On the Multiple Threshold Decoding of LDPC codes over GF(q)

Alexey Frolov and Victor Zyablov
Inst. for Information Transmission Problems
Russian Academy of Sciences
Moscow, Russia
Email: {alexey.frolov, zyablov}@iitp.ru

***Abstract*—We consider the decoding of LDPC codes over $GF(q)$ with the low-complexity majority algorithm from [1]. A modification of this algorithm with multiple thresholds is suggested. A lower estimate on the decoding radius realized by the new algorithm is derived. The estimate is shown to be better than the estimate for a single threshold majority decoder. At the same time the transition to multiple thresholds does not affect the order of complexity.**

I. Introduction

In this paper we consider the decoding of LDPC codes [2], [3] over $\mathbb{F}_q$ with the low-complexity majority algorithm from [1]. In [1, Theorem 1] a lower estimate on the relative decoding radius ρ realized by the low-complexity majority algorithm is derived. Let us describe the result in more detail. Let N denote the code length. In [1] it is proved that there exist LDPC codes over $\mathbb{F}_q$ (with probability $p_N : \lim_{N\to\infty} p_N \to 1$) capable of correcting any error vector of weight[1] $W \leq \rho N$ with the decoding complexity $O(N \log N)$. We first improve the estimate on ρ.

Then we consider multiple threshold decoding of LDPC codes over $\mathbb{F}_q$. Multiple threshold majority decoding for binary LDPC codes was first introduced in [4]. In [4] it was shown that transition to multiple thresholds increases the decoding radius of the majority algorithm (in the binary case the algorithm is usually called bit-flipping algorithm [5], [6]) without affecting the order of complexity. In this paper we generalize the ideas of [4] to the case of non-binary LDPC codes.

Our contribution is as follows. We first improve the estimate on the relative decoding radius ρ for the single threshold case. Then we suggest the majority decoding algorithm with multiple thresholds for LDPC codes over $\mathbb{F}_q$. A lower estimate on the decoding radius realized by the new algorithm is derived. The estimate is shown to be at least 1.21 times better than the estimate for a single threshold majority decoder. At the same time analogously the result from [4] the transition to multiple thresholds does not affect the order of complexity.

II. Preliminaries

Let us consider the construction of LDPC code $\mathcal{C}$ over $\mathbb{F}_q$. To construct such a code we use a bipartite graph, which is called the Tanner graph [3] (see Fig. 1). The graph consists of N variable nodes $v_1, v_2, \ldots, v_N$ and M check nodes $c_1, c_2, \ldots, c_M$. We assume all the check nodes to have the same degree n_0 and all the variable nodes to have the same degree ℓ. Such Tanner graphs are called regular ones. We associate constituent codes to each of the check nodes. All the constituent codes are the same (we denote the constituent code by $\mathcal{C}_0$). We assume $\mathcal{C}_0$ to be a linear $[n_0, R_0, d_0]$-code over $\mathbb{F}_q$. Let us denote the parity-check matrix of the constituent codes by $\mathbf{H}_0$. The matrix has size $m_0 \times n_0$, where $m_0 = (1-R_0)n_0$.

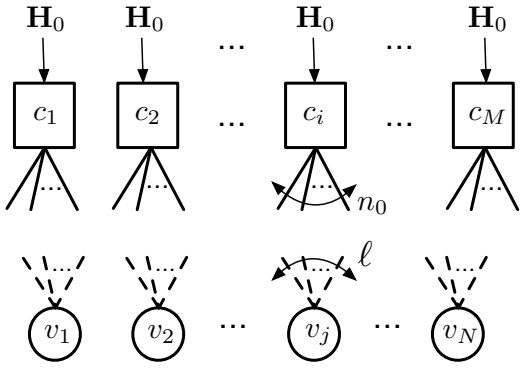

Fig. 1. Tanner graph

To check if $\mathbf{r} = (r_1, r_2, \ldots, r_N) \in \mathbb{F}_q^N$ is a codeword of $\mathcal{C}$ we associate the symbols of $\mathbf{r}$ to the variable nodes ($v_i = r_i, i = 1, \ldots, N$). The word $\mathbf{r}$ is called a codeword of $\mathcal{C}$ if all the constituent codes are satisfied (the symbols which come to the codes via the edges of the Tanner graph form codewords of the constituent codes).

It is clear the resulting code $\mathcal{C}$ is linear, so it has a parity-check matrix associated to it. We denote the matrix by $\mathbf{H}$. The code is over $\mathbb{F}_q$ and has the length N. The following inequality follows for the rate of the code $\mathcal{C}$

$$R(\mathcal{C}) \geq 1 - \ell(1 - R_0).$$

In what follows for the simplicity we consider only the case when the constituent code is an $[n_0, n_0 - 1]$ single parity-check (SPC) code over $\mathbb{F}_q$. The generalization to the case of a stronger constituent code is simple. It will be briefly explained in Remark 4.

[1]Here and in what follows by weight we mean the Hamming weight, i.e. a number of non-zero elements in a vector.

As usually we calculate the syndrome of the sequence $\mathbf{r} = (r_1, r_2, \ldots, r_N) \in \mathbb{F}_q^N$ to be decoded as follows

$$\mathbf{S} = \mathbf{H}\mathbf{r}^T.$$

In [1, Theorem 2] it is proved that there exist LDPC codes over $\mathbb{F}_q$ (with probability $p_N : \lim_{N\to\infty} p_N \to 1$) such that the following inequality holds for the syndrome weight

$$|\mathbf{S}| > L(W) = \frac{W\ell}{2} \tag{1}$$

for all error vectors of weight $W \le W^*(R,\ell) = \omega^*(R,\ell)N$.

To prove Theorem 2 in [1] a Gallager-like ensemble of LDPC codes was used. The only difference to the binary case was in multiplication of the parity-check matrix columns by non-zero elements from $\mathbb{F}_q$. In what follows we do not need the ensemble, so we omit the definition of the ensemble here. In what follows we need just an LDPC code over $\mathbb{F}_q$ which satisfies the property (1). We denote the code by $\mathcal{C}^*$.

We note, that at the same time the following trivial upper bound on the syndrome weight holds

$$|\mathbf{S}| \le U(W) = W\ell.$$

III. Single threshold majority decoding algorithm

Let us describe a single-threshold majority decoding algorithm from [1]. See Algorithm III for full description, here we give some comments and explanations. The algorithm is an iterative hard decision decoding algorithm. On each iteration the algorithm checks all the symbols from the sequence to be decoded ($\mathbf{r} = (r_1, r_2, \ldots, r_N)$). For each of the symbols the replacement criterion (see below) is checked. If the symbol satisfies the criterion, then its value is replaced with a new value, syndrome is updated and the algorithm continues with the next symbol.

Remark 1: It is important to note, that the algorithm works with the symbols consequently. This means, that in case of replacement all the changes are introduced to the sequence to be decoded and to the syndrome and then the algorithm goes to the next symbol.

Now let us consider the replacement criterion. Assume the algorithm is considering the symbol r_i. The corresponding variable node v_i is connected to ℓ constituent codes. Each of these codes sends a message to v_i calculated based on values of another variable nodes connected to it (usual message passing rule). So we have ℓ messages coming to v_i. Let $A_{\max}$ denote a subset of equal non-zero messages of maximal cardinality, let $a = |A_{\max}|$ and v be a value of the messages from $A_{\max}$. Let a threshold θ be an integer such that $0 \le \theta < \ell$. At last let z be a number of zero messages. The replacement criterion is as follows. If $a - z > \theta$ we replace the symbol r_i with v.

Remark 2: Note, that within the section $\theta = 0$, we introduced the parameter here just for our convenience. We will use it in the next section.

And the last thing we have not mention yet is a stopping criterion. We stop the algorithm if no changes in $\mathbf{r}$ were made during the iteration.

Algorithm 1 Single threshold majority decoding algorithm

Input: received sequence $\mathbf{r}$, threshold $\theta : 0 \le \theta < \ell$
Output: decoded sequence $\mathbf{c}$, failure flag F
Initialization: $\mathbf{S} \leftarrow \mathbf{H}\mathbf{r}^T$; $b \leftarrow 1$
while $b = 1$ **do**
  $b \leftarrow 0$
  for all $1 \le i \le N$ **do**
    calculate ℓ messages for r_i
    $A_{\max} \leftarrow$ maximal subset of equal non-zero messages
    $a \leftarrow |A_{\max}|$; $v \leftarrow$ value from $A_{\max}$
    $z \leftarrow$ number of zero messages
    if $a - z > \theta$ **then**
      $r_i \leftarrow v$
      update $\mathbf{S}$
      $b \leftarrow 1$
    end if
  end for
end while
$F \leftarrow 1$
$\mathbf{c} \leftarrow \mathbf{r}$
if $|\mathbf{S}| = 0$ **then**
  $F \leftarrow 0$
end if

Lemma 1 ([1, Theorem 3]): Let

$$|\mathbf{S}| > \frac{W\ell}{2}$$

then there exist a symbol whose replacement leads to the syndrome weight reduction (at least by 1).

Proof: A more general proof will be given in the next section. ∎

Theorem 1 ([1, Theorem 4]): Let $\mathcal{C}^*$ be an LDPC code over $\mathbb{F}_q$, satisfying (1). If the number of errors in the received sequence

$$W \le W^*/2,$$

the Algorithm 1 (with $\theta = 0$) will correct all the errors with the complexity $O(N \log N)$.

Here we refine the result of the previous theorem

Theorem 2 (Single threshold): Let $\mathcal{C}^*$ be an LDPC code over $\mathbb{F}_q$, satisfying (1). If the number of errors in the received sequence

$$W \le W^{(S)} = \frac{W^*}{2}\frac{\ell+2}{\ell+1},$$

the Algorithm 1 (with $\theta = 0$) will correct all the errors with the complexity $O(N \log N)$.

Proof: To prove the theorem we need to prove that the number of errors at each step of the algorithm is less or equal to W^* (see condition (1) and Lemma 1).

Any error vector can mapped to a point of the following coordinate system: "syndrome weight – number of errors" (see

Fig. 2). At the same time it is clear, that each point in the coordinate system corresponds to multiple error vectors. First, let us add the lines $L(W)$ and $U(W)$ to Fig. 2. Recall, that the syndrome weight of any error vector with $W \le W^*$ satisfies the inequality

$$L(W) < |\mathbf{S}| \le U(W).$$

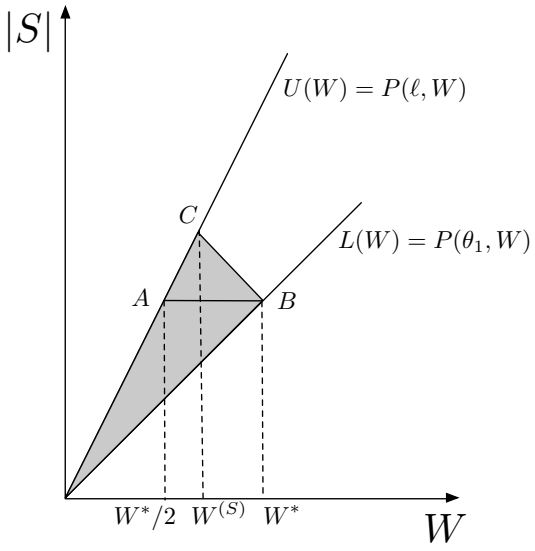

Fig. 2. Single threshold

Let us consider the decoding process. It corresponds to some trajectory in the coordinate system. We start from the initial error vector. With each replacement the syndrome weight decreases (we move down at least by 1) and the number of errors increases (we can introduce errors) or decreases by 1 (so we move right or left by 1). The decoding is successful if we finish at the origin.

The area of correctable error vectors is filled by gray color in Fig. 2. Let us explain this fact. Assume we start from the point C (see Fig. 2) and only introduce errors. In this situation we move right and down by 1 with each step (move along the line CB). We can not come to the point B as it lies on the (strict) lower bound $L(W)$ so it is clear that the number of errors can not become greater than W^*. In this case the decoding (and the trajectory) finishes at origin. To finish the proof we just need to calculate the coordinate of intersection of two lines: $U(W)$ and CB (starts in W^* and has a slope equal to -1). The previous estimate ($W^*/2$, point A) is also shown in Fig. 2.

The proof of the complexity estimate coincides with the proof from [1]. We omit it here. ■

Corollary 1: Let us introduce a notation

$$\alpha^{(S)} = \frac{\ell + 2}{2(\ell + 1)}$$

and consider the asymptotic ($N \to \infty$) estimate of the relative decoding radius realized by Algorithm 1. We have

$$\rho^{(S)} \ge \frac{W^{(S)}}{N} = \alpha^{(S)} \omega^*.$$

In the next section we will increase the estimate by means of transition to multiple decoding thresholds.

IV. Decoding with multiple thresholds

Let us first introduce the sequence of integer thresholds (let $t \ge 1$)

$$0 = \theta_1 < \theta_2 < \ldots < \theta_t < \ell.$$

Now we are ready to describe the multiple threshold decoding algorithm. The idea of the new algorithm is in consequent applying the Algorithm 1 with different replacement thresholds to the sequence to be decoded. We start from the largest threshold θ_t and end with $\theta_1 = 0$. Please see Algorithm 2 full description below for more details.

Algorithm 2 Multiple threshold majority decoding algorithm

Input: received sequence $\mathbf{r}$, t thresholds $0 = \theta_1 < \theta_2 < \ldots < \theta_t < \ell$
Output: decoded sequence $\mathbf{c}$, failure flag F
Initialization: $\mathbf{S} \leftarrow \mathbf{H}\mathbf{r}^T$
for all $0 \le i \le t-1$ **do**
  Apply Algorithm 1 with $\theta = \theta_{t-i}$
  $\mathbf{r} \leftarrow$ output of Algorithm 1
end for
$F \leftarrow 1$
$\mathbf{c} \leftarrow \mathbf{r}$
if $|\mathbf{S}| = 0$ **then**
  $F \leftarrow 0$
end if

Remark 3: We note, that the implementation of the Algorithm 2 is not optimal. It is much better to implement it in such a way. First calculate the syndrome, then sort all the symbols in a descending order of $a - z$ value (see previous section), then change the symbols consequently and update the sorted list. But nevertheless we see here that the complexity of Algorithm 2 is no more than t times the complexity of Algorithm 1. So the order of complexity is $O(N \log N)$.

To estimate the decoding radius of the Algorithm 2 we need the following Lemma.

Lemma 2: Let θ be an integer, $0 \le \theta < \ell$, let

$$|\mathbf{S}| > P(\theta, W) = W \frac{\ell + \theta}{2}$$

then there exist a symbol whose replacement leads to the syndrome weight reduction by at least by $\theta + 1$.

Proof: Consider a subgraph of the Tanner graph that contains only erroneous symbols (the number of errors is equal to W) and constituent codes connected to these symbols. Within the proof we work with this subgraph only.

Let us introduce the following notation:

- A is the set of codes that detect an error ($|A| = |\mathbf{S}|$);

- A_i, $i = 1, \ldots, n_0$, is the subset of A containing only the codes with precisely i incoming edges ($a_i = |A_i|$);
- $A_{\geq 2} = A \backslash A_1$ is a subset of A containing only the codes with at least 2 incoming edges ($a_{\geq 2} = |A_{\geq 2}|$);
- C is the set of codes that contain errors but do not detect them ($c = |C|$);
- $e_{A_1}^{(i)}$ is the number of edges outgoing from a symbol i and incoming to A_1;
- $e_C^{(i)}$ is the number of edges outgoing from a symbol i and incoming to C.

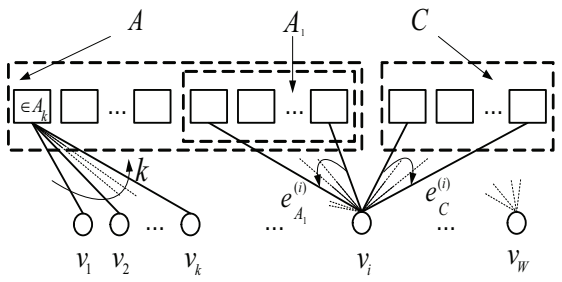

Fig. 3. A subgraph of Tanner graph

In Fig. 3 we present an example of a subgraph of the Tanner graph and illustrate the introduced notation.

First note, that if the condition

$$e_{A_1}^{(i)} > e_C^{(i)} + \theta$$

holds for the i-th symbol, then the replacement of it will lead to the syndrome weight reduction by at least by $\theta + 1$. To prove this it is sufficient to mention that the codes with the only error will give equal messages.

Then we claim that if

$$a_1 > \sum_{i=1}^{W} e_C^{(i)} + W\theta,$$

then there exist a symbol i such that $e_{A_1}^{(i)} > e_C^{(i)} + \theta$.

And to finish the proof we need to count the edges in the subgraph. The number of edges outgoing from W erroneous symbols is $W\ell$. These edges can come to either codes that have detected an error ($A = A_1 \cup A_{\geq 2}$) or to codes that have not detected errors but contain them (C). Let us estimate the number of edges incoming to each of the three sets of codes:

- The number of edges leading to codes of the set A_1 is $\sum_{i=1}^{W} e_{A_1}^{(i)} = a_1$;
- The number of edges leading to codes of the set $A_{\geq 2}$ is at least $2(|\mathbf{S}| - a_1)$ (here we use the fact every code has at least two incoming edges);
- The number of edges leading to codes of the set C is $\sum_{i=1}^{W} e_C^{(i)}$.

Thus

$$W\ell \geq a_1 + 2(|\mathbf{S}| - a_1) + \sum_{i=1}^{W} e_C^{(i)}.$$

After some transformations, we have

$$a_1 - \sum_{i=1}^{W} e_C^{(i)} \geq 2|\mathbf{S}| - W\ell.$$

This immediately implies that if the condition of the Lemma holds then

$$a_1 > \sum_{i=1}^{W} e_C^{(i)} + W\theta.$$

■

Theorem 3 (Multiple thresholds): Let $\mathcal{C}^*$ be an LDPC code over $\mathbb{F}_q$, satisfying (1). Let $0 = \theta_1 < \theta_2 < \ldots < \theta_t < \ell$ be a sequence of thresholds. If the number of errors in the received sequence

$$W \leq W_{t+1},$$

where

$$W_i = W_{i-1} \frac{\ell + 3\theta_{i-1} + 2}{\ell + 2\theta_{i-1} + \theta_i + 2},\ W_1 = W^*, \theta_{t+1} = \ell,$$

the Algorithm 2 will correct all the errors with complexity $O(N \log N)$.

Proof: The area of correctable error vectors is shown in Fig. 4. For now the area is more difficult because the slope at threshold θ_i is equal to $\theta_i + 1$. To prove the Theorem we need to consequently calculate coordinates of intersection of the area bound and lines $P(\theta_i, W)$.

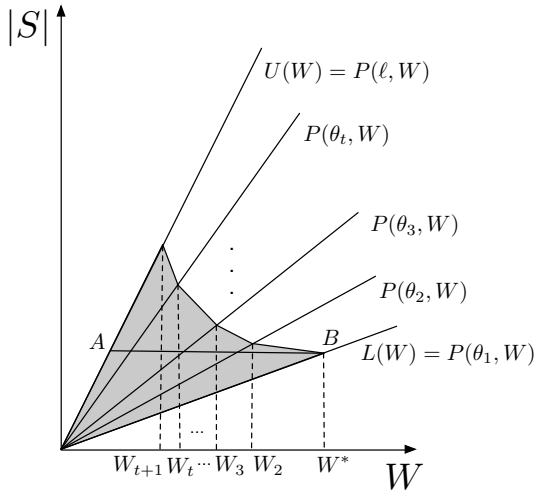

Fig. 4. Multiple thresholds

■

The most interesting case for us is the case when we have all the thresholds from 0 to $\ell - 1$. In this case

$$W^{(M)} = \prod_{i=0}^{\ell-1} \frac{\ell + 3i + 2}{\ell + 3i + 3} W^*.$$

Let us introduce a notation

$$\alpha^{(M)} = \prod_{i=0}^{\ell-1} \frac{\ell + 3i + 2}{\ell + 3i + 3}$$

TABLE I
RESULTS FOR $q = 16$

R; ℓ	ω^*	$\rho^{(S)}$	$\rho^{(M)}$
0.125; 45	0.0103	0.0053	0.0065
0.25; 43	0.0095	0.0049	0.0060
0.375; 40	0.0085	0.0044	0.0054
0.5; 31	0.0072	0.0037	0.0046
0.625; 24	0.0053	0.0028	0.0034
0.75; 24	0.0033	0.0017	0.0021
0.875; 26	0.0015	0.0008	0.0010

TABLE II
RESULTS FOR $q = 64$

R; ℓ	ω^*	$\rho^{(S)}$	$\rho^{(M)}$
0.125; 21	0.0156	0.0082	0.0099
0.25; 24	0.0131	0.0068	0.0083
0.375; 20	0.0104	0.0054	0.0066
0.5; 22	0.0081	0.0042	0.0052
0.625; 27	0.0059	0.0031	0.0038
0.75; 24	0.0037	0.0019	0.0024
0.875; 26	0.0017	0.0009	0.0011

and consider the asymptotic ($N \to \infty$) estimate of the relative decoding radius realized by Algorithm 2 (when we have all the thresholds). We have

$$\rho^{(M)} \geq \frac{W^{(M)}}{N} = \alpha^{(M)}\omega^*.$$

In Fig. 5 the comparison of $\alpha^{(S)}$ and $\alpha^{(M)}$ is shown.

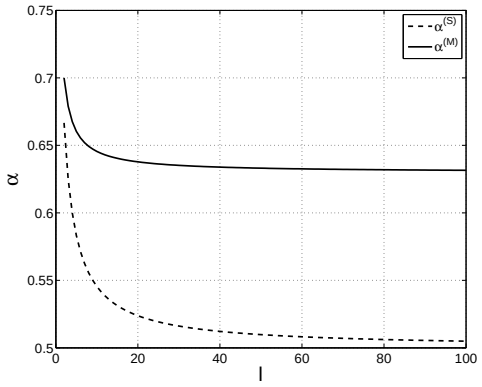

Fig. 5. The dependency of $\alpha^{(S)}$ and $\alpha^{(M)}$ on ℓ

At last let us calculate the value of $\alpha^{(M)}$ when ℓ is big. It is easy to check, that

$$\lim_{\ell\to\infty} \alpha^{(M)} = 2^{-2/3} = 0.6300...$$

Remark 4 (Generalized LDPC codes): Here we briefly consider the case of generalized LDPC codes, i.e. the case when the constituent codes are not SPC codes but some more powerful codes. All our theorems work in this case if we use the so-called generalized syndrome rather then an ordinary syndrome. Generalized syndrome consists of syndromes of constituent codes. The weight of generalized syndrome is just the number of unsatisfied constituent codes. We would like to point out, that analogously to [1] the transition to generalized LDPC codes does not lead to a gain in the decoding radius.

V. NUMERICAL RESULTS

The numerical results are given in Table I for $q = 16$ and Table II for $q = 64$. In each Table the dependencies of ω^*, $\rho^{(S)}$ and $\rho^{(M)}$ on the code rate R are presented. Note, that ℓ (in each case) is chosen to maximize the functions. For our case the maximal values of ω^*, $\rho^{(S)}$ and $\rho^{(M)}$ were achieved for the same ℓ, the value of ℓ is also given in the Tables.

We note, that the value of $\rho^{(M)}/\rho^{(S)} \geq 1.21$ for all the rates we considered. So transition to multiple thresholds leads to the gain in the decoding radius without affecting the order of complexity. To the best knowledge of the authors the obtained estimates are currently the best estimates of the decoding radius for low-complexity majority decoder of LDPC codes over $\mathbb{F}_q$.

VI. CONCLUSION

We improved the estimate on the relative decoding radius ρ for the single threshold majority decoder of LDPC codes over $\mathbb{F}_q$. The majority decoding algorithm with multiple thresholds is suggested. A lower estimate on the decoding radius realized by the new algorithm is derived. The estimate is shown to be at least 1.21 times better than the estimate for a single threshold majority decoder. At the same time analogously the result from [4] the transition to multiple thresholds does not affect the order of complexity.

All the results are obtained for the case when the constituent codes are SPC codes over $\mathbb{F}_q$. The case of more powerful constituent codes is considered. It is shown that analogously to [1] the transition to generalized LDPC codes does not lead to a gain in the decoding radius.

To the best knowledge of the authors the obtained estimates are currently the best estimates of the decoding radius for low-complexity majority decoder of LDPC codes over $\mathbb{F}_q$.

ACKNOWLEDGMENT

This work was partially supported by Russian Science Foundation grant 14-50-00150.

REFERENCES

[1] A. Frolov and V. Zyablov. Asymptotic Estimation of the Fraction of Errors Correctable by Q-ary LDPC Codes. *Probl. Inf. Transm.*, vol. 46, no. 2, pp. 142–159, 2010.
[2] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge: MIT Press, 1963.
[3] R. Tanner. A recursive approach to low complexity codes. *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.
[4] S. Kovalev, Decoding of Low-Density Codes. *Probl. Inf. Transm.*, vol. 27, no. 4, pp. 51–56, 1991.
[5] V. Zyablov and M. Pinsker, Estimation of the error-correction complexity for Gallager low-density codes. *Probl. Inf. Transm.*, vol. 11, no 1, pp. 23–36, 1975.
[6] M. Sipser and D.A. Spielman, Expander Codes. *IEEE Trans. Inf. Theory*, 1996, vol. 42, no. 6, pp. 1710–1722.