

LDPC codes constructed from cubic symmetric graphs

Dean Crnković

(*E-mail: deanc@math.uniri.hr*)

Sanja Rukavina

(*E-mail: sanjar@math.uniri.hr*)

and

Marina Šimac

(*E-mail: msimac@math.uniri.hr*)

Department of Mathematics

University of Rijeka

Radmile Matejčić 2, 51000 Rijeka, Croatia

Abstract

Low-density parity-check (LDPC) codes have been the subject of much interest due to the fact that they can perform near the Shannon limit. In this paper we present a construction of LDPC codes from cubic symmetric graphs. The constructed codes are $(3,3)$ -regular and the vast majority of the corresponding Tanner graphs have girth greater than four. We analyse properties of the obtained codes and present bounds for the code parameters, the dimension and the minimum distance. Furthermore, we give an expression for the variance of the syndrome weight of the constructed codes. Information on the LDPC codes constructed from bipartite cubic symmetric graphs with less than 200 vertices is presented as well. Some of the constructed codes are optimal, and some have an additional property of being self-orthogonal or linear codes with complementary dual (LCD codes).

Keywords: LDPC code, cubic graph, arc-transitive graph, bipartite graph

MSC 2020 Codes: 94B05, 05C99

1 Introduction and preliminaries

We assume that the reader is familiar with the basic facts of graph theory and coding theory. We refer the reader to [1, 9] and [14] for related background materials on graphs and codes, respectively. In this paper we consider only non-trivial finite connected graphs without loops and multiple edges.

A binary $[n, k]$ linear code \mathcal{C} is a k -dimensional subspace of the vector space \mathbb{F}_2^n . For $x, y \in \mathbb{F}_2^n$, the number $d(x, y) = |\{i : x_i \neq y_i, 1 \leq i \leq n\}|$ is called the Hamming distance. The minimum distance of a code \mathcal{C} is the number $d = \min\{d(x, y) : x, y \in \mathcal{C}\}$. Through the paper, a binary $[n, k]$ linear code with the minimum distance d will be called an $[n, k, d]$ code. An optimal code is a code which achieves the theoretical upper bound for the minimum distance.

The codewords of an $[n, k, d]$ code satisfy $m \geq n - k$ parity-check equations. Every parity-check equation can be presented as a binary vector of length n having j -th position equal to 1 if the corresponding codeword bit is included in that parity-check equation. The set of m parity-check equations can be presented with an $m \times n$ parity-check matrix $H = [h_{i,j}]$. If $h_{i,j} = 1$, then the i -th parity-check equation contains the j -th codeword bit. The rows of the parity-check matrix span the null space (or dual code) \mathcal{C}^\perp of \mathcal{C} .

A binary low-density parity-check (LDPC) code is a binary linear code defined by a sparse parity-check matrix H , which means that H contains a very small number of nonzero entries. An LDPC code is called (w_c, w_r) -regular if H has constant row sum w_r and constant column sum w_c .

An LDPC code can be presented using the Tanner graph, which gives a relation between parity-check equations and codeword bits. 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. If an LDPC code is (w_c, w_r) -regular, then each bit node has degree w_c and each check node has degree w_r . A cycle in a graph is a sequence of edges that form a path in the graph such that the first node is equal to the last one. The length of a cycle is the number of edges in it, and the girth of a graph is the length of the shortest cycle. Since a Tanner graph is bipartite, the length of a cycle must be even and at least four.

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 thus, 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. For this reason, the aim is to construct LDPC codes without short cycles, especially cycles of length four.

LDPC codes were first introduced by Gallager in the early 1960's (see [11]) and rediscovered by MacKay and Neal (see [18]). These codes have been the subject of much interest due to the fact that they can perform near the Shannon limit (see [11]). For some recent results on LDPC codes we refer the reader to [29, 32]. Over the past years researchers have constructed LDPC codes that are free of cycles of length four using various structures, including graphs (see, e.g., [8, 27]). Regular bipartite graphs with large girth constructed in [17] were used in [16] as Tanner graphs of LDPC codes. In this paper we construct LDPC codes using bipartite cubic symmetric graphs as Tanner graphs of LDPC codes.

The paper is organized as follows: in Section 2, the construction of the LDPC codes using cubic symmetric graphs is introduced, and the results about the code parameters are presented. In Section 3, an expression for the variance of a syndrome weight of the constructed LDPC codes is obtained. In Section 4, computational results and constructed LDPC codes are presented. Finally, in Section 5 we give an example that illustrates the BER performance of the constructed codes over a binary symmetric channel.

2 LDPC codes constructed from cubic symmetric graphs

Cubic graphs are 3-regular graphs, i.e. graphs in which all vertices have degree equal to three. A graph is symmetric if it is arc-transitive, i.e. if its automorphism group acts transitively on the set of arcs. Therefore, cubic symmetric graphs (CSGs) are 3-regular arc-transitive graphs. CSGs were first studied by Foster in [10]. They have since been the subject of much interest and study. Conder and Nedela proved (see [6]) that finite symmetric cubic graphs can be classified into 17 different families according to the arc-transitive actions they admit. The majority of CSGs are bipartite and it is known that there exist exactly five connected CSGs with girth less than six (the complete graph K_4 , the complete bipartite graph $K_{3,3}$, the cube,

the Petersen graph and the dodecahedron). In this paper we study LDPC codes having bipartite CSGs as the Tanner graphs.

Let \mathcal{G} be a connected CSG with $2n$ vertices. Denote by A its adjacency matrix. If \mathcal{G} is a bipartite graph, its adjacency matrix can be written as follows:

$$A = \begin{bmatrix} 0 & H \\ H^T & 0 \end{bmatrix}, \quad (1)$$

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

One can construct an LDPC code $\mathcal{C}(\mathcal{G})$ by taking the matrix H as a parity-check matrix of the code. That is to say, \mathcal{G} is the Tanner graph of the code $\mathcal{C}(\mathcal{G})$. The density of the parity-check matrix is equal to $\frac{3}{n}$ and the obtained code is a $(3, 3)$ -regular LDPC code of length n and dimension $n - \text{rank}_2(H)$, where $\text{rank}_2(H) = \frac{1}{2}\text{rank}_2(A)$. Every arc-transitive graph without isolated vertices is vertex-transitive, so it is possible to obtain H from H^T by permuting the rows and columns. Hence, the LDPC codes obtained from H and H^T are equivalent. Note that two binary codes are equivalent if and only if they are isomorphic.

If \mathcal{G} is a non-bipartite CSG, its adjacency matrix M determine a parity-check matrix of a $(3, 3)$ -regular LDPC code whose Tanner graph is a CSG having the adjacency matrix of the form (1) with $H = M$. Hence, and according to the classification of CSGs, an LDPC code constructed from a non-bipartite CSG (taking its adjacency matrix as a parity-check matrix of the code) is isomorphic to the LDPC code obtained from some bipartite CSG (that is the Tanner graph of the code) with twice a number of vertices than the initial graph. Therefore, only LDPC codes constructed from bipartite CSGs will be considered.

In the sequel, when considering a CSG \mathcal{G} , we refer to a connected bipartite CSG \mathcal{G} with $2n$ vertices. By $\mathcal{C}(\mathcal{G})$ we denote the LDPC code of length n having \mathcal{G} as its Tanner graph.

Let H be an $n \times n$ parity-check matrix of a code $\mathcal{C}(\mathcal{G})$. A bit node graph Γ is defined in the following way: it has 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. In other words, two vertices of the graph Γ are adjacent if and only if the corresponding bit nodes of the Tanner graph \mathcal{G} of the code $\mathcal{C}(\mathcal{G})$ have a common neighbour.

Theorem 1. *Let \mathcal{G} be a connected bipartite CSG with $2n$, $n \geq 7$, vertices and let H be the parity-check matrix of the code $\mathcal{C}(\mathcal{G})$. Then the corresponding bit node graph Γ is 6-regular.*

Proof. Every bipartite CSG \mathcal{G} with $2n$, $n \geq 7$, vertices has the girth at least six. A bit node v of the Tanner graph \mathcal{G} of the code $\mathcal{C}(\mathcal{G})$ has degree equal to three, and each of its neighbours is adjacent to another two bit nodes. Since \mathcal{G} does not have cycles of length four, the node v has a common neighbour with exactly six other bit nodes. In other words, the node v of Γ has degree equal to six. Hence, the graph Γ is 6-regular. \square

Theorem 2. *Let \mathcal{G} be a connected bipartite CSG with $2n$, $n \geq 7$, vertices. Let H be the parity-check matrix of the code $\mathcal{C}(\mathcal{G})$ and let Γ be the corresponding bit node graph. Then a $(0, 1)$ -matrix T of order n is the adjacency matrix of the graph Γ if and only if $H^T H = 3I + T$.*

Proof. The diagonal elements of the matrix $H^T H$ correspond to the degree of bit nodes of the Tanner graph \mathcal{G} of the code $\mathcal{C}(\mathcal{G})$, which is equal to three. Since \mathcal{G} does not have cycles of length four, the other elements of the matrix are 1 or 0 depending whether the corresponding bit nodes have a common neighbour or not. That is to say, off-diagonal elements of the matrix $H^T H$ are 1 or 0 depending whether the corresponding nodes of the graph Γ are adjacent or not. Hence, $H^T H = 3I + T$, where T is the adjacency matrix of the graph Γ .

Conversly, suppose that T is a $(0, 1)$ -matrix of order n such that $H^T H = 3I + T$. $H^T H$ is a symmetric matrix, and therefore T is a symmetric matrix. Clearly, the matrix T has zeroes on the diagonal. An off-diagonal element of T corresponds to the number of common neighbours of the corresponding bit nodes of the Tanner graph \mathcal{G} of the code $\mathcal{C}(\mathcal{G})$. Since the girth of the Tanner graph \mathcal{G} is at least six, the number of common neighbours is zero or one. Therefore, T is the adjacency matrix of the graph Γ . \square

The following results can be found in [24].

Theorem 3. *[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 4. [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.*

Due to the fact that the column weight of a parity check matrix H of a code $\mathcal{C}(\mathcal{G})$ is equal to three, Theorem 3 implies that the code $\mathcal{C}(\mathcal{G})$ is even. Moreover, the minimum distance of the code $\mathcal{C}(\mathcal{G})$ is an even number.

We will use Theorem 4 in the proof of the following theorem.

Theorem 5. *Let \mathcal{G} be a connected bipartite CSG with $2n$, $n \geq 7$, vertices and let Γ be the corresponding bit node graph. The minimum distance of the code $\mathcal{C}(\mathcal{G})$ is at least six if and only if the clique number of the graph Γ is at most three.*

Proof. The girth of the Tanner graph \mathcal{G} of the code $\mathcal{C}(\mathcal{G})$ is greater than four and, therefore, the minimum distance of the code is at least four (see [12]).

If there exists a set S in the graph \mathcal{G} which consists of four bit nodes with the property that every pair of the vertices has a common neighbour, then the sum of the corresponding columns of the parity-check matrix equals zero. Hence, the minimum distance is equal to four. In other words, if the complete graph K_4 is the subgraph of the graph Γ , then the minimum distance of the code is equal to four. Consequently, if the minimum distance of the code is at least six, then the clique number of the graph Γ is at most three.

Conversely, assume that the clique number of the graph Γ is at most three. Accordingly, it is not possible to find four columns of the parity-check matrix whose sum equals zero. As the result of Theorem 4, the minimum distance of the code is at least six. \square

In [30] Tanner gave a lower bounds for the minimum distance of a regular LDPC code with a parity-check matrix M in terms of the second largest eigenvalue μ_2 of the matrix $M^T M$.

Theorem 6. [30, Theorems 3.1 and 4.1] *If the Tanner graph of a (w_c, w_r) -regular LDPC code is connected and has n bit nodes, then the minimum distance of the code satisfies $d \geq \max\{d_1, d_2\}$, where*

$$d_1 = \frac{n(2w_c - \mu_2)}{w_c w_r - \mu_2}, \quad d_2 = \frac{2n(2w_c + w_r - 2 - \mu_2)}{w_r(w_c w_r - \mu_2)}.$$

Theorem 7. *Let \mathcal{G} be a connected bipartite CSG with $2n$, $n \geq 7$, vertices and let λ_2 be the second largest eigenvalue of its adjacency matrix A . Then the minimum distance of the code $\mathcal{C}(\mathcal{G})$ satisfies the following condition:*

$$d \geq \begin{cases} \frac{2}{5}n, & \lambda_2 \leq 2, \\ \frac{2}{9}n, & 2 < \lambda_2 \leq \sqrt{6}, \\ 4, & \sqrt{6} < \lambda_2 < 3. \end{cases}$$

Proof. Since \mathcal{G} is a bipartite graph, the spectrum of \mathcal{G} is symmetric with respect to 0. Moreover, since \mathcal{G} is 3-regular, for every eigenvalue λ of its adjacency matrix A the inequality $|\lambda| \leq 3$ holds (see [1, Theorem 11.5.1]). Furthermore, if λ is an eigenvalue of A , then λ^2 is an eigenvalue of A^2 . Let μ_2 be the second largest eigenvalue of the matrix $H^T H$, where H is the parity-check matrix of the code $\mathcal{C}(\mathcal{G})$. Using the fact that the matrices $H^T H$ and $H H^T$ have the same non-zero eigenvalues and the fact that $\lambda_2 \geq 1$ (see [21]), it follows that $\mu_2 = \lambda_2^2$.

According to Theorem 6, the minimum distance of the code $\mathcal{C}(\mathcal{G})$ satisfies $d \geq \max\{d_1, d_2\}$, where

$$d_1 = \frac{n(6 - \mu_2)}{9 - \mu_2}, \quad d_2 = \frac{2n(7 - \mu_2)}{3 \cdot (9 - \mu_2)}.$$

From this equalities one can easily obtain

$$\mu_2 = \frac{6n - 9d_1}{n - d_1}, \tag{2}$$

and

$$\mu_2 = \frac{14n - 27d_2}{2n - 3d_2}. \tag{3}$$

The inequality $d_1 \geq d_2$ holds for $\mu_2 \leq 4$, and $d_2 \geq d_1$ for $\mu_2 > 4$ (see [28]). In the first case, when $\mu_2 \leq 4$, using the equality (2), one gets that $d \geq d_1 \geq \frac{2}{5}n$. If $4 < \mu_2 \leq 6$, then the minimum distance satisfies the inequality $d \geq d_2 \geq \frac{2}{9}n$, which can be obtained using (3). For $\mu_2 \geq 6$ the minimum distance of the code is at least four, as discussed in the proof of Theorem 5. \square

Theorem 8. *Let \mathcal{G} be a connected bipartite CSG with $2n$, $n \geq 7$, vertices. Then the dimension of the code $\mathcal{C}(\mathcal{G})$ is at most $\frac{5n}{6}$.*

Proof. To determine the dimension of the code $\mathcal{C}(\mathcal{G})$ we observe the 2-rank of its parity-check matrix H . The 2-rank of the matrix H is greater or equal than the size of a maximal independent set of the bit node graph Γ . Hence, the dimension of the code is at most $n - \alpha(\Gamma)$, where n is the length of the code, i.e. the number of vertices of the graph Γ , and $\alpha(\Gamma)$ is the independence number of the graph Γ .

According to [4] every 6-regular connected graph with n vertices, other than K_7 , has an independent set which contains at least $\frac{n}{6}$ vertices. So, it follows from Theorem 1 that the inequality $\alpha(\Gamma) \geq \frac{n}{6}$ holds. Therefore, the upper bound for the dimension of the code is $\frac{5n}{6}$. \square

If an adjacency matrix A of a bipartite CSG \mathcal{G} has the full rank, then the parity-check matrix H of the LDPC code also has the full rank. Hence, the constructed LDPC code has the dimension zero, i.e. the constructed code is trivial.

We will need the following two results from [23].

Theorem 9. [23, Corollary 5] *The dimension of the nullspace of an adjacency matrix of a connected 3-arc-transitive graph which is s -regular for $s \geq 2$ is non-zero.*

Theorem 10. [23, Theorem 13] *Let p be a prime number and let \mathcal{G} be a vertex-transitive s -regular multigraph with n vertices. Let \mathbb{F} be a field of characteristic p . If $\gcd(p, s) = 1$ and n is a power of p , then the adjacency matrix of the graph \mathcal{G} is invertible over \mathbb{F} .*

Theorem 11 gives a condition for the LDPC code constructed from a CSG with $v = 2^t$ vertices to be trivial.

Theorem 11. *Let \mathcal{G} be a connected bipartite CSG with $v = 2^t$ vertices and let $\mathcal{C}(\mathcal{G})$ be the LDPC code constructed from \mathcal{G} . Then the parameters of the code $\mathcal{C}(\mathcal{G})$ are $[2^{t-1}, 0, 2^{t-1}]$.*

Proof. The length of the code is $\frac{1}{2}v = 2^{t-1}$. Every arc-transitive graph without isolated vertices is vertex-transitive, so \mathcal{G} is a vertex-transitive graph. Since \mathcal{G} is a 3-regular graph with $v = 2^t$ vertices, using Theorem 10 one concludes that the

adjacency matrix of \mathcal{G} has the full rank over \mathbb{F}_2 . Hence, the parity-check matrix of the code $\mathcal{C}(\mathcal{G})$ is the full rank matrix, so the dimension of the code $\mathcal{C}(\mathcal{G})$ is equal to 0. \square

In the case when \mathcal{G} is a connected bipartite 3-arc-transitive CSG, the dimension of the code $\mathcal{C}(\mathcal{G})$ is greater than zero. This statement follows directly from Theorem 9.

The following theorem can be found in [5]. The Gallager A algorithm is also described in that reference.

Theorem 12. [5, Theorem 2] *A column-weight-three code with Tanner graph of girth $g \geq 10$ can correct $\frac{g}{2} - 1$ errors in $\frac{g}{2}$ iterations of the Gallager A algorithm.*

The following statement is a direct consequence of Theorem 12.

Corollary 1. *Let \mathcal{G} be a bipartite CSG with the girth $g \geq 10$, and let $\mathcal{C}(\mathcal{G})$ be the LDPC code constructed from \mathcal{G} . Then $\mathcal{C}(\mathcal{G})$ can correct $\frac{g}{2} - 1$ errors in $\frac{g}{2}$ iterations of the Gallager A algorithm.*

3 The variance of a syndrome weight

A channel state information (CSI), for example the crossover probability, is very important for communication systems and it can be used for predicting a decoding efficiency. To compute a syndrome, an observed channel is converted to a binary symmetric channel (BSC) and the CSI of the original channel is derived from the estimated crossover probability of the BSC. The estimation (performed prior to decoding) of the crossover probability based on the probability of a syndrome weight was proposed in [22] and [31]. A general expression for the variance of a syndrome weight of an LDPC code (after transmission over a BSC) is given in [25]. Obtained results were applied for LDPC codes that have constant check node degree.

In this section we give the expression for the variance of a syndrome weight of an LDPC code constructed from a bipartite CSG.

Let \mathcal{C} be a binary linear code and let an $m \times n$ matrix H be its parity-check matrix with row weights r_i , $i \in \{1, \dots, m\}$. Furthermore, let $HH^T = [\lambda_{i,j}]$ be the concurrence matrix of H . Suppose a codeword $c \in \mathcal{C}$ has been sent through a BSC with crossover probability ρ and suppose that a vector y has been received. The

vector $s = y \cdot H^T$, $s = (s_1, \dots, s_m)$, is the syndrome of y . Denote by w the syndrome weight, i.e. $w = \sum_{i=1}^m s_i$.

Let f_t be the function defined by:

$$f_t(\rho) = \frac{1 - (1 - 2\rho)^t}{2}.$$

For an LDPC code whose Tanner graph is free of cycles of length four, in the case when the check nodes have the same degree r , the variance of a syndrome weight w can be calculated as follows (see [25]):

$$\text{Var}(w) = \frac{m}{2} f_{2r}(\rho) + \frac{g_1}{2} (f_{2r}(\rho) - f_{2r-2}(\rho)), \quad (4)$$

where $g_1 = \sum_{i \neq j} \lambda_{i,j}$.

The entries $\lambda_{i,j}$, $i \neq j$, of the concurrence matrix of a parity-check matrix H of an LDPC code $\mathcal{C}(\mathcal{G})$ are elements of the set $\{0, 1\}$. A value $\lambda_{i,j}$ presents the number of common neighbours for i -th and j -th check node of the Tanner graph. Hence, $\lambda_{i,j} = 1$ if the corresponding check nodes have a common neighbour, and $\lambda_{i,j} = 0$ otherwise. Using simple counting, it can be seen that each check node has a common neighbour with exactly six check nodes. Accordingly, $g_1 = 6n$. Using the equality (4), the variance of a syndrome weight can be calculated as follows:

$$\text{Var}(w) = \frac{n}{2} (7f_6(\rho) - 6f_4(\rho)).$$

4 Computational results

In this section we present information on LDPC codes constructed from the bipartite cubic symmetric graphs with less than 200 vertices. We have used cubic symmetric graphs available at [7] and follow the given notation. The parameters of the constructed LDPC codes are given in Table 1. The obtained codes have low rates and good minimum distance.

CSG	LDPC	Girth	CSG	LDPC	Girth	CSG	LDPC	Girth
6A	[3,2,2]*	4	74A	[37, 0, 37]	6	134A	[67, 0, 67]	6
8A	[4, 0, 4]	4	78A	[39,2,26]*	6	144A	[72,8,32]	8
14A	[7,3,4]	6	80A	[40, 4, 16]	10	144B	[72, 6, 30]	10
16A	[8, 0, 8]	6	86A	[43, 0, 43]	6	146A	[73, 9, 28]	6
18A	[9,2,6]*	6	90A	[45, 11, 10]	10	150A	[75,2,50]*	6
20B	[10,4,4]*	6	96A	[48, 8, 18]	6	152A	[76, 0, 76]	6
24A	[12,4,6]	6	96B	[48, 12, 8]	8	158A	[79, 0, 79]	6
26A	[13, 0, 13]	6	98A	[49,3,28]	6	162A	[81,2,54]*	6
30A	[15, 5, 6]	8	98B	[49,6,24]	6	162B	[81,2,54]*	12
32A	[16, 0, 16]	6	104A	[52, 0, 52]	6	162C	[81, 14, 18]	12
38A	[19, 0, 19]	6	110A	[55, 10, 10]*	10	168A	[84, 10, 30]	6
40A	[20, 4, 8]	8	112A	[56, 8, 14]	8	168E	[84, 13, 30]	12
42A	[21,5,10]	6	112B	[56, 8, 16]	8	168F	[84, 8, 38]*	12
48A	[24,6,10]	8	112C	[56,6,24]	10	182A	[91,3,52]	6
50A	[25, 0, 25]	6	114A	[57,2,38]*	6	182B	[91,3,52]	6
54A	[27,2,18]*	6	120A	[60, 5, 20]	8	182D	[91, 14, 26]*	12
56A	[28,6,12]	6	120B	[60, 4, 24]	10	186A	[93,2,62]*	6
56C	[28, 8, 8]*	8	122A	[61, 0, 61]	6	192A	[96, 23, 8]	8
62A	[31, 0, 31]	6	126A	[63, 5, 30]	6	192B	[96, 16, 22]	10
64A	[32, 0, 32]	8	128A	[64, 0, 64]	6	192C	[96, 18, 16]	12
72A	[36,4,18]	6	128B	[64, 0, 64]	10	194A	[97, 0, 97]	6

Table 1: Parameters of LDPC codes constructed from bipartite cubic symmetric graphs with less than 200 vertices.

The girths of the Tanner graphs of the constructed codes are at least six, except for the codes obtained from the graphs 6A and 8A (the complete bipartite graph $K_{3,3}$ and the cube, respectively) for which the girth is equal to four. The LDPC code constructed from the graph 14A is isomorphic to the LDPC code obtained from the projective plane of order two, i.e. the symmetric 2-(7, 3, 1) design, by taking the incidence matrix of the projective plane as the parity-check matrix of the code. The codes obtained from the graphs 162A and 162B are isomorphic, as well as the codes obtained from the graphs 182A and 182B. Some of the constructed codes, which are marked in bold, achieve upper bound for the minimum distance, i.e., these codes are optimal codes. Further, some of the constructed codes enjoy an additional property of being a self-orthogonal or an LCD code.

A linear code \mathcal{C} satisfying $\mathcal{C} \subseteq \mathcal{C}^\perp$, where \mathcal{C}^\perp is the dual code of the code \mathcal{C} , is called a self-orthogonal code. Some of the obtained codes are self-orthogonal. The

codes with this property are obtained from the following graphs: 14A, 30A, 40A, 56A, 80A, 90A, 98A, 98B, 112B, 112C, 120A, 120B, 144A, 146A and 182A (and 182B).

An LCD code (linear code with complementary dual) is a linear code \mathcal{C} which satisfies $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$. LCD codes were introduced by Massey in [20]. These codes have an important role in cryptography. Lately, there has been much interest and a lot of work has been done regarding this topic (see, e.g., [3, 13, 15]). The codes labeled with * in Table 1 are LCD codes.

The codes constructed from the graphs 6A, 18A, 54A, 78A, 114A, 150A, 162A (and 162B), and 186A are unique LCD codes with the given parameters, up to equivalence (see [13, Proposition 2.5, Theorem 4.5]). According to the classification of LCD codes given in [13], there exists exactly five LCD codes with the parameters [10, 4, 4]. In this paper, an [10, 4, 4] LCD code was obtained using the adjacency matrix of the cubic symmetric graph 20B.

From Corollary 1 it follows that the codes from the CSGs 90A, 110A, 112C, 120B, 128B, 144B and 192B can correct 4 errors in 5 iterations of the Gallager A algorithm, and the codes from the graphs 162B, 162C, 168E, 168F, 182D and 192C can correct 5 errors in 6 iterations of that algorithm.

Remark 1. *The obtained LDPC codes have small rate. To obtain higher rate codes one can do the following. If A is the parity-check matrix of an $[n, k, d]$ LDPC code \mathcal{C} constructed from a bipartite cubic symmetric graph, one can use the matrix $A' = [A \mid I_n]$ as the parity-check matrix of an LDPC code \mathcal{C}' , where I_n is the identity matrix of order n . The code \mathcal{C}' is an irregular LDPC code of length $2n$ and dimension n , i.e. with rate equal 0.5. The minimum distance of the code is 4, and the girth of the Tanner graph is preserved, i.e. the girth of the Tanner graph of the obtained code is the same as the girth of the Tanner graph of the initial code. Instead of the matrix I_n one can use an $n \times l$ matrix B consisting of l columns of the matrix I_n to obtain an LDPC code with the parity-check matrix $[A \mid B]$ that has length $n + l$ and dimension at least k . The minimum distance of the code is equal to 4 for $l \geq 3$.*

5 Simulation results

As an illustration, we present simulation results of the $[24, 6, 10]$ and $[96, 18, 16]$ LDPC codes, derived from the the cubic symmetric graphs $48A$ and $192C$, on 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 at [26], which employs the construction from [18, 19]. The codes are decoded with the sum-product decoding algorithm and the maximum number of iteration is set to 50. Figures 1 and 2 show the performance of the codes.

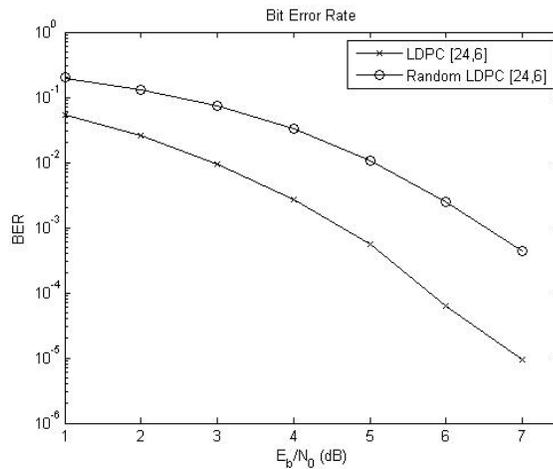


Figure 1: BER performance of the $[24, 6, 10]$ LDPC code derived from the graph $48A$

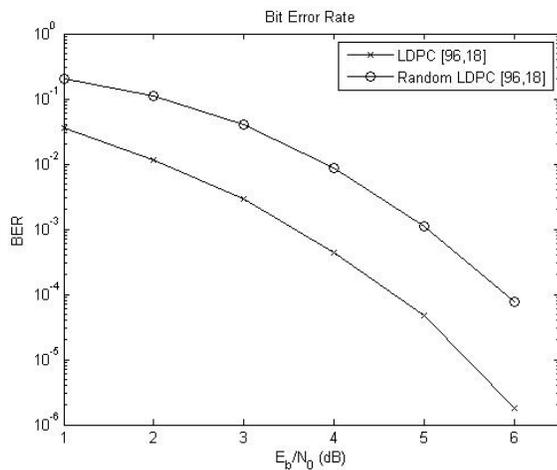


Figure 2: BER performance of the [96, 18, 16] LDPC code derived from the graph 192C

It can be seen from Figures 1 and 2 that the LDPC codes constructed from the cubic symmetric graphs, comparing to randomly generated LDPC codes, have better BER performance.

Acknowledgement

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

References

- [1] R. Balakrishnan, K. Ranganathan, A Textbook of Graph Theory, Springer, New York, 2012.
- [2] W. Bosma, J.Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, 1994. <http://magma.maths.usyd.edu.au/magma>.
- [3] C. Carlet, S. Guilley, Complementary Dual Codes for Counter-Measures to Side-Channel Attacks, Coding Theory and Applications (2015), 97–105

- [4] P. A. Catlin, Brooks' graph-coloring theorem and the independence number, *J. Comb. Theory* 27 (1979), 42–48.
- [5] S. K. Chilappagari, D. V. Nguyen, B. V. Vasic, M. W. Marcellin, Girth of the Tanner graph and error correction capability of LDPC codes, 46th Annual Allerton Conference on Communication, Control and Computing, 2008, 1238–1245.
- [6] M. Conder, R. Nedela, A refined classification of symmetric cubic graphs, *J. Algebra* 322 (2009), 722–740.
- [7] M. Conder, B. McKay, G. Royle, Cubic symmetric graphs (The Foster Census), Online available at <http://staffhome.ecm.uwa.edu.au/~00013890/remote/foster/>, Accessed on 18/01/2020.
- [8] D. Crnković, S. Rukavina, M. Šimac, LDPC codes from μ -geodetic graphs obtained from block designs, *Graphs Combin.* 35 (2019), 451–469.
- [9] R. Diestel, *Graph theory*, Springer-Verlag, Berlin Heidelberg, 2017.
- [10] R. M. Foster, Geometrical Circuits of Electrical Networks, *Trans. Amer. Inst. Elec. Engin.* 51 (1932), 309–317.
- [11] R. G. Gallager, *Low-Density Parity-Check Codes*, MIT Press, Cambridge, MA, 1963.
- [12] M. Greferath, C. Roßing, L. Storme, Current Research Topics in Galois Geometry, Galois geometries and low-density parity-check codes, Nova Science Publishers, 2011, 245–275.
- [13] M. Harada, K. Saito, Binary linear complementary dual codes, *Cryptogr. Commun.* 11 (2019), 677–696.
- [14] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
- [15] J. D. Key, B. G. Rodrigues, LCD codes from adjacency matrices of graphs, *Appl. Algebr. Eng. Comm.* 29 (2018), 227–244.

- [16] J.-L. Kim, U. N. Peled, I. Perepelitsa, V. Pless, Explicit construction of families of LDPC codes with no 4-cycles, *IEEE Trans. Inform. Theory* 50 (2004), 2378–2388.
- [17] F. Lazebnik, V. A. Ustimenko, Explicit construction of graphs with arbitrary large girth and of large size, *Discrete Appl. Math.* 60 (1995), 275–284.
- [18] D. J. C. MacKay, R. M. Neal, Near Shannon Limit Performance of Low Density Parity Check Codes, *Electronics Letters* 32 (1997), 457–458.
- [19] D. J. C. MacKay, R. M. Neal, Good error-correcting codes based on very sparse matrices, *IEEE Trans. Inform. Theory* 45 (1999), 399–431.
- [20] J. L. Massey, Linear codes with complementary duals, *Discrete Math.* 106/107 (1992), 337–342.
- [21] A. Nilli, On the second eigenvalue of a graph, *Discrete Math.* 91 (1991), 207–210.
- [22] G. Lechner, C. Pacher, Estimating Channel Parameters from the Syndrome of a Linear Code, *IEEE Commun. Letters* 17 (2013), 2148–2151.
- [23] P. Potočnik, P. Spiga, G. Verret, On the nullspace of arc-transitive graphs over finite fields, *J. Algebr. Comb.* 36 (2012), 389–401.
- [24] W. E. Ryan, S. Lin, *Channel Codes: Classical and Modern*, Cambridge University Press, 2009.
- [25] C. Pacher, P. Grabenweger, D. E. Simos, Weight distribution of the syndrome of linear codes and connections to combinatorial designs, 2016 *IEEE Int. Symp. Info. (ISIT)*, 2016, 3038–3042.
- [26] R. M. Neal, Software for Low Density Parity Check (LDPC) codes, Release of 2012-02-11. <http://www.cs.utoronto.ca/~radford/>.
- [27] J. Rosenthal, P. O. Vontobel, Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis, 38th Allerton Conference on Communication, Control and Computing, 2000, 248–257.

- [28] T. Shibuya, M. Onikubo, K. Sakaniwa, On Tanner's Lower Bound for the Minimum Distance of Regular LDPC Codes Based on Combinatorial Designs, *IEICE Trans. Fundamentals E86-A* (2003), 2428–2434.
- [29] J. Singh, M. Gupta, J. S. Bhullar, Construction of girth-8 $(3, L)$ -QC-LDPC codes of smallest CPM size using column multipliers, *Des. Codes Cryptogr.* 88 (2020), 41–49.
- [30] R. M. Tanner, Minimum-distance bounds by graph analysis, *IEEE Trans. Inform. Theory* 47 (2001), 808–821.
- [31] V. Toto-Zarasoá, A. Roumy, C. Guillemot, Maximum Likelihood BSC Parameter Estimation for the Slepian-Wolf Problem, *IEEE Commun. Lett.* 15 (2011), 232–234.
- [32] H. Xu, B. Bai, D. Feng, C. Sun, On the girth of Tanner $(3,11)$ quasi-cyclic LDPC codes, *Finite Fields Appl.* 46 (2017), 65–89.