Low-Density Parity-Check Codes Based on Steiner Quadruple Systems and Permutation Matrices

Fedor Ivanov, Victor Zyablov

Email: fii@iitp.ru, zyablov@iitp.ru

Institute for Information Transmission Problems,
Russian Academy of Science

XIV International Workshop on "Algebraic and Combinatorial Coding Theory"
07-13 September, 2014
Svetlogorsk, Russia

Outline

- Short Introduction
- Main definitions and notation
- LDPC codes based on $SQS(2^m - 1)$ and permutation matrices
- Some properties of LDPC codes based on $SQS(2^m - 1)$ and permutation matrices
- Construction of LDPC codes based on $SQS(2^m - 1)$ and permutation matrices with $d \geq 6$
- Simulation results

Introduction

- Random Gallager codes (1960)
- LDPC codes based on permutation matrices (quasi-cyclic codes)
- LDPC codes based on combinatorial structures ($STS(v)$, latin squares, finite geometries)
- LDPC codes based on Steiner triple systems and permutation matrices (Ivanov, Zyablov, 2013)

Main definitions and notation

Definition

Steiner system $S(v,k,t)$ is the pare (X,B), where X is a set of v elements, and B is a class of k-subsets of X (called blocks), since any t-subset of X is included in exactly one of blocks of class B. System $S(v,4,2)$ we will call Steiner quadruple system.

- A system $S(v,4,2)$ is denoted by $SQS(v)$.
- Under $\mathcal{H}(m)$ we will imply binary $[2^m-1, 2^m-m-1, 3]$ Hamming code.

LDPC codes based on $SQS(2^m - 1)$ and permutation matrices - base matrix

$$\mathbf{H}_f = [c_1(x)c_2(x)\ldots c_N(x)]$$

- $N = A(3, 2^m - 1) = \frac{(2^m-1)(2^m-2)}{6}$
- $c_i(x)$, $1 \leq i \leq N$ – weight-3 codeword of $\mathcal{H}(m)$

$$\mathbf{H}^+ = [h_1(x)h_2(x)\ldots h_{N_1}(x)],$$

- $h_r(x) = c_i(x) + c_j(x)\, mod\, 2 : (c_i(x), c_j(x)) = 1,\ 1 \leq i < j \leq N$
- $N_1 = (2^m - 1)(2^{m-1} - 1)(2^{m-2} - 1)$

LDPC codes based on $SQS(2^m-1)$ and permutation matrices - 4-cycles elimination

1. Represent the matrix $\mathbf{H}^+$ in the following form:

$$\mathbf{H}^+ = \begin{pmatrix} v_1(x) \\ v_2(x) \\ \dots \\ v_{2^m-1}(x) \end{pmatrix},$$

where $s_j(x) = (s_{j_1}, s_{j_2}, \dots, s_{j_{N_1}})$ is the vector of the length N_1 over $GF(2)$.

2. Calculate all elementvise products $< s_i(x), s_j(x) >$ for all $1 \leq i < j \leq 2^m - 1$:

$$s_{ij} =< s_i(x), s_j(x) >= (s_{ij}^{(1)}, s_{ij}^{(2)}, \dots, s_{ij}^{(N_1)}),$$

where

$$s_{ij}^{(k)} = s_{i_k} s_{j_k}, \ 1 \leq k \leq N_1.$$

3. Associate vector s_{ij} with the set

$$\tilde{S_{ij}} = \{k : s_{ij}^{(k)} = 1\} = \{\tilde{s}_1, \tilde{s}_2, \dots, \tilde{s}_v\}, \ v = |\tilde{S_{ij}}|.$$

4. Set to zero all columns $h_{\tilde{s}_2}$, $h_{\tilde{s}_3}$, ..., $h_{\tilde{s}_v}$ of the $\mathbf{H}^+$.
5. Exclude all zero columns from the $\mathbf{H}^+$. Denote the obtained matrix by $\tilde{\mathbf{H}}_4$.

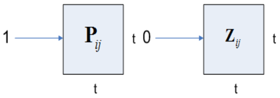
LDPC codes based on $SQS(2^m - 1)$ and permutation matrices - lifted matrix

The matrix $\tilde{\mathbf{H}}_4$ has the size $(2^m - 1) \times N_2$.

$$\{Set\, of\, columns\, of\, \tilde{\mathbf{H}}_4\} \subset S(2^m, 4, 2)$$

.

m	$N = A(3, 2^m - 1)$	N_2
5	155	44
6	651	214
7	2667	970
8	10795	4120



Choose an arbitrary natural number K such that $2^m - 1 < K \leq N_2$. Form a matrix $\mathbf{H}_4$ by choosing an arbitrary K-element, $2^m - 1 < K \leq N_2$ ordered subset of the set of the columns of the matrix $\tilde{\mathbf{H}}_4$. The matrix $\mathbf{H}_4$ thus obtained is of size $t(2^m - 1) \times N_2 t$, the column weight is 4.

LDPC codes based on $SQS(2^m - 1)$ and permutation matrices - ensemble definition

By choosing an arbitrary numbers $m > 4$, $2^m - 1 < K \leq N_2$ and choosing random $t \times t$ permutation matrices, $t > 1$, we define an ensemble of irregular low-density parity-check codes of length $n = Kt$. We denote the obtained ensemble by $\mathcal{E}_{SQS}(m, K, t)$.

Definition

An arbitrary code $\mathcal{C} \in \mathcal{E}_{SQS}(m, K, t)$ will be called a low-density parity-check code based on permutation matrices and $SQS(2^m - 1)$.

Some properties of LDPC codes based on $SQS(2^m - 1)$ and permutation matrices - rate

Theorem

Let R_{SQS} be the rate of a code $\mathcal{C} \in \mathcal{E}_{SQS}(m, K, t)$, then

$$\frac{1}{2^m} \leq R_{SQS} < 1 - \frac{6}{2^{m-1} - 1}.$$

m	R_{SQS}^{upper}	R_{SQS}
5	0.6	0.2955
6	0.8065	0.7056
7	0.9048	0.8691
8	0.9528	0.9381

- R_{SQS} - the maximal achievable rate for codes in the $\mathcal{E}_{SQS}(m, K, t)$
- R_{SQS}^{upper} - the upper bound for R_{SQS}

Some properties of LDPC codes based on $SQS(2^m - 1)$ and permutation matrices - girth and minimum distance

Theorem

Let g *is a girth of parity-check matrix* $\mathbf{H}_4$ *of code* $\mathcal{C} \in \mathcal{E}_{SQS}(m, K, t)$, *then*

$$g \geq 6.$$

Theorem

Let $d_{\min}$ *be a minimum distance of an LDPC code* $\mathcal{C} \in \mathcal{E}_{SQS}(m, K, t)$, *then*

$$5 \leq d_{\min} \leq 5t.$$

Some properties of LDPC codes based on $SQS(2^m - 1)$ and permutation matrices: minimum distance increasing - main theorem

Theorem

Let the minimum distance $\widetilde{d}$ of a code with parity-check matrix $\tilde{\mathbf{H}}_4$ is 5. Extend $\tilde{\mathbf{H}}_4$ to a matrix $\mathbf{H}_4$ by employing a permutation matrices. Then, if at least one cycle of length 6 is transformed into a cycle of greater length in every combination of five linearly dependent columns of $\tilde{\mathbf{H}}_4$, then the minimum distance of the code with parity-check matrix $\mathbf{H}$ is at least 6.

Construction of LDPC codes based on $SQS(2^m - 1)$ and permutation matrices with $d \geq 6$

$$\mathbf{B} = \begin{pmatrix} 0 & a_0 & 2a_0 & \dots & (n_0-1)a_0 \\ 0 & a_1 & 2a_1 & \dots & (n_0-1)a_1 \\ \multicolumn{5}{c}{\dotfill} \\ 0 & a_{l-1} & 2a_{l-1} & \dots & (n_0-1)a_{l-1} \end{pmatrix},$$

where $0 \leq a_0 < a_1 < a_2 < \ldots < a_{l-1}$ is a sequence of natural numbers.

Construction of LDPC codes based on $SQS(2^m - 1)$ and permutation matrices with $d \geq 6$

Theorem

If in the matrix $\mathbf{B}$ every $b_{ij} = (j-1)a_{i-1}$ is replaced by the matrix of b_{ij} multiple cyclic shift of columns of identity matrix $\mathbf{I}$ with size $t \times t$, and the following condition is performed for any ordered triple $\{a_i, a_j, a_k\}$, $i < j < k$, of the sequence $\{a_0, a_1, \ldots, a_{l-1}\}$

$$\frac{a_k - a_i}{(a_k - a_i, a_j - a_i)} \geq n_0,$$

where $(\cdot\,,\cdot)$ is a greatest common divisor, then the matrix

$$\widetilde{\mathbf{B}} = \begin{pmatrix} \mathbf{I} & \mathbf{I_{a_0}} & \mathbf{I_{2a_0}} & \cdots & \mathbf{I_{(n_0-1)a_0}} \\ \mathbf{I} & \mathbf{I_{a_1}} & \mathbf{I_{2a_1}} & \cdots & \mathbf{I_{(n_0-1)a_1}} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \mathbf{I} & \mathbf{I_{a_{l-1}}} & \mathbf{I_{2a_{l-1}}} & \cdots & \mathbf{I_{(n_0-1)a_{l-1}}} \end{pmatrix}$$

does not contain any cycle of length 6 for any value of parameter

$$t \geq (a_{l-1} - a_0)(n_0 - 1) + 1.$$

Construction of LDPC codes based on $SQS(2^m - 1)$ and permutation matrices with $d \geq 6$

Consider $\{0, 1, n_0, n_0^2, \ldots, n_0^{l-2}\}$.

Lemma

The following inequality is held for any ordered triple $\{n_0^x, n_0^y, n_0^z\}$ *when* $0 \leq x < y < z \leq l-2$

$$\frac{n_0^z - n_0^x}{(n_0^z - n_0^x, n_0^y - n_0^x)} \geq n_0.$$

Construction of LDPC codes based on $SQS(2^m - 1)$ and permutation matrices with $d \geq 6$

Theorem

The matrix

$$\widehat{\mathbf{B}} = \begin{pmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I} & \dots & \mathbf{I} \\ \mathbf{I} & \mathbf{I_1} & \mathbf{I_2} & \dots & \mathbf{I_{n_0-1}} \\ \hdotsfor{5} \\ \mathbf{I} & \mathbf{I_{{n_0}^{l-2}}} & \mathbf{I_{2{n_0}^{l-2}}} & \dots & \mathbf{I_{(n_0-1){n_0}^{l-2}}} \end{pmatrix}$$

does not contain any cycle of length 6 *for any value of the parameter* $t \geq n_0^{l-2}(n_0 - 1) + 1$, *where* t *is the size of identity matrix* $\mathbf{I}$.

Thus, choosing four parameters l, n_0, m, k so that the following system of inequalities is held

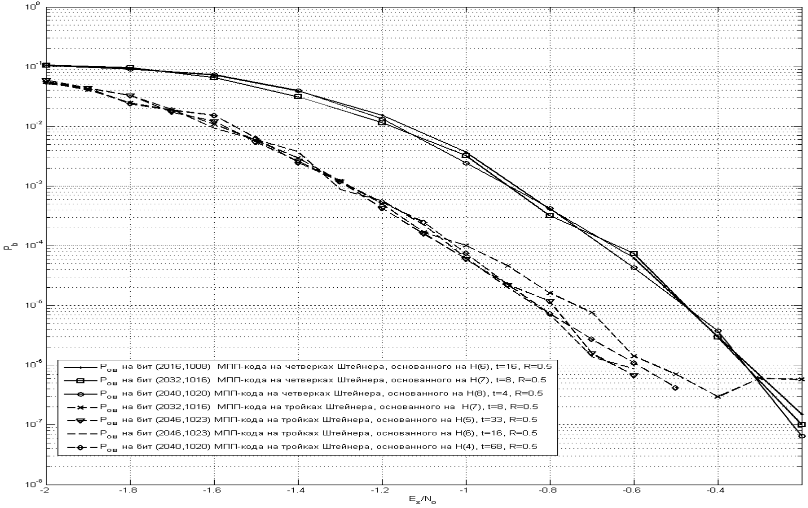
$$\begin{cases} t \geq n_0^{l-2}(n_0 - 1) + 1, \\ ln_0 \geq 4K, \end{cases}$$

one can construct the parity-check matrix $\mathbf{H}$ of LDPC code based on $SQS(2^m - 1)$ and permutation matrices with length $n = Kt$ and minimum distance $d \geq 6$. It is sufficient to select the unique circulants which are formed the matrix $\widehat{\mathbf{B}}$ as the permutation matrices.

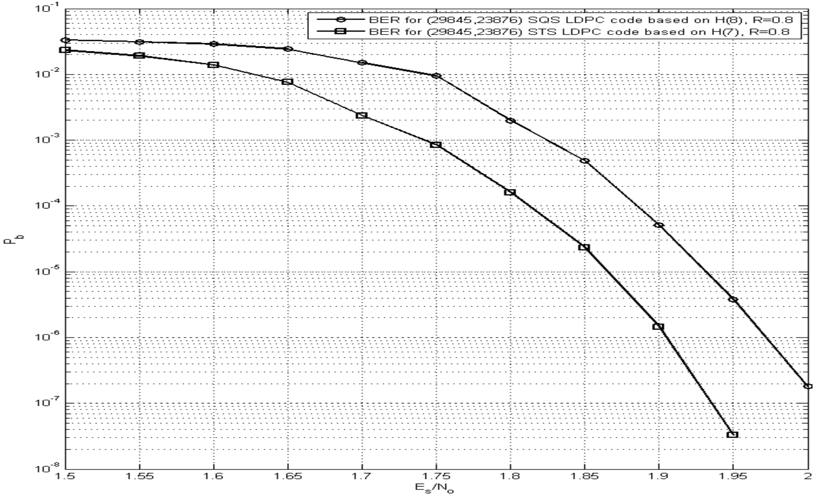
Simulation setup

- AWGN channel
- BPSK modulation
- Sum-Product decoding algorithm
- Soft input
- Maximal number of iterations - 50

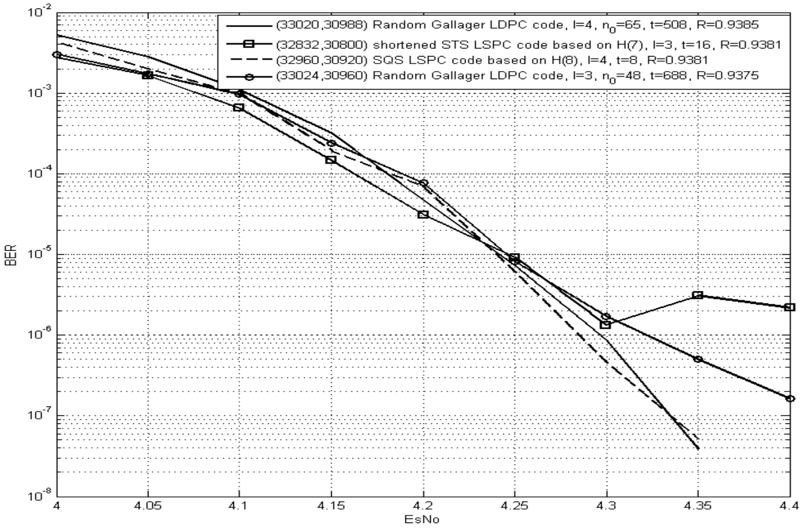
Simulation results - $R = 0.5,\ N \approx 2000$



Simulation results - $R = 0.8,\ N \approx 30000$



Simulation results - $R \approx 0.938$, $N \approx 33000$



Conclusion

1. New ensemble of structured LDPC codes is presented
2. Some properties of proposed codes are obtained
3. Some conditions that guarantee strict increasing in minimum distance are received.

Thank you for the attention!