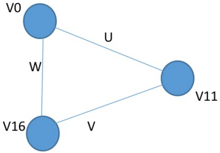
$$B = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 3 & 4 \\ 0 & 3 & 2 & 1 \end{bmatrix}.$$

In the parity-check matrix H, a 6-cycle with variable nodes v_0, v_{10}, v_{16}, v_0 and check nodes c_0, c_7, c_{10} have 3 labels u, v, w as their indices (see the next figure). Also, the edges of the VN graph are colored by these 3 labels.

$$N = 5, \quad B = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 3 & 4 \\ 0 & 3 & 2 & 1 \end{bmatrix},$$

$$H = \left[\begin{array}{c|c|c|c}
1_{u}.... & 1.... & 1_{u}.... & 1.... \\
.1... & .1... & .1... & .1... \\
..1.. & ..1.. & ..1.. & ..1.. \\
...1. & ...1. & ...1. & ...1. \\
....1 & ....1 & ....1 & ....1 \\
1.... & ..1.. & ...1. & ....1 \\
.1... & ...1. & ....1 & 1.... \\
..1.. & ....1 & 1_{v}.... & .1_{v}... \\
...1. & 1.... & .1... & ..1.. \\
....1 & .1... & ..1.. & ...1. \\
1_{w}.... & ...1. & ..1.. & .1_{w}... \\
.1... & ....1 & ...1. & ..1.. \\
..1.. & 1.... & ....1 & ...1. \\
...1. & .1... & 1.... & ....1 \\
....1 & ..1.. & .1... & 1....
\end{array}\right].$$


V0
C0
C10
V11
V16
C7


V0
U
W
V11
V16
V

Q. Huang, Q. Diao, S. Lin, K. Abdel-Ghaffar, IEEE Int. Symp. Inform. Theory (ISIT) (2011)

The (a, b) ETSs that cause high decoding failure rates and exert a strong influence on the error floor are those with $\frac{b}{a} < 1$.

Q. Huang, Q. Diao, S. Lin, K. Abdel-Ghaffar, IEEE Int. Symp. Inform. Theory (ISIT) (2011)

In an LDPC code with column weight m, the lower bound on the size of an ETS with $\frac{b}{a} < 1$ is $m + 1$.

F. Amirzade and M.-R. Sadeghi, IEEE Trans. Commun. (2018)

The VN graph of an (a, b) ETS with column weight m has the conditions:

- If a is an even number, then b is also an even number.
- If a is an odd number, then parameters m and b both are even or odd.

- The (a, b) ETSs with $\frac{b}{a} < 1$ in the Tanner graph of an LDPC code with girth 6 and column weight 3 are $(4, 0), (4, 2), (5, 1), (5, 3), (6, 0), (6, 2), (6, 4)$ ETSs and so on.

- In a fully connected QC-LDPC code with girth 6 and column weight 3, the Tanner graph contains (a, b) ETSs with $\frac{b}{a} < 1$ like $(4, 0), (4, 2), (5, 1), (5, 3)$ ETSs and so on.

We show that the Tanner graph of a fully connected QC-LDPC code with girth 6 and column weight 3 contains no $(5, 1)$ ETS.

Next we construct fully connected QC-LDPC codes with girth 6 and column weight 3 whose Tanner graphs are also free of $(4, 0)$ and $(4, 2)$ ETSs.

Our construction holds for q a prime power such that $q - 1 = d_1 d_2 \dots d_\ell$, where for $i, j \in \{1, 2, \dots, \ell\}$, $i \neq j$, we have $\gcd(d_i, d_j) = 1$. In this talk we show it for 3 factors only, $q - 1 = abc$.

Consider finite field $\mathbb{F}_q$ such that $q - 1 = abc$, where a, b and c are pairwise relatively prime, and let α be a primitive element of $\mathbb{F}_q$.

Consider the following three cyclic subgroups of $\mathbb{F}_q^*$:

$$\begin{aligned} G_1 &= \{\delta^0 = 1, \delta, \delta^2, \ldots, \delta^{a-1}\}; \quad \delta = \alpha^{bc}; \\ G_2 &= \{\beta^0 = 1, \beta, \beta^2, \ldots, \beta^{b-1}\}; \quad \beta = \alpha^{ac}; \\ G_3 &= \{\gamma^0 = 1, \gamma, \gamma^2, \ldots, \gamma^{c-1}\}; \quad \gamma = \alpha^{ab}. \end{aligned}$$

For $0 \le k < c$, build the following $a \times b$ matrix W_k:

$$W_k = \begin{bmatrix} \delta^0\beta^0 - \gamma^k & \delta^0\beta^1 - \gamma^k & \ldots & \delta^0\beta^{b-1} - \gamma^k \\ \delta^1\beta^0 - \gamma^k & \delta^1\beta^1 - \gamma^k & \ldots & \delta^1\beta^{b-1} - \gamma^k \\ \vdots & \vdots & \ddots & \vdots \\ \delta^{a-1}\beta^0 - \gamma^k & \delta^{a-1}\beta^1 - \gamma^k & \ldots & \delta^{a-1}\beta^{b-1} - \gamma^k \end{bmatrix}.$$

Then, $B = [W_0 \ W_1 \ W_2 \cdots W_{c-1}]$ is our exponent matrix with $N = q - 1$.

Example

Consider the finite field $\mathbb{F}_{31}$ and $\alpha = 3$ a primitive element. We factor $31 - 1 = 30$ as the product of $2 \times 3 \times 5$. Set $a = 3$, $b = 2$ and $c = 5$. Form three cyclic subgroups of the multiplicative group of $\mathbb{F}_{31}$, $G_1 = \{\delta^0, \delta^1, \delta^2\}$, $G_2 = \{\beta^0, \beta^1\}$ and $G_3 = \{\gamma^0, \gamma^1, \gamma^2, \gamma^3, \gamma^4\}$. To clarify the construction we, first, form W_0:

$$W_0 = \begin{bmatrix} \delta^0\beta^0 - \gamma^0 & \delta^0\beta^1 - \gamma^0 \\ \delta^1\beta^0 - \gamma^0 & \delta^1\beta^1 - \gamma^0 \\ \delta^2\beta^0 - \gamma^0 & \delta^2\beta^1 - \gamma^0 \end{bmatrix} = \begin{bmatrix} 0 & \alpha^{15} - 1 \\ \alpha^{10} - 1 & \alpha^{25} - 1 \\ \alpha^{20} - 1 & \alpha^{5} - 1 \end{bmatrix}$$

Since $\alpha = 3$, in $\mathbb{F}_{31}$ we have $\alpha^{10} - 1 = \alpha^{13}, \alpha^{20} - 1 = \alpha^{18}$, $\alpha^{15} - 1 = \alpha^{9}, \alpha^{25} - 1 = \alpha^{20}$ and $\alpha^{35} - 1 = \alpha^{10}$. Then

$$W_0 = \begin{bmatrix} 0 & \alpha^{9} \\ \alpha^{13} & \alpha^{20} \\ \alpha^{18} & \alpha^{10} \end{bmatrix}.$$

Example (cont.)

After obtaining all W_ks, where $0 \leq k < 5$, and concatenating them in a matrix we achieve the following exponent matrix

$$B = \begin{bmatrix} 0 & \alpha^9 & \alpha^6 & \alpha^{22} & \alpha^{13} & \alpha^{17} & \alpha^{16} & \alpha^5 & \alpha^{15} & \alpha^{16} \\ \alpha^{13} & \alpha^{20} & \alpha^2 & \alpha^{29} & \alpha^7 & \alpha^9 & \alpha^{29} & \alpha^{24} & \alpha^{27} & \alpha^{18} \\ \alpha^{18} & \alpha^{10} & \alpha^8 & \alpha^{14} & \alpha^{16} & \alpha^{26} & \alpha^{30} & \alpha^{17} & \alpha^1 & \alpha^{13} \end{bmatrix}.$$

If we substitute all nonzero elements of B by CPMs and the zero element by the ZM then the null space of the resulting parity-check matrix gives a QC-LDPC code with length 300.

We want to guarantee girth at least 6, and we want to remove small ETS's.

J. Li, K. Liu, S. Lin and K. Abdel-Ghaffar
IEEE Trans. Commun. (2014)

Let B be the exponent matrix of a QC-LDPC code. A necessary and sufficient condition for the Tanner graph to have girth at least 6 is that every 2×2 submatrix in the exponent matrix B contains at least one zero entry or is non-singular.

Using this result we then prove our girth result.

Theorem

There is no singular 2 by 2 matrix in the exponent matrix B. The Tanner graph corresponding to the exponent matrix $B = [W_0 \ W_1 \ W_2 \cdots W_{c-1}]$ has girth at least 6.

Theorem

Let B' be a $3 \times n$ submatrix of the exponent matrix B.

If B' satisfies the following conditions, then B' results in a fully connected $(3, n)$-regular QC-LDPC code with girth 6 whose Tanner graph is free of $(4, 0)$ and $(4, 2)$ ETSs:

I) if α^d is the determinant of a 2×2 submatrix of B', then $2d \not\equiv 0 \pmod{q-1}$;

II) if α^d and $\alpha^{d'}$ are the determinants of two 2×2 submatrices of B' with same row indices, then $d \not\equiv d' \pmod{q-1}$.

Example

Consider the finite field $\mathbb{F}_{2^8}$. We factor $2^8 - 1 = 255 = (3)(5)(17)$. Set $a = 5$, $b = 3$ and $c = 17$. If we take $i \in \{0, 1, 2\}$, $j = 0$ and $k \in \{1, \dots, 9\}$, then the submatrix B' of the exponent matrix B constructs a $(3, 9)$-regular QC-LDPC code with length 2295, dimension 1530, girth 6 and free of $(4, 0)$ and $(4, 2)$ ETSs:

$$\begin{bmatrix} \alpha^{33} & \alpha^{66} & \alpha^{31} & \alpha^{132} & \alpha^{199} & \alpha^{62} & \alpha^{248} & \alpha^{9} & \alpha^{144} \\ \alpha^{240} & \alpha^{40} & \alpha^{236} & \alpha^{171} & \alpha^{50} & \alpha^{157} & \alpha^{4} & \alpha^{181} & \alpha^{91} \\ \alpha^{182} & \alpha^{225} & \alpha^{128} & \alpha^{80} & \alpha^{179} & \alpha^{217} & \alpha^{70} & \alpha^{87} & \alpha^{117} \end{bmatrix}.$$

To find B', we apply the previous theorem and the two conditions to a computer-based search algorithm to search for all $3 \times n$ submatrices of B which result in $(3, n)$-regular QC-LDPC codes with girth 6 and free of $(4, 0)$ and $(4, 2)$ ETSs.

Conclusions and further work

We provide a new algebraic construction of QC-LDPC codes whose Tanner graph has girth at least 6 based on multiplicative cyclic subgroups of a finite field. Then, we give conditions for an exponent matrix to have a Tanner graph which is free of $(4, 0)$ and $(4, 2)$ ETSs. We also prove that the Tanner graphs of fully connected $(3, n)$-regular QC-LDPCs contain no $(5, 1)$ ETS.

Further work:

- Give necessary conditions to have girth 8 Tanner graphs.
- Provide an analytical rank for the parity-check matrix.
- Initial experiments look promising. Compare with other methods for fully connected $(3, n)$-regular QC-LDPC codes with girth 6.