ISSN 0032-9460, Problems of Information Transmission, 2013, Vol. 49, No. 4, pp. 333–347. © Pleiades Publishing, Inc., 2013.
Original Russian Text © F.I. Ivanov, V.V. Zyablov, 2013, published in Problemy Peredachi Informatsii, 2013, Vol. 49, No. 4, pp. 41–56.

CODING THEORY

Low-Density Parity-Check Codes Based on Steiner Systems and Permutation Matrices

F. I. Ivanov and V. V. Zyablov

Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow
fii@iitp.ru zyablov@iitp.ru

Received May 15, 2013; in final form, August 27, 2013

Abstract—An algorithm for generating parity-check matrices of regular low-density parity-check codes based on permutation matrices and Steiner triple systems $S(v, 3, 2)$, $v = 2^m - 1$, is proposed. Estimations of the rate, minimum distance, and girth for obtained code constructions are presented. Results of simulation of the obtained code constructions for an iterative "belief propagation" (Sum-Product) decoding algorithm applied in the case of transmission over a binary channel with additive Gaussian white noise and BPSK modulation are presented.

DOI: 10.1134/S0032946013040042

1. INTRODUCTION

Low-density parity-check codes (LDPC codes) were proposed by Gallager in [1]. These are linear block codes defined by their parity-check matrices $\boldsymbol{H}$ characterized by a relatively small number of ones in their rows and columns. It is often convenient to consider an LDPC code as its Tanner graph [2], where connected symbol and code vertices are used for representation of rows and columns of a parity-check matrix.

An important characteristic of an LDPC code is absence of cycles of certain lengths. A cycle of length 4 (4-cycle) can be understood as a rectangle in the parity-check matrix whose vertices are ones. The absence of 4-cycles can be defined with the help of scalar product of all rows (or columns) in the parity-check matrix. If every pairwise scalar product of rows (or columns) in the parity-check matrix is not greater than 1, then 4-cycles are absent. Cycles of larger lengths are defined by the girth of the Tanner graph.

Apart from random LDPC codes, various algebraic constructions of low-density parity-check codes based on permutation matrices [3–12], projective geometries [13], and other combinatorial constructions [14, 15] are often used in practice. The main advantage of such approach is the possibility to obtain code construction with deterministic characteristics such as girth and minimum distance.

The main objective of this work is to construct and explore properties of an ensemble of low-density parity-check codes based on two algebraic constructions simultaneously: Steiner triple systems $S(v, 3, 2)$ and permutation matrices. The authors are not aware of works where Steiner triple systems and permutation matrices are simultaneously used for constructing parity-check matrices of LDPC codes.

We propose a simple generation method for parity-check matrices of such codes with $v = 2^m - 1$. For the obtained ensemble, we give lower and upper bounds on the code rate and lower bounds on the minimum distance and girth bound were. For the proposed constructions of parity-check matrices, we prove that the girth is at least 6 and the minimum distance is at least 4.

One of major advantages of this class of codes is the possibility for decoding parallelization [16].

It should be noted that LDPC-codes based on Steiner triple systems were also considered in [15], but in contrast to codes proposed in this paper, their decoding algorithm cannot be parallelized.

The paper is organized as followed. In Section 2 we introduce main definitions and notation which we need in what follows. Section 3 contains an algorithm for generating weight-3 codewords of a Hamming code. Section 4 presents an algorithm for generating parity-check matrices of codes proposed in this paper. In Section 5 we explore the obtained ensemble. In Section 6 we give an example of a code construction with minimum distance at least 6. Simulation results for the obtained code constructions are contained in Section 7. Comparison with known LDPC code constructions is conducted.

2. MAIN DEFINITIONS AND NOTATION

Definition 1. A Steiner system $S(v, k, t)$ is a pair (X, B) where X is a set of v elements and B is a class of k-subsets of X (called blocks) so that any t-subset of X is contained in exactly one block of the class B. A system $S(v, 3, 2)$ is called a Steiner triple system.

We will use the following notation:

- A system $S(v, 3, 2)$ is denoted by STS(v);
- Let $c(x)$ be a polynomial over $GF(2)$; then by $w(c(x))$ we mean the Hamming weight of $c(x)$;
- By $\mathcal{H}(m)$ we mean a binary $[2^m - 1, 2^m - m - 1, 3]$ Hamming code.

It is commonly known that $\mathcal{H}(m)$ is a perfect code. In 1847, Kirkman proved that STS(v) exists if and only if $v \equiv 1,\ 3 \pmod 6$.

In this paper we consider the case of $v = 2^m - 1$, $m > 1$, $m \in \mathbb{N}$. It is easy to note that if $m = 2k$, $k \in \mathbb{N}$, we have $2^m - 1 \equiv 3 \pmod 6$, and if $m = 2k + 1$, $2^m - 1 \equiv 1 \pmod 6$. Thus, the requirements of Kirkman's theorem are satisfied. Also, it is commonly known that weight-3 codewords of $\mathcal{H}(m)$ form a system STS($2^m - 1$).

For details on Steiner triple systems, see [17].

3. GENERATION OF WEIGHT-3 CODEWORDS OF $\mathcal{H}(m)$

Consider a Hamming code $\mathcal{H}(m)$, $m > 3$. We will represent all weight-3 codewords as $c(x) = x^{i_1} + x^{i_2} + x^{i_3}$, where $0 \le i_1 < i_2 < i_3 \le 2^m - 2$. A codeword $c(x)$ will be chosen so that all the $2^m - 2$ cyclic shifts of its coordinates are different. Also we define p to be the minimum natural number for which $c^{2^p}(x) \equiv c(x) \bmod (x^{2^m-1} - 1)$ holds.

Since $c(x)$ is a weight-3 codeword, $c^2(x), c^4(x), c^8(x), \ldots, c^{2^{p-1}}(x)$ are different weight-3 codewords.

Since $c^{2^m}(x) \equiv c(x) \bmod (x^{2^m-1} - 1)$, we have $p \le m$. It is easy to show that $p = m$ if $2^m - 1$ is a prime. Indeed, without loss of generality we may assume that $0 = i_1 < i_2 < i_3 \le 2^m - 2$. Then the equality $c^{2^p}(x) \equiv c(x) \bmod (x^{2^m-1} - 1)$ implies $i_2 2^p i_3 2^p \equiv i_2 i_3 \bmod (2^m - 1)$, which is equivalent to $i_2 i_3 (2^p - 1)(2^p + 1) \equiv 0 \bmod (2^m - 1)$. It is obvious that if $2^m - 1$ is a prime, this relation holds only if $p = m$.

However, in some cases, $p = m$ can be obtained even for a composite $2^m - 1$. The table presents values of p for some polynomials $c(x) \in \mathcal{H}(m)$, $w(c(x)) = 3$.

Since the code $\mathcal{H}(m)$ is cyclic, together with any codeword $c(x) \in \mathcal{H}(m)$ it contains $x^j c(x)$, $j = 1, \ldots, 2^m - 2$. Thus, a codeword $c(x) \in \mathcal{H}(m)$, $w(c(x)) = 3$, generates

$$N_3(c(x)) = p(2^m - 1)$$

codewords $c_j(x)$, $w(c_j(x)) = 3$.

Table

m	$c(x)$	p
4	x^4+x+1	2
5	x^5+x^2+1	5
6	x^6+x+1	6
7	x^7+x+1	7

The weight spectrum $A(w, 2^m-1)$ of the Hamming code $\mathcal{H}(m)$ is considered in [18]:

$$A(3, 2^m-1) = \frac{(2^m-1)(2^m-2)}{6}.$$

Thus, in the case of a prime 2^m-1, there are

$$N_{cl}(m) = \frac{A(3, 2^m-1)}{N_3(c(x))} = \frac{2^{m-1}-1}{3m}$$

codewords $\widetilde{c}_1(x), \widetilde{c}_2(x), \ldots, \widetilde{c}_{N_{cl}(m)}(x)$ such that any codeword $\widetilde{c}_i(x)$ in this set generates $N_3(\widetilde{c}_i(x)) = m(2^m-1)$ codewords of weight 3, but no codeword $x^k\widetilde{c}_j^{2^t}(x)$, $0 \le k \le 2^m-2$, $0 \le t < p$, can be obtained from $\widetilde{c}_i(x)$, $i \ne j$, using the algorithm discussed above.

4. LDPC CODES BASED ON PERMUTATION MATRICES AND STS(2^m-1)

Consider the Hamming code $\mathcal{H}(m)$, $m > 3$. Using the method proposed in Section 3, we construct $p(2^m-1)$ polynomials $\widetilde{c}_1(x), \ldots, \widetilde{c}_{p(2^m-1)}(x)$, $p \ge 2$, from polynomials $p\, c(x), \ldots, c^{2^{p-1}}(x)$. We arrange the obtained polynomials in the form of a matrix $\widetilde{\boldsymbol{H}}$ as follows:

$$\widetilde{\boldsymbol{H}} = \big[c(x), xc(x), \ldots, x^{2^m-2}c(x) \mid \ldots \mid c^{2^{p-1}}(x), xc^{2^{p-1}}(x), \ldots, x^{2^m-2}c^{2^{p-1}}(x)\big].$$

Now rewrite $\widetilde{\boldsymbol{H}}$ in the form

$$\widetilde{\boldsymbol{H}} = [\boldsymbol{S}_0, \ldots, \boldsymbol{S}_{p-1}],$$

where

$$\boldsymbol{S}_j = \big[c^{2^j}(x), xc^{2^j}(x), \ldots, x^{2^m-2}c^{2^j}(x)\big], \quad 0 \le j \le p-1.$$

A submatrix $\boldsymbol{S}_j$ is a square matrix of size $(2^m-1)\times(2^m-1)$. It is easy to check that the weight of any row or column of $\boldsymbol{S}_j \subset \widetilde{\boldsymbol{H}}$ is 3. This follows from the fact that any of three powers of $c^{2^j}(x)$ independently of each other runs over the complete system of residues modulo 2^m-1.

Thus, $\widetilde{\boldsymbol{H}}$ is of size $(2^m-1)\times p(2^m-1)$, the weight of each row is $\widetilde{n}_0 = 3p$, and the weight of each column is $\widetilde{l} = 3$.

The size of $\widetilde{\boldsymbol{H}}$ can be made a multiple of $p(2^m-1)$ by replacing each of the $3p(2^m-1)$ ones with an arbitrary $t\times t$ permutation matrix $\boldsymbol{P}_{ij}$ and each of the $p(2^m-1)^2 - 3p(2^m-1)$ zeros with the zero $t\times t$ matrix $\boldsymbol{Z}_{ij}$. Denote the result of this transformation of $\widetilde{\boldsymbol{H}}$ by $\widehat{\boldsymbol{H}}$; then $\widehat{\boldsymbol{H}}$ is a low-density $t(2^m-1)\times pt(2^m-1)$ matrix with each row having weight $n_0 = \widetilde{n}_0 = 3p$, and each column, weight $l = \widetilde{l} = 3$.

Choose an arbitrary natural k such that $2 \le k \le p$. Form a matrix $\boldsymbol{H}$ by choosing an arbitrary k-element, $1 < k \le p$, ordered subset $\langle \boldsymbol{S}_{i_1}, \ldots, \boldsymbol{S}_{i_k}\rangle \subset [\boldsymbol{S}_0, \ldots, \boldsymbol{S}_{p-1}]$, $0 \le i_j \le p-1$, $1 \le j \le k$. The matrix $\boldsymbol{H}$ thus obtained is of size $t(2^m-1)\times kt(2^m-1)$, the row weight is $3k$, and the column weight is 3.

Thus, by choosing arbitrary numbers $m > 3$ and $2 \le k \le p$ and choosing $3k(2^m-1)$ random $t\times t$ permutation matrices, $t > 1$, we define an ensemble of regular low-density parity-check $(3, 3k)$-codes of length $n = kt(2^m-1)$. We denote the obtained ensemble by $\mathcal{E}_{\mathrm{STS}}(m, k, t)$.

Definition 2. An arbitrary code $\mathcal{C} \in \mathcal{E}_{\mathrm{STS}}(m, k, t)$ will be called a low-density parity-check code based on permutation matrices and $\mathrm{STS}(2^m - 1)$.

5. SOME PROPERTIES OF LDPC CODES FROM THE $\mathcal{E}_{\mathrm{STS}}(m, k, t)$ ENSEMBLE

We obtain an upper and lower bound for the rate of codes in the $\mathcal{E}_{\mathrm{STS}}(m, k, t)$ ensemble.

Theorem 1. *Let R be the rate of an LDPC code $\mathcal{C} \in \mathcal{E}_{\mathrm{STS}}(m, k, t)$. Then*

$$\frac{1}{2} \le R \le 1 - \frac{1}{m}.$$

Proof. The condition $R \ge \frac{1}{2}$ is obtained by choosing the minimum value $k = 2$. The condition $R \le 1 - \frac{1}{m}$ follows since $p \le m$. $\triangle$

However, it should be noted that the rate R does not take all possible values from the segment $\left[\frac{1}{2}, 1 - \frac{1}{m}\right]$ but only takes finitely many values according to the parameter k.

In Section 3, the question was considered of the number of weight-3 codewords that cannot be obtained from each other by cyclic shifts and raising to a power. Finding such codewords allows us to slightly increase the rate of a resulted code. Consider the following example.

Example 1. Let $m = 7$. Consider the Hamming code of length 127 with generator polynomial $c(x) = x^7 + x + 1$. Since $2^7 - 1 = 127$ is a prime number, for this code we have

$$N_{cl}(7) = \frac{A(3, 2^7 - 1)}{N_3(c(x))} = \frac{2^{7-1} - 1}{21} = 3.$$

Thus, there are three polynomials such that neither of them can be obtained from another by a shift or raising to a power. These polynomials divide all $A(3, 127) = 2667$ weight-3 codewords into three equinumerous subsets M_1, M_2, M_3, $|M_i| = 889$, $i = 1, 2, 3$, such that no element of one subset can be represented via shifts or powers of elements of the other two.

Consider an arbitrary subset M_i. Without loss of generality, we may fix $i = 1$. According to the table given above, there is a polynomial $c(x)$ in M_1 such that the smallest p for which $c^{2^p}(x) \equiv c(x) \bmod (x^{127} - 1)$ is 7. Thus, the highest rate of a code whose parity-check matrix $\boldsymbol{H}_1$ is obtained by concatenation of all elements of M_1 and application of the procedure from Section 3 is $R_{\max} = 1 - \frac{1}{m} = \frac{6}{7} \approx 0.8571$.

The same is true for codes based on M_2 and M_3. We denote their parity-check matrices by $\boldsymbol{H}_2$ and $\boldsymbol{H}_3$, respectively.

Let us write the obtained matrices in succession. The obtained matrix

$$\boldsymbol{H} = [\boldsymbol{H}_1\, \boldsymbol{H}_2\, \boldsymbol{H}_3]$$

is a parity-check matrix of an LDPC code with the maximum rate

$$R_{\max} = 1 - \frac{1}{3m} = \frac{20}{21} \approx 0.9524.$$

Moreover, all properties that hold for its three subcodes are also valid for the obtained code.

Now let us estimate the minimum distance of a code based on $\mathrm{STS}(2^m - 1)$.

Theorem 2. *Let $d_{\min}$ be the minimum distance of an LDPC code $\mathcal{C}$ based on* $\mathrm{STS}(2^m - 1)$. *Then*

$$d_{\min} \ge 4.$$

Proof. It was proved in [15] that the minimum distance $\widetilde{d}_{\min}$ of a code whose parity-check matrix is the incidence matrix of a system $S(v,k,t)$ is at least $k+1$. Thus, the minimum distance of a code with parity-check matrix $\widetilde{\boldsymbol{H}}$ is at least 4. Hence, the minimum distance of a code with parity-check matrix $\boldsymbol{H}$ is also at least 4. $\triangle$

Example 2. Consider the Hamming code $\mathcal{H}(5)$. From the table given in Section 3, it follows that $p=5$. Thus, there are LDPC codes based on $S(31,3,2)$ with rates $R \in \left\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}\right\}$. For the polynomial $c(x)$, we choose $c(x) = x^5 + x^2 + 1$. Consider the matrix

$$\widetilde{\boldsymbol{H}} = [\boldsymbol{S}_0, \ldots, \boldsymbol{S}_4].$$

Choosing the ordered subset

$$\langle \boldsymbol{S}_1, \boldsymbol{S}_3 \rangle \subset [\boldsymbol{S}_0, \ldots, \boldsymbol{S}_4],$$

we construct the matrix $\widetilde{\boldsymbol{H}}_2 = [\boldsymbol{S}_1, \boldsymbol{S}_3]$.

One can verify that the minimum distance of the code with parity-check matrix $\widetilde{\boldsymbol{H}}_2$ is 6. Thus, the minimum distance d of the code whose parity-check matrix $\boldsymbol{H}$ is obtained by $\widetilde{\boldsymbol{H}}_2$ using the method described in Section 4 is at least 6.

In [15] it was proved that the girth g in the incidence matrix of $S(v,3,2)$ is 6; at the same time, the above-mentioned method for increasing the size of $\widetilde{\boldsymbol{H}}$ does not decrease g. Thus, we have the following result.

Theorem 3. *Let g be the girth of the parity-check matrix $\boldsymbol{H}$ of a code $\mathcal{C}$ based on* $\mathrm{STS}(2^m-1)$. *Then*

$$g \geq 6.$$

Now let us determine a condition guaranteeing a strict increase in the minimum distance when replacing each of the $3k(2^m-1)$ ones in $\widetilde{\boldsymbol{H}} = [\boldsymbol{S}_0, \ldots, \boldsymbol{S}_{k-1}]$ with matrices of cyclic p_{ij}-shifts (i.e., cyclic shifts by p_{ij} positions).

Theorem 4. *Let the minimum distance $\widetilde{d}$ of a code with parity-check matrix $\widetilde{\boldsymbol{H}}$ be* 4. *Consider all combinations of four linearly dependent columns in $\widetilde{\boldsymbol{H}}$. If, upon replacing ones in the columns with matrices of cyclic p_{ij}-shifts, in each of such combinations at least one cycle of length* 6 *is transformed into a cycle of greater length, then the minimum distance of the obtained code is $d \geq 6$.*

Proof. Consider the parity-check matrix $\widetilde{\boldsymbol{H}}$. Since $\widetilde{d}=4$, any three of its columns are linearly independent and there is at least one combination of four linearly dependent columns. Choose any of such combinations $\boldsymbol{h}_{i_1}, \boldsymbol{h}_{i_2}, \boldsymbol{h}_{i_3}, \boldsymbol{h}_{i_4}$. By properties of Steiner triple systems, the weight of any row in the matrix $\boldsymbol{H}_i$ obtained by concatenation of such columns is 2, and the weight of any column is 3. A configuration of such columns is shown in Fig. 1.

Consider a codeword of the code with parity-check matrix $\widetilde{\boldsymbol{H}}$:

$$\widetilde{\boldsymbol{c}} = (0\ldots0\underbrace{1}_{i_1}0\ldots0\underbrace{1}_{i_2}0\ldots0\underbrace{1}_{i_3}0\ldots0\underbrace{1}_{i_4}0\ldots0).$$

In the matrix $\widetilde{\boldsymbol{H}}$, replace every one with a $t\times t$ matrix of a cyclic p_{ij}-shift of columns of the identity matrix $\boldsymbol{I}$ and replace every zero with the $t \times t$ zero matrix. Similarly, replace every zero in $\boldsymbol{c}$ with the all-zero vector of length t and replace every of the four ones with an arbitrary vector $\boldsymbol{c}_{i_j}$, $j=1,\ldots,4$, of length t and weight 1. It is easy to note that if the four ones are arranged so that two (or more) of them belong to the same vector of length t, then the obtained vector is not a codeword. This follows from the linear independence of any three columns of the parity-check matrix $\widetilde{\boldsymbol{H}}$. Therefore, we are interested in the case where all the four ones are contained in different vectors of length t.

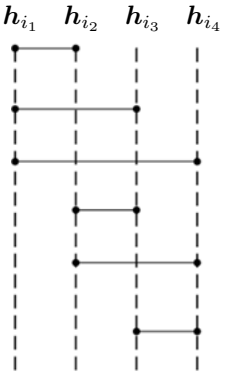

Fig. 1. Configuration of four linearly dependent columns $\boldsymbol{h}_{i_1}, \boldsymbol{h}_{i_2}, \boldsymbol{h}_{i_3}, \boldsymbol{h}_{i_4}$.

For this case, let us compute the product $\boldsymbol{H}\boldsymbol{c}^T$, where $\boldsymbol{H}$ is obtained from $\widetilde{\boldsymbol{H}}$ by the method described above, and $\boldsymbol{c}$ is obtained from $\widetilde{\boldsymbol{c}}$. Let $\boldsymbol{H}\boldsymbol{c}^T = 0$; then this matrix equation is equivalent to the following system of six equations:

$$\begin{cases} \boldsymbol{I}_{p_{11}}\boldsymbol{c}_{i_1} + \boldsymbol{I}_{p_{12}}\boldsymbol{c}_{i_2} = 0, \\ \boldsymbol{I}_{p_{21}}\boldsymbol{c}_{i_1} + \boldsymbol{I}_{p_{23}}\boldsymbol{c}_{i_3} = 0, \\ \boldsymbol{I}_{p_{31}}\boldsymbol{c}_{i_1} + \boldsymbol{I}_{p_{34}}\boldsymbol{c}_{i_4} = 0, \\ \boldsymbol{I}_{p_{42}}\boldsymbol{c}_{i_2} + \boldsymbol{I}_{p_{43}}\boldsymbol{c}_{i_3} = 0, \\ \boldsymbol{I}_{p_{52}}\boldsymbol{c}_{i_2} + \boldsymbol{I}_{p_{54}}\boldsymbol{c}_{i_4} = 0, \\ \boldsymbol{I}_{p_{63}}\boldsymbol{c}_{i_3} + \boldsymbol{I}_{p_{64}}\boldsymbol{c}_{i_4} = 0. \end{cases} \tag{1}$$

In this system, the first index in p_{ij} means the number of the equation, and the second, the column number. Since linear dependence is preserved under permutation of columns, such enumeration is always possible.

Let vectors $\boldsymbol{c}_{i_1}, \boldsymbol{c}_{i_2}, \boldsymbol{c}_{i_3}, \boldsymbol{c}_{i_4}$ of length t contain one in positions i_1, i_2, i_3, i_4, respectively. Since

$$\boldsymbol{I}_{p_{jk}}\boldsymbol{c}_{i_k} = \boldsymbol{c}_{(i_k+p_{jk}) \bmod t}, \quad k = 1, \ldots, 4, \quad j = 1, \ldots, 6,$$

system (1) of vector equations with matrix coefficients is equivalent to the following system in residues modulo t:

$$\begin{cases} i_1 - i_2 \equiv p_{12} - p_{11} \pmod t, \\ i_1 - i_3 \equiv p_{23} - p_{21} \pmod t, \\ i_1 - i_4 \equiv p_{34} - p_{31} \pmod t, \\ i_2 - i_3 \equiv p_{43} - p_{42} \pmod t, \\ i_2 - i_4 \equiv p_{54} - p_{52} \pmod t, \\ i_3 - i_4 \equiv p_{64} - p_{63} \pmod t. \end{cases} \tag{2}$$

In this system, i_1, i_2, i_3, i_4 are variables and p_{ij} are constants. Therefore, system (2) can be represented in the matrix form

$$\boldsymbol{X}\begin{pmatrix} i_1 \\ i_2 \\ i_3 \\ i_4 \end{pmatrix} = \boldsymbol{P},$$

where the coefficient matrix $\boldsymbol{X}$ over the ring of residues modulo t is of the form

$$\boldsymbol{X} = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

with $\operatorname{rank}(\boldsymbol{X}) = 3$, and $\boldsymbol{P}$ is the column of free parameters:

$$\boldsymbol{P} = \begin{pmatrix} p_{12} - p_{11} \\ p_{23} - p_{21} \\ p_{34} - p_{31} \\ p_{43} - p_{42} \\ p_{54} - p_{52} \\ p_{64} - p_{63} \end{pmatrix}.$$

According to the Kronecker–Capelli theorem, system (2) is consistent if and only if $\operatorname{rank}(\boldsymbol{X}) = \operatorname{rank}(\boldsymbol{X} \,|\, P)$.

By elementary transformations of the matrix $(\boldsymbol{X} \,|\, P)$, we obtain that $\operatorname{rank}(\boldsymbol{X} \,|\, P)$ coincides with the rank of the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & y \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

where

$$y = (p_{43} - p_{42}) + (p_{21} - p_{23}) + (p_{12} - p_{11}) \mod t.$$

According to [19], the condition $y = 0$ means that a cycle of length six exists in the matrix

$$\begin{pmatrix} \boldsymbol{I}_{p_{11}} & \boldsymbol{I}_{p_{12}} & \boldsymbol{0} \\ \boldsymbol{I}_{p_{21}} & \boldsymbol{0} & \boldsymbol{I}_{p_{23}} \\ \boldsymbol{0} & \boldsymbol{I}_{p_{42}} & \boldsymbol{I}_{p_{43}} \end{pmatrix}.$$

The same relations for the coefficients can be obtained by computing the rank of $(\boldsymbol{X} \,|\, P)$ in other ways.

Thus, if at least one of the relations of the form

$$(p_{43} - p_{42}) + (p_{21} - p_{23}) + (p_{12} - p_{11}) \equiv 0 \mod t \tag{3}$$

is violated, system (2) is inconsistent and, hence, has no solutions for any i_1, i_2, i_3, i_4.

This means that if at least one of relations of the form (3) in every linear combination of four columns (in block sense) of the parity-check matrix $\boldsymbol{H}$ is violated, a vector of weight 4 (or less) cannot be a codeword. Thus, $d > 4$. But an odd-weight vector cannot be a codeword for this code construction; hence, d cannot be less than 6. $\triangle$

Remark. It should be noted that a weight-6 codeword cannot be obtained on the chosen configuration of four columns because in that case column weights are different and a sum of the columns does not give a codeword. Thus, the minimum weight of a codeword obtained on this configuration of columns cannot be less than 8.

Now let us present a constructive method for lifting any combination of four linearly dependent columns of $\widetilde{\boldsymbol{H}}$ by matrices of cyclic p_{ij}-shifts so that to satisfy the conditions of Theorem 4.

Theorem 5. *Let $1 \le p_1 < p_2 < p_3$ be natural numbers, and let $t \ge p_3^3$. Consider a matrix $\boldsymbol{H}_i = [\boldsymbol{h}_{i_1} \dots \boldsymbol{h}_{i_4}]$ obtained by concatenation of a linear combination (see Fig. 1) of columns $\boldsymbol{h}_{i_1}, \boldsymbol{h}_{i_2}, \boldsymbol{h}_{i_3}, \boldsymbol{h}_{i_4}$ of $\widetilde{\boldsymbol{H}}$, where i_j, $j = 1, \dots, 4$, are indices of the columns $\boldsymbol{h}_{i_j}$ in the matrix $\widetilde{\boldsymbol{H}}$. Following the method described in Section 4, transform $\boldsymbol{H}_i$ into a matrix of the following form*:

$$\boldsymbol{H}_p = \begin{pmatrix} \boldsymbol{I} & \boldsymbol{I}_{p_1} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{I} & \boldsymbol{0} & \boldsymbol{I}_{p_1^2} & \boldsymbol{0} \\ \boldsymbol{I} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}_{p_1^3} \\ \boldsymbol{0} & \boldsymbol{I}_{p_2} & \boldsymbol{I}_{p_2^2} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{I}_{p_3} & \boldsymbol{0} & \boldsymbol{I}_{p_2^3} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}_{p_3^2} & \boldsymbol{I}_{p_3^3} \end{pmatrix},$$

where $I_{p_k^r}$ is the matrix of a cyclic p_k^r-shift of columns of the $t \times t$ identity matrix $\boldsymbol{I}$. Then the minimum weight of a codeword $\boldsymbol{c}_p$ such that $\boldsymbol{H}_p \boldsymbol{c}_p^T = \boldsymbol{0}$ cannot be less than 8.

Proof. It follows from Theorem 4 that for the validity of this statement it suffices to show that expression of the form (3) does not hold for at least one cycle of length 6.

For instance, consider a cycle formed on the last columns of $\boldsymbol{H}_p$. Expression (3) for it is of the form

$$(p_2^2 - p_2) + (p_3 - p_2^3) + (p_3^3 - p_3^2) \equiv 0 \mod t.$$

It follows from the condition of the theorem that $(p_2^2 - p_2) + (p_3 - p_2^3) + (p_3^3 - p_3^2) < p_3^3$. Indeed, assuming that $p_3 = p_2 + \delta$ with $\delta \ge 1$, the last inequality can be transformed into

$$-p_2^3 - 2p_2\delta - (\delta^2 - \delta) < 0,$$

which is valid for any $p_2 > 0$ and $\delta \ge 1$.

At the same time, one can show that

$$(p_2^2 - p_2) + (p_3 - p_2^3) + (p_3^3 - p_3^2) > 0.$$

After some transformations, we obtain

$$(p_2^2 - p_2) + (p_3 - p_2^3) + (p_3^3 - p_3^2) = (p_3 - p_2)(1 - (p_3 + p_2) + p_3^2 + p_2 p_3 + p_2^2).$$

Thus, it remains to show that

$$1 - (p_3 + p_2) + p_3^2 + p_2 p_3 + p_2^2 > 0.$$

To this end, we again employ the change of variables $p_3 = p_2 + \delta$, $\delta \ge 1$. Then the last inequality is equivalent to a quadratic inequality with respect to p_2

$$3p_2^2 + (3\delta - 2)p_2 + (\delta^2 - \delta + 1) > 0,$$

which is valid for any $p_2 > 0$ and $\delta \ge 1$, since its discriminant is

$$D = -3\delta^2 - 8 < 0.$$

Thus, by combining the inequalities

$$(p_2^2 - p_2) + (p_3 - p_2^3) + (p_3^3 - p_3^2) < p_3^3$$

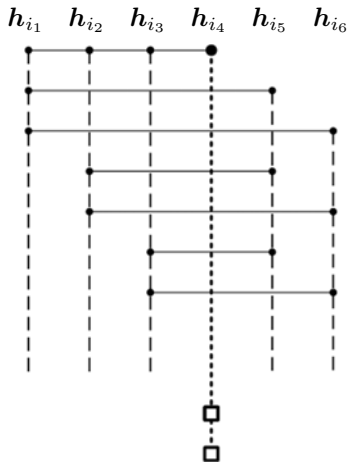

Fig. 2. Configuration of six columns with a weight-4 row.

and

$$(p_2^2 - p_2) + (p_3 - p_2^3) + (p_3^3 - p_3^2) > 0,$$

we conclude that

$$(p_2^2 - p_2) + (p_3 - p_2^3) + (p_3^3 - p_3^2) \not\equiv 0 \mod t.$$

According to Theorem 4 and the remark, this means that the minimum weight of a codeword obtained on this configuration of columns cannot be less than 8.

Similarly it can be shown that expressions of the form (3) do not hold for any cycle of length 6 in the matrix $\boldsymbol{H}_p$. $\triangle$

Thus, weight-6 codewords can be formed only on configurations of six columns $\boldsymbol{h}_{i_1}, \ldots, \boldsymbol{h}_{i_6}$ of the parity-check matrix. Let us form a matrix $\boldsymbol{H}_i = [\boldsymbol{h}_{i_1} \ldots \boldsymbol{h}_{i_6}]$ by concatenation of these columns.

It is obvious that none of the rows is of odd weight. It is also obvious that no row of $\boldsymbol{H}_i$ can have weight 6. Indeed, if the weight of at least one row of $\boldsymbol{H}_i$ is 6, then, in accordance with properties of Steiner triple systems, the weight of any row of the matrix $\widetilde{\boldsymbol{H}}_i$ obtained from $\boldsymbol{H}_i$ by removing the weight-6 row is 1 (otherwise, this would mean existence of a 4-cycle). However, weight-6 codewords cannot be formed on this configuration of columns.

At the same time, from the fact that any five columns of $\boldsymbol{H}_i$ are linearly independent and that adding the remaining column results in appearance of linear dependence, it follows that none of the rows of $\boldsymbol{H}_i$ has weight 4. Otherwise, to avoid appearance of 4-cycles, there should be two rows of weight 1.

Let us explain the last claim. Assume that among the six chosen columns there are four that intersect by a single 1. Then a row of weight 4 occurs in $\boldsymbol{H}_i$. Without loss of generality, we may assume that this condition occurs for columns $\boldsymbol{h}_{i_1}, \ldots, \boldsymbol{h}_{i_4}$. This set of columns cannot intersect by any other 1; otherwise, this would mean the presence of a 4-cycle. Since the weight of every column must be equal to 3, column $\boldsymbol{h}_{i_1}$ must intersect with $\boldsymbol{h}_{i_5}$ and $\boldsymbol{h}_{i_6}$, and these intersections must involve different ones; otherwise, a row of weight 3 is formed. Analogous conditions hold also for columns $\boldsymbol{h}_{i_2}$ and $\boldsymbol{h}_{i_3}$. Thus, a choice of ones in columns $\boldsymbol{h}_{i_1}, \boldsymbol{h}_{i_2}, \boldsymbol{h}_{i_3}$ completely determines columns $\boldsymbol{h}_{i_5}$ and $\boldsymbol{h}_{i_6}$. But this implies that column $\boldsymbol{h}_{i_4}$ of weight 3 can intersect with neither $\boldsymbol{h}_{i_5}$ nor $\boldsymbol{h}_{i_6}$. As a result, two rows of weight 1 are formed.

Figure 2 illustrates the above reasoning.

Thus, we have proved the following statement.

Lemma 1. *Nonzero rows of the matrix* $\boldsymbol{H}_i = [\boldsymbol{h}_{i_1} \dots \boldsymbol{h}_{i_6}]$ *which form a weight*-6 *codeword have weight* 2.

Applying the reasoning used in Theorem 4 and the remark, we can formulate the following theorem.

Theorem 6. *Consider weight*-6 *codewords of a code with parity-check matrix* $\widetilde{\boldsymbol{H}}$. *All combinations of six linearly dependent columns of* $\widetilde{\boldsymbol{H}}$ *correspond to these codewords. If upon lifting the parity-check matrix* $\widetilde{\boldsymbol{H}}$ *to a matrix* $\boldsymbol{H}$ *by replacing each* 1 *in these columns with matrices of cyclic* p_{ij}*-shifts using the method described in Section* 4, *in any of these combinations at least one cycle of length* 8 *is transformed into a cycle of greater length, then the minimum weight of a codeword that meets all of parity-check conditions formed by these columns is* 12.

Theorems 4 and 6 imply important consequences.

Corollary 1. *Let the minimum distance* $\widetilde{d}$ *of a code with parity-check matrix* $\widetilde{\boldsymbol{H}}$ *be* 4. *Extend* $\widetilde{\boldsymbol{H}}$ *to a matrix* $\boldsymbol{H}$ *by employing matrices of cyclic* p_{ij}*-shifts using the method described in Section* 4. *Then, if at least one cycle of length* 6 *is transformed into a cycle of greater length in every combination of four linearly dependent columns of* $\widetilde{\boldsymbol{H}}$ *and if at least one cycle of length* 8 *is transformed into a cycle of greater length in every combination of six linearly dependent columns of* $\widetilde{\boldsymbol{H}}$, *then the minimum distance of the code with parity-check matrix* $\boldsymbol{H}$ *is at least* 8.

Corollary 2. *If* $\boldsymbol{H}$ *is the parity-check matrix of a code based on a system* $\mathrm{STS}(2^m - 1)$ *and if the girth of* $\boldsymbol{H}$ *is*

$$g \geq 10,$$

then the minimum distance of the code is

$$d_{\min} \geq 8.$$

6. CONSTRUCTION OF AN LDPC CODE BASED ON STS($2^m - 1$) AND PERMUTATION MATRICES WITH $d_{\min} \geq 6$

According to Theorem 4, an LDPC code obtained by the method described in Section 4 (where matrices of cyclic shifts are chosen as permutation matrices) has minimum distance 6 if and only if at least one cycle of length 6 is transformed into a cycle of greater length in every linear combination of four columns in the "frame" matrix $\widetilde{\boldsymbol{H}}$. Thus, if the whole parity-check matrix $\boldsymbol{H}$ does not contain cycles of length 6, then the minimum distance of a code with this parity-check matrix is at least 6. An algorithm for generating this parity-check matrix is proposed in this section.

Consider an $l \times n_0$ matrix

$$\boldsymbol{B} = \begin{pmatrix} 0 & a_0 & 2a_0 & \dots & (n_0-1)a_0 \\ 0 & a_1 & 2a_1 & \dots & (n_0-1)a_1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & a_{l-1} & 2a_{l-1} & \dots & (n_0-1)a_{l-1} \end{pmatrix},$$

where $0 \leq a_0 < a_1 < a_2 < \dots < a_{l-1}$ is a sequence of natural numbers. The following statement was proved in [20].

Theorem 7. *If every* $b_{ij} = (j-1)a_{i-1}$ *in the matrix* $\boldsymbol{B}$ *is replaced by the matrix of a cyclic* b_{ij}*-shift of columns of the* $t \times t$ *identity matrix* $\boldsymbol{I}$ *and if for any ordered triple* $\{a_i, a_j, a_k\}$, $i < j < k$, *in the sequence* $\{a_0, a_1, \dots, a_{l-1}\}$ *the condition*

$$\frac{a_k - a_i}{(a_k - a_i, a_j - a_i)} \geq n_0$$

holds, where $(\cdot,\cdot)$ *is the greatest common divisor, then the matrix*

$$\widetilde{\boldsymbol{B}} = \begin{pmatrix} \boldsymbol{I} & \boldsymbol{I}_{a_0} & \boldsymbol{I}_{2a_0} & \dots & \boldsymbol{I}_{(n_0-1)a_0} \\ \boldsymbol{I} & \boldsymbol{I}_{a_1} & \boldsymbol{I}_{2a_1} & \dots & \boldsymbol{I}_{(n_0-1)a_1} \\ \dots & \dots & \dots & \dots & \dots \\ \boldsymbol{I} & \boldsymbol{I}_{a_{l-1}} & \boldsymbol{I}_{2a_{l-1}} & \dots & \boldsymbol{I}_{(n_0-1)a_{l-1}} \end{pmatrix}$$

contains no cycles of length 6 *for any value of the parameter*

$$t \geq (a_{l-1} - a_0)(n_0 - 1) + 1.$$

Thus, if one extends the "frame" matrix $\widetilde{\boldsymbol{H}}$ to a parity-check matrix $\boldsymbol{H}$ of an LDPC code based on STS$(2^m - 1)$ and permutation matrices using cyclic shift matrices obtained from the $l \times n_0$ matrix $\widetilde{\boldsymbol{B}}$, then the minimum distance of the obtained code is $d \geq 6$.

It is easy to note that if $\widetilde{\boldsymbol{B}}$ has n_0 ones in each row and l ones in each column, then, in order to construct a matrix of a $(3, 3k)$-regular LDPC code based on STS$(2^m - 1)$ and permutation matrices, it is necessary and sufficient that

$$ln_0 \geq 3k(2^m - 1).$$

Let us consider a special case of the sequence which appears in Theorem 7: $\{0, 1, n_0, n_0^2, \dots, n_0^{l-2}\}$. We prove the following lemma for this sequence.

Lemma 2. *For any ordered triple* $\{n_0^x, n_0^y, n_0^z\}$ *with* $0 \leq x < y < z \leq l - 2$ *we have*

$$\frac{n_0^z - n_0^x}{(n_0^z - n_0^x, n_0^y - n_0^x)} \geq n_0.$$

Proof. Indeed,

$$\frac{n_0^z - n_0^x}{(n_0^z - n_0^x, n_0^y - n_0^x)} = \frac{n_0^x(n_0^{z-x} - 1)}{(n_0^x(n_0^{z-x} - 1), n_0^x(n_0^{y-x} - 1))} = \frac{n_0^{z-x} - 1}{(n_0^{z-x} - 1, n_0^{y-x} - 1)}.$$

Since the greatest common divisor of two natural numbers is not greater than the minimum of them, we have

$$\frac{n_0^{z-x} - 1}{(n_0^{z-x} - 1, n_0^{y-x} - 1)} \geq \frac{n_0^{z-x} - 1}{n_0^{y-x} - 1}.$$

Define $y - x = k$. Since $x < y < z$, we have $z - x \geq k + 1$; therefore,

$$\frac{n_0^{z-x} - 1}{n_0^{y-x} - 1} \geq \frac{n_0^{k+1} - 1}{n_0^k - 1}.$$

But the inequality

$$\frac{n_0^{k+1} - 1}{n_0^k - 1} \geq n_0$$

is valid for any $n_0 > 1$. $\triangle$

Based on Lemma 2 and Theorem 7, we can formulate the following result.

Theorem 8. *The matrix*

$$\widehat{\boldsymbol{B}} = \begin{pmatrix} \boldsymbol{I} & \boldsymbol{I} & \boldsymbol{I} & \dots & \boldsymbol{I} \\ \boldsymbol{I} & \boldsymbol{I}_1 & \boldsymbol{I}_2 & \dots & \boldsymbol{I}_{n_0-1} \\ \dots & \dots & \dots & \dots & \dots \\ \boldsymbol{I} & \boldsymbol{I}_{n_0{}^{l-2}} & \boldsymbol{I}_{2n_0{}^{l-2}} & \dots & \boldsymbol{I}_{(n_0-1)n_0{}^{l-2}} \end{pmatrix}$$

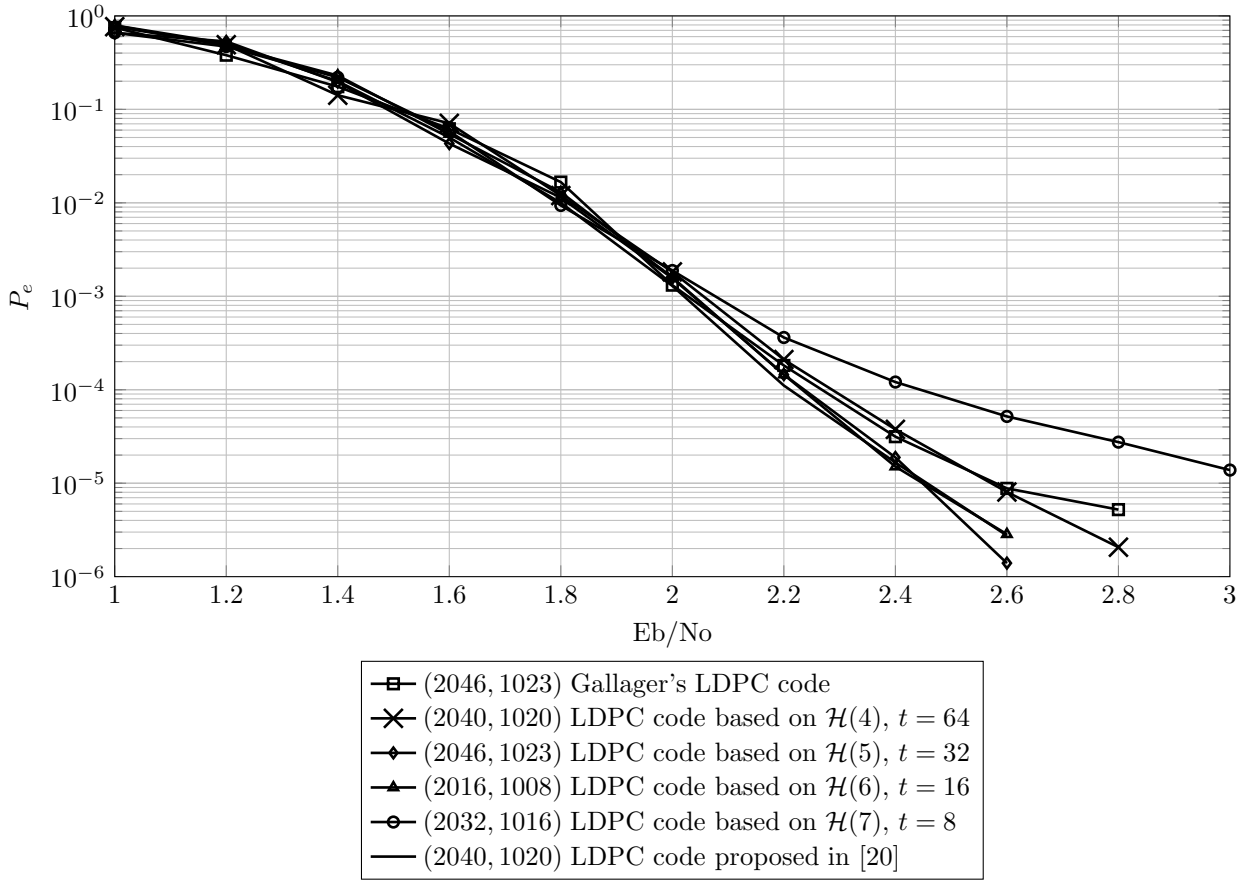

Fig. 3. Frame error probability (P_e) versus signal-to-noise ratio (Eb/No) for Gallager's code, the code proposed in [20], and codes from the ensemble $\mathcal{E}_{\mathrm{STS}}(m, k, t)$ with $k = 2$, $l = 3$, $n_0 = 6$, and $R = 0.5$.

contains no cycles of length 6 *for any value of* $t \geq n_0^{l-2}(n_0 - 1) + 1$, *where* t *is the size of the identity matrix* $\boldsymbol{I}$.

Thus, choosing four parameters l, n_0, m, k so that the system of inequalities

$$\begin{cases} t \geq n_0^{l-2}(n_0 - 1) + 1, \\ ln_0 \geq 3k(2^m - 1) \end{cases}$$

is satisfied, we can construct a parity-check matrix $\boldsymbol{H}$ of a $(3, 3p)$-regular LDPC code based on $\mathrm{STS}(2^m - 1)$ and permutation matrices with length $n = kt(2^m - 1)$ and minimum distance $d \geq 6$. It is sufficient to choose distinct circulants forming the matrix $\widehat{\boldsymbol{B}}$ as permutation matrices.

7. SIMULATION RESULTS

A MatLab function was written for generating parity-check matrices of LDPC codes based on $\mathrm{STS}(2^m - 1)$. Simulation was made by methods of simulation modeling with the use of MatLab. For an information transmission channel, we chose a binary BSPK channel with additive white Gaussian noise. For a decoding algorithm, we chose an iterative Sum-Product algorithm with "soft input" working with a code representation in the form of a bipartite Tanner graph. The maximum number of iterations was limited by 50.

Simulation results presented in Fig. 3 show that the code from the ensemble $\mathcal{E}_{\mathrm{STS}}(4, 2, 64)$ behaves hardly different from that of a random Gallager's code at the same lengths. At the

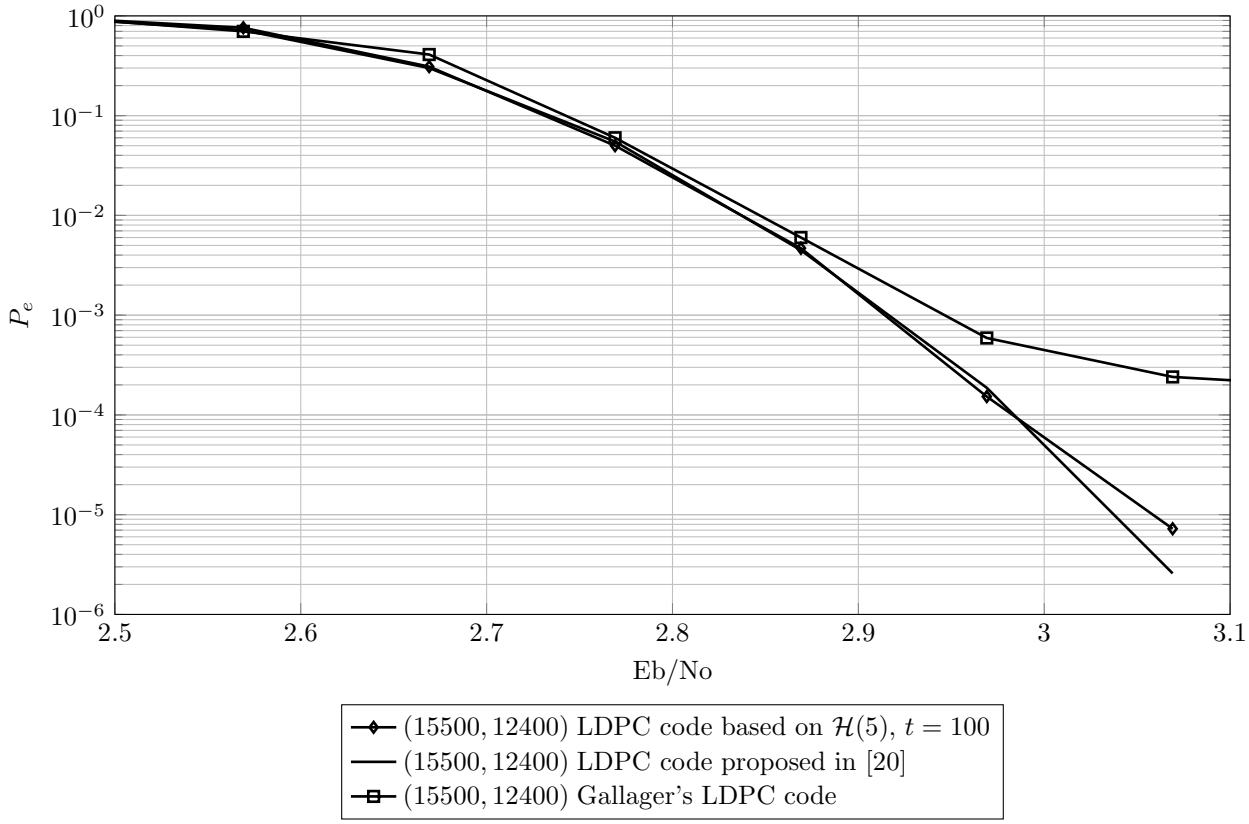

Fig. 4. Frame error probability (P_e) versus signal-to-noise ratio (Eb/No) for Gallager's code, the code proposed in [20], and the code from the ensemble $\mathcal{E}_{\mathrm{STS}}(5, 5, 100)$, $l = 3$, $n_0 = 15$, $R = 0.8$.

same time, codes from the ensembles $\mathcal{E}_{\mathrm{STS}}(5, 2, 32)$ and $\mathcal{E}_{\mathrm{STS}}(6, 2, 16)$, as well as codes proposed in [20], also demonstrate a similar behavior and gain almost half an order in error probability per frame against the random Gallager's code and code from $\mathcal{E}_{\mathrm{STS}}(4, 2, 64)$ under the signal-to-noise ratio of 2.6 dB. We may also mention a moderate efficiency gain of codes from the $\mathcal{E}_{\mathrm{STS}}(5, 2, 32)$ ensemble against the codes proposed in [20] and codes from $\mathcal{E}_{\mathrm{STS}}(6, 2, 16)$.

These findings allow us to conclude about practical usability of codes from $\mathcal{E}_{\mathrm{STS}}(5, 2, 32)$ and $\mathcal{E}_{\mathrm{STS}}(6, 2, 16)$. At the same time, we must mention unsatisfactory behavior of codes from $\mathcal{E}_{\mathrm{STS}}(7, 2, 8)$ which lose almost an order and a half in error probability per frame against the best code constructions under the signal-to-noise ratio of 2.6 dB.

Simulation results presented in Fig. 4 show that the code from the ensemble $\mathcal{E}_{\mathrm{STS}}(5, 5, 100)$ with rate $R = 0.8$ and length $n = 15500$ gains almost two orders in error probability per frame against the random Gallager's code with the same parameters under the signal-to-noise ratio of 3.07 dB. But at the same time this code behaves slightly worse than the code proposed in [20]. Nevertheless, codes from the ensemble $\mathcal{E}_{\mathrm{STS}}(m, k, t)$ (with large admissible values of k) can be used in practical applications where high-rate codes are needed.

8. CONCLUSION

In this paper, a simple method is proposed for generating parity-check matrices $\boldsymbol{H}$ of LDPC codes based on Steiner triple systems and permutation matrices. Estimates for the rate, minimum distance, and girth are derived. A condition that guarantees a strict increase in the minimum

distance is obtained. Simulation results allow us to conclude that the obtained code constructions are not worse than Gallager's codes proposed in [1].

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. Tanner, R.M., A Recursive Approach to Low Complexity Codes, *IEEE Trans. Inform. Theory*, 1981, vol. 27, no. 5, pp. 533–547.
3. 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*, 2006, pp. 679–683.
4. 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*, 2006.
5. 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, 2008*, pp. 180–185.
6. Kim, S., No, J.-S., Chung, H., and 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.
7. Ivanov, F.I., Zyablov, V.V., and Potapov, V.G., Low-Density Parity-Check Codes Based on Galois Fields, *Inform. Processes*, 2012, vol. 12, no. 1, pp. 68–83. Available at `http://www.jip.ru/2012/68-83-2012.pdf`.
8. Ivanov, F.I., Zyablov, V.V., and Potapov, V.G., Estimation of Minimum Length of Cycles in Quasi-Cyclic Regular LDPC Codes Based on Permutation Matrices, *Inform. Control Syst.*, 2012, no. 3 (58), pp. 42–45.
9. Zyablov, V.V., Ivanov, F.I., and Potapov, V.G., Comparison of Various Constructions of Binary LDPC Codes Based on Permutation Matrices, *Inform. Processes*, 2012, vol. 12, no. 1, pp. 31–52. Available at `http://www.jip.ru/2012/31-52-2012.pdf`.
10. Ivanov, F.I., Zyablov, V.V., and Potapov, V.G., Low-Density Parity-Check Codes Based on Independent Subgroups, in *Proc. XIII Int. Sympos. on Problems of Redundancy in Information and Control Systems (RED'2012), St. Petersburg, Russia*, 2012, pp. 31–34.
11. 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, 2012*, pp. 162–167.
12. 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.
13. 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.
14. 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.
15. Johnson, S., Low-Density Parity-Check Codes from Combinatorial Designs, *PhD Thesis, Newcastle, Australia: School of Electrical Engineering and Computer Science, Univ. of Newcastle*, 2004.
16. Ivanov, F.I., Zhilin, I.V., Zyablov, V.V., Decoding Algorithm for Low-Density Parity-Check Codes with High Parallelization, *Inform. Control Syst.*, 2012, no. 6 (61), pp. 53–59.
17. Hall, M., Jr., A Survey of Combinatorial Analysis, in *Some Aspects of Analysis and Probability*, Surveys in Appl. Math., vol. 4, New York: Wiley, 1958, pp. 35–104. Translated under the title *Kombinatornyi Analiz*, Moscow: Inostr. Lit., 1963.

18. MacWilliams, F.J. and Sloane, N.J.A., *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977. Translated under the title *Teoriya kodov, ispravlyayushchikh oshibki*, Moscow: Svyaz', 1979.

19. Fossorier, M.P.C., Quasi-cyclic Low-Density Parity-Check Codes from Circulant Permutation Matrices, *IEEE Trans. Inform. Theory*, 2004, vol. 50, no. 8, pp. 1788–1793.

20. Zhang, G., Sun, R., and Wang, X., Construction of Girth-Eight QC-LDPC Codes from Greatest Common Divisor, *IEEE Commun. Lett.*, 2013, vol. 17, no. 2, pp. 369–372.