Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 162–167*

The score of the minimum length of cycles in generalized quasi-cyclic regular LDPC codes

Fedor Ivanov fii@iitp.ru
IITP RAS
Victor Zyablov zyablov@iitp.ru
IITP RAS
Vladimir Potapov potapov@iitp.ru
IITP RAS

Abstract. In this paper we construct an ensemble of regular generalized quasi-cyclic LDPC codes, which are based on permutation matrices. For the resulting code construction the condition of absence of cycles of the length 4 is proved. The results of the received code constructions are presented for the iterative algorithm Sum-Product when the codeword is transmitted over channel with additive Gaussian white noise (AGWN).

1 Introduction

R. Gallager was the first to describe pseudo-random code construction with low-density parity-check (LDPC codes) and suggested the algorithm of generation of the check matrix **H** of these codes [1].

It is often comfortable to consider the matrix **H** of the LDPC code as Tanner's graph [2], where the connected symbolic and code vertices are used for the presentation of the rows and columns of **H** .

One of the most important characteristics of LDPC code is the absence of the cycle of a certain length. The cycle of the length 4 can be understood as the formation in check matrix a rectangle, which vertices are ones. The absence of the cycle of the length 4 can be defined with the help of scalar product of all rows (or columns) of the check matrix. If every pairwise scalar product of all rows (or columns) of the check matrix is less than 1, that means the absence of the cycle of the length 4. The cycles of a bigger length are defined by the minimal length of the cycle in Tanner's graph.

Apart from the random LDPC codes the algebraic LDPC codes are used. Particularly, if the check-matrix of the LDPC code **H** consists only of cyclic shifts of a unit matrix **I**, it is called quasi-cyclic. It is enough for quasi-cyclic codes to formulate the absence of the cycles of minimal length, as it was done in the work [3].

LDPC codes are classified into two groups: regular (check matrix consists exactly of l ones in each column and n_0 ones in each row) and irregular (the

amount of ones in the row and column is variable). In this work only the regular code constructions are considered.

Our main aim is to work out and to investigate the constructions of the LDPC codes, which check matrix $\mathbf{H}$ consists of several matrices $\mathbf{H}_1$, $\mathbf{H}_2$, ..., $\mathbf{H}_k$ quasi-cyclic LDPC codes with lengthes n_1, n_2, ..., n_k. The condition of absence of the cycles of the length 4 is proved for the resulting code construction. It is shown that it reduces the absence of the cycles of the length 4 in each matrix $\mathbf{H}_1$, $\mathbf{H}_2$, ..., $\mathbf{H}_k$. The resulting statement generalizes Gabidulin's result, formulated in [3].

2 Code structure and girth analysis

Definition 1. *Let* $\mathbf{I}$ *– is the* $m \times m$ *identity matrix. Let* $\mathbf{I}_{p_{ij}}$ *– a right cyclic shift on a* p_{ij} *of columns of a unit matrix* $\mathbf{I}$, $p_{ij} \in \mathbb{N}$, $0 \leq p < m$, $1 \leq i \leq l$, $1 \leq j \leq n_0$, $l \leq n_0$. *Then the check matrix*

$$\mathbf{H} = \begin{pmatrix} \mathbf{I}_{p_{11}} & \mathbf{I}_{p_{12}} & \dots & \mathbf{I}_{p_{1n_0}} \\ \mathbf{I}_{p_{21}} & \mathbf{I}_{p_{22}} & \dots & \mathbf{I}_{p_{2n_0}} \\ \dots & \dots & \dots & \dots \\ \mathbf{I}_{p_{l1}} & \mathbf{I}_{p_{l2}} & \dots & \mathbf{I}_{p_{ln_0}} \end{pmatrix}$$

determines the ensemble of regular (l, n_0) *binary LDPC codes of the length* $n = mn_0$, *that we will define as* $\mathcal{E}_{QC}(l, n_0, m)$. *Elements of the ensemble* $\mathcal{E}_{QC}(l, n_0, m)$ *are received with the help of an equiprobable sample of* $p_{ij} \in \mathbb{N}$. *The arbitrary code* $\mathcal{C} \in \mathcal{E}_{QC}(l, n_0, m)$ *will be called quasi-cyclic LDPC code.*

Definition 2. *Let* $\mathbf{H}_1$, $\mathbf{H}_2$, ..., $\mathbf{H}_k$, $k \geq 2$ *are check matrixes of regular* (l, n_0) *binary quasi-cyclic LDPC codes of the lengthes* $n_i = m_i n_0$*:*

$$\mathbf{H}_i = \begin{pmatrix} \mathbf{I}_{p_{11}^{(i)}} & \mathbf{I}_{p_{12}^{(i)}} & \dots & \mathbf{I}_{p_{1n_0}^{(i)}} \\ \mathbf{I}_{p_{21}^{(i)}} & \mathbf{I}_{p_{22}^{(i)}} & \dots & \mathbf{I}_{p_{2n_0}^{(i)}} \\ \dots & \dots & \dots & \dots \\ \mathbf{I}_{p_{l1}^{(i)}} & \mathbf{I}_{p_{l2}^{(i)}} & \dots & \mathbf{I}_{p_{ln_0}^{(i)}} \end{pmatrix}.$$

Then the matrix

$$\mathbf{H} = \begin{pmatrix} \begin{pmatrix} \mathbf{I}_{p_{11}^{(1)}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{p_{11}^{(2)}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{p_{11}^{(k)}} \end{pmatrix} & \dots & \begin{pmatrix} \mathbf{I}_{p_{1n_0}^{(1)}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{p_{1n_0}^{(2)}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{p_{1n_0}^{(k)}} \end{pmatrix} \\ \vdots & & \vdots \\ \begin{pmatrix} \mathbf{I}_{p_{l1}^{(1)}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{p_{l1}^{(2)}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{p_{l1}^{(k)}} \end{pmatrix} & \dots & \begin{pmatrix} \mathbf{I}_{p_{ln_0}^{(1)}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{p_{ln_0}^{(2)}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{p_{ln_0}^{(k)}} \end{pmatrix} \end{pmatrix}$$

determines the ensemble of regular (l, n_0) *binary LDPC codes of the length* $n = n_0 \sum\limits_{i=1}^{k} m_i = \sum\limits_{i=1}^{k} n_i$*, that we will define as* $\mathcal{E}_{QQC}(l, n_0, m)$*. Elements of the ensemble* $\mathcal{E}_{QQC}(l, n_0, m)$ *are received with the help of an equiprobable sample without replacement of parity matrixes* $\mathbf{H}_1$*,* $\mathbf{H}_2$*, ...,* $\mathbf{H}_k$*,* $k \geq 2$*. The arbitrary code* $\mathcal{C} \in \mathcal{E}_{QQC}(l, n_0, m)$ *will be called generalized quasi-cyclic LDPC code.*

The main result of this work can be formulated as the following theorem:

Theorem 1. *If the matrix* $\mathbf{H}$ *of the generalized quasi-cyclic code consists of the matrices* $\mathbf{H}_1$*,* $\mathbf{H}_2$*, ...,* $\mathbf{H}_k$*,* $k \geq 2$*, then* $\mathbf{H}$ *does not have cycles of the length* 4 *if and only if* $\mathbf{H}_1$*,* $\mathbf{H}_2$*, ...,* $\mathbf{H}_k$ *do not have cycles of the length* 4*.*

Proof. Let

$$\mathbf{H} = \begin{pmatrix} \mathbf{P}_{11} & \mathbf{P}_{12} & \dots & \mathbf{P}_{1n_0} \\ \dots & \dots & \dots & \dots \\ \mathbf{P}_{l1} & \mathbf{P}_{l2} & \dots & \mathbf{P}_{ln_0} \end{pmatrix}$$

is a check matrix of code $\mathcal{C} \in \mathcal{E}_{QQC}(l, n_0, m)$, where

$$\mathbf{P}_{ij} = \begin{pmatrix} \mathbf{I}_{p_{ij}^{(1)}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{p_{ij}^{(2)}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{p_{ij}^{(k)}} \end{pmatrix} \triangleq \left[\mathbf{I}_{p_{ij}^{(1)}}, \dots, \mathbf{I}_{p_{ij}^{(k)}} \right].$$

It is easy to show that

$$\mathbf{P}_{ij}\mathbf{P}_{ks} = \left[\mathbf{I}_{p_{ij}^{(1)} + p_{ks}^{(1)}}, \dots, \mathbf{I}_{p_{ij}^{(k)} + p_{ks}^{(k)}} \right].$$

Since $\mathbf{P}_{ij}$ is a permutation matrix, then

$$\mathbf{P}_{ij}^{-1} = \mathbf{P}_{ij}^{T} = \left[\mathbf{I}_{m_1 - p_{ij}^{(1)}}, \ldots, \mathbf{I}_{m_k - p_{ij}^{(k)}}\right].$$

In [3] it was proved that the block matrix $\begin{pmatrix} \mathbf{R} & \mathbf{S} \\ \mathbf{P} & \mathbf{Q} \end{pmatrix}$ formed by the permutation matrixes, does not have the cycles of the length 4 only when $(\mathbf{P}\mathbf{R}^T) \diamond (\mathbf{Q}\mathbf{S}^T) = \mathbf{0}$, where $\mathbf{A} \diamond \mathbf{B}$ is a Hadamard product of matrices $\mathbf{A}$ and $\mathbf{B}$.

Let $\mathbf{P} = \left[\mathbf{I}_{m_1 - p_1^{(1)}}, \ldots, \mathbf{I}_{m_k - p_1^{(k)}}\right]$, $\mathbf{R} = \left[\mathbf{I}_{m_1 - p_2^{(1)}}, \ldots, \mathbf{I}_{m_k - p_2^{(k)}}\right]$, $\mathbf{S} = \left[\mathbf{I}_{m_1 - p_3^{(1)}}, \ldots, \mathbf{I}_{m_k - p_3^{(k)}}\right]$, $\mathbf{Q} = \left[\mathbf{I}_{m_1 - p_4^{(1)}}, \ldots, \mathbf{I}_{m_k - p_4^{(k)}}\right]$, then the condition $(\mathbf{P}\mathbf{R}^T) \diamond (\mathbf{Q}\mathbf{S}^T) = \mathbf{0}$ can be expressed as

$$\left[\mathbf{I}_{m_1 - p_1^{(1)} + p_2^{(1)}}, \ldots, \mathbf{I}_{m_k - p_1^{(k)} + p_2^{(k)}}\right] \diamond \left[\mathbf{I}_{m_1 - p_3^{(1)} + p_4^{(1)}}, \ldots, \mathbf{I}_{m_k - p_3^{(k)} + p_4^{(k)}}\right] = \mathbf{0}.$$

The latter condition is equivalent to saying that

$$\begin{cases} p_2^{(1)} - p_1^{(1)} \neq p_4^{(1)} - p_3^{(1)} \\ p_2^{(2)} - p_1^{(2)} \neq p_4^{(2)} - p_3^{(2)} \\ \ldots \\ p_2^{(k)} - p_1^{(k)} \neq p_4^{(k)} - p_3^{(k)} \end{cases}$$

[3, Theorem 1] asserts, that matrix $\mathbf{H} = \begin{pmatrix} \mathbf{P}_{11} & \mathbf{P}_{12} & \ldots & \mathbf{P}_{1n_0} \\ \ldots & \ldots & \ldots & \ldots \\ \mathbf{P}_{l1} & \mathbf{P}_{l2} & \ldots & \mathbf{P}_{ln_0} \end{pmatrix}$ made of permutation matrixes, does not have cycles of the length 4 only when any of its submatrix $\mathbf{H}_1$ in the form

$$\mathbf{H}_1 = \begin{pmatrix} \mathbf{P}_{p_{i_1 j_1}} & \mathbf{P}_{p_{i_1 j_2}} \\ \mathbf{P}_{p_{i_2 j_1}} & \mathbf{P}_{p_{i_2 j_2}} \end{pmatrix}$$

where $(1 \leq i_1 < i_2 \leq l,\ 1 \leq j_1 < j_2 \leq n_0)$ does not have cycles of the length 4.

Thus the matrix $\mathbf{H}$ of the generalized quasi-cyclic LDPC code does not contain cycles of length 4 only when

$$\begin{cases} p_{i_2 j_1}^{(1)} - p_{i_1 j_1}^{(1)} \neq p_{i_2 j_2}^{(1)} - p_{i_1 j_2}^{(1)} \\ p_{i_2 j_1}^{(2)} - p_{i_1 j_1}^{(2)} \neq p_{i_2 j_2}^{(2)} - p_{i_1 j_2}^{(2)} \\ \ldots \\ p_{i_2 j_1}^{(k)} - p_{i_1 j_1}^{(k)} \neq p_{i_2 j_2}^{(k)} - p_{i_1 j_2}^{(k)} \end{cases}$$

The relation $p_{i_2 j_1}^{(t)} - p_{i_1 j_1}^{(t)} \neq p_{i_2 j_2}^{(t)} - p_{i_1 j_2}^{(t)}$ is the condition of absence of cycles of length 4 in the check matrix $\mathbf{H}_t$, $1 \leq t \leq k$. □

3 Results of the modeling

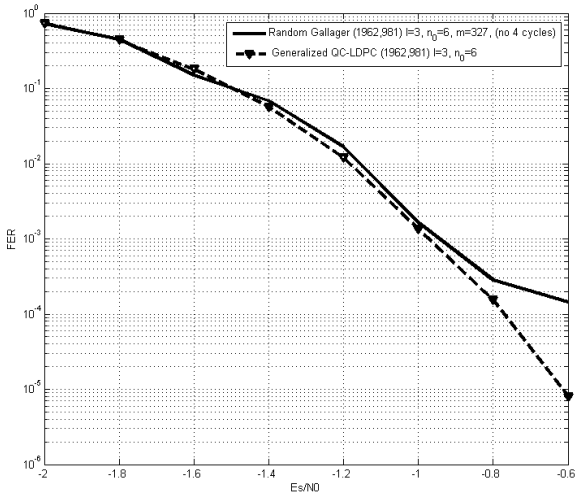
To demonstrate the possibilities of building codes from the ensemble $\mathcal{E}_{QQC}(l, n_0, m)$ in accordance with proved theorem we will consider the following example:

Example 1. *Let* $\mathbf{H}_1$, $\mathbf{H}_2$, $\mathbf{H}_3$ *are check matrixes of the regular* $(3, 6)$ *quasi-cyclic LDPC codes with lengthes* $n_1 = 6m_1 = 6 \cdot 80 = 480$, $n_2 = 6m_2 = 6 \cdot 113 = 678$, $n_3 = 6m_3 = 6 \cdot 134 = 804$. *The minimum length of a cycle for every matrix* $\mathbf{H}_i$, $(i = 1, 2, 3)$ *is* 8.

The matrix $\mathbf{H}$ *of the generalized quasi-cyclic LDPC code consisting of the matrices* $\mathbf{H}_1$, $\mathbf{H}_2$, $\mathbf{H}_3$ *has has a minimum length of cycles* 8.

The resulting $(3, 6)$ *generalized quasi-cyclic LDPC code has length* $n = n_1 + n_2 + n_3 = 1962$.

The modeling of this code construction was done with the methods of simulating with the use of MatLab. For the information channel transmission there was chosen a channel with additive white Gaussian noise (AWGN). For the algorithm of decoding there was chosen an iterative algorithm Sum-Product with "soft input". The maximum number of iterations is 50.



Pic. 1 The dependence between the error probability per frame (FER) and the signal-to-noise ratio (EsN0) for the random Gallager code and code from $\mathcal{E}_{QQC}(l, n_0, m)$.

As it follows from the pic. 1, $(3, 6)$ code from $\mathcal{E}_{QQC}(l, n_0, m)$ with the length $n = 1962$, also practically wins the order of the probability of an error on the frame of a random Gallager's code with correlation of the signal-noise -0.6 Db.

4 Conclusion

The results of the modeling show, that the described generalized quasi-cyclic codes do not yield an ensemble of Gallager codes, while having an easier structure of a check-matrix.

Moreover, the results of modeling allow us to make a conclusion that there is an opportunity of practical usage of the given code constructions.

References

[1] R. G. Gallager, Low-Destiny Parity-Check Codes, *M.I.T. Press*, Massachusetts, 1963.

[2] M. Tanner A Recursive Approach to Low Complexity Codes, *IEEE Trans. Inform. Theory*, **27** (5), 533–547, 1981.

[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,* IEEE, 2006, 679–683.