Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 175–180*

LDPC codes based on Steiner quadruple systems and permutation matrices

Fedor Ivanov fii@iitp.ru
Victor Zyablov zyablov@iitp.ru
IITP RAS

Abstract. An algorithm for generating parity-check matrices of high-rate low-density parity-check codes based on permutation matrices and Steiner system $S(v, 4, 2)$ is proposed. The estimations of rate, minimum distance and girth for derived code constructions are presented. The results of simulation of obtained code constructions for an iterative "belief propagation" (Sum-Product) decoding algorithm, applied in the case of transmission of a code word via a binary channel with an additive Gaussian white noise and BPSK modulation, are presented.

1 Introduction

Low-density parity-check codes (LDPC-codes) were proposed by Gallager in [1]. There are linear block codes defined by their parity-check matrices $\mathbf{H}$ characterized by a relatively small number of ones in their rows and columns.

An important characteristic of an LDPC code is absence of cycles of certain length. A cycle of length 4 (4-cycle) can be understood as a rectangle in the parity-check matrix whose vertices are ones.

Apart from random LDPC codes, various algebraic constructions of low-density parity-check codes based on permutation matrices [2]- [3], projective geometries [4], and other combinatorial constructions [5, 6] are often used in practice.

The main objective of this work is to construct and explore properties of an ensemble of low-density parity-check codes based on two algebraic constructions simultaneously: Steiner system $S(v, 4, 2)$ and permutation matrices.

2 Main definitions and notation

Definition 1. *A Steiner system $S(v, k, t)$ is a pair (X, B), where X is a set of v elements, and B is a class of k-subsets of X (called blocks) so that any t-subset of X is contained in exactly one of blocks of the class B. System $S(v, 3, 2)$ is named Steiner triple system.*

We will use the following notation:

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

It is commonly known that weight-3 codewords of $\mathcal{H}(m)$ form a system $STS(2^m-1)$.

3 LDPC codes based on $S(v,4,2)$ and permutation matrices

Consider the matrix $\mathbf{H}_f$ consisted of all $A(3,2^m-1)$ weight-3 codewords of $\mathcal{H}(m)$:

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

where $N = A(3,2^m-1) = \frac{(2^m-1)(2^m-2)}{6}$ and $c_i(x)$, $1 \le i \le N$ is a weight-3 codeword of $\mathcal{H}(m)$. Thus, $\mathbf{H}_f$ is of size $(2^m-1)\times N$. Form the matrix $\mathbf{H}^+$ from the matrix $\mathbf{H}_f$ as following:

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

where $h_r(x) = c_i(x) + c_j(x) \,mod\, 2 : (c_i(x), c_j(x)) = 1$, $(c_i(x), c_j(x))$ is the scalar product of the polynomials $c_i(x)$ and $c_j(x)$, $1 \le i < j \le N$, $1 \le r \le N_1$, $N_1 = (2^m-1)(2^{m-1}-1)(2^{m-2}-1)$. I. e. $\mathbf{H}^+$ is consisted of all modulo 2 sums of such weight-3 codewords $c_i(x)$ and $c_j(x)$ as they have one common unity. Now we delete all 4-cycles from the $\mathbf{H}^+$ in accordance with the following rule:

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 $1 \le i < j \le 2^m-1$:

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

   where

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

3. Associate vector s_{ij} with the set

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

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 $\tilde{\mathbf{H}}_4$. The matrix $\tilde{\mathbf{H}}_4$ has the size $(2^m - 1) \times N_2$. It is obvious that the columns of $\tilde{\mathbf{H}}_4$ form a subset of $SQS(2^m)$ There are some values of N_2 depending on m in the table.

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

The size of $\tilde{\mathbf{H}}_4$ can be made a multiple of N_2 by replacing each of the ones with an arbitrary $t \times t$ permutation matrix $\mathbf{P}_{ij}$ and each of the zeros with the zero $(t \times t)$ matrix $\mathbf{Z}_{ij}$. Denote the result of this transformation of $\tilde{\mathbf{H}}_4$ by $\hat{\mathbf{H}}_4$; then $\hat{\mathbf{H}}_4$ is a low-density $t(2^m - 1) \times N_2 t$ matrix with each column having weight 4.

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 if of size $t(2^m - 1) \times N_2 t$, the column weight is 4.

Thus, 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 $n = N_2 t$. We denote the obtained ensemble by $\mathcal{E}_{SQS}(m, K, t)$.

Definition 2. *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 $SQS(2^m - 1)$.*

4 Some properties of LDPC codes from the $\mathcal{E}_{SQS}(m, K, t)$ ensemble

Now let us formulate some properties of codes in the $\mathcal{E}_{SQS}(m, K, t)$ ensemble. We initially obtain an upper and lower bounds for the rate of codes in the $\mathcal{E}_{SQS}(m, K, t)$ ensemble.

Theorem 1. *Let R_{SQS} be the rate of a code $\mathcal{C} \in \mathcal{E}_{SQS}(m, K, t)$, then*

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

From the method of construction of codes in $\mathcal{E}_{SQS}(m, K, t)$ it follows that the parity-check matrix $\mathbf{H}_4$ is free of 4-cycles. Thus, we have the following result.

Theorem 2. *Let g is a girth of parity-check matrix $\mathbf{H}_4$ of code $\mathcal{C}$, based on $SQS(2^m - 1)$, then*

$$g \geq 6.$$

Now let us estimate the minimum distance of a proposed codes.

Theorem 3. *Let $d_{\min}$ be a minimum distance of an LDPC code $\mathcal{C}$, based on $SQS(2^m - 1)$, then*

$$d_{\min} \geq 5.$$

Now let us determine a condition guaranteeing a strict increase in the minimum distance when replacing each of the ones in $\tilde{\mathbf{H}}_4$ with permutation matrices. The main result of this work is the following.

Theorem 4. *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 permutation matrices using the method described in Section III. 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.*

5 Simulation results

MatLab functions were written for generating parity-check matrices of LDPC codes based on $SQS(2^m - 1)$. Simulation was made by methods of simulation modelling with the use of MatLab. For an information transmission channel, we chose a binary BPSK channel with additive white Gaussian noise. For a decoding algorithm, we chose an iterative algorithm Sum-Product. The maximum number of iterations was limited by 50.

Simulation results presented in Fig. 1 show that the code from the ensemble $\mathcal{E}_{SQS}(8, 4120, 8)$ behaves hardly diffent from that of a random column-weight 4 Gallager's code at the same length. At the same time, shortened STS LDPC code proposed in [7] and a random column-weight 3 Gallager's code demonstrate unsatisfactory behaviour, which lose almost one order in error probability per bit against the two above-mentioned constructions.

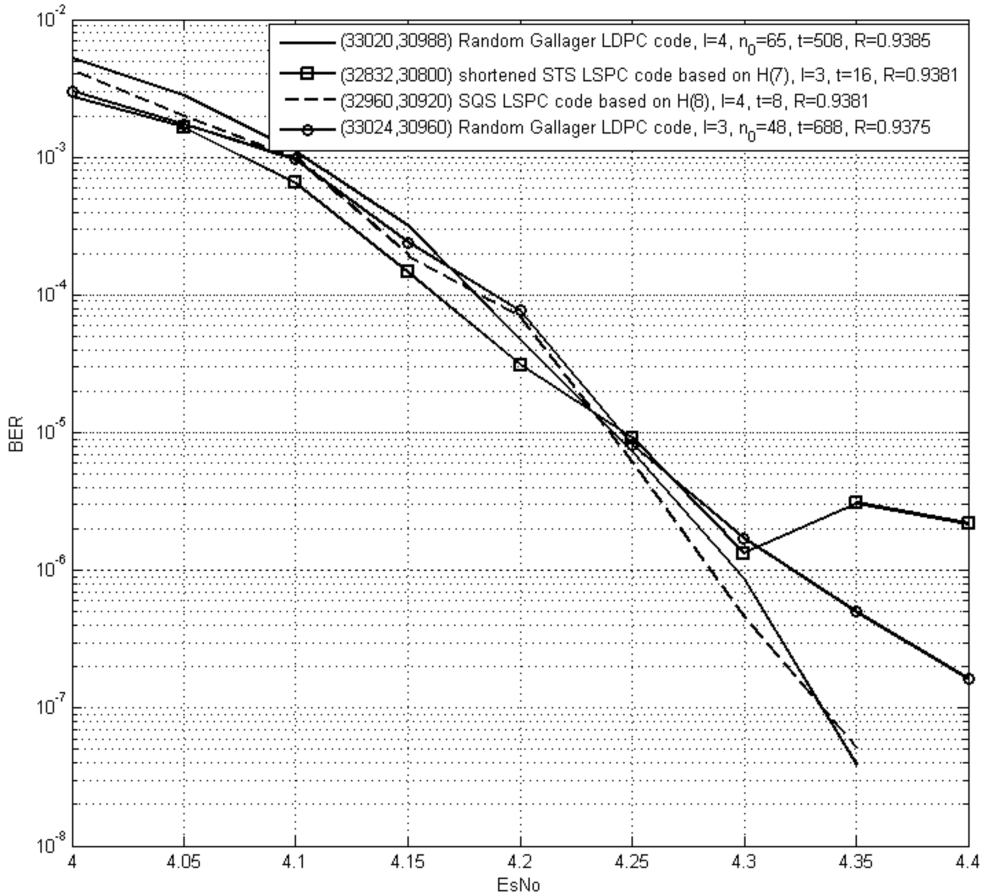

Figure 1: Bit error probability versus signal-to-noise ratio (Es/No) for Gallager's codes ($l = 3, 4$), STS LDPC code and SQS LDPC code, $R = 0.938$

6 Conclusion

In this paper, a method is proposed for generating parity-check matrix $\mathbf{H}$ of LDPC code based on $SQS(2^m - 1)$ and permutation matrices. Estimates for the rate, minimum distance and girth are derived. A condition that guarantees a strict increase in the minimum distance is obtained. Simulation results allow us to conclude that the obtained code constructions based on $SQS(2^m-1)$ with column weight 4 are not worse than Gallager's codes with the same parameters in the case when $R = 0.938$.

Although a simulation results show that the code from the ensemble $\mathcal{E}_{SQS}(8, 4120, 8)$ behaves hardly different from that of a random column-weight 4 Gallager's code at the same length and $R = 0.938$, we should mention that apart from random Gallager's codes our proposed codes on one hand have a such deterministic characteristics as minimum distance and girth and on the other in the case of circulant permutation matrices their encoding complexity is $O(n \log n)$ [8] (for a random code we have complexity $O(n^2)$) and their decoding algorithm can be parallelized [9].

References

[1] R. G. Gallager, *Low-Destiny Parity-Check Codes.* Cambridge, MA: MIT Press, 1963.

[2] E. Gabidulin, A. Moinian and B. Honary, "Generalized Construction of Quasi-Cyclic Regular LDPC Codes Based on Permutation Matrices", *In Proceedings of IEEE International Symposium on Information Theory,* pp. 679–683, 2006.

[3] M. Hagiwara, K. Nuida and T. Kitagawa, "On the Minimal Length of Quasi-cyclic LDPC Codes with Girth ≥ 6", *In Proc. 2006 Int. Sympos. on Information Theory and Its Applications (ISITA'2006)*, Korea: Seoul, 2006.

[4] Y. Kou, S. Lin and M. Fossorier, "Low-Density Parity Check Codes Based on Finite Geometries: A Rediscovery and New Results", *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2711–2736, 2001.

[5] B. Vasic, K. Pedagani and M. Ivkovic, "High-Rate Girth-Eight Low-Density Parity-Check Codes on Rectangular Integer Lattices", *IEEE Trans. Commun.*, vol. 52, no. 8, pp. 1248–1252, 2004.

[6] S. Johnson, "Low-Density Parity-Check Codes from Combinatorial Designs", *PhD Thesis*, Australia: Newcastle, 2004.

[7] F. Ivanov, V. Zyablov, "Low-Density Parity-Check Codes Based on Steiner Triple Systems and Permutation Matrices", *Problems of Information Transmission*, vol. 49, no. 4, pp. 41-56, 2013.

[8] Li Zongwang,Chen Lei, Zeng Lingqi, Lin Shu and W.H Fong, "Efficient encoding of quasi-cyclic low-density parity-check codes", *IEEE Transactions on Communications*, vol. 54, no. 1, pp. 71–81, 2006.

[9] F.I Ivanov, I.V. Zhilin, V.V. Zyablov, "Decoding Algorithm for Low-Density Parity-Check Codes with High Parallelization", *Inform. Control Syst.*, vol. 61, no. 6, pp. 53–59, 2012.