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

Fedor Ivanov

Email: fii@iitp.ru

Institute for Information Transmission Problems,
Russian Academy of Science

XV International Workshop on Algebraic and Combinatorial Coding Theory (ACCT)
18-24 June, 2016
Albena, Bulgaria

Outline

- Definitions and notation
- Circulant matrices
- Auxiliary statements
- Code structure
- Lower bound on the minimum distance of proposed codes
- Simulation and numerical results
- Conclusion

Definitions and notation - I

Notation

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* $d_{min} = n_0$*.*

Definitions and notation - I

Notation

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

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

Definitions and notation - I

Notation

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

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

Notation

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

Definitions and notation - II

Notation

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

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

Definitions and notation - II

Notation

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

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

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

Circulant matrices

Definition

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 $\mathbf{I}$.

Circulant matrices

Definition

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 $\mathbf{I}$.

Matrix $\mathbf{I}_p$ is an circulant with column and row weights 1. Also it is evident that $\mathbf{I}_{mk} = \mathbf{I}$ for all $k \in \mathbb{Z}$.

Circulant matrices

Definition

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 $\mathbf{I}$.

Matrix $\mathbf{I}_p$ is an circulant with column and row weights 1. Also it is evident that $\mathbf{I}_{mk} = \mathbf{I}$ for all $k \in \mathbb{Z}$. Moreover:

$$\mathbf{I}_{p_1} \cdot \mathbf{I}_{p_2} = \mathbf{I}_{p_1+p_2 \mod m},$$

$$\mathbf{I}_p^t = \mathbf{I}_{tp_1 \mod m},$$

in particular if $p_1 \in \mathbb{N}$, $0 \leq p_1 \leq m$, then

$$\mathbf{I}_{p_1}^{-1} = \mathbf{I}_{m-p_1}.$$

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 $\mathbf{I}_1$.

Auxiliary statements

If

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

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

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

Auxiliary statements

If

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

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

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

Lemma

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 $pw \equiv 0 \mod m$.

Auxiliary statements

If

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

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

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

Lemma

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 $pw \equiv 0 \mod m$.

Corollary

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 $w = 0$.

Code structure - I

Let us consider a parity-check matrix of $\mathbf{H}_b$ of $\mathcal{R}(n_0)$:

$$\mathbf{H}_b = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

Code structure - I

Let us consider a parity-check matrix of $\mathbf{H}_b$ of $\mathcal{R}(n_0)$:

$$\mathbf{H}_b = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

Choose:

- $m > 1$, $m \in \mathbb{N}$

Code structure - I

Let us consider a parity-check matrix of $\mathbf{H}_b$ of $\mathcal{R}(n_0)$:

$$\mathbf{H}_b = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

Choose:

- $m > 1,\ m \in \mathbb{N}$
- $k_0 > 0,\ k_0 \in \mathbb{N}$

Code structure - I

Let us consider a parity-check matrix of $\mathbf{H}_b$ of $\mathcal{R}(n_0)$:

$$\mathbf{H}_b = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

Choose:

- $m > 1,\ m \in \mathbb{N}$
- $k_0 > 0,\ k_0 \in \mathbb{N}$
- $2(n_0 - 1)k^2$ arbitraty matrices $\mathbf{I}_{p_j}$, $p_j \in \mathbb{N}$, $j = 1..2(n_0 - 1)k_0^2$ from $\mathcal{I}_m$

Code structure - II

$$1 \rightarrow \begin{array}{|c|c|c|}\hline \mathbf{P}_{11} & \cdots & \mathbf{P}_{1k_0} \\ \hline \cdots & \ddots & \cdots \\ \hline \mathbf{P}_{k_0 1} & \cdots & \mathbf{P}_{k_0 k_0} \\ \hline \end{array} = \mathbf{Q}_i$$

Code structure - II

$$1 \rightarrow \begin{array}{|c|c|c|} \hline \mathbf{P}_{11} & \cdots & \mathbf{P}_{1k_0} \\ \hline \cdots & \ddots & \cdots \\ \hline \mathbf{P}_{k_0 1} & \cdots & \mathbf{P}_{k_0 k_0} \\ \hline \end{array} = \mathbf{Q}_i$$

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

Code Structure - III

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

Code Structure - III

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

- Size of **H** is $mk_0(n_0 - 1) \times mkn_0$

Code Structure - III

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

- Size of $\mathbf{H}$ is $mk_0(n_0 - 1) \times mkn_0$
- All rows have weight $2k_0$

Code Structure - III

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

- Size of $\mathbf{H}$ is $mk_0(n_0-1) \times mkn_0$
- All rows have weight $2k_0$
- Weights of first mk_0 columns are $k_0(n_0-1)$, other columns have weight k_0

Code Structure - IV

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 $\mathcal{E}_{RC}(m, k_0, n_0)$.

Code Structure - IV

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

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.

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

Lemma

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 $\mathbf{c} \in \mathcal{C}$: $||\mathbf{c}||$ is even.

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

Lemma

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 $\mathbf{c} \in \mathcal{C}$: $||\mathbf{c}||$ is even.

Lemma

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 $d_{min}(\mathcal{C}) \geq 4$.

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

Lemma

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 $\mathbf{c} \in \mathcal{C}$: $||\mathbf{c}||$ is even.

Lemma

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 $d_{min}(\mathcal{C}) \geq 4$.

Lemma

Let $\mathbf{H}$ is the parity-check matrix of code $\mathcal{C}$ from $\mathcal{E}_{RC}(m, 2, n_0)$. If this matrix is free of cycles of length 4 and $m > 5$ is prime number, then $d_{min}(\mathcal{C}) \geq 8$.

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

Theorem

Let $\mathbf{H}$ *is the parity-check matrix of code* $\mathcal{C}$ *from* $\mathcal{E}_{RC}(m, 2, k_0)$*, and, moreover, let at least one sub-matrix* $(\mathbf{Q}_i\ \mathbf{Q}_{n_0+i-1})$ *of* $\mathbf{H}$ $(i = 1..n_0 - 1)$ *is free of cycles of length* 8*, then* $d_{min}(\mathcal{C}) \geq 10$*.*

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

Theorem

Let $\mathbf{H}$ is the parity-check matrix of code $\mathcal{C}$ from $\mathcal{E}_{RC}(m, 2, k_0)$, and, moreover, let at least one sub-matrix $(\mathbf{Q}_i\ \mathbf{Q}_{n_0+i-1})$ of $\mathbf{H}$ $(i = 1..n_0 - 1)$ is free of cycles of length 8, then $d_{min}(\mathcal{C}) \geq 10$.

Corollary

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 $d_{min}(\mathcal{C}) \geq 10$.

Simulation Results - Setup

- AWGN channel

Simulation Results - Setup

- AWGN channel
- BPSK modulation

Simulation Results - Setup

- AWGN channel
- BPSK modulation
- Sum-Product decoding algorithm

Simulation Results - Setup

- AWGN channel
- BPSK modulation
- Sum-Product decoding algorithm
- 50 iterations

Simulation Results - Setup

- AWGN channel
- BPSK modulation
- Sum-Product decoding algorithm
- 50 iterations

Simulation Results - Setup

- AWGN channel
- BPSK modulation
- Sum-Product decoding algorithm
- 50 iterations

Table: 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
181	4	2	1448	0.2521	≥ 10

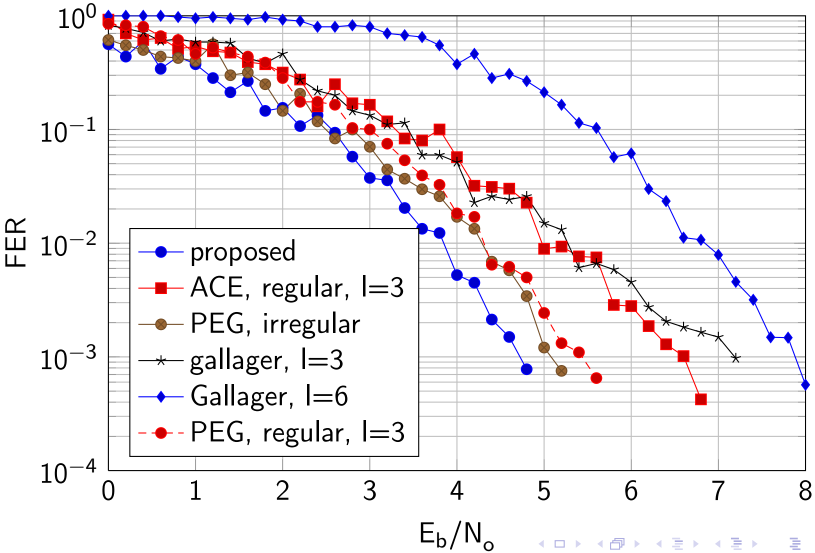
Numerical results for $n = 56$

EbNo	-1	0	1	2	3	4
P_b, error rate	0.26	0.24	0.21	0.19	0.16	0.13
N_{err}, proposed	11.00	10.95	10.48	9.70	8.60	7.28
$D(N_{err})$, proposed	4.95	5.15	5.53	5.96	6.43	5.97
N_{err}, PEG	10.54	10.44	9.97	9.29	8.36	7.20
N_{err}, ACE	10.14	9.98	9.45	8.61	7.41	6.04

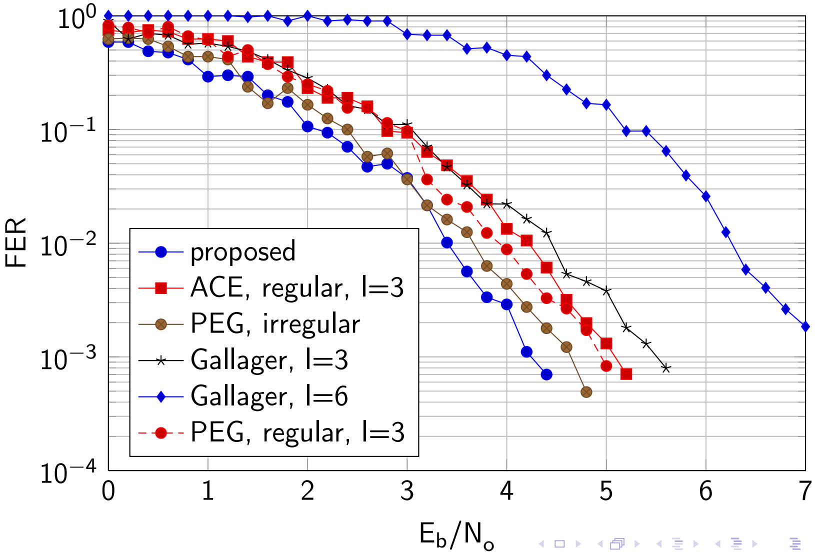
Numerical results for $n = 88$

EbNo	-1	0	1	2	3	4
P_b, error rate	0.26	0.24	0.21	0.19	0.16	0.13
N_{err}, proposed	18.01	17.82	17.02	15.70	13.78	11.53
$D(N_{err})$, proposed	8.72	8.25	9.35	10.25	10.79	9.90
N_{err}, PEG	16.04	16.50	15.97	15.19	13.58	11.43
N_{err}, ACE	17.26	16.79	15.91	14.47	12.49	10.20

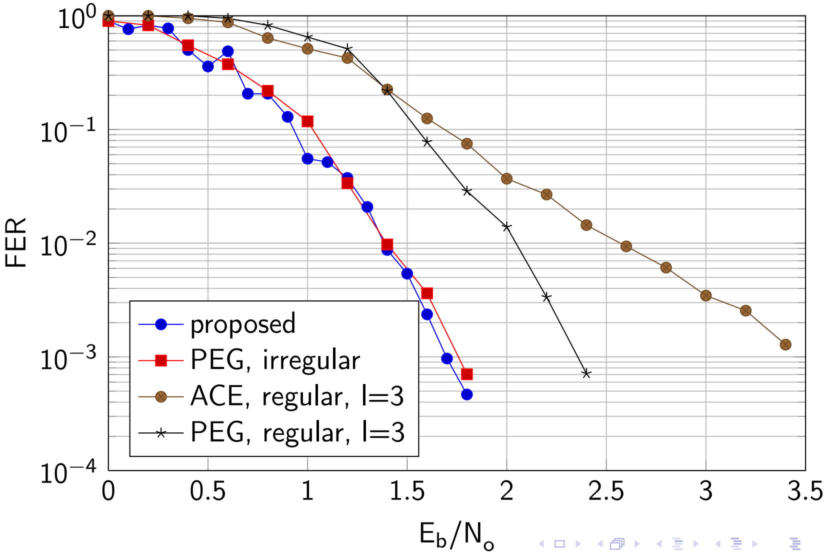
Simulation Results, FER versus E_b/N_o $n = 56$



Simulation Results, FER versus E_b/N_o $n = 88$



Simulation Results, FER versus E_b/N_o $n = 1448$



Conclusion

1. New ensemble of low-rate LDPC codes was suggested

Conclusion

1. New ensemble of low-rate LDPC codes was suggested
2. A lower bound on minimal distance of proposed codes was obtained

Conclusion

1. New ensemble of low-rate LDPC codes was suggested
2. A lower bound on minimal distance of proposed codes was obtained
3. Simulation and numerical results allow us to conclude that proposed codes have an excellent performance even for very small code lengths

Thank you for your attention!