(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 May 2018 (17.05.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/088923 A1

(51) International Patent Classification:
H03M 13/11 (2006.01) *H03M 13/03* (2006.01)

(21) International Application Number:
PCT/RU2016/000777

(22) International Filing Date:
14 November 2016 (14.11.2016)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: HUAWEI TECHNOLOGIES CO., LTD. [CN/CN]; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong, 518129 (CN).

(72) Inventor; and
(71) Applicant *(for RU only)*: **USATYUK, Vasily Stanislavovich** [RU/CN]; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong, 518129 (CN).

(72) Inventors: **VOROBYEV, Ilya Viktorovich**; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong, 518129 (CN). **POLIANSKII, Nikita Andreevich**; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong, 518129 (CN). **SVISTUNOV, German Viktorovich**; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong, 518129 (CN).

(74) Agent: LAW FIRM "GORODISSKY & PARTNERS" LTD.; MITS Alexander Vladimirovich, POPOVA Elizaveta Vitalievna, B. Spasskaya str., 25, bldg. 3, Moscow, 129090 (RU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM,

(54) Title: METHOD AND APPARATUS FOR ENCODING AND DECODING OF VARIABLE LENGTH QUASI-CYCLIC LOW-DENSITY PARITY-CHECK, QC-LDPC, CODES

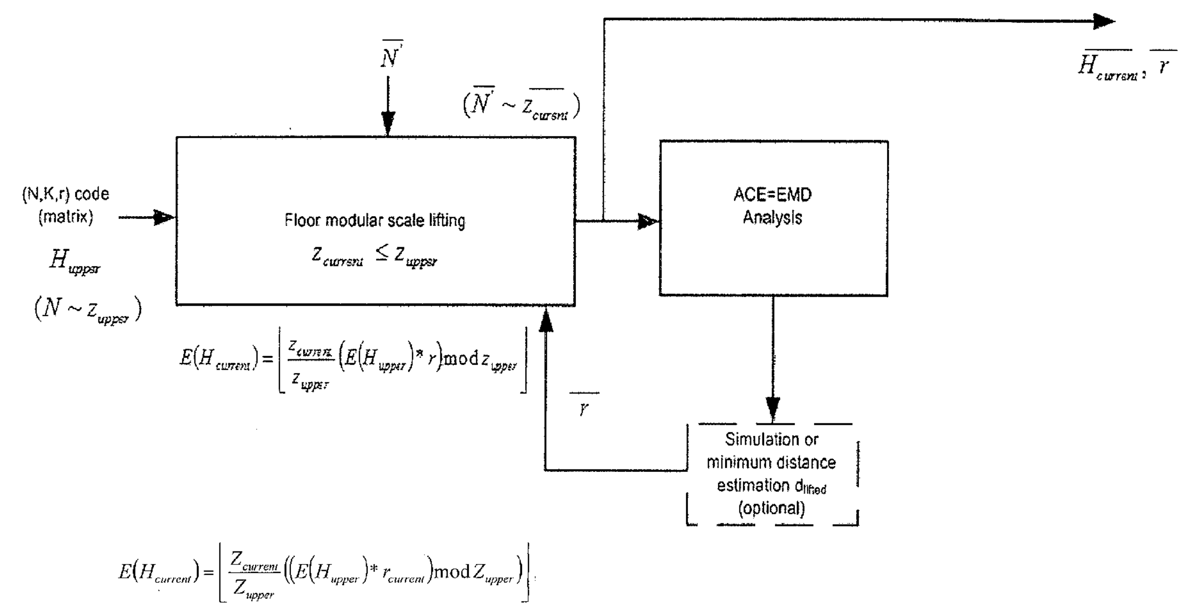


Fig. 2

(57) Abstract: A method for quasi-cyclic low-density parity-check (QC-LDPC) encoding and decoding of a data packet by a lifted matrix is provided, the method comprising: lifting the QC-LDPC code for maximal code length Nmax and maximal circulant size Z_{upper} of the base matrix; generating a plurality of optimal values r, for a plurality of circulants $Z_1, Z_2,\ldots, Z_{upper}$ based on the QC-LDPC code lifted for maximal length N_{max}, $0 \le r; \le Z_{upper} - 1$; saving the generated plurality of optimal values r; corresponding to the plurality of circulants Z,, $Z_2,\ldots, Z_{upper}$ and a matrix for the QC-LDPC code lifted for maximal length N_{max} in the memory unit; receiving a current circulant Z current from the plurality of circulants $Z_1, Z_2,\ldots, Z_{upper}$; selecting a current optimal

WO 2018/088923 A1

[Continued on next page]

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

value $r_{current}$ from the plurality of optimal values r; stored in the memory unit corresponding to the current circulant $Z_{current}$; and lifting the base matrix based on the current optimal value $r_{current}$, wherein a floor scale modular lifting of the base matrix is calculated as: where $E(H_{upper})$ is a value of circulant shift in the base matrix for maximal circulant size; wherein $0 \leq r_{current} \leq z_{upper}$ 1 and $r_{current}$ =1 is excluded. The apparatus for QC-LDPC encoding and decoding of a data packet by a lifted matrix is further provided.

METHOD AND APPARATUS FOR ENCODING AND DECODING OF VARIABLE LENGTH QUASI-CYCLIC LOW-DENSITY PARITY-CHECK, QC-LDPC, CODES

TECHNICAL FIELD

The present invention relates to a method for quasi-cyclic low-density parity-check (QC-LDPC) encoding and decoding and an apparatus for quasi-cyclic low-density parity-check encoding and decoding.

The present invention also relates to a computer-readable storage medium storing program code, the program code comprising instructions for carrying out such a method.

BACKGROUND

Error-correcting coding is an efficient method to improve capacity of a communication system. Wireless systems require employing a large set of code with different length and rate. For example LTE provides more than several thousand of different code lengths and rates using a hardware friendly interleaver and simply puncturing pattern, but the sequential nature of the BCJR decoder of Turbo code significantly limits parallelism – decoder throughput. Hence, it is thus a problem how to create a compact representation of QC-LDPC codes, which supports sets of QC-LDPC codes with different lengths and rates. Other problems to be solved include getting additive increase of circulant size to minimize gap between several lengths of code; to define some block-structured memory efficient puncture pattern with minimal performance lost; and to maximize number of variable node in block-structured which recover under practical number iteration.

A problem of existing floor lifting methods is the possibility of appearing of short cycles in parity check matrices and bad weight spectrum of codewords. This leads to lower code gain.

SUMMARY OF THE INVENTION

The objective of the present invention is to provide a method for quasi-cyclic low-density parity-check encoding and decoding and an apparatus for quasi-cyclic low-density parity-check encoding and decoding, wherein the method for QC-LDPC encoding and decoding and the apparatus for QC-LDPC encoding and decoding overcome one or more of the above-mentioned problems of the prior art. Aspects of the invention provide error correction, especially to channel coding for wireless communication, such as WI-FI or 5G communication.

The foregoing and other objects are achieved by the features of the independent claims. Further implementation forms are apparent from the dependent claims, the description and the figures.

A first aspect of the invention provides a method for quasi-cyclic low-density parity-check (QC-LDPC) encoding and decoding of a data packet by a lifted matrix, obtained by floor scale modular lifting of a base matrix of QC-LDPC code, the method comprising: lifting the QC-LDPC code for maximal code length $N_{\max}$ and maximal circulant size Z_{upper} of the base matrix, $N_{\max} = Z_{upper} * L$, wherein L is a column in the base matrix; generating a plurality of optimal values r_i for a plurality of circulants $Z_1, Z_2, ..., Z_{upper}$ based on the QC-LDPC code lifted for maximal length $N_{\max}$, $0 \leq r_i \leq Z_{upper} - 1$; saving the generated plurality of optimal values r_i corresponding to the plurality of circulants $Z_1, Z_2, ..., Z_{upper}$ and a matrix for the QC-LDPC code lifted for maximal length $N_{\max}$ in the memory unit. These steps may be made offline only once. The method further comprises receiving a current circulant $Z_{current}$ from the plurality of circulants $Z_1, Z_2, ..., Z_{upper}$; selecting a current optimal value $r_{current}$ from the plurality of optimal values r_i stored in the memory unit corresponding to the current circulant $Z_{current}$; and lifting the base matrix based on the current optimal value $r_{current}$, wherein a floor lifting of the base matrix is calculated as: $E(H_{current}) = \left\lfloor \frac{Z_{current}}{Z_{upper}} \left(\left(E(H_{upper}) * r_{current} \right) \bmod Z_{upper} \right) \right\rfloor$, where $E(H_{upper})$ is a value of circulant shift in the base matrix for maximal circulant size; wherein $0 \leq r_{current} \leq Z_{upper} - 1$ and $r_{current} = 1$ is excluded. Therefore, a QC-LDPC mother code lifting method with flexible length and rate is provided to be used for encoding and decoding of data packets. This method provides memory efficient QC-LDPC code representation with maximal flexibility of length and rate. The overall code performance is also therefore increased due to providing memory consumption and processing speed increase.

The methods according to the first aspect of the invention can be performed by a computer-readable storage medium according to the second aspect of the invention. Further features or implementations of the method according to the first aspect of the invention can perform the functionality of an apparatus for QC-LDPC encoding and decoding according to the third aspect of the invention and its different implementation forms.

In a first implementation of the method for QC-LDPC encoding and decoding of a data packet by a lifted matrix according to the first aspect, generating the plurality of optimal values r_i for the plurality of circulants $Z_1, Z_2, \ldots, Z_{upper}$ further comprises: constructing a plurality of families of parity-check matrixes, each family corresponds to value r in a plurality of values $r_1, r_2, \ldots, r_k$ corresponding to code lengths $N_1, N_2, N_3, \ldots, N_k$; and based on the plurality of the families of the parity-check matrixes, selecting the plurality of optimal values r_i for the plurality of circulants $Z_1, Z_2, \ldots, Z_{upper}$ by multi-parameter filtering. Using at least one parity-check matrix a set of code can be represented with minimal performance degradation and high memory efficiency.

In a second implementation of the method for QC-LDPC encoding and decoding of a data packet by a lifted matrix according to the first implementation of the first aspect, the multi-parameter filtering includes at least on of: Extrinsic Message Degree, ACE Spectrum, Tanner Spectral Bound, Code Distance, Codeword's weight spectrum enumerator, Trapping Set Weight Enumerator, simulations result. All these ways of choosing best r value provide improved filtering quality due to better consideration of multiple parameters and enable choosing the optimal r value to be used in a lifting procedure.

In a third implementation of the method for QC-LDPC encoding and decoding of a data packet by a lifted matrix according to any of the first or second implementations of the first aspect, constructing the plurality of the families of the parity-check matrixes is performed using formula: $E_r(H_{upper}) = E(H_{upper}) \cdot r \bmod Z_{upper}$. Using $E_r(H_{upper})$ provides additional flexibility due to possibility to choose r value to avoid critical points.

A second aspect of the invention refers to a a computer-readable storage medium storing program code, the program code comprising instructions for carrying out the method of the first aspect or one of the implementations of the first aspect.

A third aspect of the invention refers to an apparatus for quasi-cyclic low-density parity-check (QC-LDPC) encoding and decoding of a data packet by a lifted matrix, obtained by floor scale modular lifting of a base matrix of QC-LDPC code, the apparatus comprising a processing unit and a memory unit, the memory unit storing: a maximal length $N_{\max}$ and a maximal circulant size Z_{upper} of the base matrix, a matrix for the QC-LDPC code lifted for maximal length $N_{\max}$; and a plurality of optimal values r_i corresponding to a plurality of circulants $Z_1, Z_2, ..., Z_{upper}$, the plurality of optimal values r_i is generated based on the QC-LDPC code lifted for maximal length $N_{\max}$ and maximal circulant size Z_{upper} of the base matrix, wherein $N_{\max} = Z_{upper} * L$, L is a column in the base matrix and $0 \le r_i \le Z_{upper} - 1$. The processing unit is configured to: receive a current circulant $Z_{current}$ from the plurality of circulants $Z_1, Z_2, ..., Z_{upper}$; select a current optimal value $r_{current}$ from the plurality of optimal values r_i stored in the memory unit corresponding to the current circulant $Z_{current}$; and lift the base matrix based on the current optimal value $r_{current}$, wherein a floor lifting of the base matrix is calculated as: $E(H_{current}) = \left\lfloor \frac{Z_{current}}{Z_{upper}} \left(\left(E(H_{upper}) * r_{current} \right) \bmod Z_{upper} \right) \right\rfloor$, where $E(H_{upper})$ is a value of circulant shift in the base matrix for maximal circulant size; wherein $0 \le r_{current} \le Z_{upper} - 1$ and $r_{current} = 1$ is excluded.

In a first implementation of the apparatus for QC-LDPC encoding and decoding of a data packet by a lifted matrix of the third aspect, generating the plurality of optimal values r_i for the plurality of circulants $Z_1, Z_2, ..., Z_{upper}$ comprises: constructing a plurality of families of parity-check matrixes, each family corresponds to value r in a plurality of values $r_1, r_2, ..., r_k$ corresponding to code lengths $N_1, N_2, N_3, ..., N_k$; and based on the plurality of the families of the parity-check matrixes, selecting the plurality of optimal values r_i for the plurality of circulants $Z_1, Z_2, ..., Z_{upper}$ by multi-parameter filtering.

In a second implementation of the apparatus for QC-LDPC encoding and decoding of a data packet by a lifted matrix according to the first implementation of the third aspect, the multi-parameter filtering includes at least on of: Extrinsic Message Degree, ACE Spectrum, Tanner

Spectral Bound, Code Distance, Codeword's weight spectrum enumerator, Trapping Set Weight Enumerator, simulations result.

In a third implementation of the apparatus for QC-LDPC encoding and decoding of a data packet by a lifted matrix according to any of the first or second implementations of the third aspect, the processing unit is further configured to construct the plurality of the families of the parity-check matrixes using formula: $E_r(H_{upper}) = E(H_{upper}) \cdot r \bmod Z_{upper}$.

All the implementations of the first aspect may be easily combined and used together with all the implementations of the third aspect.

These and other aspects of the invention will be apparent from the embodiments described below.

BRIEF DESCRIPTION OF THE DRAWINGS

To illustrate the technical features of embodiments of the present invention more clearly, the accompanying drawings provided for describing the embodiments are introduced briefly in the following. The accompanying drawings in the following description are merely some embodiments of the present invention, modifications on these embodiments are possible without departing from the scope of the present invention as defined in the claims.

FIG. 1 is a flow chart of a method for QC-LDPC encoding and decoding of a data packet by a lifted matrix in accordance with an embodiment of the present invention,

FIG. 2 shows generating a lifting value r for floor-scale modular lifting method in accordance with the present invention,

FIG. 3 shows an example of critical points elimination due to changing r values,

FIG. 4 is a block diagram illustrating an apparatus for QC-LDPC encoding and decoding of a data packet by a lifted matrix in accordance with an embodiment of the present invention,

FIGS. 5-7 show comparison of the floor lifting in accordance with the present invention with traditional floor lifting.

Detailed Description of the Embodiments

FIG. 1 illustrates a method 100 for QC-LDPC encoding and decoding of a data packet by a lifted matrix in accordance with the first aspect of the invention. The lifted matrix is obtained by floor scale modular lifting of a base matrix of QC-LDPC code. The method starts at block 101, where the QC-LDPC code for maximal code length $N_{\max}$ and maximal circulant size Z_{upper} of the base matrix is lifted.

$$N_{\max} = Z_{upper} * L, \tag{1}$$

wherein L is a column in the base matrix.

At step 102 a plurality of optimal values r_i for a plurality of circulants $Z_1, Z_2, ..., Z_{upper}$ is generated based on the QC-LDPC code lifted for maximal length $N_{\max}$, $0 \leq r_i \leq Z_{upper} - 1$. The generated plurality of optimal values r_i corresponding to the plurality of circulants $Z_1, Z_2, ..., Z_{upper}$ and a matrix for the QC-LDPC code lifted for maximal length $N_{\max}$ are saved in the memory unit at step 103. At step 104 a current circulant $Z_{current}$ from the plurality of circulants $Z_1, Z_2, ..., Z_{upper}$ is received. Then a current optimal value $r_{current}$ is selected from the plurality of optimal values r_i stored in the memory unit corresponding to the current circulant $Z_{current}$ (step 105). Finally at step 106 the base matrix is lifted based on the current optimal value $r_{current}$. A floor lifting of the base matrix is calculated as:

$$E(H_{current}) = \left\lfloor \frac{Z_{current}}{Z_{upper}} \left(\left(E(H_{upper}) * r_{current} \right) \bmod Z_{upper} \right) \right\rfloor, \tag{2}$$

where $E(H_{upper})$ is a value of circulant shift in the base matrix for maximal circulant size; wherein $0 \leq r_{current} \leq Z_{upper} - 1$ and $r_{current} = 1$ is excluded.

The method for QC-LDPC encoding and decoding in accordance with the present invention may be widely used, for example in cryptography, in data transfer and for data storage.

A (J,L) regular QC-LDPC code of length N is usually defined by a parity-check matrix

$$H=\begin{bmatrix} I(p_{0,0}) & I(p_{0,1}) & \cdots & I(p_{0,L-1}) \\ I(p_{1,0}) & I(p_{1,1}) & & I(p_{1,L-1}) \\ \vdots & \vdots & \ddots & \vdots \\ I(p_{J-1,0}) & I(p_{J-1,1}) & \cdots & I(p_{J-1,L-1}) \end{bmatrix} \quad (3)$$

where $1 \le j \le J-1, 1 \le l \le L-1$ and $I(p_{j,l})$ represents the $p \times p$ circulant permutation matrix obtained by cyclically right-shifting the $p \times p$ identity matrix $I(0)$ by $p_{j,l}$ positions, with $p = N / L$.

For a specific QC-LDPC code the corresponding "base matrix" ("mother matrix" or protograph) is defined as the matrix of circulant shift that defines the QC-LDPC code:

$$B=\begin{bmatrix} p_{0,0} & p_{0,1} & \cdots & p_{0,L-1} \\ p_{1,0} & p_{1,1} & & p_{1,L-1} \\ \vdots & \vdots & \ddots & \vdots \\ p_{J-1,0} & p_{J-1,1} & \cdots & p_{J-1,L-1} \end{bmatrix} \quad (4).$$

Mask matrix for which regular QC-LDPC code can become irregular for different column weight case or QC-LDPC regular code with zero block circulant may be defined as:

$$M=\begin{bmatrix} m_{0,0} & m_{0,1} & \cdots & m_{0,L-1} \\ m_{1,0} & m_{1,1} & & m_{1,L-1} \\ \vdots & \vdots & \ddots & \vdots \\ m_{J-1,0} & m_{J-1,1} & \cdots & m_{J-1,L-1} \end{bmatrix}. \quad (5)$$

$$\mathrm{H} = H \otimes M, \quad (6)$$

where $\otimes$ is Hadamard product.

Lifting is operation under base matrix (protograph), by using of which code with different authomorphism or circulant size from a similar base matrix can be obtained.

Normally floor-lifting of base matrix is calculated by formula:

$$E(H_{current}) = \left\lfloor \frac{z_{current}}{z_{upper}} E(H_{upper}) \right\rfloor, \quad (7)$$

where $z_{current}$ – lifting size of circulant,

z_{upper} – maximal circulant size of base matrix,

$E(H_{upper})$ – value of circulant shift in base matrix for maximal size of circulant.

Length of code N from $z_{current} * VN_{protograph}$ to $z_{upper} * VN_{protograph}$ with some additive step between $z_{current} : step : z_{upper}$, where $VN_{protograph}$ is number of variable nodes in base matrix.

The method according to the present invention uses random matrix design approach lifting QC-LDPC directly from mask matrix (base matrix or protograph).

A cycle of even length $2K$ in H is defined by $2K$ positions such that:

1) Two consecutive positions are obtained by changing alternatively column of row only;
2) All positions are distinct except first and last one;

Two consecutive elements of the path belong to different circulant permutation matrices. So a chain of circulant permutation matrices can be defined:

$$I(p_{i_0,j_0}), I(p_{i_0,j_1}), I(p_{i_1,j_1}), I(p_{i_1,j_2}), \ldots, I(p_{i_{K-1},j_{K-1}}), I(p_{i_{K-1},j_0}), I(p_{i_0,j_0}) \quad (8)$$

where $i_a \neq i_{a+1}, j_a \neq j_{a+1}$, for all $0 \leq a \leq K-1$.

As each part of cycle is one, the circulant permutation matrix $I(p_{i,j})$ participating in cycle cannot be empty. Using these shifts of identity matrix necessary and sufficient conditions of existing of the cycle can be defined as:

$$\sum_{a=0}^{K-1} p_{i_a,j_a} - p_{i_a,j_{a+1}} \equiv 0 \ (mod\ N) \quad (9)$$

Fig. 2 illustrates generating a lifting value r for floor-scale modular lifting method. To generate a lifting value (code for flexible length $N_1 < N_2 < N_3 < N_4 < \ldots < N_k < N_{\max}$) using floor scale modular approach QC-LDPC lifted for maximal length $N_{\max}$ is used. This matrix can be lifted using simulation annulling, hill-climbing, guest-and-search, PEG, ACE+PEG or any another algorithms.

$$M = \begin{bmatrix} m_{0,0} & m_{0,1} & \cdots & m_{0,L-1} \\ m_{1,0} & m_{1,1} & & m_{1,L-1} \\ \vdots & \vdots & \ddots & \vdots \\ m_{J-1,0} & m_{J-1,1} & \cdots & m_{J-1,L-1} \end{bmatrix} \quad (10)$$

The input for floor modular scale lifting represents a QC-LDPC code lifted for maximal circulant size Z_{upper} with L variable nodes (columns in base matrix) and J parity-check (rows in base matrix):

$$Z_{upper} * L = N_{\max} . \quad (11)$$

Circulant sizes for which lifting this base matrix is desired: $Z_1 < Z_2 < \ldots < Z_k < Z_{upper}$, to get lengths $Z_1 * L = N_1 < Z_2 * L = N_2 < Z_3 * L = N_3 < Z_4 * L = N_4 < \ldots < Z_{upper} * L = N_{\max}$. The output of the floor modular scale lifting represents scale values $r_1, r_2, \ldots, r_k$ for every circulant sizes $Z_1, Z_2, \ldots, Z_k$. By using these values it is possible to generate code for every code lengths $N_1, N_2, N_3, \ldots, N_k$ in a fast manner using formula (12).

QC-LDPC code lifted for maximal code length is received and for every value $r_1, r_2, \ldots, r_k$ (related to circulants size $Z_1, Z_2, \ldots, Z_k$) which corresponds to codes with lengths $N_1, N_2, N_3, \ldots, N_k$ using formula (12) i parity-check matrixes are determined. Every $r_{current}$ can be in the range $1 \ldots Z_i - 1$. After using multi-parameter sieving, best value r is chosen based on: Extrinsic Message Degree, ACE Spectrum, Tanner Spectral Bound, Code Distance, Codeword's weight spectrum enumerator, Trapping Set Weight Spectrum Enumerator, simulation result, as shown in Fig. 2 by ACE=EMD Analysis.

This procedure may be made offline only once, then a matrix lifted for maximal length is saved along with r values.

After value r_i is got for every circulant $Z_1, Z_2, \ldots, Z_{upper}$ parity-check matrix for every length $N_1, N_2, N_3, \ldots, N_k$ can be constructed using formula:

$$E_r(H_{upper}) = E(H_{upper}) \cdot r \bmod z_{upper} \quad (12)$$

where r is integer $1 \le r \le z_{upper} - 1$ and $GCD(r, z_{upper}) = 1$.

For any path P shift d'_P in the $E_r(H_{upper})$ is equal to r times of shift d_P by same path in $E(H_{upper})$:

$$d'_P \equiv \sum_{a=0}^{K-1} rp_{i_a,j_a} - rp_{i_a,j_{a+1}} \left(mod\ z_{upper}\right) \equiv$$

$$\equiv r \sum_{a=0}^{K-1} p_{i_a,j_a} - p_{i_a,j_{a+1}} \left(mod\ z_{upper}\right) \equiv r\, d_P \tag{13}$$

When $GCD\left(r, z_{upper}\right) = 1$, $d'_P \equiv 0 \left(mod\ z_{upper}\right)$ in the same time with $d_P \equiv 0 \left(mod\ z_{upper}\right)$.

So, structure of cycles of $E(H_{upper})$ and $E\_r(H_{upper})$ are equivalent. In comparison with classical floor lifting approach, this method provides additional freedom and flexibility. Such r can be chosen as to avoid catastrophic (critical) points and to improve quality of graph in general, example of improving using change of r is presented in Fig 3.

Combining formula (12) with formula (7) of classical floor-lifting of base matrix the following formula for a floor lifting can be obtained:

$$E\left(H_{current}\right) = \left\lfloor \frac{z_{current}}{z_{upper}} \left(\left(E\left(H_{upper}\right) * r_{current}\right) \bmod z_{upper}\right) \right\rfloor, \tag{14}$$

where $r_{current}$ – scale factor, being an integer value from 0... z_{upper}-1

$CGD\left(r_{current}, z_{upper}\right) = 1$.

This increases freedom and flexibility of floor lifting.

For each $z_{current}$ we can find such $r_{current}$ that bring best possible quality of $E(H_{current})$. This method can be applied to any QC-LDPC codes to get flexible length properties.

Fig. 4 illustrates an apparatus 200 for QC-LDPC encoding and decoding of a data packet by a lifted matrix comprising a processing unit 201 and a memory unit 202. The memory unit 202 stores: a maximal length $N_{\max}$ and a maximal circulant size Z_{upper} of the base matrix, a matrix for the QC-LDPC code lifted for maximal length $N_{\max}$; and a plurality of optimal values r_i corresponding to a plurality of circulants $Z_1, Z_2, ..., Z_{upper}$. The plurality of optimal values r_i is generated based on the QC-LDPC code lifted for maximal length $N_{\max}$ and maximal circulant size Z_{upper} of the base matrix. The processing unit 201 is configured to: receive a current circulant $Z_{current}$ from the plurality of circulants $Z_1, Z_2, ..., Z_{upper}$; select a current optimal value $r_{current}$ from the plurality of optimal values r_i stored in the memory unit corresponding to the current circulant $Z_{current}$; and lift the base matrix based on the current optimal value $r_{current}$.

Comparison of the floor lifting in accordance with the present invention with traditional floor lifting is further provided with the reference to Figs. 5-7. For simplicity of the comparison, the extended irregular repeat-accumulate (EIRA) QC-LDPC base matrix is lifted. Designed QC-LDPC is:

60	54	75	-1	69	38	-1	9	84	4	8	39	32	64	92	79	1	56	17	0	7	0	-1	-1
-1	73	-1	3	10	70	25	37	46	-1	47	46	44	56	55	81	43	59	62	53	0	0	0	-1
92	81	86	58	4	-1	66	-1	13	81	92	56	48	94	20	29	44	22	2	21	-1	-1	0	0
31	-1	83	71	-1	89	11	42	23	40	62	31	81	74	82	25	42	13	86	70	7	-1	-1	0

Table 1 contains a comparison of the lifting approach in accordance with the provided method and a traditional floor lifting approach based on the number of cycles.

Floor scale modular lifting in accordance with provided method			Traditional floor lifting		
$z_{current}$	cycles	Number of cycles; r	$z_{current}$	cycles	Number of cycles; r
24	6	669 ; r = 4	24	4	2 ; r = 1
28	6	583 ; r = 28	28	4	2 ; r = 1
32	6	508 ; r = 52	32	4	1 ; r = 1
36	6	439 ; r = 20	36	4	1 ; r = 1
40	6	420 ; r = 28	40	4	1 ; r = 1
44	6	364 ; r = 76	44	4	1 ; r = 1
48	6	238 ; r = 2	48	4	1 ; r = 1
52	6	341 ; r = 20	52	4	1 ; r = 1
56	6	217 ; r = 14	56	4	1 ; r = 1
60	6	195 ; r = 10	60	4	1 ; r = 1
64	6	179 ; r = 74	64	6	263 ; r = 1
68	6	177 ; r = 86	68	6	223 ; r = 1
72	6	151 ; r = 58	72	6	228 ; r = 1
76	6	153 ; r = 94	76	6	223 ; r = 1
80	6	144 ; r = 14	80	6	205 ; r = 1

84	6	139 ; r = 82	84	6	201 ; r = 1
88	6	130 ; r = 38	88	6	197 ; r = 1
92	6	132 ; r = 86	92	6	178 ; r = 1
z_{upper} =96	6	68 ; r = 1	z_{upper} =96	6	173 ; r = 1

Table 1

Comparison based on the ACE Spectrum for lifting with circulant size $z_{current}$ = 60, N=1440 is provided in Fig. 5, where ACE Spectrum of floor scale modular lifting in accordance with the provided method (left) and traditional floor lifting (right) under similar base matrix are provided.

BER performance comparison of traditional floor-lifting QC-LDPC and QC-LDPC lifted using the provided approach of same base-matrix under min-sum decoder 15 iterations under AWGN channel is illustrated in Fig. 6. FER performance comparison of traditional floor-lifting QC-LDPC and QC-LDPC lifted using the provided approach of same base-matrix under min-sum decoder 15 iterations under AWGN channel is illustrated in Fig. 7.

Using the floor scale modular lifting method described in the present description the following two parity-check matrix of Repeat Accumulate QC-LDPC code may be designed:

12x24 circulant from 28 to 2304 with step 4, length 672 to 55296 with step 96, rate 0.5

1105	1626	-1	-1	-1	1737	-1	-1	-1	-1	-1	-1	526	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
1704	-1	1327	-1	-1	-1	1340	-1	1438	-1	-1	-1	-1	0	0	-1	-1	-1	-1	-1	-1	-1	-1	-1
-1	-1	662	206	-1	-1	-1	1510	-1	-1	-1	-1	-1	-1	0	0	-1	-1	-1	-1	-1	-1	-1	-1
-1	869	416	-1	348	40	-1	-1	-1	53	-1	-1	-1	-1	-1	0	0	-1	-1	-1	-1	-1	-1	-1
2196	-1	-1	1566	-1	1	-1	-1	-1	-1	2219	-1	-1	-1	-1	-1	0	0	-1	-1	-1	-1	-1	-1
2167	-1	1346	-1	2146	-1	-1	261	-1	-1	-1	2033	0	-1	-1	-1	-1	0	0	-1	-1	-1	-1	-1
-1	792	-1	857	696	-1	1273	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	0	0	-1	-1	-1	-1
-1	1435	181	-1	-1	-1	-1	-1	1028	-1	2292	1029	-1	-1	-1	-1	-1	-1	-1	0	0	-1	-1	-1
3	-1	-1	1427	370	-1	-1	-1	1414	527	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	0	0	-1	-1
1433	2215	-1	-1	-1	-1	42	1294	-1	-1	371	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	0	0	-1
-1	-1	2188	1927	-1	1007	512	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	0	0
-1	1140	-1	1589	-1	-1	-1	1567	-1	1761	-1	1684	526	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	0

and

6x24 circulant from 4 to 2304 with step 4 length 96 to 55296 with step 96, rate 0.75

984	581	2108	942	855	1987	1404	-1	1365	-1	2025	-1	-1	667	719	804	-1	-1	899	0	-1	-1	-1	-1
682	737	1893	932	2126	185	1472	522	-1	377	1122	1161	-1	-1	-1	-1	934	212	-1	0	0	-1	-1	-1
83	1971	342	858	1726	2205	815	-1	-1	109	671	-1	1876	442	-1	447	1576	-1	0	-1	0	0	-1	-1
201	907	1490	191	272	1986	970	616	1393	-1	-1	646	-1	-1	930	270	-1	629	-1	-1	-1	0	0	-1
2158	2244	1820	390	1445	2051	861	-1	1454	1022	1163	-1	139	742	-1	-1	-1	-1	-1	-1	-1	-1	0	0
679	421	874	2035	1806	723	2097	884	-1	-1	-1	19	1449	-1	1793	-1	1081	275	899	-1	-1	-1	-1	0

The foregoing descriptions are only implementation manners of the present invention, the scope of the present invention is not limited to this. Any variations or replacements can be easily made through person skilled in the art. Therefore, the protection scope of the present invention should be subject to the protection scope of the attached claims.

CLAIMS

1. A method (100) for quasi-cyclic low-density parity-check, QC-LDPC, encoding and decoding of a data packet by a lifted matrix, obtained by floor scale modular lifting of a base matrix of a QC-LDPC code,

the method (100) comprising:

lifting (101) the QC-LDPC code for a maximal code length $N_{\max}$ and a maximal circulant size Z_{upper} of the base matrix, $N_{\max} = Z_{upper} * L$, wherein L is the number of columns of the base matrix;

generating (102) a plurality of optimal values r_i for a plurality of circulants $Z_1, Z_2, ..., Z_{upper}$ based on the QC-LDPC code lifted for maximal length $N_{\max}$, $0 \le r_i \le Z_{upper} - 1$;

saving (103) the generated plurality of optimal values r_i corresponding to the plurality of circulants $Z_1, Z_2, ..., Z_{upper}$ and a matrix for the QC-LDPC code lifted for maximal length $N_{\max}$ in a memory unit; and

receiving (104) a current circulant $Z_{current}$ from the plurality of circulants $Z_1, Z_2, ..., Z_{upper}$;

selecting (105) a current optimal value $r_{current}$ from the plurality of optimal values r_i stored in the memory unit corresponding to the current circulant $Z_{current}$; and

lifting (106) the base matrix based on the current optimal value $r_{current}$, wherein a floor lifting of the base matrix is calculated as:

$$E(H_{current}) = \left\lfloor \frac{Z_{current}}{Z_{upper}} \left(\left(E(H_{upper}) * r_{current} \right) \bmod Z_{upper} \right) \right\rfloor,$$

where $E(H_{upper})$ is a value of circulant shift in the base matrix for maximal circulant size;

wherein $0 \le r_{current} \le Z_{upper} - 1$ and $r_{current} = 1$ is excluded.

2. The method of claim 1, wherein generating the plurality of optimal values r_i for the plurality of circulants $Z_1, Z_2, ..., Z_{upper}$ further comprises:

constructing a plurality of families of parity-check matrixes, each family corresponds to value r in a plurality of values $r_1, r_2, ..., r_k$ corresponding to code lengths $N_1, N_2, N_3, ..., N_k$; and

based on the plurality of the families of the parity-check matrixes, selecting the plurality of optimal values r_i for the plurality of circulants $Z_1, Z_2, ..., Z_{upper}$ by multi-parameter filtering.

3. The method of claim 2, wherein the multi-parameter filtering includes at least one of: Extrinsic Message Degree, ACE Spectrum, Tanner Spectral Bound, Code Distance, Codeword's weight spectrum enumerator, Trapping Set Weight Enumerator, simulations result.

4. The method of any of claims 2-3, wherein constructing the plurality of the families of the parity-check matrixes is performed using equation:

$$E_r(H_{upper}) = E(H_{upper}) \cdot r \bmod Z_{upper}.$$

5. A computer readable storage medium storing program code, the program code comprising instructions, which when performed on a computer cause the computer to perform the method according to any of claims 1-4.

6. An apparatus (200) for quasi-cyclic low-density parity-check, QC-LDPC, encoding and decoding of a data packet by a lifted matrix, obtained by floor scale modular lifting of a base matrix of QC-LDPC code,
the apparatus (200) comprising a processing unit (201) and a memory unit (202),
the memory unit (202) storing:

a maximal length $N_{\max}$ and a maximal circulant size Z_{upper} of the base matrix,

a matrix for the QC-LDPC code lifted for maximal length $N_{\max}$; and

a plurality of optimal values r_i corresponding to a plurality of circulants $Z_1, Z_2, ..., Z_{upper}$, the plurality of optimal values r_i is generated based on the QC-LDPC code lifted for maximal length $N_{\max}$ and maximal circulant size Z_{upper} of the base matrix,

wherein $N_{\max} = Z_{upper} * L$, L is a column in the base matrix and $0 \le r_i \le Z_{upper} - 1$;

the processing unit (201) configured to:

receive a current circulant $Z_{current}$ from the plurality of circulants $Z_1, Z_2, ..., Z_{upper}$;

select a current optimal value $r_{current}$ from the plurality of optimal values r_i stored in the memory unit corresponding to the current circulant $Z_{current}$; and

lift the base matrix based on the current optimal value $r_{current}$, wherein a floor lifting of the base matrix is calculated as:

$$E(H_{current}) = \left\lfloor \frac{Z_{current}}{Z_{upper}} \left(\left(E(H_{upper}) * r_{current} \right) \bmod Z_{upper} \right) \right\rfloor,$$

where $E(H_{upper})$ is a value of circulant shift in the base matrix for maximal circulant size;

wherein $0 \le r_{current} \le Z_{upper} - 1$ and $r_{current} = 1$ is excluded.

7. The apparatus of claim 6, wherein, generating the plurality of optimal values r_i for the plurality of circulants $Z_1, Z_2, \ldots, Z_{upper}$ comprises:

constructing a plurality of families of parity-check matrixes, each family corresponds to value r in a plurality of values $r_1, r_2, \ldots, r_k$ corresponding to code lengths $N_1, N_2, N_3, \ldots, N_k$; and

based on the plurality of the families of the parity-check matrixes, selecting the plurality of optimal values r_i for the plurality of circulants $Z_1, Z_2, \ldots, Z_{upper}$ by multi-parameter filtering.

8. The apparatus of claim 7, wherein the multi-parameter filtering includes at least one of: Extrinsic Message Degree, ACE Spectrum, Tanner Spectral Bound, Code Distance, Codeword's weight spectrum enumerator, Trapping Set Weight Enumerator, simulations result.

9. The apparatus of any of claims 7-8, wherein the processing unit is further configured to construct the plurality of the families of the parity-check matrixes using equation:

$$E_r(H_{upper}) = E(H_{upper}) \cdot r \bmod Z_{upper}.$$

100

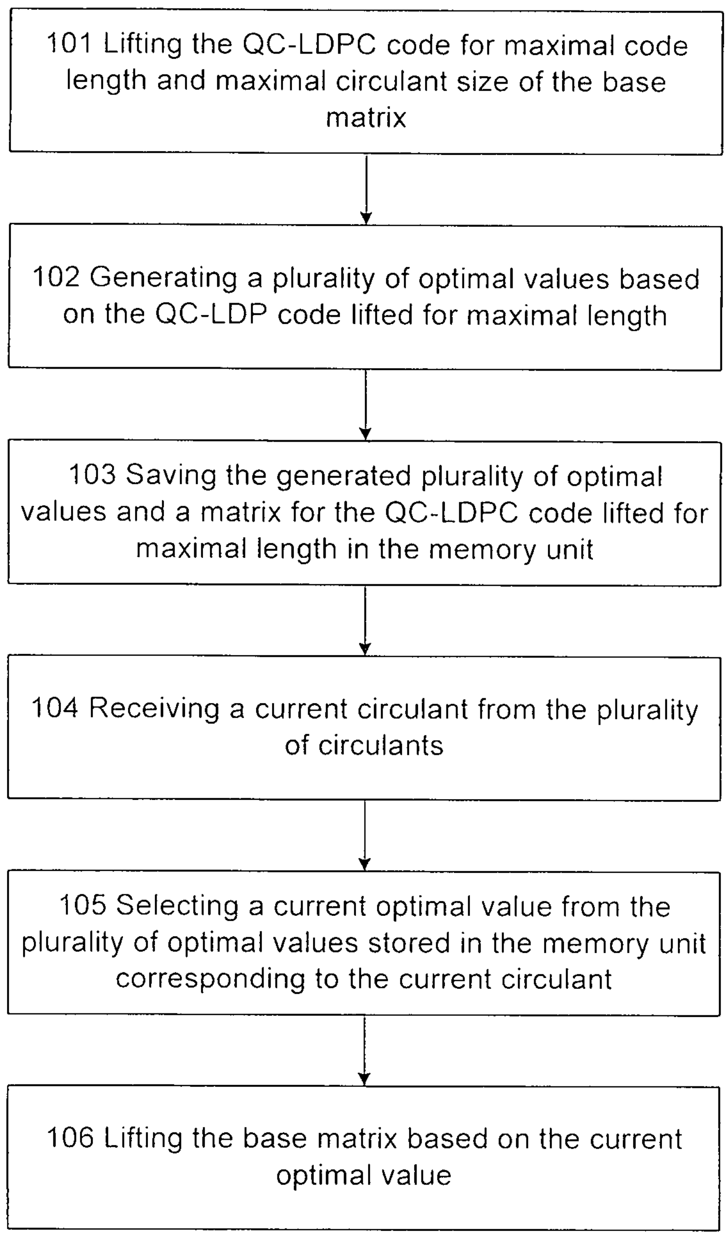

101 Lifting the QC-LDPC code for maximal code length and maximal circulant size of the base matrix
102 Generating a plurality of optimal values based on the QC-LDP code lifted for maximal length
103 Saving the generated plurality of optimal values and a matrix for the QC-LDPC code lifted for maximal length in the memory unit
104 Receiving a current circulant from the plurality of circulants
105 Selecting a current optimal value from the plurality of optimal values stored in the memory unit corresponding to the current circulant
106 Lifting the base matrix based on the current optimal value

Fig. 1

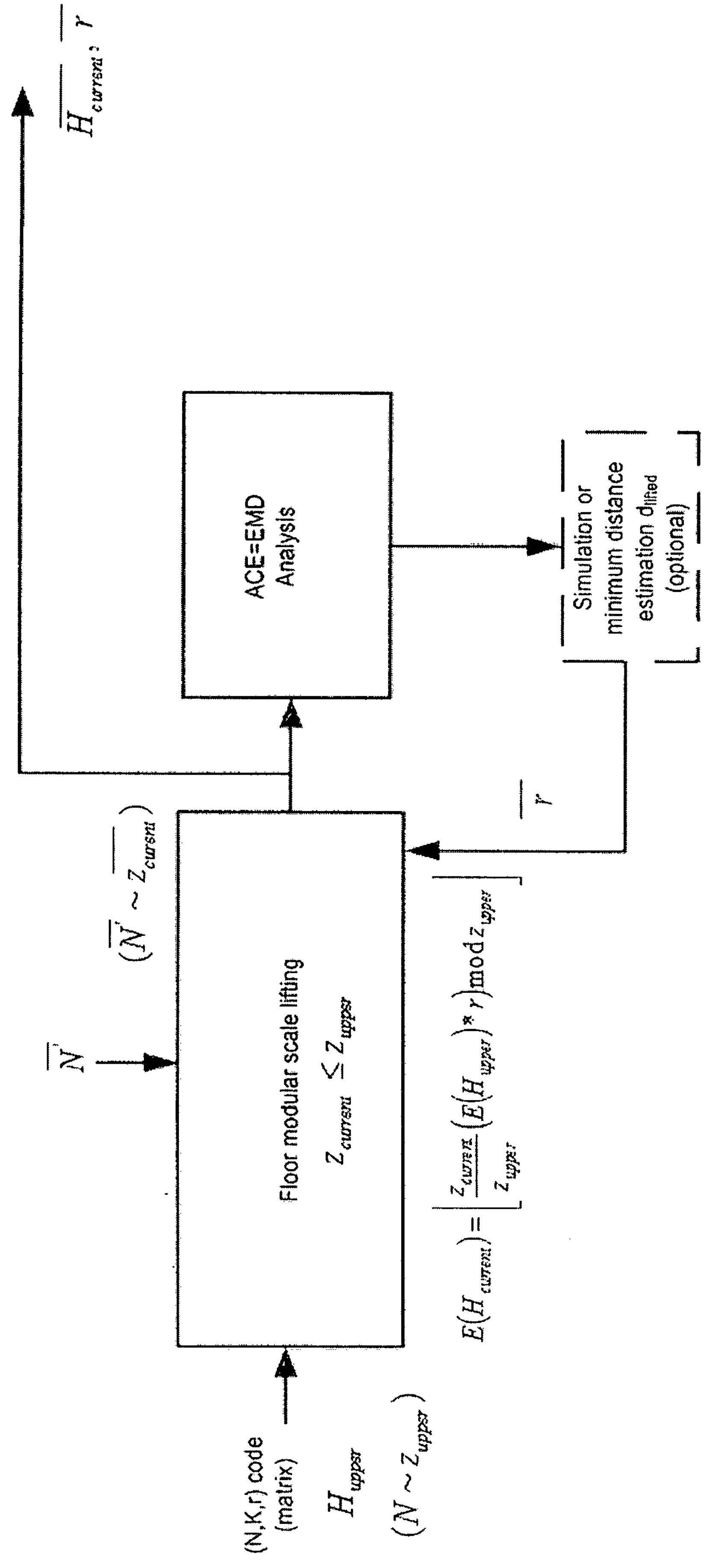
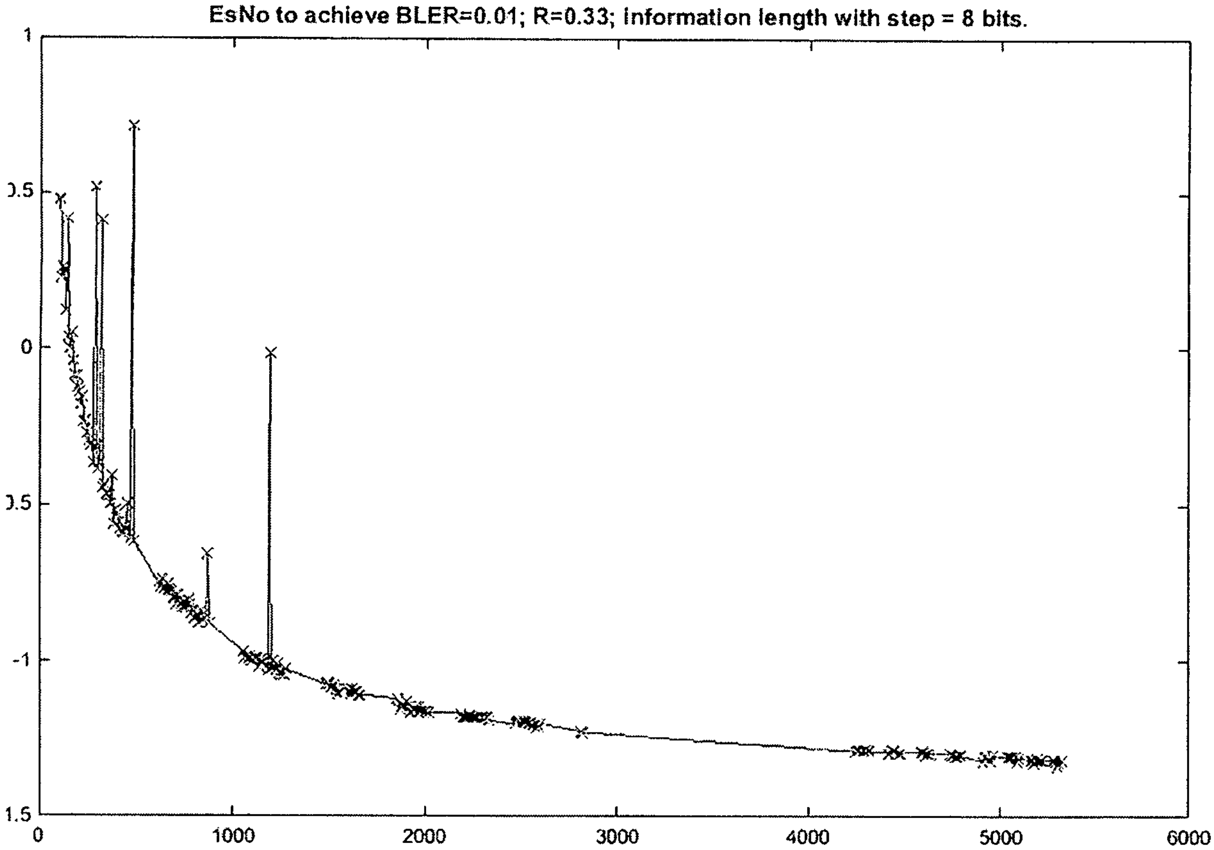

(N,K,r) code
(matrix)
H_{upper}
$(N \sim Z_{upper})$
Floor modular scale lifting
$Z_{current} \leq Z_{upper}$
$E(H_{current}) = \left\lfloor \frac{Z_{current}}{Z_{upper}} \left(E(H_{upper}) * r\right) \right\rfloor \bmod Z_{upper}$
$\overline{N'}$
$(\overline{N'} \sim \overline{Z_{current}})$
ACE=EMD
Analysis
Simulation or
minimum distance
estimation d_{lifted}
(optional)
$\overline{r}$
$\overline{H_{current}}, \overline{r}$

Fig. 2


EsNo to achieve BLER=0.01; R=0.33; information length with step = 8 bits.
1
0.5
0
-0.5
-1
-1.5
0
1000
2000
3000
4000
5000
6000

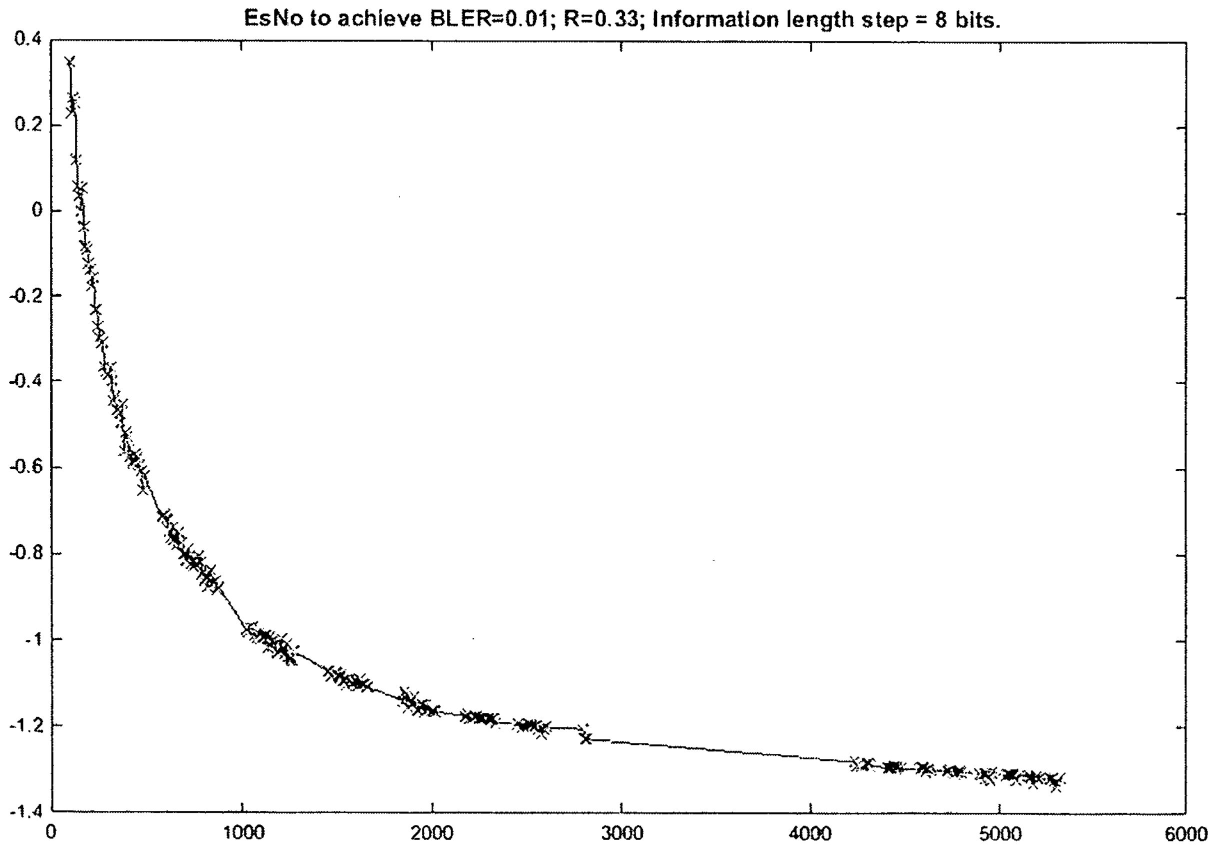

EsNo to achieve BLER=0.01; R=0.33; Information length step = 8 bits.
0.4
0.2
0
-0.2
-0.4
-0.6
-0.8
-1
-1.2
-1.4
0
1000
2000
3000
4000
5000
6000

Fig. 3

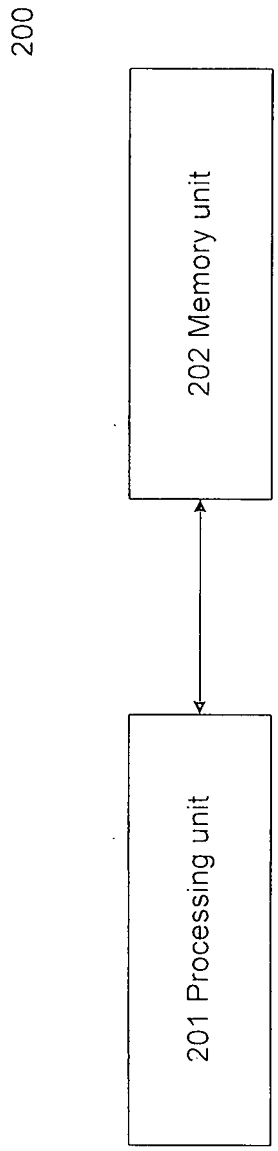
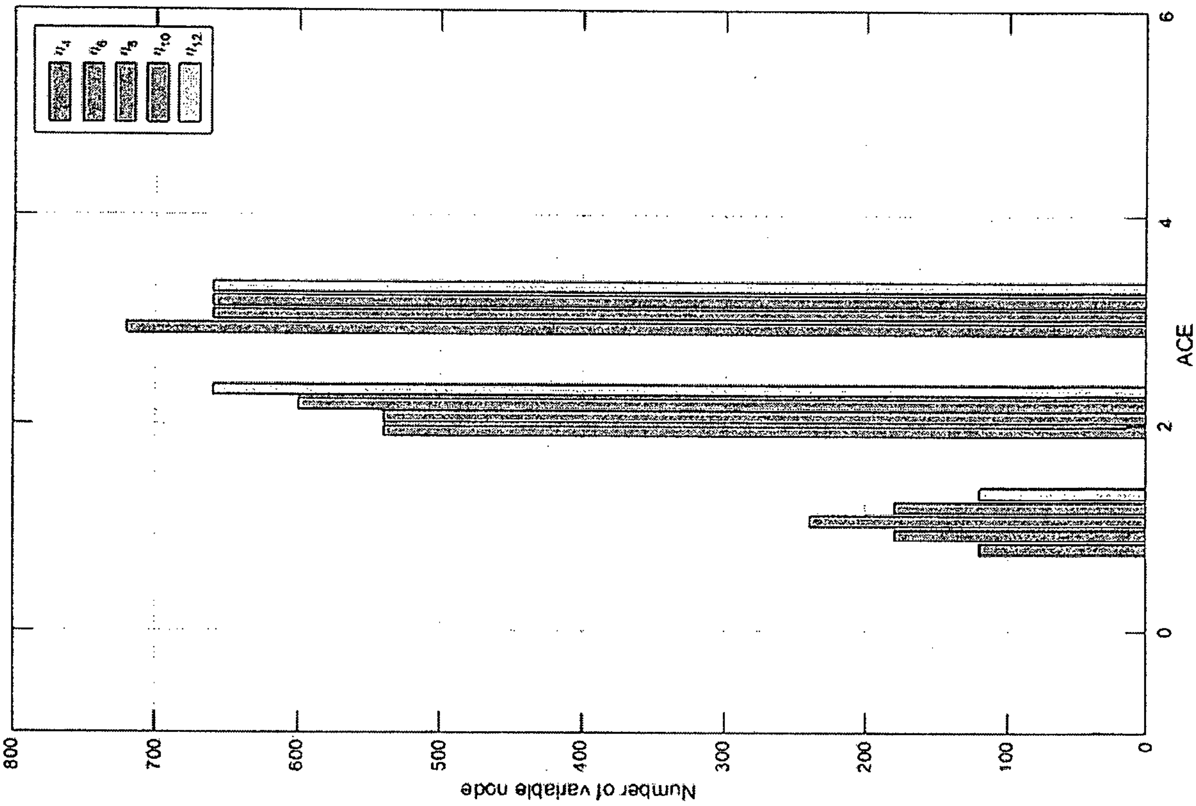


Fig. 4


Number of variable node
ACE
0
100
200
300
400
500
600
700
800
2
4
6
η_4
η_6
η_8
η_{10}
η_{12}

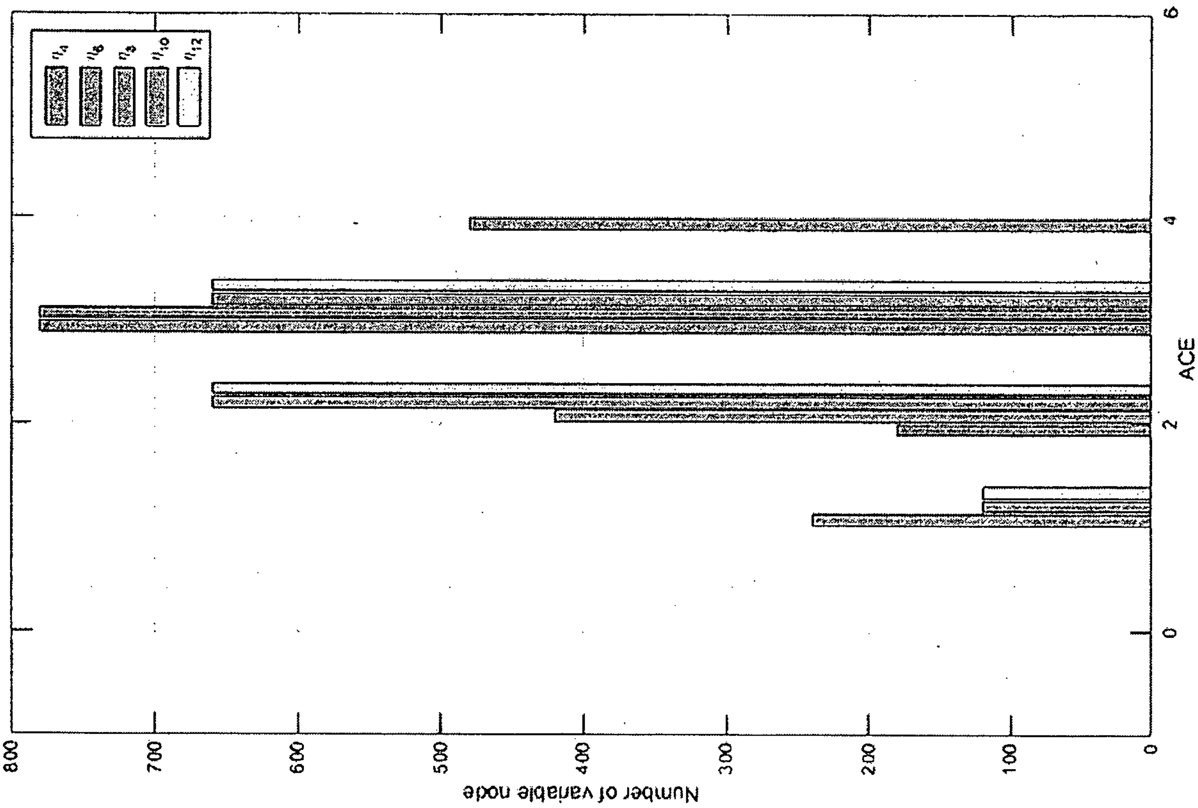

Number of variable node
ACE
0
100
200
300
400
500
600
700
800
2
4
6
η_4
η_6
η_8
η_{10}
η_{12}

Fig. 5

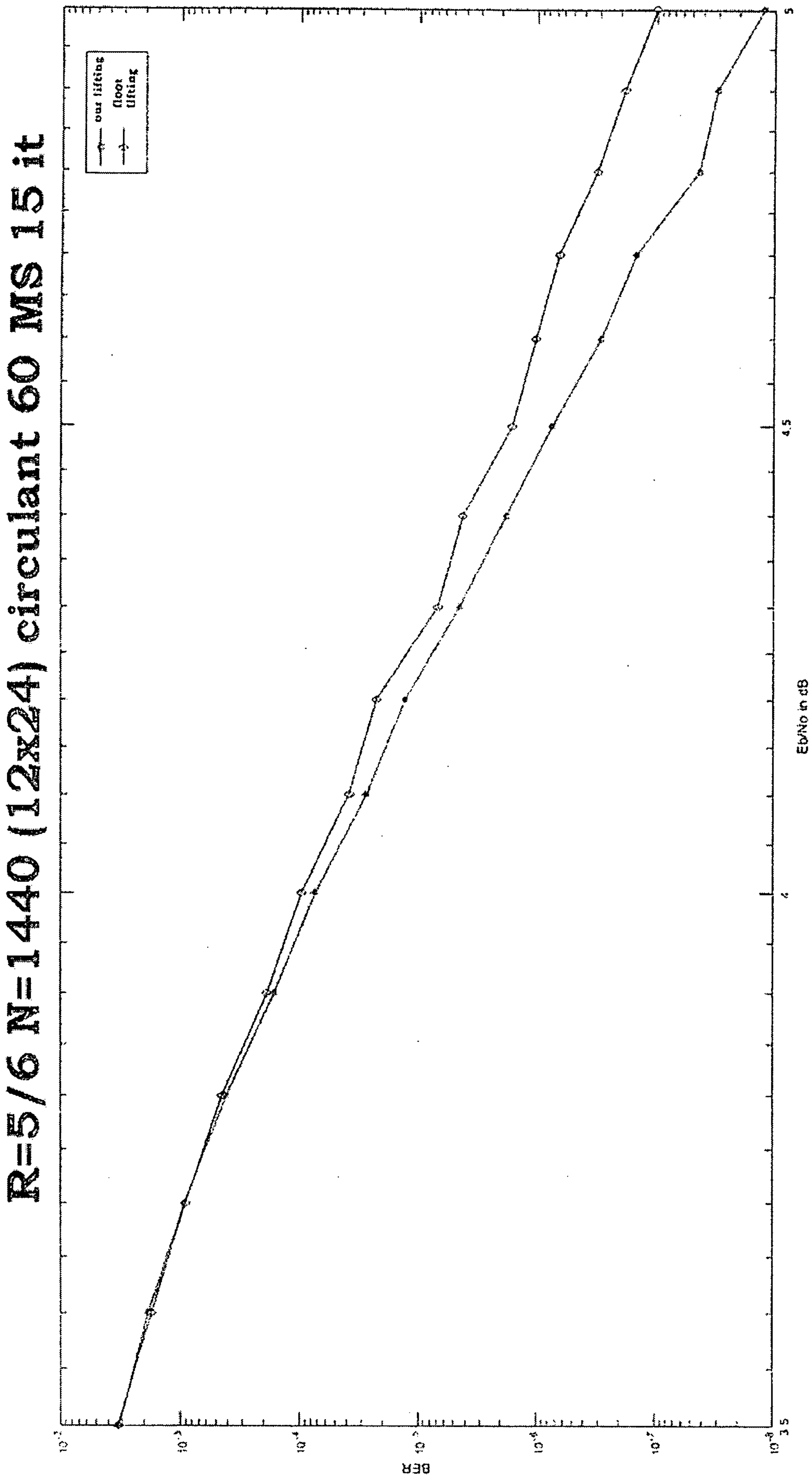

R=5/6 N=1440 (12x24) circulant 60 MS 15 it
our lifting
floor lifting
Eb/No in dB
BER
3.5
4
4.5
5

Fig. 6

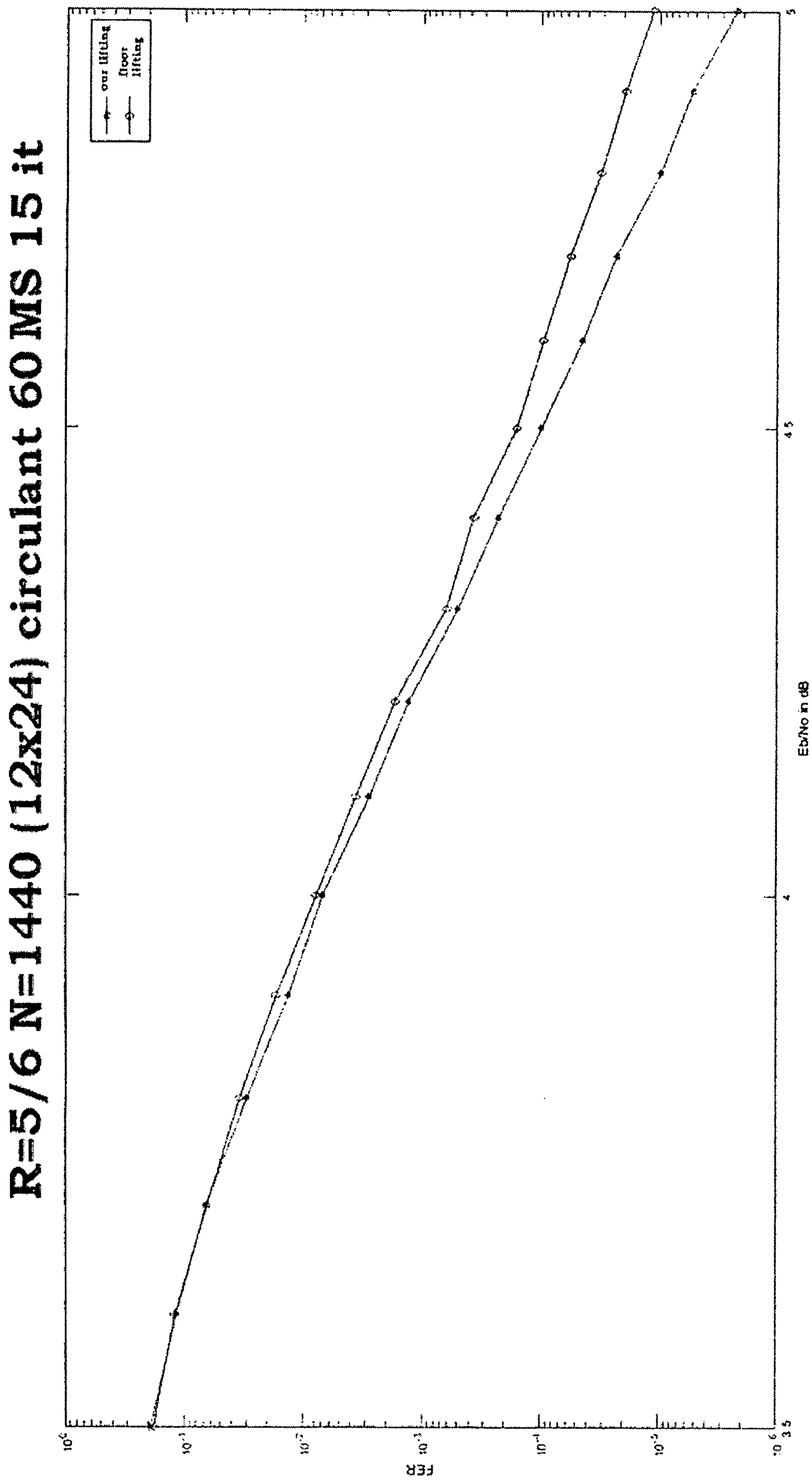

R=5/6 N=1440 (12x24) circulant 60 MS 15 it
our lifting
floor lifting
Eb/No in dB
FER

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/RU2016/000777

A. CLASSIFICATION OF SUBJECT MATTER
INV. H03M13/11 H03M13/03
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H03M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SEHO MYUNG ET AL: "Lifting Methods for Quasi-Cyclic LDPC Codes", IEEE COMMUNICATIONS LETTERS, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 10, no. 6, 1 June 2006 (2006-06-01), pages 489-491, XP001546983, ISSN: 1089-7798, DOI: 10.1109/LCOMM.2006.1638625 the whole document -----	1-9
A	"LDPC coding for OFDMA PHY ; C80216e-05_066r3", IEEE DRAFT; C80216E-05_066R3, IEEE-SA, PISCATAWAY, NJ USA, vol. 802.16e, 27 January 2005 (2005-01-27), pages 1-16, XP017625567, [retrieved on 2005-02-15] the whole document -----	1-9

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2017	01/08/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Offer, Elke

2

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2010/257425 A1 (YUE GUOSEN [US] ET AL) 7 October 2010 (2010-10-07) the whole document	1-9
A	MING JIANG ET AL: "An improved variable length coding scheme using structured LDPC codes", PROC., IEEE INTERNATIONAL CONFERENCE ON WIRELESS COMMUNICATIONS AND SIGNAL PROCESSING, WCSP 2010, 21 October 2010 (2010-10-21), pages 1-5, XP031800170, ISBN: 978-1-4244-7556-8 the whole document	1-9

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/RU2016/000777

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010257425 A1	07-10-2010	NONE	