LDPC codes from cubic semisymmetric graphs[*]

Dean Crnković [ID], Sanja Rukavina [ID], Marina Šimac [†] [ID]

Department of Mathematics, University of Rijeka,
Radmile Matejčić 2, 51000 Rijeka, Croatia

Abstract

In this paper we study LDPC codes having cubic semisymmetric graphs as their Tanner graphs. We discuss the structure of the smallest absorbing sets of these LDPC codes. Further, we give the expression for the variance of the syndrome weight of the constructed codes, and present computational and simulation results.

Keywords: LDPC code, cubic graph, semisymmetric graph.

Math. Subj. Class. (2020): 94B05, 05C99

1   Introduction and preliminaries

Throughout this paper we assume graphs to be finite, simple and connected. For the concepts and notation related to the graph theory and coding theory, we refer the reader to [10] and [15], respectively.

In this paper we use cubic semisymmetric graphs for the construction of LDPC codes. A graph is called a 3-regular graph, i.e. a cubic graph, if every vertex of the graph has the degree equal to three. A graph is edge-transitive (vertex-transitive) if its automorphism group acts transitively on the set of edges (set of vertices). A regular graph is semisymmetric if it is edge-transitive, but not vertex-transitive. It has been proved that every semisymmetric graph is necessarily bipartite with two parts of equal size (see [14]).

Semisymmetric graphs were first studied by Folkman in 1967 (see [12]). He proposed a construction of semisymmetric graphs and constructed the smallest semisymmetric graph with 20 vertices and 40 edges (the Folkman graph). Furthermore, it has been proved that there are no semisymmetric graphs with $2p$ or $2p^2$ vertices for a prime number p.

---

[*]This work has been fully supported by Croatian Science Foundation under the project 6732.
[†]Corresponding author.
    E-mail addresses: deanc@math.uniri.hr (Dean Crnković), sanjar@math.uniri.hr (Sanja Rukavina), msimac@math.uniri.hr (Marina Šimac)

A cubic semisymmetric graph is a 3-regular graph which is semisymmetric. A construction of cubic semisymmetric graphs and the (non)existence of graphs with a certain number of vertices have been a subject of many studies. For example, in [20], the existence of the unique cubic semisymmetric graph with $2p^3$ vertices for a prime number p, the Gray graph of order 54, was proved. In [11], the condition for the existence of cubic semisymmetric graphs with $6p^3$ vertices was given, and a construction of such graphs was described. The classification of cubic semisymmetric graphs with at most 768 vertices was given in [4]. All of the listed graphs have girth at least eight.

The dual code $\mathcal{C}^\perp$ of an $[n, k]$ linear code $\mathcal{C}$ is an $[n, n-k]$ code defined by

$$\mathcal{C}^\perp = \left\{ x \in \mathbb{F}_p^n \mid x \cdot y = 0, \ \forall y \in \mathcal{C} \right\},$$

where $\cdot$ is the standard inner product. A generator matrix of the code $\mathcal{C}^\perp$ is called a parity-check matrix of $\mathcal{C}$.

A binary low-density parity-check (LDPC) code is a binary linear code defined by a sparse parity-check matrix H. That is to say, H contains a very small number of nonzero entries. An LDPC code is (w_c, w_r)-regular if the weight of each column is equal to w_c, and the weight of each row is equal to w_r.

LDPC codes can be presented using Tanner graphs, which were introduced by Tanner in [26]. The Tanner graph of an LDPC code 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. If an LDPC code is (w_c, w_r)-regular, the corresponding Tanner graph is a biregular bipartite graph in which vertices are of degree w_c or w_r.

The decoding performance of an LDPC code depends on the structure of the corresponding Tanner graph; the existence of short cycles in the Tanner graph of a code establishes a correlation between iterations in the process of decoding, and therefore, has a negative impact on the bit error rate (BER) performance of the code. The shorter the cycles are, the more significant the effect is. Furthermore, the iterative decoding performance of an LDPC code is related with the existence of certain undesirable substructures of the corresponding Tanner graph. For an AWGN channel, substructures that are called trapping sets, determine error floor performance of an LDPC code. It has been proved that absorbing sets, as a special type of trapping sets, have an important role in the error floor (see [25]).

Various combinatorial structures, including graphs, were used for a construction of LDPC codes without cycles of length four (see, e.g., [6, 16, 17, 23]). In [7], the authors investigated a family of LDPC codes constructed by taking bipartite cubic symmetric graphs as the Tanner graphs. In this paper, we construct LDPC codes from cubic semisymmetric graphs and study the smallest absorbing sets in the corresponding Tanner graphs.

The paper is organized as follows. In Section 2, the construction of the family of LDPC codes using cubic semisymmetric graphs is presented, some properties of the obtained codes are analyzed and the results regarding the code parameters are given. Furthermore, the expression for the variance of the syndrome weight of the constructed LDPC codes is presented. In Section 3, the structure of the smallest absorbing sets is studied. Sections 4 and 5 contain computational and simulation results.

2   LDPC codes constructed from cubic semisymmetric graphs

Let $\mathcal{G}$ be a connected cubic semisymmetric graph with $2n$ vertices, and denote by A its adjacency matrix. Since every semisymmetric graph is bipartite with two parts of equal size, its adjacency matrix can be written as follows

$$A = \begin{bmatrix} 0 & H \\ H^T & 0 \end{bmatrix}, \tag{2.1}$$

where H is an $n \times n$ matrix.

Taking the matrix H as a parity-check matrix, one can construct a $(3, 3)$-regular LDPC code $\mathcal{C}_H(\mathcal{G})$ of length n. The dimension of that code is equal to $n - \text{rank}_2(H)$, where $\text{rank}_2(H) = \frac{1}{2}\,\text{rank}_2(A)$. Furthermore, the density of the parity-check matrix H is equal to $\frac{3}{n}$. For the constructed code $\mathcal{C}_H(\mathcal{G})$, the cubic semisymmetric graph $\mathcal{G}$ is its Tanner graph.

From the fact that semisymmetric graphs are edge-transitive, but not vertex-transitive, it follows that H^T determines another LDPC code $\mathcal{C}_{H^T}(\mathcal{G})$. The code $\mathcal{C}_{H^T}(\mathcal{G})$ is a $(3, 3)$-regular LDPC code of length n, and its dimension is equal to $n - \text{rank}_2(H)$ as well.

Let H and H^T be $n \times n$ parity-check matrices of the codes $\mathcal{C}_H(\mathcal{G})$ and $\mathcal{C}_{H^T}(\mathcal{G})$, respectively. For the code $\mathcal{C}_H(\mathcal{G})$, the bit node graph Γ_b is defined in the following way: vertices of the graph correspond to codeword bits, and two vertices are adjacent if and only if the corresponding bits are included in the same parity-check equation. In other words, two vertices of the graph Γ_b are adjacent if and only if the corresponding bit nodes of the Tanner graph of the code $\mathcal{C}_H(\mathcal{G})$ have a common neighbour. Similarly, the vertices of the check node graph Γ_c correspond to parity-check equations of the code, and two vertices are adjacent if and only if the corresponding parity-check equations have a bit in common. That is to say, two vertices of the graph Γ_c are adjacent if and only if the corresponding check nodes of the Tanner graph of the code $\mathcal{C}_H(\mathcal{G})$ have a common neighbour. Note that the check node graph Γ_c of the code $\mathcal{C}_H(\mathcal{G})$ is the bit node graph of the code $\mathcal{C}_{H^T}(\mathcal{G})$.

Theorem 2.1. *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.*

Proof. Let v be a bit node of the Tanner graph $\mathcal{G}$. The degree of the node v is equal to three, and each of its neighbours is adjacent to another two bit nodes. Using the fact that $\mathcal{G}$ does not have cycles of length four, it follows that v has a common neighbour with exactly six other bit nodes. In other words, the degree of a vertex of the graph Γ_b is equal to six, i.e., the graph Γ_b is 6-regular. In the same way it can be concluded that the graph Γ_c is also 6-regular. □

Theorem 2.2. *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.*

Proof. Let us consider the $n \times n$ matrix $H^T H = [h_{i,j}]$. The degree of a bit node of the Tanner graph $\mathcal{G}$ of the code $\mathcal{C}_H(\mathcal{G})$ is equal to three, hence $h_{i,i} = 3$, $i \in \{1, \ldots, n\}$. An element $h_{i,j}$, $i \neq j$, of the matrix H is equal to one or zero depending on whether the corresponding nodes of the graph Γ_b are adjacent or not. Accordingly, $T_b = H^T H - 3I$, where T_b is the adjacency matrix of the graph Γ_b.

Conversely, let $T_b = [t_{i,j}]$ be an $n \times n$ $(0,1)$-matrix with the property that $T_b = H^T H - 3I$. $H^T H$ is a symmetric matrix and, consequently, T_b is also a symmetric matrix such that $t_{i,i} = 0$, $i \in \{1, \ldots, n\}$. The girth of the Tanner graph $\mathcal{G}$ is greater than four, so $h_{i,j}$, $i \neq j$, is equal to zero or one, and represents the number of common neighbours of the corresponding bit nodes of the Tanner graph $\mathcal{G}$ of the code $\mathcal{C}_H(\mathcal{G})$. It follows that T_b is the adjacency matrix of the graph Γ_b.

An analog statement for the matrix T_c can be formed similarly by observing check nodes of the Tanner graph of the code $\mathcal{C}_H(\mathcal{G})$. □

A clique of a graph G is a complete subgraph of the graph G. The clique number of the graph G, denoted by $\omega(G)$, is the number of vertices in a clique of the largest size in G, i.e. the order of a complete subgraph of G of maximum possible size for G. In the sequel, the clique number of the bit node graph Γ_b and the check node graph Γ_c will be examined.

Lemma 2.3. *Let $\mathcal{G}$ be a connected cubic semisymmetric graph. 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. The clique numbers of the graphs Γ_b and Γ_c are at least three.*

Proof. Each check node of the Tanner graph $\mathcal{G}$ is a common neighbour of every pair of its three adjacent bit nodes. Thus, each check node determines the complete graph K_3 as a subgraph of the bit node graph Γ_b. Similarly, each bit node of the Tanner graph determines the complete graph K_3 as a subgraph of the check node graph Γ_c. Hence, $\omega(\Gamma_b), \omega(\Gamma_c) \geq 3$. □

Lemma 2.4. *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 the complete graph K_4 is not a subgraph of Γ_b or Γ_c.*

Proof. Suppose that K_4 is a subgraph of the graph Γ_b. Let the bit nodes u_1, u_2, u_3, u_4 be the vertices of K_4. We have the following two possibilities:

(a) One of the check nodes (say v_1) in the corresponding subgraph of the Tanner graph $\mathcal{G}$ has degree three. Let u_1, u_2 and u_3 be the bit nodes adjacent with v_1. Furthermore, let the check node v_2 be a common neighbour of u_1 and u_4. Since u_2 and u_4 are adjacent in Γ_b, they have a common neighbour v_3 in $\mathcal{G}$. Then $u_1 v_1 u_2 v_3 u_4 v_2 u_1$ is a cycle of length six, which is impossible since the girth of the graph $\mathcal{G}$ is greater than six.

(b) The check nodes in the corresponding subgraph of the Tanner graph $\mathcal{G}$ have degrees at most two. Let the check node v_i be a common neighbour of the bit nodes u_1 and u_{i+1}, $i = 1, 2, 3$. Since u_2 and u_4 are adjacent in Γ_b, they have a common neighbour v_4 in $\mathcal{G}$. Then $u_1 v_1 u_2 v_4 u_4 v_3 u_1$ is a cycle of length six, which contradicts the fact that the girth of the graph $\mathcal{G}$ is greater than six.

Analog arguments yield that K_4 is not a subgraph of Γ_c. $\qquad\qquad\square$

The following theorem is a direct consequence of Lemmas 2.3 and 2.4.

Theorem 2.5. *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 $\omega(\Gamma_b) = \omega(\Gamma_c) = 3$.*

In the sequel, we discuss the minimum distance of the codes $\mathcal{C}_H(\mathcal{G})$ and $\mathcal{C}_{H^T}(\mathcal{G})$. The following results from [24] will be used.

Theorem 2.6 ([24, Theorem 3.1])**.** *Let $\mathcal{C}$ be a binary linear code with a parity-check matrix H. Then there exists a codeword in $\mathcal{C}$ with weight w if and only if there are w columns in H whose vector sum is a zero vector.*

Theorem 2.7 ([24, Theorem 3.2])**.** *Let $\mathcal{C}$ be a binary linear code with a parity-check matrix H. Then the minimum distance of the code $\mathcal{C}$ is equal to the smallest number of columns in H whose vector sum is a zero vector.*

The column weight of parity check matrices H and H^T of codes $\mathcal{C}_H(\mathcal{G})$ and $\mathcal{C}_{H^T}(\mathcal{G})$ is equal to three, and according to Theorem 2.6, the codes are even. Therefore, the minimum distance of the codes is an even number.

Theorem 2.8. *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 $d(\mathcal{C}_H^T(\mathcal{G})) \geq 6$.*

Proof. The column weight of the parity-check matrix H of the code $\mathcal{C}_H(\mathcal{G})$ is equal to three, and since the graph $\mathcal{G}$ does not have cycles of length four, it follows that the minimum distance of the code is at least four (see [13]). Assume that the minimum distance of the code is equal to four. As a consequence of Theorem 2.7, four columns of the parity-check matrix whose sum equals zero exist. Therefore, a set S in the graph $\mathcal{G}$, which consists of four bit nodes such that each pair of the vertices has a different common neighbour in $\mathcal{G}$, exists. Moreover, the set S determines the complete graph K_4 as a subgraph of the bit node graph Γ_b. Using Theorem 2.5, we conclude that the minimum distance of the code is at least six.

Observing check nodes of the Tanner graph of the code $\mathcal{C}_H(\mathcal{G})$, and the check node graph Γ_c, one can prove the statement for the minumum distance of the code $\mathcal{C}_{H^T}(\mathcal{G})$. $\quad\square$

In [7, Theorem 1], the minimum distance of an LDPC code constructed from a bipartite cubic symmetric graph is expressed using the second largest eigenvalue of the adjacency matrix of that graph. In a similar way, using the result given in Theorem 2.8, one can prove the following theorem.

Theorem 2.9. *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 $d \in \{d(\mathcal{C}_H(\mathcal{G})), d(\mathcal{C}_H^T(\mathcal{G}))\}$.

Remark 2.10. The results given above refer to the LDPC codes constructed from connected cubic semisymmetric graphs with girth greater than six. According to the classification of cubic semisymmetric graphs with at most 768 vertices (see [4]), all such graphs have girth at least eight. Consequently, all of the associated LDPC codes have properties stated above.

Theorem 2.11. *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.*

Proof. The 2-rank of the parity-check matrix of a binary code determines its dimension. The 2-rank of the matrix H is equal to the 2-rank of the matrix H^T and, therefore, it is sufficent to observe the matrix H and the corresponding code $\mathcal{C}_H(\mathcal{G})$. A maximal independent set of Γ_b determines $\alpha(\Gamma_b)$ linearly independent columns of the parity check matrix H. These columns have the property that no two columns have an entry equal to one at the same position. Due to the fact that Γ_b is a 6-regular graph, there are $6\alpha(\Gamma_b)$ ones at different positions within the columns. Therefore, adding any other $\alpha(\Gamma_b) - 1$ columns of the matrix, a set of $2\alpha(\Gamma_b) - 1$ linearly independent columns of the parity check matrix is defined. Hence, 2-rank of the matrix H is at least $2\alpha(\Gamma_b) - 1$.

As a consequence, the dimension of the code is at most $n - 2\alpha(\Gamma_b) + 1$, where n is the length of the code, i.e. the number of vertices of the graph Γ_b, and $\alpha(\Gamma_b)$ is the independence number of the graph Γ. $\qquad\square$

2.1 The variance of syndrome weight

To predict a decoding efficiency one can use a channel state information (CSI) (e.g. the crossover probability, a signal-to-noise ratio), which has an important role for communication systems. The estimation (performed prior to decoding) of the crossover probability based on the probability of syndrome weight was proposed in [18] and [27].

The expression for the variance of the syndrome weight of the LDPC codes constructed from bipartite cubic symmetric graphs is given in [7]. In a similar way, one can obtain the expression for the variance of the syndrome weight of the LDPC codes constructed from cubic semisymmetric graphs which is given by

$$Var(w) = \frac{n}{2}\left(7f_6(\rho) - 6f_4(\rho)\right),$$

where the function f_t is defined by $f_t(\rho) = \frac{1-(1-2\rho)^t}{2}$ (see [22]).

3 Absorbing sets

Let $G = G(C)$ be the Tanner graph of an LDPC code C which is determined by an $m \times n$ parity check matrix H. A (κ, τ) trapping set is a set T, that consists of κ bit nodes, having the property that the induced subgraph $G[T]$ has exactly τ check nodes of odd degree. The most harmful trapping sets are those with small sizes and small ratios $\frac{\tau}{\kappa}$. If the Tanner graph of an LDPC code does not have trapping sets with size smaller than the minimum distance of the code, then the error floor of the code is dominated by the minimum distance (see [9]). Let T be a trapping set. If every bit node in $G[T]$ is connected with fewer check nodes of odd degree than check nodes of even degree, then T is called an absorbing set.

Let A be a $(\kappa, \tau)-$ trapping set in the Tanner graph of an $(3, w_r)$ LDPC code. Using simple counting it can be seen that τ is an even number if κ is even, and an odd number if κ is odd.

The results in the sequel refer to the LDPC codes for which the corresponding Tanner graphs have girth at least six. We examine the existence of the smallest absorbing sets in the Tanner graphs of the LDPC codes constructed from the cubic semisymmetric graphs.

Theorem 3.1. *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 $\mathcal{G}$.*

Proof. The proof follows directly from the definition of an absorbing set and the fact that the Tanner graph of the code has no cycles of length four. □

Theorem 3.2. *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.*

Proof. Let A be a $(3, 3)$-absorbing set, which is the only possible structure of an absorbing set of size three in the Tanner graph of the codes (see Figure 1). The proof follows directly from the fact that the absorbing set defines a cycle of length six in the Tanner graph. □
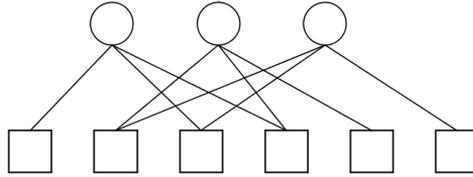

Figure 1: The only possible structure of an absorbing set of size three in the Tanner graph of the LDPC codes $\mathcal{C}_H(\mathcal{G})$. and $\mathcal{C}_{H^T}(\mathcal{G})$.

Theorem 3.3. *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.*

Proof. Since the size of an absorbing set is an even number, and according to the previous observations, the possible structures for absorbing sets of size four in the Tanner graph of the codes are $(4, 0)$, $(4, 2)$ and $(4, 4)$ absorbing sets (see Figure 2(a), (b) and (c), respectively). The proof follows directly from the fact that $(4, 0)$ and $(4, 2)$ absorbing sets define the complete graph K_4 as a subgraph of the graph Γ_b. □
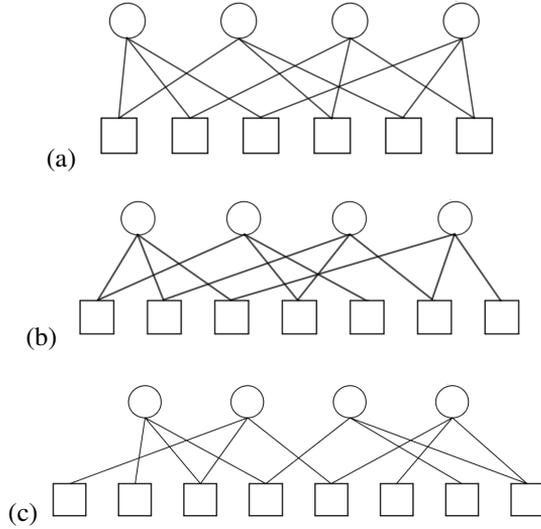
Figure 2: The possible structures of an absorbing set of size four in the Tanner graph of the LDPC codes $\mathcal{C}_H(\mathcal{G})$ and $\mathcal{C}_{H^T}(\mathcal{G})$.

4 Computational results

Within this section the parameters of the LDPC codes obtained from cubic semisymmetric graphs are presented. For the construction of the cubic semisymmetric graphs we have employed the method presented in [1]. The parameters of the constructed codes can be seen in Table 1. The parameter v denotes the number of vertices of the corresponding cubic semisymmetric graph.

v	**LDPC$_1$**	**LDPC$_2$**	v	**LDPC$_1$**	**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 1: The parameters of LDPC codes constructed from cubic semisymmetric graphs with less than 1000 vertices (using the method presented in [1]).

The Tanner graphs of the constructed codes have girth at least eight. The codes $\mathcal{C}_H(\mathcal{G})$ and $\mathcal{C}_{H^T}(\mathcal{G})$ are isomorphic in the case when the number of vertices of the cubic semisymmetric graph G is $486, 546, 720$ or 798.

Remark 4.1. Lately, much interest has been devoted to LCD codes, which have an important application in cryptography, in protection against side-channel and fault attacks (see [2]). Self-orthogonal codes can be used to construct quantum error-correcting codes, which can protect quantum information in quantum computations and quantum communications (see [3]).

The LDPC codes marked in bold are self-orthogonal codes, and those labeled with * in Table 1 are LCD codes.

Remark 4.2. Codes $\mathcal{C}_H(\mathcal{G})$ and $\mathcal{C}_{H^T}(\mathcal{G})$ constructed from a cubic semisymmetric graph (CSSG) have the same length and dimension, and, in general, different minimum distance. Thus, the construction gives diversity in code parameters for the same graph, which is not the case for LDPC codes which are constructed in [7] using cubic symmetric graphs (CSGs).

According to the classification of CSSGs with at most 768 vertices (see [4]), all the graphs have girth at least eight, while according to [5] many CSGs have girth equal to six. Moreover, semisymmetric graphs form a wider family than symmetric graphs.

Furthermore, we have compared the parameters of the LDPC codes constructed from CSSGs to the parameters of the LDPC codes constructed from CSGs. The results are shown in Table 2. It can be concluded that, for the same code length, the LDPC codes from CSSGs achieve higher code rate than those constructed using CSGs. When $n = 27$, the code rate is four times greater.

n	Rate (CSSG)	Rate (CSG)
27	0.296	0.074
56	0.214	$\{0.107, 0.143\}$
60	0.233	$\{0.067, 0.083\}$
72	0.222	$\{0.083, 0.111\}$

Table 2: Rates od LDPC codes constructed from cubic symmetric and semisymmetric graphs with the same length.

5 Simulation results

In this section, we present simulation results of the LDPC codes derived from the cubic semisymmetric graphs, over the additive white gaussian noise (AWGN) channel. We have compared the codes with randomly generated LDPC codes of the same length and dimension and a parity-check matrix with a column weight equal to three. For randomly generated codes we have used the software for LDPC codes available on [21], which employs the construction from [8, 19]. The codes are decoded with the sum-product decoding algorithm and the maximum number of iteration is set to 50. Figures 3 - 6 show the performance of the codes.

Remark 5.1. The LDPC codes that we are aware of were not adequate for the comparison with the LDPC codes obtained in this paper because of the different parameters of the codes. Thus, we have used the best known random construction for LDPC codes. It has been proved in [8] that the construction leads to LDPC codes with performance close to the Shannon limit. Moreover, the best results were obtained in the case of the smallest possible column weight.
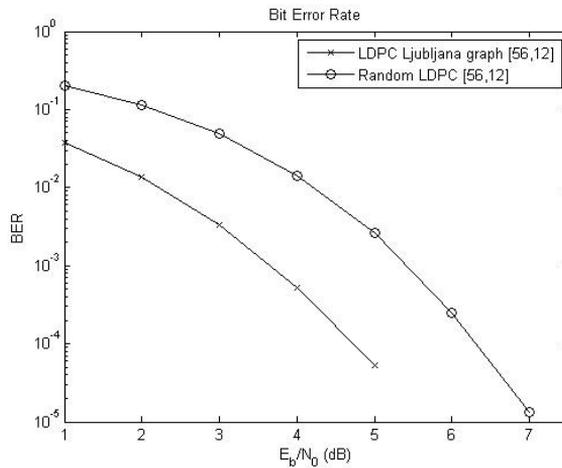

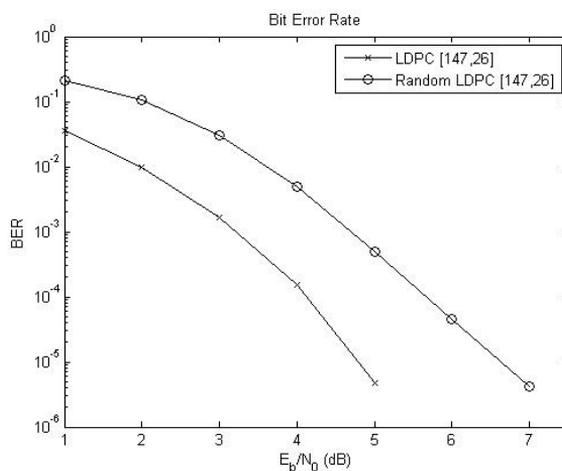Figure 3: BER performance of the $[56, 12, 16]$ LDPC code derived from the Ljubljana graph.

Figure 4: BER performance of the $[147, 26, 26]$ LDPC code derived from the cubic semisymmetric graph with 294 vertices.
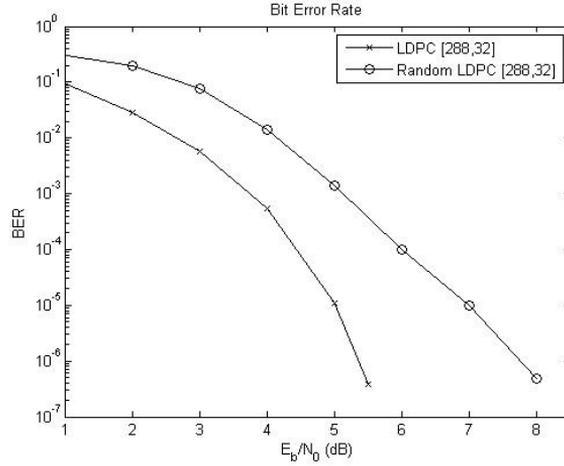
Figure 5: BER performance of the $[288, 32, 56]$ LDPC code derived from the cubic semisymmetric graph with 576 vertices.
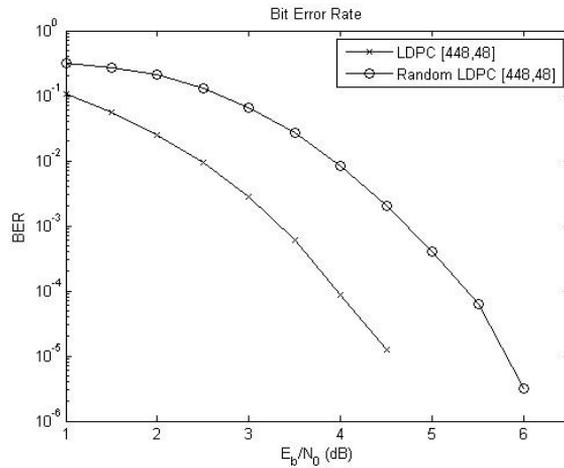

Figure 6: BER performance of the $[448, 48, 100]$ LDPC code derived from the cubic semisymmetric graph with 896 vertices.

The obtained simulation results indicate better BER performance of the codes constructed from the cubic semisymmetric graphs than randomly generated LDPC codes.

ORCID iDs

Dean Crnković ⓘ https://orcid.org/0000-0002-3299-7859
Sanja Rukavina ⓘ https://orcid.org/0000-0003-3365-7925
Marina Šimac ⓘ https://orcid.org/0000-0001-9291-3365

References

[1] A. Bretto and L. Gillibert, G-graphs: An efficient tool for constructing symmetric and semisymmetric graphs, *Discrete Appl. Math.* **156** (2008), 2719–2739, doi:10.1016/j.dam.2007.11.011.

[2] J. Bringer, C. Carlet, H. Chabanne, S. Guilley and H. Maghrebi, Orthogonal direct sum masking, in: *Information Security Theory and Practice. Securing the Internet of Things. WISTP 2014. Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, volume 8501, 2014 pp. 40–56, doi:10.1007/978-3-662-43826-8_4.

[3] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction and orthogonal geometry, *Phys. Rev. Lett.* **78** (1997), 405–408, doi:10.1103/physrevlett.78.405.

[4] M. Conder, A. Malnič, D. Marušič and P. Potočnik, A census of semisymmetric cubic graphs on up to 768 vertices, *J. Algebr. Comb.* **23** (2006), 255–294, doi:10.1007/s10801-006-7397-3.

[5] M. Conder and R. Nedela, A refined classification of symmetric cubic graphs, *J. Algebra* **322** (2009), 722–740, doi:10.1016/j.jalgebra.2009.03.011.

[6] D. Crnković, S. Rukavina and M. Šimac, LDPC codes from μ-geodetic graphs obtained from block designs, *Graphs Comb.* **35** (2019), 451–469, doi:10.1007/s00373-019-02007-4.

[7] D. Crnković, S. Rukavina and M. Šimac, LDPC codes constructed from cubic symmetric graphs, *Appl. Algebra Eng. Commun. Comput.* (2020), doi:10.1007/s00200-020-00468-2.

[8] R. M. N. D. J. C. MacKay, Near Shannon limit performance of low density parity check codes, *Electron. Lett.* **32** (1996), 1645–1646, doi:10.1049/el:19961141.

[9] Q. Diao, Y. Y. Tai, S. Lin and K. Abdel-Ghaffar, Trapping set structure of finite geometry ldpc codes, in: *2012 IEEE International Symposium on Information Theory Proceedings*, 2012 pp. 3088–3092, doi:10.1109/isit.2012.6284130.

[10] R. Diestel, *Graph Theory*, Springer-Verlag, Berlin Heidelberg, 2017, doi:10.1007/978-3-662-53622-3.

[11] Y.-Q. Feng, M. Ghasemi and C. Wang, Cubic semisymmetric graphs of order $6p^3$, *Discrete Math.* **310** (2010), 2345–2355, doi:10.1016/j.disc.2010.05.018.

[12] J. Folkman, Regular line-symmetric graphs, *J. Comb. Theory* **3** (1967), 215–232, doi:10.1016/S0021-9800(67)80069-3.

[13] M. Greferath, C. Rößing and L. Storme, Galois geometries and low-density parity-check codes, in: *Current Research Topics in Galois Geometry*, Nova Science Publishers/Novinka, New York, pp. 245–270, 2014.

[14] F. Harary, *Graph Theory*, Addison-Wesley Publishing Company, 1969, doi:10.1201/9780429493768.

[15] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003, doi:10.1017/cbo9780511807077.

[16] F. Ivanov and V. Zyablov, LDPC codes based on steiner quadruple systems and permutation matrices, in: *Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory*, Nova Science Publishers/Novinka, New York, pp. 175–180, 2014, http://www.moi.math.bas.bg/acct2014/acct2014end.html.

[17] J.-L. Kim, U. N. Peled, I. Perepelitsa, V. Pless and S. Friedland, Explicit construction of families of LDPC codes with no 4-cycles., *IEEE Trans. Inf. Theory* **50** (2004), 2378–2388, doi:10.1109/tit.2004.834760.

[18] G. Lechner and C. Pacher, Estimating channel parameters from the syndrome of a linear code, *IEEE Commun. Lett.* **17** (2013), 2148–2151, doi:10.1109/lcomm.2013.091113.131646.

[19] D. J. C. MacKay, Good error-correcting codes based on very sparse matrices, *IEEE Trans. Inf. Theory* **45** (1999), 399–431, doi:10.1109/18.748992.

[20] A. Malnič, D. Marušič and C. Wang, Cubic edge-transitive graphs of order 2p3, *Discrete Mathematics* **274** (2004), 187–198, doi:10.1016/S0012-365X(03)00088-8.

[21] R. M. Neal, *Software for Low Density Parity Check (LDPC) codes*, University of Toronto, 2012, https://www.cs.toronto.edu/~radford/ldpc.software.html.

[22] C. Pacher, P. Grabenweger and D. E. Simos, Weight distribution of the syndrome of linear codes and connections to combinatorial designs, in: *2016 IEEE International Symposium on Information Theory (ISIT)*, IEEE Press, 2016 pp. 3038–3042, doi:10.1109/isit.2016.7541857.

[23] J. Rosenthal and P. O. Vontobel, Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis, in: *38th Allerton Conference on Communication, Control and Computing*, 2000 pp. 248–257, https://www.math.uzh.ch/aa/index.php?publication-show&key1=Coding%20Theory&key2=Joachim%20Rosenthal.

[24] W. E. Ryan and S. Lin, *Channel codes. Classical and modern*, Cambridge University Press, 2009, doi:10.1017/cbo9780511803253.

[25] C. Schlegel and S. Zhang, On the dynamics of the error floor behavior in (regular) LDPC codes, *IEEE Trans. Inf. Theory* **56** (2010), 3248–3264, doi:10.1109/tit.2010.2048448.

[26] R. M. Tanner, A recursive approach to low complexity codes, *IEEE Trans. Inf. Theory* **27** (1981), 533–547, doi:10.1109/tit.1981.1056404.

[27] V. Toto-Zarasoa, A. Roumy and C. Guillemot, Maximum likelihood BSC parameter estimation for the Slepian-Wolf problem, *IEEE Commun. Lett.* **15** (2011), 232–234, doi:10.1109/lcomm.2011.122810.102182.