On some LDPC codes

Marina Šimac (msimac@math.uniri.hr)

(a joint work with Dean Crnković and Sanja Rukavina)

Department of Mathematics, University of Rijeka, Croatia

This work has been fully supported by Croatian Science Foundation under the project 6732.

Combinatorial Designs and Codes 2021

July 15, 2021

Outline of the Talk

- Introduction
- LDPC codes constructed from cubic semisymmetric graphs
- Computational and simulation results

D. Crnković, S. Rukavina, M. Šimac, LDPC codes from cubic semisymmetric graphs, submitted

D. Crnković, S. Rukavina, M. Šimac, LDPC codes constructed from cubic symmetric graphs, Appl. Algebra Engrg. Comm. Comput. (2020), https://doi.org/10.1007/s00200-020-00468-2

Introduction

Definition

A $[n,k]$ **linear code** $\mathcal{C}$ is a k-linear subspace of the vector space $\mathbb{F}_q^n$. When $q=2$, we say that $\mathcal{C}$ is a **binary linear** code.

Definition

The Hamming distance between two vectors $x,y \in \mathbb{F}_q^n$:

$$d(x,y) = |\{i \mid x_i \neq y_i,\ 1 \leq i \leq n\}|.$$

The minimum distance of a code $\mathcal{C}$:

$$d = min\{d(x,y) : x,y \in \mathcal{C}\}$$

An $[n,k]$ linear code with minimum distance d will be denoted by $[n,k,d]$ code.

Definition

Given a linear $[n, k]$ code C, a **generator matrix** G of C is a $k \times n$ matrix whose rows form a basis for a linear code.

Definition

The **dual code** of a linear code $C \subset \mathbb{F}_q^n$ is the code $C^\perp \subset \mathbb{F}_q^n$ where

$$C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot y = 0, \ \forall y \in C\}.$$

Definition

A **parity-check matrix** H of a linear code C is a generator matrix of its dual code.

$$x \in C \ \Leftrightarrow \ H \cdot x^T = 0$$

LDPC codes

Definition

A binary low-density parity-check (LDPC) code is a binary linear code defined by a sparse parity-check matrix H.
An LDPC code is called $(w_c, w_r)-$**regular** if H has constant row sum w_r and constant column sum w_c. Otherwise it is called an **irregular LDPC code**.

Example

(2,3)-regular LDPC code:

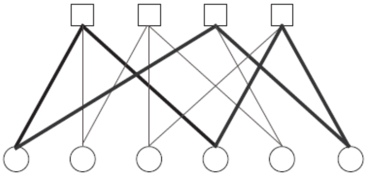
$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Tanner graph

The Tanner graph is a bipartite graph that consists of two sets of vertices: bit nodes that correspond to codeword bits and check nodes that correspond to parity-check equations.
An edge connects a bit node to a check node if that bit is included in the corresponding parity-check equation.

Example

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



Aim is to construct LDPC codes **without** short cycles, especially cycles of length four!

LDPC codes constructed from cubic semisymmetric graphs

Definition

Cubic graphs are 3-regular graphs.
A graph is **semisymmetric** if it is edge-transitive, but not vertex-transitive.
Cubic semisymmetric graphs (CSSG) are 3-regular semisymmetric graphs.

Remark

Every semisymmetric graph is necessarily bipartite with two parts of equal size.

M. Conder, A. Malnič, D Marušič, P. Potočnik, A census of semisymmetric cubic graphs on up to 768 vertices, J. Algebraic Combin. 23 (2006), 255–294.

Let $\mathcal{G}$ be a connected CSSG with $2n$ vertices. Denote by A its adjacency matrix.

$$A = \begin{bmatrix} 0 & H \\ H^T & 0 \end{bmatrix}.$$

The matrices H, H^T $\Rightarrow$ parity-check matrices of the codes $\mathcal{C}_H(\mathcal{G})$, $\mathcal{C}_{H^T}(\mathcal{G})$.

$\Rightarrow$ for the constructed codes, the cubic semisymmetric graph $\mathcal{G}$ is its Tanner graph.

Codes $\mathcal{C}_H(\mathcal{G})$, $\mathcal{C}_{H^T}(\mathcal{G})$:

- $(3,3)$-regular LDPC codes of length n and dimension $n - rank_2(H)$
- the minimum distance of the codes is an even number

Definition

Let H be $n \times n$ parity-check matrix of the code $\mathcal{C}_H(\mathcal{G})$.

- **The bit node graph** Γ_b: n vertices that correspond to codeword bits, and two vertices are adjacent if and only if the corresponding bits are included in the same parity-check equation.
- **The check node graph** Γ_c: n vertices that correspond to parity-check equations, and two vertices are adjacent if and only if corresponding parity-check equations have a bit in common.

Theorem

Let $\mathcal{G}$ be a connected cubic semisymmetric graph with girth at least six and let H be the parity-check matrix of the code $\mathcal{C}_H(\mathcal{G})$. Then the corresponding bit node graph Γ_b and check node graph Γ_c are 6-regular.

Theorem

Let $\mathcal{G}$ be a connected cubic semisymmetric graph with $2n$ vertices and girth at least six. Further, let H be the parity-check matrix of the code $\mathcal{C}_H(\mathcal{G})$ and let Γ_b and Γ_c be the corresponding bit node graph and check node graph, respectively. Matrices T_b and T_c are square $(0,1)$-matrices of order n satisfying $T_b = H^T H - 3I$ and $T_c = HH^T - 3I$ if and only if T_b and T_c are the adjacency matrices of the graphs Γ_b and Γ_c, respectively.

Theorem

Let $\mathcal{G}$ be a connected cubic semisymmetric graph with girth greater than six. Further, let $\mathcal{C}_H(\mathcal{G})$ be the corresponding LDPC code and let Γ_b and Γ_c be its bit node and check node graph, respectively. Then $\omega(\Gamma_b) = \omega(\Gamma_c) = 3$.

Theorem

Let $\mathcal{G}$ be a connected cubic semisymmetric graph with girth greater than six. Let $d(\mathcal{C}_H(\mathcal{G}))$ and $d(\mathcal{C}_H^T(\mathcal{G}))$ be the minimum distances of the codes $\mathcal{C}_H(\mathcal{G})$ and $\mathcal{C}_{H^T}(\mathcal{G})$, respectively. Then $d(\mathcal{C}_H(\mathcal{G})) \geq 6$ and $d(\mathcal{C}_H^T(\mathcal{G})) \geq 6$.

Theorem

Let $\mathcal{G}$ be a connected cubic semisymmetric graph with $2n$ vertices and girth greater than six. Let λ_2 be the second largest eigenvalue of its adjacency matrix A. Let $d(\mathcal{C}_H(\mathcal{G}))$ and $d(\mathcal{C}_H^T(\mathcal{G}))$ be the minimum distances of the codes $\mathcal{C}_H(\mathcal{G})$ and $\mathcal{C}_{H^T}(\mathcal{G})$, respectively. Then the following inequalities hold

$$d \geq \begin{cases} \frac{2}{5}n, & \lambda_2 \leq 2, \\ \frac{2}{9}n, & 2 < \lambda_2 \leq \sqrt{6}, \\ 6, & \sqrt{6} < \lambda_2 < 3, \end{cases}$$

where $d \in \{d(\mathcal{C}_H(\mathcal{G})), d(\mathcal{C}_H^T(\mathcal{G}))\}$.

Theorem

Let $\mathcal{G}$ be a connected cubic semisymmetric graph with $2n$ vertices. Then the dimension of the codes $\mathcal{C}_H(\mathcal{G})$ and $\mathcal{C}_{H^T}(\mathcal{G})$ is at most $n - 2\alpha(\Gamma_b) + 1$, where $\alpha(\Gamma_b)$ is the independence number of the bit node graph Γ_b.

Absorbing sets

Definition

Let $G = G(C)$ be the Tanner graph of an LDPC code C which is determined with a parity check matrix H.
A (κ, τ) **trapping set** is a subset T that consist of κ bit nodes with the property that induced subgraph $G[T]$ has exactly τ check nodes of odd degree.
If every bit node in $G[T]$ is connected with fewer check nodes of odd degree than check nodes of even degree, T forms a trapping set which is called **absorbing set**.

Theorem

Let the Tanner graph of the LDPC code $\mathcal{C}_H(\mathcal{G})$ be a connected cubic semisymmetric graph $\mathcal{G}$ with girth at least six. Then there is no absorbing set of size smaller than three in the graph $\mathcal{G}$.

Theorem

Let $\mathcal{G}$ be a connected cubic semisymmetric graph with girth greater than six, which is the Tanner graph of the LDPC codes $\mathcal{C}_H(\mathcal{G})$ and $\mathcal{C}_{H^T}(\mathcal{G})$. The Tanner graph $\mathcal{G}$ has no absorbing set of size three.

Theorem

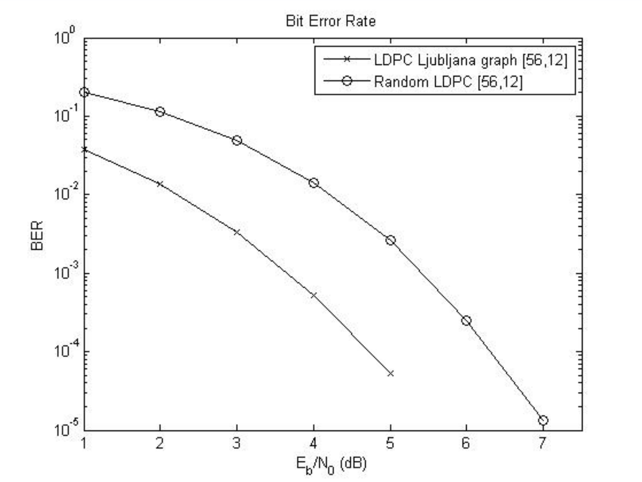
Let $\mathcal{G}$ be a connected cubic semisymmetric graph with girth greater than six, which is the Tanner graph of the LDPC codes $\mathcal{C}_H(\mathcal{G})$ and $\mathcal{C}_{H^T}(\mathcal{G})$. The only possible structure for an absorbing set of size four is $(4,4)$-absorbing set.

Results

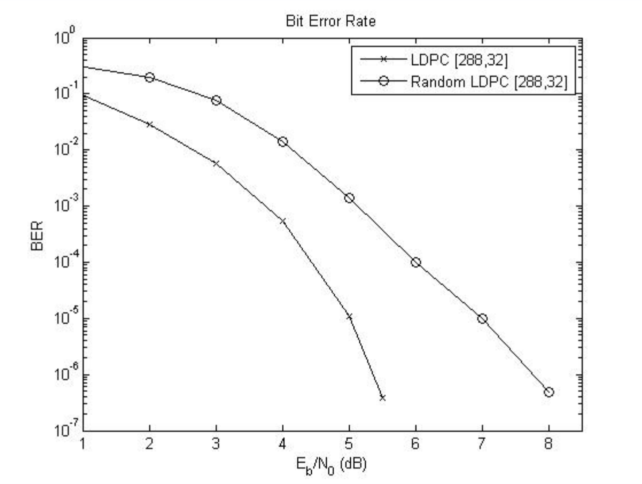
v	$\mathbf{LDPC}_1$	$\mathbf{LDPC}_2$	v	$\mathbf{LDPC}_1$	$\mathbf{LDPC}_2$
54	$[27, 8, 6]$	$[27, 8, 8]^*$	448	$[224, 33, 32]$	**[224,33,32]**
112	$[56, 12, 14]$	**[56,12,16]**	486	$[243, 2, 162]^*$	$[243, 2, 162]^*$
120	$[60, 14, 8]$	**[60,14,12]**	546	$[273, 5, 130]$	$[273, 5, 130]$
144	$[72, 16, 12]^*$	$[72, 16, 14]^*$	576	$[288, 32, 48]$	$[288, 32, 56]$
216	$[108, 16, 24]$	$[108, 16, 32]$	672	$[336, 47, 14]$	$[336, 47, 42]$
240	$[120, 22, 16]$	$[120, 22, 24]$	702	$[351, 8, 78]$	$[351, 8, 104]^*$
294	$[147, 26, 14]$	$[147, 26, 26]$	720	**[360,10,120]**	**[360,10,120]**
336	$[168, 24, 14]$	$[168, 24, 42]$	784	$[392, 12, 98]$	**[392,12,112]**
378	$[189, 11, 42]$	$[189, 11, 56]$	798	$[399, 5, 190]$	$[399, 5, 190]$
384	$[192, 35, 16]$	$[192, 35, 18]$	864	$[432, 32, 96]$	$[432, 32, 108]$
400	**[200,24,32]**	**[200,24,60]**	882	$[441, 44, 42]$	$[441, 44, 78]$
432	$[216, 24, 48]$	$[216, 24, 60]$	896	$[448, 48, 84]$	**[448,48,100]**

Table: The parameters of LDPC codes constructed from cubic semisymmetric graphs with less than 1000 vertices.

BER performance of the $[56, 12, 16]$ LDPC code derived from the Ljubljana graph



BER performance of the $[288, 32, 56]$ LDPC code derived from the cubic semisymmetric graph with 576 vertices



Thank you for your attention!