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

F. Ivanov V. Zyablov V. Potapov

Institute for Information Transmission Problems
Russian Academy of Sciences

Algebraic and Combinatorial Coding Theory ACCT2012, 20.06.12

Outline

- Code structure
- Main result
- Results of the modeling
- Conclusion

Parity check matrix of the preudo-random LDPC code

$\mathbf{H}_0$ – check matrix of the parity check code n_0.
Write block diagonal matrix $\mathbf{H}_b$, with b check matrixes $\mathbf{H}_0$ on the main diagonal, where b is large.
Size $\mathbf{H}_0$ – $1 \times n_0$,
size $\mathbf{H}_b$ – $b \times bn_0$.
$\pi(\mathbf{H}_b)$ – random columns permutation $\mathbf{H}_b$.
Matrix $\mathbf{H}$ consists of $\ell > 2$ such permutations as a layers.
Size $\mathbf{H}$ – $\ell b \times bn_0$. $\mathbf{H}$ determines the ensemble of regular (l, n_0) random binary LDPC codes of the length $n = bn_0$, that we will define as $\mathcal{E}(l, n_0, b)$

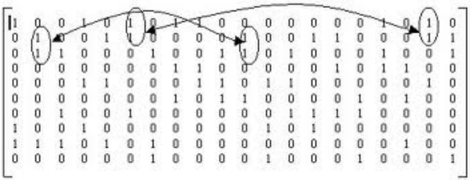
$$\mathbf{H}_0 = \underbrace{111...1}_{n_0}$$

$$\mathbf{H}_b = \begin{pmatrix} \underbrace{\begin{matrix} \mathbf{H}_0 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathrm{H}_0 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_0 \end{matrix}}_{b} \end{pmatrix},$$

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \\ \vdots \\ \mathbf{H}_\ell \end{pmatrix} = \begin{pmatrix} \pi_1(\mathbf{H}_b) \\ \pi_2(\mathbf{H}_b) \\ \vdots \\ \pi_\ell(\mathbf{H}_b) \end{pmatrix}$$

Cycles in the parity check matrix of the LDPC code

The cycle of the length 4 can be understood as the formation in check matrix a rectangle, which vertices are ones.



Cycles of the length 4 in the parity check matrix of the $(3, 10)$ LDPC code

Theorem

If every pairwise scalar product of all rows (or columns) of the check matrix $\mathbf{H}$ *is less than* 1*, than* $\mathbf{H}$ *does not contain cycles of the length* 4*.*

Structure of the check matrix of the quasi-cyclic LDPC codes

Definition

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.

The condition of the absence of the cycles of the length 4 for the quasi-cyclic LDPC codes

Theorem

Let

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

is the check matrix of the quasi-cyclic LDPC code, then $\mathbf{H}$ *does not contain cycles of the length* 4 *if and only if for every submatrix*

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

$(1 \le i_1 < i_2 \le l,\ 1 \le j_1 < j_2 \le n_0)$ *the following condition is performed:*

$$p_{i_2 j_1} - p_{i_1 j_1} \neq p_{i_2 j_2} - p_{i_1 j_2}.$$

Structure of the check matrix of the qeneralized quasi-cyclic LDPC codes

Definition

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 $n_i = m_i n_0$:

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

Structure of the check matrix of the qeneralized quasi-cyclic LDPC codes

Then the matrix

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

determines the ensemble of regular (l, n_0) binary LDPC codes of the length $n = n_0 \sum_{i=1}^{k} m_i = \sum_{i=1}^{k} n_i$, that we will define as $\mathcal{E}_{QQC}(l, n_0, m)$.

Structure of the check matrix of the qeneralized quasi-cyclic LDPC codes

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

Theorem

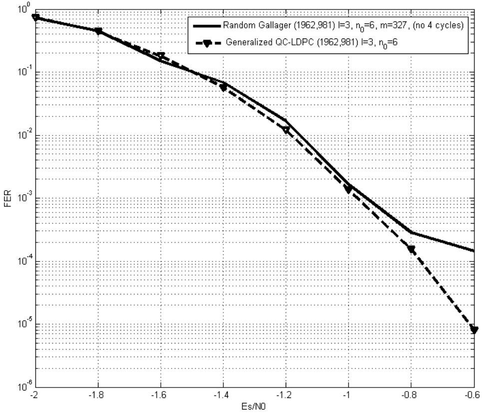
If the matrix $\mathbf{H}$ *of the generalized quasi-cyclic code consists of the matrices* $\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_k$, $k \geq 2$, *then* $\mathbf{H}$ *does not have cycles of the length* 4 *if and only if* $\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_k$ *do not have cycles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

Example of the qeneralized quasi-cyclic LDPC code

Example

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 $n = n_1 + n_2 + n_3 = 1962$.

Results of the modeling



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

Conclusion

- New LDPC code structure was discovered.
- For this construction the condition of the absence of the cycles of the length 4 was proved.
- Results of modeling allow us to make a conclusion that there is an opportunity of practical usage of the given code construction.

References

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

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

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.

Thank you for your attention.