ISSN 0032-9460, Problems of Information Transmission, 2017, Vol. 53, No. 3, pp. 229–241. © Pleiades Publishing, Inc., 2017.
Original Russian Text © F.I. Ivanov, 2017, published in Problemy Peredachi Informatsii, 2017, Vol. 53, No. 3, pp. 30–43.

CODING THEORY

A Special Class of Quasi-cyclic Low-Density Parity-Check Codes Based on Repetition Codes and Permutation Matrices[1]

F. I. Ivanov

Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow, Russia
e-mail: fii@iitp.ru

Received February 29, 2016; in final form, February 27, 2017

Abstract—We propose a new ensemble of binary low-density parity-check codes with parity-check matrices based on repetition codes and permutation matrices. The proposed class of codes is a subensemble of quasi-cyclic codes. For the constructed ensemble, we obtain minimum distance estimates. We present simulation results for the proposed code constructions under the (Sum-Product) iterative decoding algorithm for transmission over an additive white Gaussian noise channel using binary phase-shift keying.

DOI: 10.1134/S0032946017030048

1. INTRODUCTION

Binary low-density parity-check (LDPC) codes were proposed by Gallager in [1]. These are linear block codes defined via parity-check matrices $\boldsymbol{H}$ characterized by relatively few ones in their rows and columns.

Apart from random LDPC codes, different algebraic constructions of low-density parity-check codes are often used in practice, in particular LDPC codes based on permutation matrices [2–11], projective geometries [12], and other combinatorial constructions [13, 14].

The main objective of this article is construction and investigation of properties of the LDPC codes ensemble based on two algebraic constructions simultaneously: $[n_0, 1, n_0]$ repetition code ($n_0 \in \mathbb{N}$, $n_0 > 1$) and permutation matrices. As a result, we obtain an ensemble of low-rate ($R \leq 0.5$) quasi-cyclic LDPC codes possessing an efficient coding algorithm (based on shift registers) as well as a regular structure convenient for storage.

For the obtained ensemble, we give a lower bound on the code distance.

The paper is organized as follows. In Section 2 we introduce basic definitions and notation which are used throughout the paper. Section 3 contains an algorithm for generating parity-check matrices of the proposed codes. In Section 4 we study the resulting ensemble. Section 5 contains results of computer simulations for the obtained code ensemble and comparison with known LDPC code constructions.

2. BASIC DEFINITIONS AND NOTATION

By $GF^m(2)$ ($m > 1$, $m \in \mathbb{N}$) we understand the space of length-m binary vectors with vector operations performed according to the rules of the field $GF(2)$.

[1] The research was carried out at the Institute for Information Transmission Problems of the Russian Academy of Sciences at the expense of the Russian Science Foundation, project no. 14-50-00150.

Let $\boldsymbol{y} \in GF^m(2)$, then $\|\boldsymbol{y}\|$ is the Hamming weight of $\boldsymbol{y}$.

If $\boldsymbol{y} \in GF^m(2)$, then $\operatorname{supp}(\boldsymbol{y})$ denoted the support of $\boldsymbol{y}$, i.e., $\operatorname{supp}(\boldsymbol{y}) = \{j : y_j = 1\}$.

Let $\boldsymbol{y} \in GF^m(2)$ and $p \in \mathbb{Z}$, then $p + \operatorname{supp}(\boldsymbol{y})$ denotes the set $p + \operatorname{supp}(\boldsymbol{y}) = \{j + p \bmod m : y_j = 1\}$.

A basis for constructing LDPC codes considered in the paper is the following widely known code construction.

Definition 1. Let $n_0 > 1$, $n_0 \in \mathbb{N}$, then $\mathcal{R}(n_0)$ is the $[n_0, 1, n_0]$ repetition code of length n_0 with minimum distance $d = n_0$.

Definition 2. Let $m > 1$, $m \in \mathbb{N}$, and let $\boldsymbol{I}$ be the $m \times m$ identity matrix. Choose an arbitrary $p \in \mathbb{Z}$; then by $\boldsymbol{I}_p$ we understand the matrix obtained as the pth right cyclic shift of columns of $\boldsymbol{I}$.

It is clear that the matrix $\boldsymbol{I}_p$ is a circulant with row (column) weight 1. It is also easily seen that $\boldsymbol{I}_{mk} = \boldsymbol{I}$ for all integers k. Furthermore,

$$\boldsymbol{I}_{p_1} \cdot \boldsymbol{I}_{p_2} = \boldsymbol{I}_{p_1 + p_2 \bmod m},$$
$$\boldsymbol{I}_p^t = \boldsymbol{I}_{tp_1 \bmod m};$$

in particular, if $p_1 \in \mathbb{N}$, $0 \le p_1 \le m$, then

$$\boldsymbol{I}_{p_1}^{-1} = \boldsymbol{I}_{m - p_1}.$$

Thus, the set $\mathcal{I}_m = \{\boldsymbol{I}_p : p \in \mathbb{Z}\}$ of $m \times m$ matrices $\boldsymbol{I}_p$ forms a multiplicative cyclic group of order m with generator $\boldsymbol{I}_1$.

Clearly, action of the group $\mathcal{I}_m$ on the set $GF^m(2)$ is cyclic shift of coordinates of a vector $\boldsymbol{y} \in GF^m(2)$: $\boldsymbol{c} = \boldsymbol{y}\boldsymbol{I}_p$, and if $\operatorname{supp}(\boldsymbol{y})$ is the support of $\boldsymbol{y}$, then $\operatorname{supp}(\mathbf{c}) = p + \operatorname{supp}(\boldsymbol{y})$.

Next we prove a simple lemma to be used below.

Lemma. *Let* $\boldsymbol{I}_p \in \mathcal{I}_m$, $\boldsymbol{y} \in GF^m(2)$, *and* $\|\boldsymbol{y}\| = w$. *Then* $\operatorname{supp}(\boldsymbol{y}) = p + \operatorname{supp}(\boldsymbol{y})$ *implies* $pw \equiv 0 \bmod m$.

Proof. Let $\operatorname{supp}(\boldsymbol{y}) = \{i_1, i_2, \ldots, i_w\}$. Then $p + \operatorname{supp}(\boldsymbol{y}) = \{i_1 + p \bmod m, i_2 + p \bmod m, \ldots, i_w + p \bmod m\}$. The fact that $\operatorname{supp}(\boldsymbol{y}) = p + \operatorname{supp}(\boldsymbol{y})$ implies that for any $i_j \in \operatorname{supp}(\boldsymbol{y})$ there exists $i_k + p \bmod m \in p + \operatorname{supp}(\boldsymbol{y})$: $i_j \equiv i_k + p \bmod m$. Sum up the last congruences over $k, j = 1, \ldots, w$. Then the right-hand sides of the equations will take the same values as the left-hand ones (maybe, in a different order):

$$\sum_{j=1}^{w} i_j \equiv \sum_{k=1}^{w} (i_k + p) \bmod m,$$
$$\sum_{j=1}^{w} i_j \equiv \sum_{k=1}^{w} i_k + pw \bmod m,$$
$$pw \equiv 0 \bmod m. \quad \triangle$$

The lemma has an important consequence.

Corollary 1. *If* $\boldsymbol{y} \in GF^m(2)$, $\|\boldsymbol{y}\| = w$, $p \in \mathbb{Z}$, *and* $m \in \mathbb{Z}$ *is a prime, then* $\operatorname{supp}(\boldsymbol{y}) = p + \operatorname{supp}(\boldsymbol{y})$ *only if* $w = m$ *or* $w = 0$.

3. CONSTRUCTION OF AN ENSEMBLE OF BINARY LOW-DENSITY PARITY-CHECK CODES WITH PARITY-CHECK MATRICES BASED ON REPETITION CODES AND PERMUTATION MATRICES

This section describes the most general method for constructing LDPC codes based on repetition codes $\mathcal{R}(n_0)$ and permutation matrices.

Consider a parity-check matrix $\boldsymbol{H}_b$ of the $[n_0, 1, n_0]$ code of length n_0 and rate $R = 1/n_0$. We choose $m > 1$, $k > 0$, $m, k \in \mathbb{N}$; also, we consider the group $\mathcal{I}_m$ and choose $2(n_0 - 1)k^2$ arbitrary matrices $\boldsymbol{I}_{p_j}$, $p_j \in \mathbb{N}$, $j = 1, \ldots, 2(n_0-1)k^2$ from $\mathcal{I}_m$. Then we divide the set $\mathcal{S}$ of selected matrices into $2(n_0 - 1)$ equinumerous sets $\mathcal{S}_i$, $i = 1, \ldots, 2(n_0 - 1)$, $|\mathcal{S}_i| = k^2$, and compose from elements of each set $\mathcal{S}_i$ a $k \times k$ block matrix $\boldsymbol{Q}_i$ (hereinafter, indices p_{ij} of matrices $\boldsymbol{I}$ and $\boldsymbol{Q}_i$ should be understood as $p_{i,j}$):

$$\boldsymbol{Q}_i = \begin{pmatrix} \boldsymbol{I}_{p_{i1}} & \boldsymbol{I}_{p_{i2}} & \boldsymbol{I}_{p_{i3}} & \ldots & \boldsymbol{I}_{p_{ik}} \\ \boldsymbol{I}_{p_{i(k+1)}} & \boldsymbol{I}_{p_{i(k+2)}} & \boldsymbol{I}_{p_{i(k+3)}} & \ldots & \boldsymbol{I}_{p_{i(2k)}} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \boldsymbol{I}_{p_{i(k^2-k+1)}} & \boldsymbol{I}_{p_{i(k^2-k+2)}} & \boldsymbol{I}_{p_{i(k^2-k+3)}} & \ldots & \boldsymbol{I}_{p_{ik^2}} \end{pmatrix}.$$

It is clear that the matrix $\boldsymbol{Q}_i$, composed of k^2 circulants, has size $mk \times mk$ and contains k ones in each row and column.

Replace each one in the matrix $\boldsymbol{H}_b$ with $\boldsymbol{Q}_i$ and each zero with the all-zero $mk \times mk$ matrix $\boldsymbol{Z}$; then the resulting matrix

$$\boldsymbol{H} = \begin{pmatrix} \boldsymbol{Q}_1 & \boldsymbol{Q}_{n_0} & 0 & 0 & \ldots & 0 \\ \boldsymbol{Q}_2 & 0 & \boldsymbol{Q}_{n_0+1} & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \boldsymbol{Q}_{n_0-1} & 0 & 0 & \ldots & 0 & \boldsymbol{Q}_{2(n_0-1)} \end{pmatrix}$$

has size $mk(n_0 - 1) \times mkn_0$, weights of all its rows are $2k$, weights of the first mk columns are $k(n_0 - 1)$, and the other columns have weight k. We will consider $\boldsymbol{H}$ as a parity-check matrix of an LDPC code.

Thus, choosing arbitrary integers $m > 1$ and $k > 0$ and also $2(n_0 - 1)k^2$ random elements from the group $\mathcal{I}_m$, we define an ensemble of row-regular LDPC codes of length $n = mkn_0$. We denote the resulting ensemble by $\mathcal{E}_{RC}(m, k, n_0)$.

Definition 3. An arbitrary code $\mathcal{C} \in \mathcal{E}_{RC}(m, k, n_0)$ is called a low-density parity-check code based on permutation matrices and $\mathcal{R}(n_0)$.

4. ANALYSIS OF THE MINIMUM DISTANCE OF LDPC CODES FROM THE ENSEMBLE $\mathcal{E}_{RC}(m, k, n_0)$

First of all, let us show that the weight of any codeword of a code from the ensemble $\mathcal{E}_{RC}(m, k, n_0)$ (under nonrestrictive conditions on k and n_0) is even.

Theorem 1. *Let $\mathcal{C} \in \mathcal{E}_{RC}(m, k, n_0)$; then for all k and n_0 (except for the case where both k is even and n_0 is odd) and for all $\boldsymbol{c} \in \mathcal{C}$ we have $\|\boldsymbol{c}\| = 2t$, $t \in \mathbb{N}$.*

Before passing to the proof, let us first introduce a number of additional definitions. Let $\boldsymbol{y} \in GF^n(2)$. A vector $\boldsymbol{y}$ of length $n = mkn_0$ can be represented in the following form:

$$\boldsymbol{y} = (\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_{n_0}), \quad \boldsymbol{y}_i \in GF^{mk}(2).$$

Now we write down the syndrome $\boldsymbol{S}$ for $\boldsymbol{y}$:

$$\boldsymbol{S} = (\boldsymbol{S}_1, \ldots, \boldsymbol{S}_{n_0-1})^T = \boldsymbol{H}\boldsymbol{y}^T,$$

where

$$\boldsymbol{S}_i = \boldsymbol{Q}_i \boldsymbol{y}_1^T + \boldsymbol{Q}_{n_0+i-1} \boldsymbol{y}_{i+1}^T.$$

Definition 4. We call the vector $\boldsymbol{S}_i \in GF^{mk}(2)$ the ith component of the syndrome $\boldsymbol{S}$ (or the ith syndrome-component).

Further, since $\boldsymbol{y}_i \in GF^{mk}(2)$, we have the following representation:

$$\boldsymbol{y}_i = (\boldsymbol{y}_{i1}, \boldsymbol{y}_{i2}, \ldots, \boldsymbol{y}_{ik}), \quad \boldsymbol{y}_{ij} \in GF^m(2).$$

Then

$$\boldsymbol{Q}_i \boldsymbol{y}_j^T = \begin{pmatrix} \boldsymbol{I}_{p_{i1}} & \boldsymbol{I}_{p_{i2}} & \boldsymbol{I}_{p_{i3}} & \ldots & \boldsymbol{I}_{p_{ik}} \\ \boldsymbol{I}_{p_{i(k+1)}} & \boldsymbol{I}_{p_{i(k+2)}} & \boldsymbol{I}_{p_{i(k+3)}} & \ldots & \boldsymbol{I}_{p_{i(2k)}} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \boldsymbol{I}_{p_{i(k^2-k+1)}} & \boldsymbol{I}_{p_{i(k^2-k+2)}} & \boldsymbol{I}_{p_{i(k^2-k+3)}} & \ldots & \boldsymbol{I}_{p_{ik^2}} \end{pmatrix} (\boldsymbol{y}_{j1}, \boldsymbol{y}_{j2}, \ldots, \boldsymbol{y}_{jk})^T.$$

Thus, if we represent $\boldsymbol{S}_i$ in the form

$$\boldsymbol{S}_i = (\boldsymbol{S}_{i_1}, \boldsymbol{S}_{i_2}, \ldots, \boldsymbol{S}_{i_k}), \quad \boldsymbol{S}_{i_j} \in GF^m(2),$$

then

$$\boldsymbol{S}_{i_j} = \sum_{s=1}^{k} \boldsymbol{I}_{p_{i,((j-1)k+s)}} \boldsymbol{y}_{1s}^T + \sum_{s=1}^{k} \boldsymbol{I}_{p_{(n_0+i-1),((j-1)k+s)}} \boldsymbol{y}_{(i+1)s}^T.$$

Definition 5. Let $\boldsymbol{y} = (\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_{n_0})$, $\boldsymbol{y}_i \in GF^{mk}(2)$, where $\boldsymbol{y}_i = (\boldsymbol{y}_{i1}, \boldsymbol{y}_{i2}, \ldots, \boldsymbol{y}_{ik})$, $\boldsymbol{y}_{ij} \in GF^m(2)$; then we call $\boldsymbol{y}_1$ the information part of $\boldsymbol{y}$. Moreover, we say that $\boldsymbol{y}_{ij}$ is contained in the information segment of $\boldsymbol{y}$ if $i = 1$ ($i = 2, \ldots, n_0$).

Definition 6. Let $\boldsymbol{y}_{ij} \in GF^m(2)$. We say that $\boldsymbol{y}_{ij}$ is a part of the syndrome-component $\boldsymbol{S}_t$ if

$$\boldsymbol{y}_{ij} \in \{\boldsymbol{y}_{11}, \boldsymbol{y}_{12}, \ldots, \boldsymbol{y}_{1k}\} \cup \{\boldsymbol{y}_{(t+1)1}, \boldsymbol{y}_{(t+1)2}, \ldots, \boldsymbol{y}_{(t+1)k}\}.$$

Remark. Sometimes, instead of the phrase "$\boldsymbol{y}_{ij}$ is a part of the syndrome-component $\boldsymbol{S}_t$" we will say that the syndrome-component $\boldsymbol{S}_t$ contains $\boldsymbol{y}_{ij}$.

Now we proceed to the proof of Theorem 1.

Proof. We choose an arbitrary code $\mathcal{C} \in \mathcal{E}_{RC}(m, k, n_0)$. Since k cannot be even when n_0 is odd, then either $n_0 k$ is even or k and $(n_0 - 1)k$ are both odd. If k and $(n_0 - 1)k$ are both odd, then all columns of the parity-check matrix $\boldsymbol{H}$ of $\mathcal{C}$ are of odd weights. It is known that weights of all codewords of a code $\mathcal{C}$ whose parity-check matrix contains only odd-weight columns are even.

Now consider the case where $n_0 k$ is even. Assume that $\boldsymbol{u} \in \mathcal{C}$ but $\|\boldsymbol{u}\| = 2t + 1$ for some $t \in \mathbb{N}$. We represent $\boldsymbol{u}$ as

$$\boldsymbol{u} = (\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{n_0}), \quad \boldsymbol{u}_i = (\boldsymbol{u}_{i1}, \boldsymbol{u}_{i2}, \ldots, \boldsymbol{u}_{ik}), \quad \boldsymbol{u}_{ij} \in GF^m(2).$$

Since the vector $\boldsymbol{u}$ can be represented as $n_0 k$ vectors of length m and since $n_0 k$ is even, $\boldsymbol{u}$ has an odd weight if and only if $\boldsymbol{u}$ consists of an odd number of odd-weight vectors and an odd number of even-weight vectors. Since each component of $\boldsymbol{S}$ contains $2k$ vectors $\boldsymbol{u}_{ij}$, $i = 1, \ldots, n_0$, $j = 1, \ldots, k$, there is at least one $\boldsymbol{S}_i$ that contains an odd number of odd-weight vectors and an odd number of even-weight vectors.

If

$$\boldsymbol{S}_i = (\boldsymbol{S}_{i_1}, \boldsymbol{S}_{i_2}, \ldots, \boldsymbol{S}_{i_k}),$$

we have $\boldsymbol{S}_i = \boldsymbol{0}$ if and only if $\boldsymbol{S}_{i_j} = \boldsymbol{0}$, $j = 1, \ldots, k$.

Let us show that for $\|\boldsymbol{u}\| = 2t + 1$ none of the $\boldsymbol{S}_{i_j}$ can be zero. Without loss of generality, we may assume that $j = 1$. In this case

$$\boldsymbol{S}_{i_1} = \sum_{s=1}^{k} \boldsymbol{I}_{p_{is}} \boldsymbol{u}_{1s}^T + \sum_{s=1}^{k} \boldsymbol{I}_{p_{(n_0+i-1),s}} \boldsymbol{u}_{(i+1)s}^T.$$

The condition that the component $\boldsymbol{S}_{i_1}$ is zero is equivalent to the condition that all rows of

$$\boldsymbol{M} = \begin{pmatrix} \boldsymbol{I}_{p_{i1}}\boldsymbol{u}_{11}^T \\ \boldsymbol{I}_{p_{i2}}\boldsymbol{u}_{12}^T \\ \cdots \\ \boldsymbol{I}_{p_{ik}}\boldsymbol{u}_{1k}^T \\ \boldsymbol{I}_{p_{(n_0+i-1),1}}\boldsymbol{u}_{(i+1)1}^T \\ \boldsymbol{I}_{p_{(n_0+i-1),2}}\boldsymbol{u}_{(i+1)2}^T \\ \cdots \\ \boldsymbol{I}_{p_{(n_0+i-1),k}}\boldsymbol{u}_{(i+1)k}^T \end{pmatrix}^T$$

have even weights. At the same time, for any $\boldsymbol{u} \in GF^m(2)$ and $\boldsymbol{I}_p \in \mathcal{I}_m$ we have $\|\boldsymbol{u}\| = \|\boldsymbol{u}\boldsymbol{I}_p\|$, so the number of ones in $\boldsymbol{M}$ is the same as in the vector $(\boldsymbol{u}_1\ \boldsymbol{u}_{i+1})$, each component of which is contained in $\boldsymbol{S}_i$. But, by the assumption, the weight of this vector is odd, so the number of ones in $\boldsymbol{M}$ is odd, and hence all its rows cannot have even weights; this means that our assumption that $\|\boldsymbol{u}\| = 2t+1$ is not true. Contradiction. $\triangle$

The study of the minimum distance of codes from the ensemble $\mathcal{E}_{RC}(m,k,n_0)$ is closely related to the concept of a cycle in a parity-check matrix. Recall that a cycle of length 4 in a parity-check matrix means a rectangle with ones in its corners.

For quasi-cyclic LDPC codes there is a simple method for searching for cycles of length 4.

Let $\boldsymbol{B} = (\boldsymbol{I}_{p_{ij}})_{i,j=1,1}^{l,n_0}$, and let $I_{p_{ij}} \in \mathcal{I}_m$ be a parity-check matrix of a quasi-cyclic LDPC code of length $n = mn_0$. Then we have the following.

Theorem 2. *A matrix $\boldsymbol{B}$ contains cycles of length 4 if and only if it has at least one submatrix of the form*

$$\begin{pmatrix} \boldsymbol{I}_{p_{i_1j_1}} & \boldsymbol{I}_{p_{i_1j_2}} \\ \boldsymbol{I}_{p_{i_2j_1}} & \boldsymbol{I}_{p_{i_2j_2}} \end{pmatrix}, \quad 1 \le i_1 < i_2 \le l, \quad 1 \le j_1 < j_2 \le n_0,$$

such that

$$(p_{i_1j_1} + p_{i_2j_2}) - (p_{i_2j_1} + p_{i_1j_2}) \equiv 0 \mod m.$$

Proof. See the proof of Theorem 2 in [7]. $\triangle$

Now we point out an obvious relationship between the minimum distance of codes from the ensemble $\mathcal{E}_{RC}(m,k,n_0)$ and short cycles in parity-check matrices $\boldsymbol{H}$.

Theorem 3. *Let $\boldsymbol{H}$ be a parity-check matrix of some code $\mathcal{C}$ from the ensemble $\mathcal{E}_{RC}(m,k,n_0)$ for which the conditions of Theorem 1 are satisfied. If $\boldsymbol{H}$ does not contain any cycles of length 4, then $d_{\min}(\mathcal{C}) \ge 4$.*

Proof. Given that the weights of columns (rows) of $\boldsymbol{H}$ are greater than 1, the absence of cycles of length 4 means that the parity-check matrix does not contain identical columns, whence $d_{\min}(\mathcal{C}) \ge 3$, but since by Theorem 3 a codeword weight cannot be odd, we have $d_{\min}(\mathcal{C}) \ge 4$. $\triangle$

To simplify all further proofs, we will assume that $n_0 = 4$ and $k = 2$, though all further conclusions can easily be generalized to the case of $n_0 > 4$ and $k = 2$.

The matrix $\boldsymbol{H}$ has the form

$$\boldsymbol{H} = \begin{pmatrix} \boldsymbol{I}_{p_{11}} & \boldsymbol{I}_{p_{12}} & \boldsymbol{I}_{p_{41}} & \boldsymbol{I}_{p_{42}} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{I}_{p_{13}} & \boldsymbol{I}_{p_{14}} & \boldsymbol{I}_{p_{43}} & \boldsymbol{I}_{p_{44}} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{I}_{p_{21}} & \boldsymbol{I}_{p_{22}} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}_{p_{51}} & \boldsymbol{I}_{p_{52}} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{I}_{p_{23}} & \boldsymbol{I}_{p_{24}} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}_{p_{53}} & \boldsymbol{I}_{p_{54}} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{I}_{p_{31}} & \boldsymbol{I}_{p_{32}} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}_{p_{61}} & \boldsymbol{I}_{p_{62}} \\ \boldsymbol{I}_{p_{33}} & \boldsymbol{I}_{p_{34}} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}_{p_{63}} & \boldsymbol{I}_{p_{64}} \end{pmatrix},$$

and we represent a codeword $\boldsymbol{u} \in \mathcal{C}$ as

$$\boldsymbol{u} = (\boldsymbol{u}_{11}\boldsymbol{u}_{12}\boldsymbol{u}_{21}\boldsymbol{u}_{22}\boldsymbol{u}_{31}\boldsymbol{u}_{32}\boldsymbol{u}_{41}\boldsymbol{u}_{42}), \quad \boldsymbol{u}_{ij} \in GF^m(2).$$

Let us introduce an additional definition, which will be needed in the proof of the next theorem.

Definition 7. A matrix $\boldsymbol{B} = (\boldsymbol{I}_{p_{ij}})_{i,j=1,1}^{l,n_0}$ is said to be d-nonuniform if all its minors (in the block sense) of order d ($d \le l$) are distinct (noncongruent modulo m, where m is the size of $\boldsymbol{I}_{p_{ij}}$).

Now we prove the following theorem, improving the estimate for the minimum distance of codes from the ensemble $\mathcal{E}_{RC}(m, k, n_0)$ (under some light additional restrictions).

Theorem 4. *Let $\boldsymbol{H}$ be is a parity-check matrix of a code $\mathcal{C}$ from the ensemble $\mathcal{E}_{RC}(m, 2, 4)$ for which the conditions of Theorem 3 are satisfied. Furthermore, let $m > 5$ be prime and at least one submatrix $\boldsymbol{H}$ of the form $(\boldsymbol{Q}_i\ \boldsymbol{Q}_{3+i})$ $(i = 1, \dots, n_0 - 1)$ be 2-nonuniform. Then $d_{\min}(\mathcal{C}) \ge 8$.*

Proof. All congruences in the proof are assumed to hold modulo m.

Let $\boldsymbol{u} \in \mathcal{C}$ and $\|\boldsymbol{u}\| = 4$. It is clear that if $\boldsymbol{u}$ consists of only two nonzero vectors $\boldsymbol{u}_{i_1j_1}, \boldsymbol{u}_{i_2j_2} \in GF^m(2)$, then $\|\boldsymbol{u}_{i_1j_1}\| = \|\boldsymbol{u}_{i_2j_2}\| = 2$; furthermore, these vectors should be contained in the same syndrome $\boldsymbol{S}_i$. Without loss of generality we may assume that $i = 1$, $\boldsymbol{u}_{i_1j_1} = \boldsymbol{u}_{11}$, and $\boldsymbol{u}_{i_1j_1} = \boldsymbol{u}_{12}$. Then $\boldsymbol{S}_1 = \boldsymbol{0}$ if and only if

$$\begin{cases} \boldsymbol{u}_{11} = \boldsymbol{I}_{p_{12}-p_{11}}\boldsymbol{u}_{12}, \\ \boldsymbol{u}_{11} = \boldsymbol{I}_{p_{14}-p_{13}}\boldsymbol{u}_{12}, \end{cases}$$
$$\boldsymbol{I}_{p_{12}-p_{11}}\boldsymbol{u}_{12} = \boldsymbol{I}_{p_{14}-p_{13}}\boldsymbol{u}_{12},$$
$$\boldsymbol{u}_{12} = \boldsymbol{I}_p\boldsymbol{u}_{12},$$

where

$$p = (p_{14} - p_{13}) - (p_{12} - p_{11}).$$

The absence of length-4 cycles ensures that $p \not\equiv 0 \mod m$. On the other hand, since m is prime, by Corollary 1 we have $\boldsymbol{u}_{12} = \boldsymbol{I}_p\boldsymbol{u}_{12}$ only if $\|\boldsymbol{u}_{12}\| = m$.

Proofs for the obvious cases where $\boldsymbol{u}$ consists of three nonzero vectors (two weight-1 vectors and one weight-2 vector and where $\boldsymbol{u}$ consists of four weight-1 vectors are omitted.

Thus, by Theorem 3, we have $d_{\min}(\mathcal{C}) \ge 6$.

Now we show that $\mathcal{C}$ does not contain weight-6 words. Obviously, if $\boldsymbol{u}$ ($\|\boldsymbol{u}\| = 6$) consists of t nonzero vectors and among them there is a vector with weight greater than the sum of weights of all the other $t - 1$ vectors, then such a $\boldsymbol{u}$ cannot be a codeword.

The situation where $\boldsymbol{u}$ consists of only two nonzero vectors $\boldsymbol{u}_{i_1j_1}, \boldsymbol{u}_{i_2j_2} \in GF^m(2)$ was considered above.

Arguments for the cases of $t = 3, 4, 6$ are obvious and are therefore omitted.

Let $t = 5$. Then $\boldsymbol{u}$ consists of four weight-1 vectors $\boldsymbol{u}_{i_1j_1}, \boldsymbol{u}_{i_2j_2}, \boldsymbol{u}_{i_3j_3}, \boldsymbol{u}_{i_4j_4} \in GF^m(2)$ and one vector $\boldsymbol{u}_{i_5j_5}$ of weight 2. Then either formation of at least one syndrome involves only the weight-1 vectors and hence, according to the above-proved, at least one syndrome is nonzero, or the weight-2 vector is either $\boldsymbol{u}_{11}$ or $\boldsymbol{u}_{12}$. For definiteness, we may assume that $\|\boldsymbol{u}_{11}\| = 2$. If in this case $\boldsymbol{u}_{12} = \boldsymbol{0}$, then for $\boldsymbol{u} \in \mathcal{C}$ to hold it is necessary that $\|\boldsymbol{u}_{ij}\| = 1$, $i = 2, \dots, 4$, $j = 1, 2$ but then $\|\boldsymbol{u}\| = 8$. If $\|\boldsymbol{u}_{12}\| = 1$, then for $\boldsymbol{u} \in \mathcal{C}$ to hold it is necessary that only one vector in each pair $(\boldsymbol{u}_{21}, \boldsymbol{u}_{22})$, $(\boldsymbol{u}_{31}, \boldsymbol{u}_{32})$, and $(\boldsymbol{u}_{41}, \boldsymbol{u}_{42})$ has weight 1. Without loss of generality, consider the pair $(\boldsymbol{u}_{21}, \boldsymbol{u}_{22})$ and assume that $\|\boldsymbol{u}_{21}\| = 1$. Consider the system of equations

$$\begin{cases} \boldsymbol{u}_{11} = \boldsymbol{I}_{p_{12}-p_{11}}\boldsymbol{u}_{12} + \boldsymbol{I}_{p_{41}-p_{11}}\boldsymbol{u}_{21}, \\ \boldsymbol{u}_{11} = \boldsymbol{I}_{p_{14}-p_{13}}\boldsymbol{u}_{12} + \boldsymbol{I}_{p_{43}-p_{13}}\boldsymbol{u}_{21}. \end{cases}$$

Let $\operatorname{supp}(\boldsymbol{u}_{11}) = \{u_{11}^{(1)}, u_{11}^{(2)}\}$, $\operatorname{supp}(\boldsymbol{u}_{12}) = \{u_{12}^{(1)}\}$, and $\operatorname{supp}(\boldsymbol{u}_{21}) = \{u_{21}^{(1)}\}$; then the equality

$$\boldsymbol{I}_{p_{12}-p_{11}}\boldsymbol{u}_{12} + \boldsymbol{I}_{p_{41}-p_{11}}\boldsymbol{u}_{21} = \boldsymbol{I}_{p_{14}-p_{13}}\boldsymbol{u}_{12} + \boldsymbol{I}_{p_{43}-p_{13}}\boldsymbol{u}_{21}$$

and property

$$\boldsymbol{c} = \boldsymbol{y}\boldsymbol{I}_p \mapsto \operatorname{supp}(\boldsymbol{c}) = p + \operatorname{supp}(\boldsymbol{y})$$

imply that

$$u_{12}^{(1)} + (p_{12} - p_{11}) + u_{21}^{(1)} + (p_{41} - p_{11}) \equiv u_{12}^{(1)} + (p_{14} - p_{13}) + u_{21}^{(1)} + (p_{43} - p_{13}) \bmod m.$$

From the last expression we easily obtain

$$(p_{13} - p_{11}) - (p_{14} - p_{12}) \equiv (p_{43} - p_{41}) - (p_{13} - p_{11}) \bmod m.$$

The last congruence means the determinants of the matrices

$$\begin{pmatrix} \boldsymbol{I}_{p_{11}} & \boldsymbol{I}_{p_{12}} \\ \boldsymbol{I}_{p_{13}} & \boldsymbol{I}_{p_{14}} \end{pmatrix}, \qquad \begin{pmatrix} \boldsymbol{I}_{p_{11}} & \boldsymbol{I}_{p_{21}} \\ \boldsymbol{I}_{p_{13}} & \boldsymbol{I}_{p_{23}} \end{pmatrix}$$

are congruent modulo m. Thus, the submatrix $(\boldsymbol{Q}_1\ \boldsymbol{Q}_4)$ is not 2-uniform. Similarly it can be shown that none of the matrices $(\boldsymbol{Q}_i\ \boldsymbol{Q}_{3+i})$, $i = 1, \ldots, 3$ is 2-uniform. Contradiction.

We have shown that no word $\boldsymbol{u}$ of weight 4 or 6 can be a codeword, and since the code does not contain words of weight 5 and 7, we have $d_{\min}(\mathcal{C}) \geq 8$. $\triangle$

To continue the analysis of the codes minimum distance from the ensemble $\mathcal{E}_{RC}(m, 2, 4)$, we need to define a cycle of length 8.

Definition 8. We say that a parity-check matrix $\boldsymbol{B}$ of a quasicyclic LDPC code contains a length-8 cycle if it has at least one submatrix

$$\begin{pmatrix} \boldsymbol{I}_{p_{i_1 j_1}} & \boldsymbol{I}_{p_{i_1 j_2}} & \boldsymbol{I}_{p_{i_1 j_3}} & \boldsymbol{I}_{p_{i_1 j_4}} \\ \boldsymbol{I}_{p_{i_2 j_1}} & \boldsymbol{I}_{p_{i_2 j_2}} & \boldsymbol{I}_{p_{i_2 j_3}} & \boldsymbol{I}_{p_{i_2 j_4}} \end{pmatrix}, \quad 1 \leq i_1 < i_2 \leq l, \quad 1 \leq j_1 < j_2 < j_3 < j_4 \leq n_0,$$

such that

$$(p_{i_1 j_1} - p_{i_2 j_1}) + (p_{i_1 j_2} - p_{i_2 j_2}) + (p_{i_1 j_3} - p_{i_2 j_3}) + (p_{i_1 j_4} - p_{i_2 j_4}) \equiv 0 \bmod m,$$

where m is the size of $\boldsymbol{I}_{p_{ij}}$.

Now we are ready to formulate the main result of this paper.

Theorem 5. *Let $\boldsymbol{H}$ be a parity-check matrix of a code $\mathcal{C}$ from the ensemble $\mathcal{E}_{RC}(m, 2, 4)$ for which the conditions of Theorem* 3 *are satisfied. Furthermore, let at least one of its submatrices of the form $(\boldsymbol{Q}_i\ \boldsymbol{Q}_{3+i})$ $(i = 1, \ldots, n_0 - 1)$ do not contain a length-*8 *cycle. Then $d_{\min}(\mathcal{C}) \geq 10$.*

Proof. It is necessary and sufficient to show that if $\boldsymbol{u}$ is a codeword, then $\|u\| \geq 10$. By Theorem 4, it remains to show that $\mathcal{C}$ does not contain weight-8 codewords. Assume the contrary: let $\boldsymbol{u} \in \mathcal{C}$ but $\|\boldsymbol{u}\| = 8$. The ones of the vector $\boldsymbol{u}$ can be distributed among $2 \leq t \leq 8$ vectors of length m. We perform the proof for various t.

The arguments for the cases of $t = 2, 3, 4, 6, 7$ are obvious and therefore are omitted. Let $t = 5$. There are three admissible configurations which involve five nonzero vectors $\boldsymbol{u}_{i_1 j_1}, \boldsymbol{u}_{i_2 j_2}, \boldsymbol{u}_{i_3 j_3}$, $\boldsymbol{u}_{i_4 j_4}, \boldsymbol{u}_{i_5 j_5}$:

$$\{\|\boldsymbol{u}_{i_1 j_1}\|, \|\boldsymbol{u}_{i_2 j_2}\|, \|\boldsymbol{u}_{i_3 j_3}\|, \|\boldsymbol{u}_{i_4 j_4}\|, \|\boldsymbol{u}_{i_5 j_5}\|\} = \{\{1, 1, 1, 1, 4\}, \{1, 1, 2, 2, 2\}, \{1, 1, 1, 2, 3\}\}.$$

It is easy to show (by placing vectors of different weights in the information part of $\boldsymbol{u}$) that the first two configurations cannot form a codeword, so we skip ahead to the configuration $\{1, 1, 1, 2, 3\}$.

Since the number of vectors of nonzero weights is odd, the information part of $\boldsymbol{u}$ contains at least one nonzero vector. Let a nonzero vector be only one. If its weight is 3, then for an arbitrary syndrome $\boldsymbol{S}_j$ to be $\mathbf{0}$, the total weight of vectors entering its additional part should be at least 3; however, $\|\boldsymbol{u}\| \geq 12$. If the only nonzero vector has weight 1, then there is a syndrome $\boldsymbol{S}_j$ (we may assume that $j = 1$) containing vectors of weights 3 and 2, then the weight of the additional parts of $\boldsymbol{S}_2$ and $\boldsymbol{S}_3$ is 2, and therefore, since there are no length-4 cycles in $\boldsymbol{H}$, we conclude that $\boldsymbol{S}_2, \boldsymbol{S}_3 \neq \mathbf{0}$. Analogous reasoning can easily be made in the case where the unique nonzero vector of the information part of $\boldsymbol{u}$ has weight 2. Thus, the information part of $\boldsymbol{u}$ must consist of two nonzero vectors.

Let $\|\boldsymbol{u}_{11}\| = \|\boldsymbol{u}_{12}\| = 1$; then

$$\|\boldsymbol{Q}_i(\boldsymbol{u}_{11}, \boldsymbol{u}_{12})^T\| = 2, \quad i = 1, \ldots, 3.$$

Let a weight-3 vector be in the additional part of the syndrome $\boldsymbol{S}_1$. Then, to have $\boldsymbol{S}_1 = \mathbf{0}$, the additional part of $\boldsymbol{S}_1$ must also necessarily contain the remaining weight-1 vector. Without loss of generality we may assume that a weight-2 vector belongs to the additional part of $\boldsymbol{S}_2$. Then $\boldsymbol{S}_2 \neq \mathbf{0}$ and $\boldsymbol{S}_3 \neq \mathbf{0}$ (since $\boldsymbol{H}$ does not contain length-4 cycles).

Let $\|\boldsymbol{u}_{11}\| = 3$ and $\|\boldsymbol{u}_{12}\| = 1$; then

$$\|\boldsymbol{Q}_i(\boldsymbol{u}_{11}, \boldsymbol{u}_{12})^T\| \geq 2, \quad i = 1, \ldots, 3.$$

Since the weight of the remaining nonzero vectors is 4, there is at least one $\boldsymbol{S}_j$ with

$$\|\boldsymbol{S}_j\| > 0, \quad j \in \{1, 2, 3\}.$$

Assume that $\|\boldsymbol{u}_{11}\| = 2$ and $\|\boldsymbol{u}_{12}\| = 1$; then exactly two syndromes, $\boldsymbol{S}_{j_1}$ and $\boldsymbol{S}_{j_2}$, are formed by vectors of weight $1, 1, 2$. Hence, according to Theorem 4,

$$\|\boldsymbol{S}_{j_1}\|, \|\boldsymbol{S}_{j_2}\| > 0.$$

It remains to consider the case where $\|\boldsymbol{u}_{11}\| = 3$ and $\|\boldsymbol{u}_{12}\| = 2$. Then $\boldsymbol{S}_1, \boldsymbol{S}_2, \boldsymbol{S}_3$ are formed by vectors of weights $1, 2, 3$. Consider $\boldsymbol{S}_1$, and let us assume that $\|\boldsymbol{u}_{11}\| = 3$, $\|\boldsymbol{u}_{12}\| = 2$, $\|\boldsymbol{u}_{21}\| = 1$, and $\|\boldsymbol{u}_{22}\| = 0$. Since

$$(\boldsymbol{Q}_1\ \boldsymbol{Q}_4) = \begin{pmatrix} \boldsymbol{I}_{p_{11}} & \boldsymbol{I}_{p_{12}} & \boldsymbol{I}_{p_{21}} & \boldsymbol{I}_{p_{22}} \\ \boldsymbol{I}_{p_{13}} & \boldsymbol{I}_{p_{14}} & \boldsymbol{I}_{p_{23}} & \boldsymbol{I}_{p_{24}} \end{pmatrix},$$

the equality

$$\boldsymbol{S}_1 = (\boldsymbol{Q}_1\ \boldsymbol{Q}_4)(\boldsymbol{u}_{11}\ \boldsymbol{u}_{12}\ \boldsymbol{u}_{21}\ \boldsymbol{u}_{22})^T = \mathbf{0}$$

is equivalent to a system of vector equations with matrix coefficients

$$\begin{cases} \boldsymbol{I}_{p_{11}}\boldsymbol{u}_{11} + \boldsymbol{I}_{p_{12}}\boldsymbol{u}_{12} + \boldsymbol{I}_{p_{21}}\boldsymbol{u}_{21} = \mathbf{0}, \\ \boldsymbol{I}_{p_{13}}\boldsymbol{u}_{11} + \boldsymbol{I}_{p_{14}}\boldsymbol{u}_{12} + \boldsymbol{I}_{p_{23}}\boldsymbol{u}_{21} = \mathbf{0}. \end{cases}$$

Here and in what follows, we omit the transposition sign at vectors $\boldsymbol{u}_{ij}$ to simplify the computations.

Let $\operatorname{supp}(\boldsymbol{u}_{11}) = \{u_{11}^{(1)}, u_{11}^{(2)}, u_{11}^{(3)}\}$, $\operatorname{supp}(\boldsymbol{u}_{12}) = \{u_{12}^{(1)}, u_{12}^{(2)}\}$, and $\operatorname{supp}(\boldsymbol{u}_{21}) = \{u_{21}^{(1)}\}$. Expressing $\boldsymbol{u}_{11}$ from both equations of the system

$$\begin{cases} \boldsymbol{u}_{11} = \boldsymbol{I}_{p_{12}-p_{11}}\boldsymbol{u}_{12} + \boldsymbol{I}_{p_{21}-p_{11}}\boldsymbol{u}_{21}, \\ \boldsymbol{u}_{11} = \boldsymbol{I}_{p_{14}-p_{13}}\boldsymbol{u}_{12} + \boldsymbol{I}_{p_{23}-p_{13}}\boldsymbol{u}_{21} \end{cases}$$

and introducing the notation

$$\widetilde{p}_2 = p_{12} - p_{11}, \qquad \widetilde{p}_3 = p_{21} - p_{11}, \qquad \widetilde{p}_5 = p_{14} - p_{13}, \qquad \widetilde{p}_6 = p_{23} - p_{13},$$

we pass to an equivalent system:

$$\begin{cases} \boldsymbol{u}_{11} = \boldsymbol{I}_{\tilde{p}_2}\boldsymbol{u}_{12} + \boldsymbol{I}_{\tilde{p}_3}\boldsymbol{u}_{21}, \\ \boldsymbol{u}_{11} = \boldsymbol{I}_{\tilde{p}_5}\boldsymbol{u}_{12} + \boldsymbol{I}_{\tilde{p}_6}\boldsymbol{u}_{21}. \end{cases}$$

Now from each vector equation with matrix coefficients we pass to equations over integers. Note that each of these transitions is equivalent up to an arbitrary permutation of right-hand sides of each equation over integers.

Since $|\operatorname{supp}(\boldsymbol{u}_{11})| = 3$, $|\operatorname{supp}(\boldsymbol{u}_{12})| = 2$, $|\operatorname{supp}(\boldsymbol{u}_{21})| = 1$, and $\boldsymbol{c} = \boldsymbol{y}\boldsymbol{I}_p \mapsto \operatorname{supp}(\boldsymbol{c}) = p+\operatorname{supp}(\boldsymbol{y})$, the equation $\boldsymbol{u}_{11} = \boldsymbol{I}_{\tilde{p}_2}\boldsymbol{u}_{12} + \boldsymbol{I}_{\tilde{p}_3}\boldsymbol{u}_{21}$ is equivalent to the system

$$\begin{cases} u_{11}^{(1)} \equiv u_{12}^{(1)} + \widetilde{p}_2 \mod m, \\ u_{11}^{(2)} \equiv u_{12}^{(2)} + \widetilde{p}_2 \mod m, \\ u_{11}^{(3)} \equiv u_{21}^{(1)} + \widetilde{p}_3 \mod m, \end{cases}$$

and from the equation $\boldsymbol{u}_{11} = \boldsymbol{I}_{\tilde{p}_5}\boldsymbol{u}_{12} + \boldsymbol{I}_{\tilde{p}_6}\boldsymbol{u}_{21}$ we obtain

$$\begin{cases} u_{11}^{(1)} \equiv u_{12}^{(1)} + \widetilde{p}_5 \mod m, \\ u_{11}^{(2)} \equiv u_{12}^{(2)} + \widetilde{p}_5 \mod m, \\ u_{11}^{(3)} \equiv u_{21}^{(1)} + \widetilde{p}_6 \mod m. \end{cases} \tag{1}$$

Now we sum up all equations in each system

$$\begin{aligned} u_{11}^{(1)} + u_{11}^{(2)} + u_{11}^{(3)} &\equiv u_{12}^{(1)} + u_{12}^{(2)} + u_{21}^{(1)} + 2\widetilde{p}_2 + \widetilde{p}_3 \mod m, \\ u_{11}^{(1)} + u_{11}^{(2)} + u_{11}^{(3)} &\equiv u_{12}^{(1)} + u_{12}^{(2)} + u_{21}^{(1)} + 2\widetilde{p}_5 + \widetilde{p}_6 \mod m \end{aligned}$$

and subtract the second equation from the first:

$$2(\widetilde{p}_5 - \widetilde{p}_2) \equiv \widetilde{p}_3 - \widetilde{p}_6 \mod m. \tag{2}$$

Condition (2) is required for the right-hand sides of system (1) to be vectors of weight 3. If condition (2) is not satisfied, then $\boldsymbol{S}_1 \neq \boldsymbol{0}$. Let condition (2) be satisfied; then we exclude the vector $\boldsymbol{u}_{11}$ and pass to the equation

$$\begin{gathered} \boldsymbol{I}_{\tilde{p}_2}\boldsymbol{u}_{12} + \boldsymbol{I}_{\tilde{p}_3}\boldsymbol{u}_{21} = \boldsymbol{I}_{\tilde{p}_5}\boldsymbol{u}_{12} + \boldsymbol{I}_{\tilde{p}_6}\boldsymbol{u}_{21}, \\ (\boldsymbol{I}_{\tilde{p}_3} + \boldsymbol{I}_{\tilde{p}_6})\boldsymbol{u}_{21} = (\boldsymbol{I}_{\tilde{p}_2} + \boldsymbol{I}_{\tilde{p}_5})\boldsymbol{u}_{12}. \end{gathered}$$

Since $\boldsymbol{H}$ does not contain length-4 cycles, we have $\|(\boldsymbol{I}_{\tilde{p}_3} + \boldsymbol{I}_{\tilde{p}_6})\boldsymbol{u}_{21}\| = 2$, while

$$\|(\boldsymbol{I}_{\tilde{p}_2} + \boldsymbol{I}_{\tilde{p}_5})\boldsymbol{u}_{12}\| = 2 \text{ or } 4.$$

We are only interested in the case where $\|(\boldsymbol{I}_{\tilde{p}_2} + \boldsymbol{I}_{\tilde{p}_5})\boldsymbol{u}_{12}\| = 2$, which is achieved when

$$(\widetilde{p}_2 - \widetilde{p}_5)^2 \equiv (j+1)^2 \mod m,$$

where $j \leq \lfloor m/2 \rfloor$ is the least number of zeros between ones in the vector $\boldsymbol{c} = (\boldsymbol{I}_{\tilde{p}_2} + \boldsymbol{I}_{\tilde{p}_5})\boldsymbol{u}_{12}$.

Let us explain the last congruence. If $\operatorname{supp}(\boldsymbol{u}_{12}) = \{u_{12}^{(1)}, u_{12}^{(2)}\}$, then

$$\begin{aligned} \operatorname{supp}(\boldsymbol{I}_{\tilde{p}_2}\boldsymbol{u}_{12}) &= \{u_{12}^{(1)} + \widetilde{p}_2 \mod m, u_{12}^{(2)} + \widetilde{p}_2 \mod m\}, \\ \operatorname{supp}(\boldsymbol{I}_{\tilde{p}_5}\boldsymbol{u}_{12}) &= \{u_{12}^{(1)} + \widetilde{p}_5 \mod m, u_{12}^{(2)} + \widetilde{p}_5 \mod m\}. \end{aligned}$$

It is clear that $\|(\boldsymbol{I}_{\tilde{p}_2} + \boldsymbol{I}_{\tilde{p}_5})\boldsymbol{u}_{12}\| = 2$ $\|(\boldsymbol{I}_{\tilde{p}_2} + \boldsymbol{I}_{\tilde{p}_5})\boldsymbol{u}_{12}\| = 2$ only when

$$u_{12}^{(1)} + \widetilde{p}_2 \equiv u_{12}^{(2)} + \widetilde{p}_5 \mod m \qquad \text{or} \qquad u_{12}^{(2)} + \widetilde{p}_2 \equiv u_{12}^{(1)} + \widetilde{p}_5 \mod m.$$

Denote by j the least number of zeros between ones in the vector $(\boldsymbol{I}_{\tilde{p}_2} + \boldsymbol{I}_{\tilde{p}_5})\boldsymbol{u}_{12}$; then $j+1 = |u_{12}^{(1)} - u_{12}^{(2)}|$. Then, expressing $u_{12}^{(1)}$ and $u_{12}^{(2)}$ in the last two congruences through $\widetilde{p}_2$ and $\widetilde{p}_5$ and multiplying the obtained congruences, we obtain $(\widetilde{p}_2 - \widetilde{p}_5)^2 \equiv (j+1)^2 \mod m$.

In our case $j = \widetilde{p}_6 - \widetilde{p}_3 - 1$ (we may always assume that $\widetilde{p}_6 > \widetilde{p}_3$).

Then $\|(\boldsymbol{I}_{\tilde{p}_2} + \boldsymbol{I}_{\tilde{p}_5})\boldsymbol{u}_{12}\| = 2$ only when

$$(\widetilde{p}_2 - \widetilde{p}_5)^2 \equiv (\widetilde{p}_3 - \widetilde{p}_6)^2 \mod m,$$
$$((\widetilde{p}_2 - \widetilde{p}_5) - (\widetilde{p}_3 - \widetilde{p}_6))((\widetilde{p}_2 - \widetilde{p}_5) + (\widetilde{p}_3 - \widetilde{p}_6)) \equiv 0 \mod m.$$

Since m is prime, the last equation is equivalent to the system

$$\left[\begin{array}{l} (\widetilde{p}_2 - \widetilde{p}_5) - (\widetilde{p}_3 - \widetilde{p}_6) \equiv 0 \mod m, \\ (\widetilde{p}_2 - \widetilde{p}_5) + (\widetilde{p}_3 - \widetilde{p}_6) \equiv 0 \mod m. \end{array}\right. \tag{3}$$

Let the first equation of system (3) be satisfied. Adding condition (2) to it, we obtain the system

$$\begin{cases} (\widetilde{p}_2 - \widetilde{p}_5) \equiv \widetilde{p}_3 - \widetilde{p}_6 \mod m, \\ 2(\widetilde{p}_5 - \widetilde{p}_2) \equiv \widetilde{p}_3 - \widetilde{p}_6 \mod m, \end{cases}$$

where

$$3(\widetilde{p}_5 - \widetilde{p}_2) \equiv 0 \mod m.$$

Since m is prime, the last congruence means that

$$(p_{14} + p_{11}) - (p_{13} + p_{12}) \equiv 0 \mod m.$$

This congruence is equivalent to the presence of a length-4 cycle in the submatrix $\begin{pmatrix} \boldsymbol{I}_{p_{11}} & \boldsymbol{I}_{p_{12}} \\ \boldsymbol{I}_{p_{13}} & \boldsymbol{I}_{p_{14}} \end{pmatrix}$ of the parity-check matrix $\boldsymbol{H}$. Contradiction.

Suppose that the second equation of the system (3) is satisfied. Adding condition (2) to it, we obtain the system

$$\begin{cases} (\widetilde{p}_2 - \widetilde{p}_5) \equiv -(\widetilde{p}_3 - \widetilde{p}_6) \mod m, \\ 2(\widetilde{p}_5 - \widetilde{p}_2) \equiv \widetilde{p}_3 - \widetilde{p}_6 \mod m, \end{cases}$$

where

$$\widetilde{p}_5 - \widetilde{p}_2 \equiv 0 \mod m.$$

The obtained congruence was considered above. Thus, if $\boldsymbol{H}$ does not contain length-4 cycles, then $\boldsymbol{S}_1 \neq \boldsymbol{0}$, and the proof for the case $t = 5$ is complete.

For $t = 8$, there is a unique admissible configuration which involves eight nonzero vectors $\boldsymbol{u}_{i_1 j_1}, \boldsymbol{u}_{i_2 j_2}, \ldots, \boldsymbol{u}_{i_8 j_8}$:

$$\{\|\boldsymbol{u}_{11}\|, \ldots, \|\boldsymbol{u}_{42}\|\} = \{1,1,1,1,1,1,1,1\}.$$

Four weight-1 vectors are contained in each syndrome $\boldsymbol{S}_j$. Assume that the matrix $(\boldsymbol{Q}_j\ \boldsymbol{Q}_{3+j})$ does not contain a length-8 cycle. Without loss of generality we may assume that $j = 1$. Then

$$\boldsymbol{S}_1 = (\boldsymbol{Q}_1\ \boldsymbol{Q}_4)(\boldsymbol{u}_{11}\ \boldsymbol{u}_{12}\ \boldsymbol{u}_{21}\ \boldsymbol{u}_{22})^T = \boldsymbol{0}$$

implies

$$\begin{cases} \boldsymbol{I}_{p_{11}}\boldsymbol{u}_{11} + \boldsymbol{I}_{p_{12}}\boldsymbol{u}_{12} + \boldsymbol{I}_{p_{21}}\boldsymbol{u}_{21} + \boldsymbol{I}_{p_{22}}\boldsymbol{u}_{22} = \boldsymbol{0}, \\ \boldsymbol{I}_{p_{13}}\boldsymbol{u}_{11} + \boldsymbol{I}_{p_{14}}\boldsymbol{u}_{12} + \boldsymbol{I}_{p_{23}}\boldsymbol{u}_{21} + \boldsymbol{I}_{p_{23}}\boldsymbol{u}_{22} = \boldsymbol{0}. \end{cases}$$

Let $\operatorname{supp}(\boldsymbol{u}_{11}) = \{u_{11}^{(1)}\}$, $\operatorname{supp}(\boldsymbol{u}_{12}) = \{u_{12}^{(1)}\}$, $\operatorname{supp}(\boldsymbol{u}_{21}) = \{u_{21}^{(1)}\}$, and $\operatorname{supp}(\boldsymbol{u}_{22}) = \{u_{22}^{(1)}\}$. Then we pass from the system of vector equations to a system over integers:

$$\begin{cases} (p_{11} + u_{11}^{(1)}) + (p_{12} + u_{12}^{(1)}) + (p_{21} + u_{21}^{(1)}) + (p_{22} + u_{22}^{(1)}) \equiv 0 \mod m, \\ (p_{13} + u_{11}^{(1)}) + (p_{14} + u_{12}^{(1)}) + (p_{23} + u_{21}^{(1)}) + (p_{24} + u_{22}^{(1)}) \equiv 0 \mod m. \end{cases}$$

Subtract the second equation from the first:

$$(p_{11} - p_{13}) + (p_{12} - p_{14}) + (p_{21} - p_{23}) + (p_{22} - p_{24}) \equiv 0 \mod m.$$

The latter condition means that there is a length-8 cycle in the matrix $(\boldsymbol{Q}_1\ \boldsymbol{Q}_4)$. Contradiction.

We have shown that there is no codeword $\boldsymbol{u}$ of weight 8, and since the code $\mathcal{C}$ does not contain codewords of weight 9, we have $d_{\min}(\mathcal{C}) \geq 10$. $\triangle$

This theorem can easily be generalized to a wider class of codes. Namely, we have the following result.

Corollary 2. *Let $\boldsymbol{H}$ be a parity-check matrix of some code $\mathcal{C}$ from the ensemble $\mathcal{E}_{RC}(m, 2, n_0)$, where $n_0 > 3$ and $m > 5$ is a prime. If $\boldsymbol{H}$ does not contain length-4 cycles and if at least one submatrix of $\boldsymbol{H}$ of the form $(\boldsymbol{Q}_i\ \boldsymbol{Q}_{n_0+i-1})$ $(i = 1, \ldots, n_0 - 1)$ does not contain a length-8 cycle and is 2-nonuniform, then $d_{\min}(\mathcal{C}) \geq 10$.*

It is easily seen that in the case of $n_0 > 4$, the requirement that one submatrix of $\boldsymbol{H}$ of the form $(\boldsymbol{Q}_i\ \boldsymbol{Q}_{n_0+i-1})$ $(i = 1, \ldots, n_0 - 1)$ does not contain a length-8 cycle, can be discarded because not all $\boldsymbol{S}_j$ $(j = 1, \ldots, n_0 - 1)$ contain four weight-1 vectors. Thus, we have the following result.

Corollary 3. *Let $\boldsymbol{H}$ be a parity-check matrix of some code $\mathcal{C}$ from the ensemble $\mathcal{E}_{RC}(m, 2, n_0)$, where $n_0 > 4$ and $m > 5$ is a prime. If $\boldsymbol{H}$ does not contain length-4 cycles and if at least one submatrix of $\boldsymbol{H}$ of the form $(\boldsymbol{Q}_i\ \boldsymbol{Q}_{n_0+i-1})$ $(i = 1, \ldots, n_0 - 1)$ is 2-nonuniform, then $d_{\min}(\mathcal{C}) \geq 10$.*

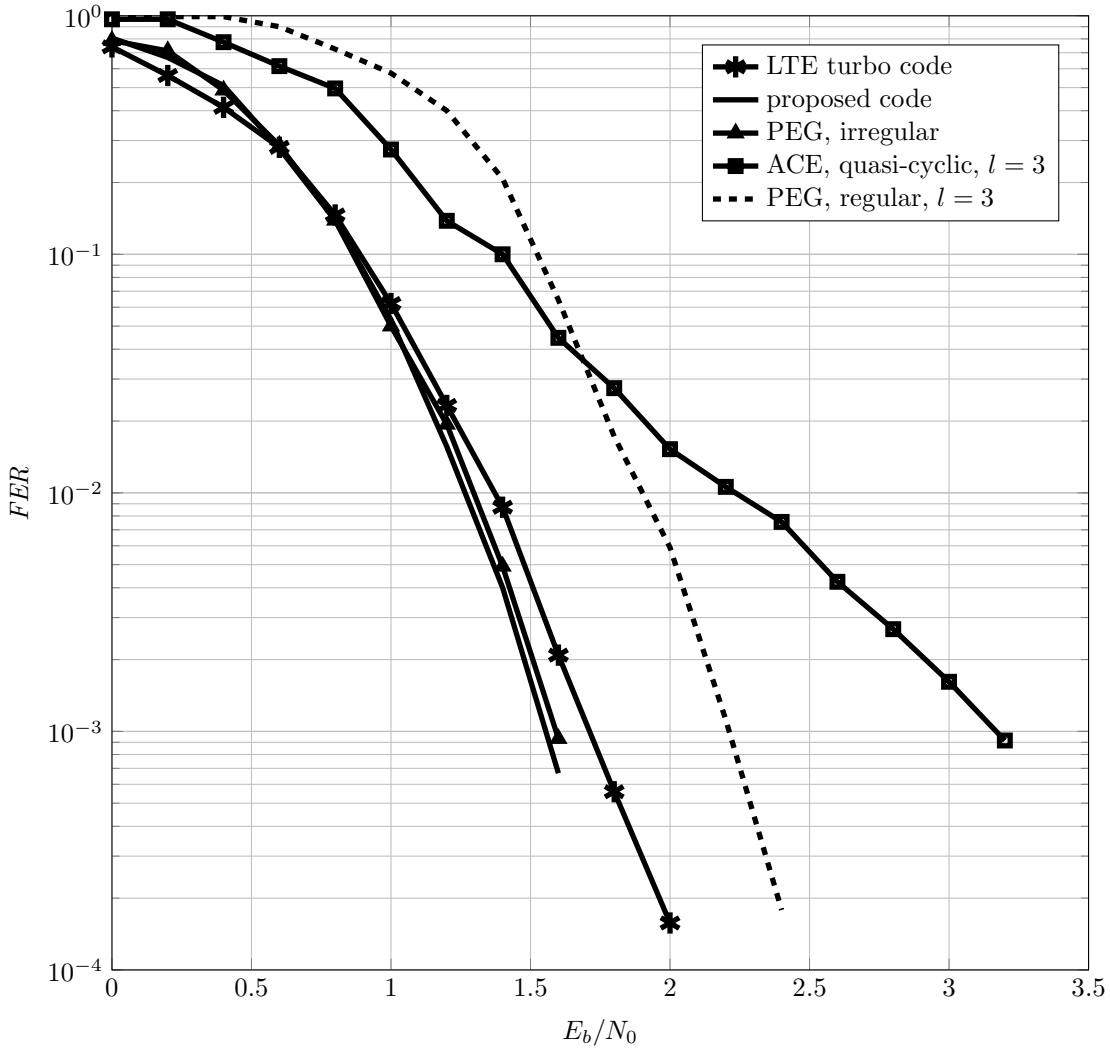
5. SIMULATION RESULTS

A function for MatLab was written to generate parity-check matrices for LDPC codes based on permutation matrices and $\mathcal{R}(n_0)$. Simulation was performed using the MatLab system. An additive white Gaussian noise (AWGN) channel with quadrature amplitude modulation (QAM-4) was chosen as a transmission channel. As a decoding algorithm, an iterative Sum-Product algorithm with "soft" input was chosen working with code representation in the bipartite Tanner graph form. The maximum number of iterations was limited by 100.

A $(1448, 365)$-code with parameters $m = 181$, $R = 0.2521$, $k = 2$, $n_0 = 4$, and $d_{\min} \geq 10$ was constructed.

For the comparative analysis (by simulation methods), we considered codes that were constructed using the *ACE* (generalized approximate cycle extrinsic message degree constrained design) algorithm [15, 16] and the *PEG* (progressive edge-growth) algorithm [17, 18]. These code constructions have the same lengths and rates as the proposed code. Furthermore, parity-check matrices of LDPC codes based on the PEG algorithm have four ones in each row, 25 percent of columns have weight 6, and the remaining 75 percent of columns have weight 2.

Also, we compare the proposed code with the binary $(1440, 352)$ turbo code of rate $R = 0.2444$ from the LTE standard.



Comparison of frame error rate (FER) versus signal-to-noise ratio per information symbol (E_b/N_0) for codes of length $n = 1448$.

Simulation results show that proposed codes behave better than codes based on the ACE and PEG algorithms. The irregular LDPC codes constructed using the PEG algorithm show almost identical behavior to the codes constructed in the paper. At the same time, codes from the $\mathcal{E}_{RC}(m, 2, n_0)$ ensemble have more regular structure, which allows to optimize the storage procedure for them, while codes built using the PEG algorithm have parity-check matrix with a random structure. In addition, it should be noted that codes proposed in the paper behave similarly to the turbo code from the LTE standard.

6. CONCLUSION

We presented a new ensemble of binary low-density parity-check codes with parity-check matrices obtained by replacing each one in the parity-check matrix of an $[n_0, 1, n_0]$ repetition code by a block matrix where each block is a permutation matrix (each zero is replaced by a zero matrix of the corresponding size). We give estimates for the minimum code distance of such codes. Computer simulation results allow us to conclude that the obtained code constructions are not inferior to codes constructed on the basis of PEG and ACE algorithms nor to the turbo code from the LTE standard.

REFERENCES

1. Gallager, R.G., *Low-Density Parity-Check Codes*, Cambridge: MIT Press, 1963. Translated under the title *Kody s maloi plotnost'yu proverok na chetnost'*, Moscow: Mir, 1966.
2. Gabidulin, E., Moinian, A., and Honary, B., Generalized Construction of Quasi-cyclic Regular LDPC Codes Based on Permutation Matrices, in *Proc. 2006 IEEE Int. Sympos. on Information Theory (ISIT'2006), Seattle, WA, USA, July 9–14, 2006*, pp. 679–683.
3. Hagiwara, M., Nuida, K., and Kitagawa, T., On the Minimal Length of Quasi-cyclic LDPC Codes with Girth ≥ 6, in *Proc. 2006 Int. Sympos. on Information Theory and Its Applications (ISITA'2006), Seoul, Korea, Oct. 29 – Nov. 1, 2006*.
4. Wang, Y., Yedidia, J.S., and Draper, S.C., Construction of High-Girth QC-LDPC Codes, in *Proc. 5th Int. Sympos. on Turbo Codes and Related Topics, Lausanne, Switzerland, Sept. 1–5, 2008*, pp. 180–185.
5. *Kim S. No J.-S. Chung H. Shin D.-J.* Quasi-cyclic Low-Density Parity-Check Codes with Girth Larger than 12, *IEEE Trans. Inform. Theory*, 2007, vol. 53, no. 8, pp. 2885–2891.
6. Ivanov, F.I., Zyablov, V.V., and Potapov, V.G., Low-Density Parity-Check Codes Based on Galois Fields, *Information Processes*, 2012, vol. 12, no. 1, pp. 68–83. Avaiable at `http://www.jip.ru/2012/68-83-2012.pdf`.
7. Ivanov, F.I., Zyablov, V.V., and Potapov, V.G., Estimation of Minimum Length of Cycles in Quasi-Cyclic Regular LDPC Codes Based on the Permutation Matrices, *Informatsionno-Upravlyayushchie Sistemy*, 2012, no. 3 (58), pp. 42–45.
8. Zyablov, V.V., Ivanov, F.I., and Potapov, V.G., Comparison of Various Constructions of Binary LDPC Codes Based on Permutation Matrices, *Information Processes*, 2012, vol. 12, no. 1, pp. 31–52. Avaiable at `http://www.jip.ru/2012/31-52-2012.pdf`.
9. *Ivanov F.I. Zyablov V.V. Potapov V.G.* Low-Density Parity-Check Codes Based on the Independent Subgroups // Proc. XIII Int. Sympos. on Problems of Redundancy in Information and Control Systems (RED'2012). St. Petersburg, Russia. September 5–10, 2012, pp. 31–34.
10. Ivanov, F.I., Zyablov, V.V., and Potapov, V.G., The Score of the Minimum Length of Cycles in Generalized Quasi-cyclic Regular LDPC Codes, in *Proc. 13th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-13), Pomorie, Bulgaria, June 15–21, 2012*, pp. 162–167.
11. Esmaeili, M. and Gholami, M., Structured Quasi-cyclic LDPC Codes with Girth 18 and Column-Weight $J \geq 3$, *Int. J. Electron. Commun. (AEÜ)*, 2010, vol. 64, no. 3, pp. 202–217.
12. Kou, Y., Lin, S., and Fossorier, M., Low-Density Parity Check Codes Based on Finite Geometries: A Rediscovery and New Results, *IEEE Trans. Inform. Theory*, 2001, vol. 47, no. 7, pp. 2711–2736.
13. Vasic, B., Pedagani, K., and Ivkovic, M., High-Rate Girth-Eight Low-Density Parity-Check Codes on Rectangular Integer Lattices, *IEEE Trans. Commun.*, 2004, vol. 52, no. 8, pp. 1248–1252.
14. Johnson, S., Low-Density Parity-Check Codes from Combinatorial Designs, *PhD Thesis*, School of Electrical Engineering and Computer Science, Univ. of Newcastle, Australia, 2004.
15. Xiao, H. and Banihashemi, A.H., Improved Progressive-Edge-Growth (PEG) Construction of Irregular LDPC Codes, *IEEE Commun. Lett.*, 2004, vol. 8, no. 12, pp. 715–717.
16. Hu, X.-Y., Eleftheriou, E., and Arnold, D.M., Regular and Irregular Progressive Edge-Growth Tanner Graphs, *IEEE Trans. Inform. Theory*, 2003, vol. 51, no. 1, pp. 386–398.
17. Tian, T., Jones, C., Villasenor, J.D., and Wesel, R.D., Construction of Irregular LDPC Codes with Low Error Floors, in *Proc. 2003 IEEE Int. Conf. on Communications (ICC'2003), Anchorage, AK, USA, May 11–15, 2003*, vol. 5, pp. 3125–3129.
18. Vukobratovic, D., Djurendic, A., and Senk, V., ACE Spectrum of LDPC Codes and Generalized ACE Design, in *Proc. 2007 IEEE Int. Conf. on Communications (ICC'2007), Glasgow, Scotland, June 24–28, 2007*, pp. 665–670.