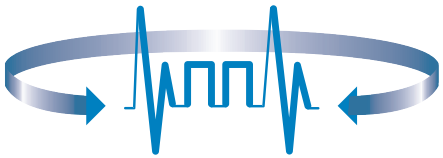
Upper Bounds on the Minimum Distance of Quasi-Cyclic LDPC codes

Alexey Frolov

Email: alexey.frolov@iitp.ru



Inst. for Information Transmission Problems
Russian Academy of Sciences

ACCT 2014
September 7–13, 2014
Svetlogorsk, Russia

Outline

Task statement

In

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.

an upper bound on the minimum distance of QC LDPC codes is derived for the case when the weight matrix has all the elements equal to one. In this case the minimum code distance is upper bounded by a quantity $(m+1)!$.

Our task is to extend the bound for the case of type-1 QC LDPC codes.

Weight matrix

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.

QC LDPC codes

For this purpose we extend the matrix $\mathbf{H}^{(W)}$ with circulant matrices (circulants) as follows:

$$\mathbf{H} = \begin{bmatrix} \mathbf{P}_{1,1} & \mathbf{P}_{1,2} & \cdots & \mathbf{P}_{1,n} \\ \mathbf{P}_{2,1} & \mathbf{P}_{2,2} & \cdots & \mathbf{P}_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{P}_{m,1} & \mathbf{P}_{m,2} & \cdots & \mathbf{P}_{m,n} \end{bmatrix},$$

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 $h_{i,j}$, $i = 1, \ldots, m$; $j = 1, \ldots, n$.

Parameters of $\mathcal{C}$:

$$N(\mathcal{C}) = ns,$$

and

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

Remark

It is easy to see that the obtained code is in fact quasi-cyclic. Consider the codeword $\mathbf{c} \in \mathcal{C}$. Let us split the codeword into n subblocks in accordance to the structure of the parity-check matrix $\mathbf{H}$:

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

then note that if we apply the same cyclic shifts in each subblock we again obtain a codeword of $\mathcal{C}$.

Example

Let us lift the weight matrix

$$\mathbf{H}^{(W)} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

E.g. we have

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

Type-w QC LDPC code

QC LDPC code is called type-w QC LDPC code if

$$\max_{1 \le i \le m, 1 \le j \le m} h_{i,j} = w.$$

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 $\mathbb{F}_2$.

The first upper bound

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

Theorem

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

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

Sketch of the proof

$$\mathbf{H}^{(W)} = \left[\begin{array}{ccc} 1 & 1 & 1 \\ 1 & 0 & 1 \end{array}\right]$$

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

Polynomial parity-check matrix

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

Matrices

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

correspond to the parity-check matrix

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

Polynomial notation

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

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

is equivalent to

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

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 $\mathbf{A}_J$.

The way how to construct low-weight codewords

Lemma

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 $\mathcal{C}$.

Example

$$\begin{array}{cccc} ? & ? & ? & ? \\ 0 & x^2 & x & x^2 \\ 1 & 0 & x^2 & x \end{array}$$

Example

$$\begin{array}{cccc} ? & ? & ? & 0 \\ 0 & x^2 & x & x^2 \\ 1 & 0 & x^2 & x \end{array}$$

Example

$$\begin{array}{cccc} x^4 & ? & ? & 0 \\ 0 & x^2 & x & x^2 \\ 1 & 0 & x^2 & x \end{array}$$

Example

$$\begin{array}{cccc} x^4 & x & ? & 0 \\ 0 & x^2 & x & x^2 \\ 1 & 0 & x^2 & x \end{array}$$

Example

$$\begin{matrix} x^4 & x & x^2 & 0 \\ 0 & x^2 & x & x^2 \\ 1 & 0 & x^2 & x \end{matrix}$$

The second upper bound

Let us arrange the columns of the matrix $\mathbf{H}^{(W)}$ in ascending order of their weights. Let l_j be a weight of the j-th column of $\mathbf{H}^{(W)}$, $t_2 > t_1$, then

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

Theorem

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 $\ell = \bar{l}(2, m+1-k)$ then

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

Remarks

Corollary

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.

Remark (Regular case)

In the regular case we have (let ℓ be the column weight, it is easy to check, that $k = \ell$)

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

Conclusion

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

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

Thank you for the attention!