Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 163–168*

Upper Bounds on the Minimum Distance of Quasi-Cyclic LDPC codes [1]

Alexey Frolov alexey.frolov@iitp.ru
Inst. for Information Transmission Problems
Russian Academy of Sciences
Moscow, Russia

Abstract. Two upper bounds on the minimum distance of type-1 quasi-cyclic low-density parity-check (QC LDPC) codes are derived. The necessary condition is given for the minimum code distance of such codes to grow linearly with the code length.

1 Introduction

In this paper we investigate the minimum code distance of QC LDPC codes [1,2]. These codes form an important subclass of LDPC codes [3]. These codes also are a subclass of protograph-based LDPC codes [4]. QC LDPC codes can be easily stored as their parity-check matrices can be easily described. Besides such codes have efficient encoding and decoding algorithms. All of these makes the codes very popular in practical applications.

In [2] an upper bound on the minimum distance of QC LDPC codes is derived for the case when the base matrix has all the elements equal to one. In this case the minimum code distance is upper bounded by a quantity $(m+1)!$, where m is a height of a base matrix and at the same time (due to the structure of the base matrix) the number of ones in a column of the base matrix. In [5] the results of [2] are generalized for the case of type-w QC LDPC codes (see Theorems 7 and 8 in [5]). Unfortunately these estimates can be applied only to a certain parity-check matrix. In this paper we obtain the upper bounds which are valid for any code from the ensemble of QC LDPC codes with the given degree distribution. This allows us to formulate the necessary condition for the minimum code distance of such codes to grow linearly with the code length. We consider only the case of so-called type-1 QC LDPC codes.

Our contribution is as follows. Two upper bounds on the minimum distance of type-1 quasi-cyclic low-density parity-check (QC LDPC) codes are derived. The necessary condition is given for the minimum code distance of such codes to grow linearly with the code length.

[1] This research has been supported by RFBR, research projects No. 13-01-12458 and No. 14-07-31197.

2 Preliminaries

In this paper we only consider binary codes. Let w be some positive integer. Consider a matrix of size $m \times n$

$$\mathbf{H}^{(W)} = [h_{i,j}] \in \{0, 1, \ldots, w\}^{m \times n}.$$

In what follows the matrix will be referred to as the weight matrix[2].

Let us construct a parity-check matrix $\mathbf{H}$ of the QC LDPC code $\mathcal{C}$. For this purpose we extend the matrix $\mathbf{H}^{(W)}$ with circulant matrices (circulants) as follows:

$$\mathbf{H} = \begin{bmatrix} \mathbf{P}_{1,1} & \mathbf{P}_{1,2} & \cdots & \mathbf{P}_{1,n} \\ \mathbf{P}_{2,1} & \mathbf{P}_{2,2} & \cdots & \mathbf{P}_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{P}_{m,1} & \mathbf{P}_{m,2} & \cdots & \mathbf{P}_{m,n} \end{bmatrix} \in \mathbb{F}_2^{ms \times ns},$$

where $\mathbf{P}_{i,j}$ is a circulant over a binary field $\mathbb{F}_2$ of size $s \times s$ ($s \geq w$) and of weight[3] $h_{i,j}$, $i = 1, \ldots, m$; $j = 1, \ldots, n$.

Let us denote the length of the code $\mathcal{C}$ by $N = ns$, such inequality follows for the rate of the code

$$R(\mathcal{C}) \geq 1 - \frac{m}{n}.$$

Remark 1. *The constructed code is a type-w QC LDPC code. In what follows we will only consider type-*1 *QC LDPC codes, i.e. $w = 1$. In this case the matrix $\mathbf{H}^{(W)}$ can be considered as a matrix over $\mathbb{F}_2$.*

Let $\mathbb{F}$ be some field, by $\mathbb{F}[x]$ we denote the ring of all the polynomials with coefficients in $\mathbb{F}$. It is well-known that the ring of circulants of size $s \times s$ over $\mathbb{F}$ is isomorphic to the factor ring $\mathbb{F}^{(s)}[x] = \mathbb{F}[x]/(x^s - 1)$. Thus with the parity-check matrix $\mathbf{H}$ we associate a polynomial parity-check matrix $\mathbf{H}(x) \in \left(\mathbb{F}_2^{(s)}[x]\right)^{m \times n}$:

$$\mathbf{H}(x) = \begin{bmatrix} p_{1,1}(x) & p_{1,2}(x) & \cdots & p_{1,n}(x) \\ p_{2,1}(x) & p_{2,2}(x) & \cdots & p_{2,n}(x) \\ \vdots & \vdots & \ddots & \vdots \\ p_{m,1}(x) & p_{m,2}(x) & \cdots & p_{m,n}(x) \end{bmatrix},$$

where $p_{i,j}(x) = \sum_{t=1}^{s} P_{i,j}(t,1)x^{t-1}$, by $P_{i,j}(t,1)$ we mean an element at the intersection of the t-th row and the first column in the matrix $P_{i,j}$.

Example 1. *Matrices*

$$\mathbf{H}^{(W)} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad \textit{and} \quad \mathbf{H}(x) = \begin{bmatrix} 0 & x^2 & x \\ 1 & 0 & x^2 \end{bmatrix}.$$

[2] in the literature the matrix is called a base matrix or a proto-matrix.

[3] the weight of a circulant is a weight of its first row.

correspond to the parity-check matrix

$$\mathbf{H} = \left[\begin{array}{ccc|ccc|ccc} 0&0&0&0&1&0&0&0&1\\ 0&0&0&0&0&1&1&0&0\\ 0&0&0&1&0&0&0&1&0\\ \hline 1&0&0&0&0&0&0&1&0\\ 0&1&0&0&0&0&0&0&1\\ 0&0&1&0&0&0&1&0&0 \end{array}\right]$$

Let us associate the vector

$$\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n),$$

where

$$\mathbf{c}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,s}), \quad i = 1, 2, \ldots, n,$$

to the vector of polynomials

$$\mathbf{c}(x) = (c_1(x), c_2(x), \ldots, c_n(x)),$$

where $c_i(x) = \sum_{t=1}^{s} c_{i,t} x^{t-1}$.

It is clear, that

$$\mathbf{H}\mathbf{c}^T = \mathbf{0} \quad \text{(in the field } \mathbb{F}_2\text{)}$$

is equivalent to

$$\mathbf{H}(x)\mathbf{c}^T(x) = \mathbf{0} \quad \text{(in the ring } \mathbb{F}_2^{(s)}[x]\text{)}.$$

By the weight of polynomial $f(x)$ we mean the number of non-zero coefficients. We denote the weight by $||f(x)||$. Let us define the weight of the vector of polynomials $\mathbf{c}(x) = (c_1(x), c_2(x), \ldots, c_n(x))$ as follows

$$||\mathbf{c}(x)|| = \sum_{i=1}^{n} ||c_i(x)||.$$

3 Minimum code distance

Let us denote the minimum code distance of the code $\mathcal{C}$ by $D(\mathcal{C})$. First we derive a simple bound.

Theorem 1. *Let $\mathcal{C}$ be a type-*1 *QC LDPC code with the weight matrix $\mathbf{H}^{(W)}$ and let d be the minimum code distance of the code which corresponds to the parity-check matrix $\mathbf{H}^{(W)}$, then*

$$D(\mathcal{C}) \leq ds. \tag{1}$$

Proof. We omit the proof here. □

Let us introduce the notation of a submatrix. Let $\mathbf{A}$ be some matrix of size $M \times N$. Let $I \subseteq \{1, 2, \ldots, M\}$ be a subset of rows, $J \subseteq \{1, 2, \ldots, N\}$ – subset of columns. By $\mathbf{A}_{I,J}$ we denote a submatrix of $\mathbf{A}$ which contains only rows with numbers in I and only columns with numbers in J. If $I = \{1, 2, \ldots, M\}$, then we use a notation $\mathbf{A}_J$.

To derive the second estimate we start with the following lemma which is the generalization of Theorem 2 from [2] and shows how to construct codewords of QC LDPC codes.

Lemma 1. *Let $\mathcal{C}$ be a type-1 QC LDPC code with the polynomial matrix $\mathbf{H}(x)$. Let $J \subset \{1, 2, \ldots, n\}$, $|J| = m+1$ and let $\Delta_j(x) = \det\left(\mathbf{H}_{\mathbf{J}\setminus\{\mathbf{j}\}}(x)\right)$, then a word $\mathbf{c}(x) = (c_1(x), c_2(x), \ldots, c_n(x))$, where*

$$c_j(x) = \begin{cases} \Delta_j(x), & j \in J, \\ 0, & \textit{otherwise.} \end{cases}$$

is a codeword of $\mathcal{C}$.

Proof. Let us show that $\mathbf{s}(x) = \mathbf{H}(x)\mathbf{c}^T(x) = \mathbf{0}$ in the ring $\mathbb{F}_2^{(s)}[x]$. We only give the proof for the first element of the syndrome:

$$s_1(x) = \sum_{j=1}^{n} p_{1,j}(x)c_j(x) = \sum_{j \in J} p_{1,j}(x)\Delta_j(x).$$

Let $J = \{j_1, j_2, \ldots, j_{m+1}\}$. Note, that

$$s_1(x) = \det \left[\begin{array}{cccc} p_{1,j_1}(x) & p_{1,j_2}(x) & \cdots & p_{1,j_{m+1}}(x) \\ \hline p_{1,j_1}(x) & p_{1,j_2}(x) & \cdots & p_{1,j_{m+1}}(x) \\ p_{2,j_1}(x) & p_{2,j_2}(x) & \cdots & p_{2,j_{m+1}}(x) \\ \vdots & \vdots & \ddots & \vdots \\ p_{m,j_1}(x) & p_{m,j_2}(x) & \cdots & p_{m,j_{m+1}}(x) \end{array} \right] = 0,$$

as the matrix contains two identical rows. Analogously one can carry out the proof for the rest elements of the syndrome. □

We need to introduce a notation $\overline{l}(t_1, t_2)$. Let us arrange the columns of the matrix $\mathbf{H}^{(W)}$ in ascending order of their weights (i.e. the first columns are of small weight, the last ones are of large weight). In what follows we assume the columns of the matrix $\mathbf{H}^{(W)}$ to be in this order. Let l_j be a weight of the j-th column of $\mathbf{H}^{(W)}$, $t_2 > t_1$, then

$$\overline{l}(t_1, t_2) = \frac{1}{t_2 - t_1 + 1} \sum_{i=t_1}^{t_2} l_i.$$

Let $l_{\max}$ and $l_{\min}$ be accordingly maximum and minimum column weights in $\mathbf{H}^{(W)}$ (in our case $l_{\max} = l_n$ and $l_{\min} = l_1$).

Theorem 2. *Let $\mathcal{C}$ be a type-1 QC LDPC code with the weight matrix $\mathbf{H}^{(W)}$ of size $m \times n$, let k be an integer, such that $0 \leq k \leq m$ and let $\ell = \overline{l}(2, m+1-k)$ then*

$$D(\mathcal{C}) \leq (m+1)k!\ell^{m-k}. \tag{2}$$

Proof. Recall that the columns of the matrix $\mathbf{H}^{(W)}$ are in ascending order of their weights. Let $J = \{1, 2, \ldots, m+1\}$. Let us construct a codeword $\mathbf{c}(x)$ in accordance to Lemma 1. The last $n - |J|$ positions $\mathbf{c}(x)$ are equal to zero.

Consider $\Delta_1(x)$. Note, that

$$||\Delta_1(x)|| \leq \prod_{i=1}^{m} \min\{i, l_{m+2-i}\} \leq k! \prod_{j=2}^{m+1-k} l_j, \tag{3}$$

where l_j is a weight of the j-th column in $\mathbf{H}_J^{(W)}$. This inequality follows from the fact that the sum for $\Delta_1(x)$ contains at most $k! \prod_{j=2}^{m+1-k} l_j$ terms. Each of this terms is a monomial. Since

$$\prod_{j=2}^{m+1-k} l_j \leq \ell^{m-k},$$

then

$$||\Delta_1(x)|| \leq k!\ell^{m-k}.$$

Similar inequalities hold for all the $\Delta_j(x)$, $j \in J$. As there are at most $m+1$ non-zero positions in a codeword $\mathbf{c}(x)$, then

$$||\mathbf{c}(x)|| \leq (m+1)k!\ell^{m-k}.$$

We should also consider the case when all $\Delta_j(x) = 0 \quad \forall j \in J$. In this case Lemma 1 gives a zero codeword. We proceed as follows. We find a non-zero minor of the maximal order r, $r < m$ in the matrix $\mathbf{H}_J(x)$. Let I be a set of row numbers, S be a set of column numbers, such that $\mathbf{H}_{I,S}(x)$ is the minor. Let $S' = S \cup j$, $j \in J \backslash S$. Consider the submatrix $\mathbf{H}_{I,S'}(x)$. We construct a codeword for this submatrix in accordance to Lemma 1. Note, that this word contains al least one non-zero position. After appending this word with zeros on positions $\{1, 2 \ldots, n\} \backslash S'$, we obtain a codeword for the matrix $\mathbf{H}(x)$, as all the minors of bigger order are equal to zero. In this case we have

$$D(\mathcal{C}) \leq (r+1)k!\ell^{m-k} < (m+1)k!\ell^{m-k},$$

this completes the proof. □

Corollary 1. *Recall, that k can be chosen arbitrarily ($0 \leq k \leq m$), but the best estimate can be obtained if k is the largest integer for which the inequality $l_{m+2-k} \geq k$ is satisfied.*

Proof. To prove this fact just look at (3). □

Remark 2. *Note that the bound is better for regular codes. In this case we have (let ℓ be the column weight, it is easy to check, that $k = \ell$)*

$$D(\mathcal{C}) \leq (m+1)\ell!\ell^{m-\ell}.$$

If the base matrix is the all one matrix ($\ell = m$), we obtain the bound from [2].

Remark 3. *Note that the estimate* (2) *does not depend on s. If m and n are fixed and $s \to \infty$, then in accordance to the estimate* (2) *$D(\mathcal{C})$ is upper bounded by a constant. We also note, that in* [6] *it is proved that there exist protograph-based LDPC codes with the following properties: the minimum distance of such codes grows linearly with the code length while the sizes of the base matrix (m and n) are fixed.*

Corollary 2. *Thus, for the minimum code distance $D(\mathcal{C})$ to grow linearly with the code length $N = ns$ it is necessary, that the estimates* (1) *and* (2) *grow linearly with N.*

References

[1] M. P. C. Fossorier. Quasi-cyclic low-density parity-check codes from circulant permutation matrices. *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1793, Aug. 2004.

[2] D. J. C. MacKay and M. C. Davey. Evaluation of Gallager codes for short block length and high rate applications. in *Codes, Systems, and Graphical Models (Minneapolis, MN, 1999), B. Marcus and J. Rosenthal, Eds.* New York: Springer-Verlag, 2001, pp. 113–130.

[3] R. G. Gallager. *Low-Density Parity-Check Codes.* Cambridge, MA: M.I.T. Press, 1963.

[4] J. Thorpe. Low-density parity-check (LDPC) codes constructed from protographs. JPL, IPN Progress Rep., Aug. 2003, vol. 42–154.

[5] R. Smarandache, P. O. Vontobel. Quasi-Cyclic LDPC Codes: Influence of Proto- and Tanner-Graph Structure on Minimum Hamming Distance Upper Bounds. *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 585–607, Feb. 2012.

[6] A. Sridharan, M. Lentmaier, D. V. Trukhachev, D. J. Costello, K. Sh. Zigangirov. On the Minimum Distance of Low-Density Parity-Check Codes with Parity-Check Matrices Constructed from Permutation Matrices. *Problems Inf. Transm.*, vol. 41, no. 1, pp. 39–52, 2005.