Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 168–173*

On the minimum distance of LDPC codes based on repetition codes and permutation matrices [1]

Fedor Ivanov fii@iitp.ru
Institute for Information Transmission Problems, Russian Academy of Sciences

Abstract. A new ensemble of quasi-cyclic LDPC codes based on repetition codes and permutation matrices is presented. An estimation of minimum distance for proposed codes is obtained. The results of simulation of obtained code constructions for an iterative "belief propagation" (Sum-Product) decoding algorithm, applied in the case of transmission of a code word via a binary channel with an additive Gaussian white noise and BPSK modulation, are presented.

1 Introduction

Low-density parity-check codes (LDPC-codes) were proposed by Gallager in [1]. There are linear block codes defined by their parity-check matrices **H** characterized by a relatively small number of ones in their rows and columns. It is often convenient to consider LDPC code as it's Tanner graph [2], where connected symbolic and code vertices are used for representation of rows and columns of parity-check matrix.

An important characteristic of an LDPC code is absence of cycles of certain length. A cycle of length 4 (4-cycle) can be understood as a rectangle in the parity-check matrix whose vertices are ones. Cycles of larger length 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], projective geometries [4], and other combinatorial constructions [5] are often used in practice.

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: $[n_0, 1, n_0]$ repetition code ($n_0 > 1$) and permutation matrices. As a result we obtain low rate LDPC codes with simple encoding and good minimum distance (especially for short code lengths).

[1]The research is supported by RSCF, research project No. 14-50-00150

2 Main definitions and notation

Notation 1. *Under* $\mathcal{R}(n_0)$ *we shall assume* $[n_0, 1, n_0]$ *(*$n_0 > 1$*) repetition code of length* n_0 *and minimum distance* $d_{min} = n_0$*.*

Notation 2. *Under* $GF^m(2)$ *(*$m > 1$, $m \in \mathbb{N}$*) we shall assume a vector space of length* m *vectors over* $GF(2)$*.*

Notation 3. *Let* $\mathbf{y} \in GF^m(2)$*, then under* $||\mathbf{y}||$ *we shall assume hamming weight of* $\mathbf{y}$*.*

Notation 4. *Let* $\mathbf{y} \in GF^m(2)$*, then under* $supp(\mathbf{y})$ *we shall assume a support of* $\mathbf{y}$*, i. e.*

$$supp(\mathbf{y}) = \{j : y_j = 1\}.$$

Notation 5. *Let* $\mathbf{y} \in GF^m(2)$*,* $p \in \mathbb{Z}$*,then under the set* $p + supp(\mathbf{y})$ *we shall assume:*

$$p + supp(\mathbf{y}) = \{j + p \mod m : y_j = 1\}.$$

Definition 1. *Let* $m > 1$, $m \in \mathbb{N}$ *and* $\mathbf{I}$ *is a* $m \times m$ *unity matrix. Let us choose an arbitrary* $p \in \mathbb{Z}$*, then under* $\mathbf{I}_p$ *we shall assume a matrix of* p*-times right cyclic shift of columns (or rows) of* $\mathbf{I}$*.*

It is easy to note that the set $\mathcal{I}_m = \{\mathbf{I}_p : p \in \mathbb{Z}\}$ of $m \times m$ matrices $\mathbf{I}_p$ is a cyclic group with generator $\mathbf{I}_1$.

If

$$\mathbf{c} = \mathbf{y}\mathbf{I}_p,$$

and $supp(\mathbf{y})$ is the support of $\mathbf{y}$, then

$$supp(\mathbf{c}) = p + supp(\mathbf{y}).$$

Now let us formulate simple lemma which is the basis of the main result of this paper.

Lemma 1. *If* $\mathbf{I}_p \in \mathcal{I}_m$*,* $\mathbf{y} \in GF^m(2)$*,* $||\mathbf{y}|| = w$*, and* $supp(\mathbf{y}) = p + supp(\mathbf{y})$ *then* $pw \equiv 0 \mod m$*.*

This lemma has an important corollary:

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

3 Construction of LDPC codes based on repetition codes and permutation matrices

Let us consider a parity-check matrix $\mathbf{H}_b$ of $\mathcal{R}(n_0)$ and choose $m > 1$, $k_0 > 0$, $m, k \in \mathbb{N}$. Moreover, consider the group $\mathcal{I}_m$ and choose $2(n_0 - 1)k^2$ arbitraty matrices $\mathbf{I}_{p_j}$, $p_j \in \mathbb{N}$, $j = 1..2(n_0 - 1)k_0^2$ from $\mathcal{I}_m$. Let us separate the set $\mathcal{S}$ of chosen matrices on $2(n_0 - 1)$ equipotent subsets $\mathcal{S}_i$, $i = 1..2(n_0 - 1)$, $|\mathcal{S}_i| = k_0^2$ and compose block matrix $\mathbf{Q}_i$ from the elements of $\mathcal{S}_i$ $k_0 \times k_0$. Matrix $\mathbf{Q}_i$ has the following structure:

$$\mathbf{Q}_i = \begin{pmatrix} \mathbf{I}_{p_{i1}} & \mathbf{I}_{p_{i2}} & \mathbf{I}_{p_{i3}} & \dots & \mathbf{I}_{p_{ik_0}} \\ \mathbf{I}_{p_{i(k_0+1)}} & \mathbf{I}_{p_{i(k_0+2)}} & \mathbf{I}_{p_{i(k_0+3)}} & \dots & \mathbf{I}_{p_{i(2k_0)}} \\ \dots & \dots & \dots & \dots & \dots \\ \mathbf{I}_{p_{i(k_0^2-k_0+1)}} & \mathbf{I}_{p_{i(k_0^2-k_0+2)}} & \mathbf{I}_{p_{i(k_0^2-k_0+3)}} & \dots & \mathbf{I}_{p_{ik_0^2}} \end{pmatrix}.$$

If one substitute each unity in $\mathbf{H}_b$ on the matrix $\mathbf{Q}_i$ and each zero on $mk_0 \times mk_0$ all zeros matrix $\mathbf{Z}$ then the matrix

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

has the size $mk_0(n_0 - 1) \times mkn_0$, all rows have weight $2k_0$, weights of first mk_0 columns are $k_0(n_0 - 1)$, other columns have weight k_0.

We will consider matrix $\mathbf{H}$ as a parity-check matrix of LDPC code.

Thus, choosing an arbitrary numbers $m > 1$, $k_0 > 0$ and $2(n_0-1)k_0^2$ random elements from the group $\mathcal{I}_m$ one can determine an ensemble of LDPC codes with the length $n = mk_0n_0$. Let us denote this ensemble as $\mathcal{E}_{RC}(m, k_0, n_0)$.

Definition 2. *An arbitrary code $\mathcal{C} \in \mathcal{E}_{RC}(m, k_0, n_0)$, will be called a LDPC code based on $\mathcal{R}(n_0)$ and permutation matrices.*

4 Lower bound on the minimum distance of code from $\mathcal{E}_{RC}(m, k_0, n_0)$

In order to obtain the main result of this paper we have to formulate some auxiliary results. Since some proofs of these results are rather complex we will omit them.

One can show that the weight of any codeword from $\mathcal{C} \in \mathcal{E}_{RC}(m, k_0, n_0)$ (in the case of some limitations on k_0 and n_0) is even.

Lemma 2. *Let $\mathcal{C} \in \mathcal{E}_{RC}(m, k_0, n_0)$ then for all k_0, n_0, (expect the case when simultaneously k_0 is even, and n_0 is odd) and for any $\mathbf{c} \in \mathcal{C}$: $||\mathbf{c}|| = 2t$, $t \in \mathbb{N}$.*

Further we shall assume that conditions of lemma 2 hold. The following result provides simple estimation on the minimum distance of $\mathcal{C} \in \mathcal{E}_{RC}(m, k_0, n_0)$.

Lemma 3. *Let $\mathbf{H}$ is a parity-check matrix of code $\mathcal{C}$ from the ensemble $\mathcal{E}_{RC}(m, k_0, n_0)$. If $\mathbf{H}$ has girth greater than 4, then $d_{min}(\mathcal{C}) \geq 4$.*

In order to simplify further reasoning, we will suppose that $n_0 = 4$, $k_0 = 2$ although all derivations can be generalized for cases when $n_0 > 4$, $k_0 = 2$.

Now let us formulate the following lemma which improves the estimation on the minimum distance of codes from $\mathcal{E}_{RC}(m, k_0, n_0)$.

Lemma 4. *Let $\mathbf{H}$ is the parity-check matrix of code $\mathcal{C}$ from $\mathcal{E}_{RC}(m, 2, 4)$. If this matrix is free of cycles of length 4 and $m > 5$ is prime number, then $d_{min}(\mathcal{C}) \geq 8$.*

Now we can formulate the main result of this paper.

Theorem 1. *Let $\mathbf{H}$ is the parity-check matrix of code $\mathcal{C}$ from $\mathcal{E}_{RC}(m, 2, 4)$ for which the conditions of lemma 4 hold, and, moreover, let at least one sub-matrix $(\mathbf{Q}_i\, \mathbf{Q}_{3+i})$ of $\mathbf{H}$ ($i = 1..n_0 - 1$) is free of cycles of length 8, then $d_{min}(\mathcal{C}) \geq 10$.*

This theorem can be generalized for more wide class of codes. Namely, the following result take place:

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

One can notice that in the case when $n_0 > 4$ the requirement about absence of cycles of length 8 in $(\mathbf{Q}_i\, \mathbf{Q}_{n_0+i-1})$ ($i = 1..n_0 - 1$) can be omitted since not all syndrome components $\mathbf{S}_j$ ($j = 1..n_0 - 1$) include 4 vectors of weight 1. Thus, the following result is fulfilled:

Corollary 3. *Let $\mathbf{H}$ is the parity-check matrix of code $\mathcal{C}$ from $\mathcal{E}_{RC}(m, 2, n_0)$, where $n_0 > 4$ and $m > 5$ is prime. If $\mathbf{H}$ is free of cycles of length 4 then $d_{min}(\mathcal{C}) \geq 10$.*

5 Simulation results

In order to generate parity-check matrices of LDPC codes from $\mathcal{E}_{RC}(m, 2, n_0)$ MatLab function was written. Simulation was made by methods of simulation modelling using MatLab. For an information transmission channel, we chose

Table 1: Code constructions

m	n_0	k_0	n	R	d_{min}
7	4	2	56	0.3036	12
11	4	2	88	0.2841	16

a binary BPSK channel with additive white Gaussian noise. For a decoding algorithm, we chose an iterative algorithm Sum-Product (with maximum 50 iterations).

We considered 2 codes with the parameters presented in table 1.

It should be noted that for $(n, k) = (56, 17), (88, 25)$ there are best binary linear codes with minimum distances 17 (untyped linear code) and 24 (shortened BCH code) correspondingly. But parity-check matrices for these codes are dense therefore these codes can not be decoded with complexity $O(n \log n)$. Also it should be noted that for our proposed codes we can correct more than $\frac{d_{min}-1}{2}$ errors due to soft decision decoder. For best linear codes only bounded-distance hard decoding is known.

Table 2: Simulation results for codes $n = 56$

EbNo	-1	0	1	2	3	4
P_b, error rate	0.2641	0.2403	0.2127	0.1868	0.1578	0.1316
N_{err}, proposed	11.0040	10.9047	10.4826	9.6954	8.6023	7.2772
$D(N_{err})$, proposed	4.9043	5.1476	5.5260	5.9559	6.4265	5.9737
N_{err}, PEG	10.5425	10.4382	9.9662	9.2875	8.3359	7.1966
N_{err}, ACE	10.1423	9.9766	9.4482	8.6091	7.4053	6.0390

Table 3: Simulation results for codes $n = 88$

EbNo	-1	0	1	2	3	4
P_b, error rate	0.2641	0.2403	0.2127	0.1868	0.1578	0.1316
N_{err}, proposed	18.0075	17.8215	17.0181	15.7003	13.7815	11.5279
$D(N_{err})$, proposed	8.7169	8.2511	9.3533	10.2527	10.7915	9.9045
N_{err}, PEG	16.0402	16.4992	15.9713	15.1887	13.5802	11.4315
N_{err}, ACE	17.2638	16.7949	15.9119	14.4674	12.4906	10.1992

Simulation results presented in tables 1 – 2 allow us to conclude that our proposed codes not worse than codes based on ACE [7] and PEG [6] algorithms (in terms of an average number of corrected errors N_{err}, also we include a dispersion $D(N_{err})$ of random variable N_{err} for our proposed codes). Irregular LDPC code based on PEG algorithm shows the same behaviour as our proposed codes. In other hand, codes from $\mathcal{E}_{RC}(m, k_0, n_0)$ have more simple structure (since $\mathcal{E}_{RC}(m, k_0, n_0)$ is sub ensemble of quasi-cyclic LDPC codes). This fact allows us to optimize a storage of parity-check matrix, while codes based on PEG algorithm has random structure.

6 Conclusion

A new ensemble of quasi-cyclic LDPC codes based on repetition codes and permutation matrices is presented. An estimation of minimum distance for proposed codes is obtained. Simulation results allow us to conclude that our proposed codes not worse than codes based on ACE and PEG algorithms.

References

[1] R. G. Gallager. Low-Destiny Parity-Check Codes // Cambridge, MA: MIT Press, 1963.

[2] *M. A. Tanner.* Recursive Approach to Low Complexity Codes // IEEE Trans. Inform. Theory. 1981. V. 27. No. 5. P. 533–547.

[3] *E. Gabidulin, A.Moinian, B. Honary.* Generalized construction of quasi-cyclic regular LDPC codes based on permutation matrices // In Proceedings of IEEE International Symposium on Information Theory. 2006. P. 679–683.

[4] *Y. Kou, S. Lin, M. Fossorier.* Low-destiny parity check codes based on finite geometries: A rediscovery and new results // IEEE Trans. Inform. Theory. 2001. V. 47. P. 2711–2736.

[5] *S. Johnson.* Low-density parity-check codes from combinatorial designs // The University of Newcastle Press. Newcastle. 2004.

[6] *H .Xiao, A. H. Banihashemi.* Improved progressive-edge-growth(PEG) construction of irregular LDPC codes //IEEE Communications Letters. 2004. V. 8. No. 12. P. 715–717.

[7] *T. Tian et al.* Construction of irregular LDPC codes with low error floors //ICC'03. IEEE International Conference on. IEEE. 2003. V. 5. P. 3125–3129.