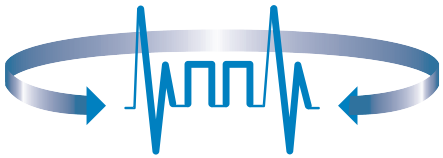
# The Analysis of Hard-Decision Multi-Threshold Decoding of Non-Binary LDPC Codes

Alexey Frolov

Email: alexey.frolov@iitp.ru



Institute for Information Transmission Problems
Russian Academy of Sciences

Coding Theory Seminar
Technion Computer Science Faculty
March 27, 2016

# Outline

# Outline

# Motivation

Non-binary LDPC codes significantly outperform their binary counterparts[1]. Moreover, non-binary LDPC codes are especially good for the channels with burst errors and high-order modulations[2]. Unfortunately, their decoding complexity is still large, that is why iterative hard and soft-reliability based decoding majority algorithms are of considerable interest for high-throughput practical applications.

We investigate the error-correcting capabilities of non-binary LDPC codes decoded with a hard-decision low-complexity majority algorithm. We perform the worst case analysis and estimate the decoding radius ($\rho N$) realized by this algorithm.

---

[1] M. C. Davey and D. MacKay, Low-density parity check codes over GF(q), *IEEE Commun. Lett.*, vol. 2, no. 6, pp. 165–167, Jun. 1998.

[2] H. Song and J. R. Cruz, Reduced-complexity decoding of Q-ary LDPC codes for magnetic recording, *IEEE Transactions on Magnetics*, vol. 39, no. 2, pp. 1081–1087, Mar. 2003.

# Our contribution

- We improved the estimate on the relative decoding radius $\rho$ for the single threshold majority decoding algorithm.
- 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 1.2 times better than the estimate for a single threshold majority decoder.
- We prove, that introducing multiple thresholds does not affect the order of decoding complexity.

# Related work

## Binary case:


- V. Zyablov and M. Pinsker, Estimation of the error-correction complexity for Gallager low-density codes. *Probl. Inf. Transm.*, vol. 11, no 1, pp. 18–28, 1975.
- M. Sipser and D.A. Spielman, Expander Codes. *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 1710–1722, 1996.
- D. Burshtein, On the error correction of regular LDPC codes using the flipping algorithm. *IEEE Trans. Inf. Theory*, vol. 54, no. 2, pp. 517–530, 2008.
- K. Zigangirov, A. Pusane, D. Zigangirov, and D. Costello, On the error-correcting capability of LDPC codes. *Probl. Inf. Transm.*, vol. 44, pp. 214–225, 2008.
- V.V. Zyablov, R. Johannesson, and M. Lončar, Low-complexity error correction of Hamming-code-based LDPC codes, *Probl. Inf. Trans.*, vol. 45, no. 2, pp. 95–109, 2009
- A. Barg and A. Mazumdar, On the number of errors correctable with codes on graphs. *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 910–919, 2011.
- P. Rybin, On the error-correcting capabilities of low-complexity decoded irregular LDPC codes. In Proc. 2014 IEEE Int. Symp. Inf. Theory, Honolulu, HI, June 29–July 4 2014, pp. 3165–3169, 2014.

# Related work

## Non-binary case:

- 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.

## Decoding with multiple thresholds:

- S. Kovalev, Decoding of Low-Density Codes. *Probl. Inf. Transm.*, vol. 27, no. 4, pp. 51–56, 1991.

# Outline

# LDPC codes over GF($q$)

An LDPC code $\mathcal{C}$ of length $N$ over GF($q$) is a null-space of an $M \times N$ sparse parity-check matrix $\mathbf{H} = [h_{i,j}]$, $1 \leq i \leq M$, $1 \leq j \leq N$, over GF($q$).

Regular case, i.e. constant row and column weights of $n_0$ and $\ell$, respectively.

Rate of the code $\mathcal{C}$

$$R(\mathcal{C}) \geq 1 - \frac{\ell}{n_0}.$$

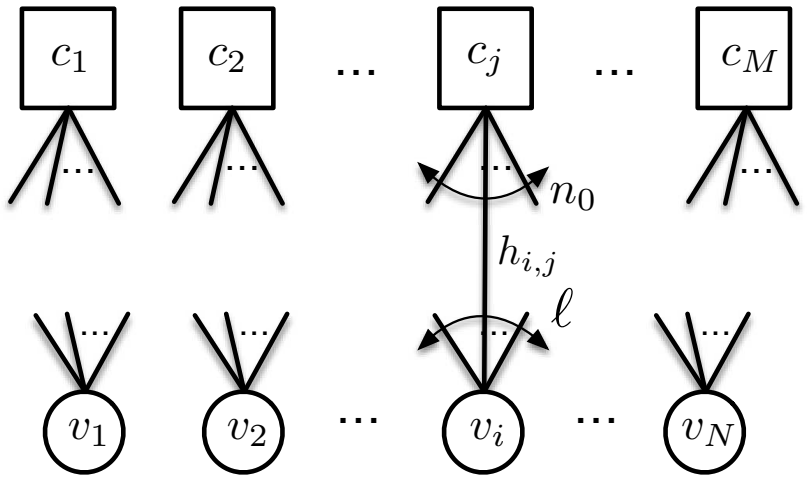
Additional notations:

$$\Gamma(i) = \{j : h_{i,j} \neq 0, 1 \leq j \leq N\}$$

and

$$\Phi(j) = \{i : h_{i,j} \neq 0, 1 \leq i \leq M\}.$$

# Tanner graph




The vertex set of the Tanner graph[3] consists of the set of variable nodes $V = \{v_1, v_2, \ldots, v_N\}$ and the set of check nodes $C = \{c_1, c_2, \ldots, c_M\}$.

The variable node $v_i$ and the check node $c_j$ are connected with an edge if and only if $h_{i,j} \neq 0$. The edge has a label $h_{i,j}$

[3] R. Tanner. A recursive approach to low complexity codes. *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.

# Tanner graph

To check if $\mathbf{r} = (r_1, r_2, \ldots, r_N) \in \mathrm{GF}(q)^N$ is a codeword of $\mathcal{C}$ we associate the symbols of $\mathbf{r}$ to the variable nodes $(v_i \leftarrow r_i, i = 1, \ldots, N)$.

Each check node $c_j$, $1 \leq j \leq N$ imposes the following linear restriction

$$c_j : \sum_{t \in \Phi(j)} h_{t,j} r_t = 0$$

and we can say, that linear $[n_0, n_0 - 1]$ single parity-check (SPC) codes over $\mathrm{GF}(q)$ are associated to the check nodes. In what follows we refer the codes as component codes.

**Definition**

The word $\mathbf{r}$ is a codeword of $\mathcal{C}$ if all the component codes are satisfied (the symbols which come to the codes via the edges of the Tanner graph form codewords of the component codes).

# Syndrome weight estimates: upper bound

We calculate the syndrome of the sequence $\mathbf{r} = (r_1, r_2, \ldots, r_N) \in \mathrm{GF}(q)^N$ to be decoded as follows

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

Let $|\mathbf{S}|$ denote the syndrome weight, let $W$ denote the number of errors in the received sequence.

Trivial upper bound

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

# Syndrome weight estimates: ensemble

To formulate the lower bound on the syndrome weight we need to define the ensemble $\mathcal{E}(N, n_0, \ell)$ of LDPC codes over GF($q$). We start with the ensemble of binary LDPC codes suggested by Gallager[4]. All the elements of non-binary ensemble $\mathcal{E}(N, n_0, \ell)$ can be obtained as follows: we replace ones in parity-check matrices of codes from the Gallager's ensemble with arbitrarily elements of $\mathrm{GF}^*(q) = \mathrm{GF}(q)\backslash\{0\}$.

[4] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge: MIT Press, 1963.

# Syndrome weight estimates: lower bound

**Theorem (Frolov, Zyablov 2010)**

*For any* $4 < \ell < n_0$ *there exists* $\omega^*(n_0, \ell) > 0$ *such that:*

- *there are codes in the ensemble* $\mathcal{E}(N, n_0, \ell)$ *for which the following inequality holds*

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

*for all error vectors of weight* $W < W^*(N, n_0, \ell) = \omega^*(n_0, \ell)N$.

- *the number of such codes* $(G(N, n_0, \ell))$ *satisfy the following relation*

$$\lim_{N\to\infty} \frac{G(N, n_0, \ell)}{|\mathcal{E}(N, n_0, \ell)|} = 1.$$

# Interconnection to expander graphs

Note, that (1) means that the underlying Tanner graph is an unbalanced bipartite $(\ell, n_0, \omega^*, \ell/2)$ expander graph[5]. This means, that for any subset of variable nodes $U \subset V$

$$|U| \leq \omega^* N \Rightarrow |\Gamma(U)| > \frac{\ell}{2}|U|,$$

where $\Gamma(U) \subset C$ is the set of check nodes connected to the set of variable nodes $U$.

The usual way to check the expansion properties of a graph is to examine its second-largest eigenvalue[6]. Unfortunately, the explicit constructions of expander graphs with expansion greater than $\ell/2$ are not known (Kahale[7] even shows that eigenvalue separation cannot certify greater expansion).

[5] M. Sipser and D.A. Spielman, Expander Codes. *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 1710–1722, 1996.

[6] N. Alon, Eigenvalues and expanders, *Combinarorica*, vol. 6, no. 2, pp. 83–96, 1986

[7] N. Kahale, On the second eigenvalue and linear expansion of regular graphs, in Proc 33rd IEEE Symp on Foundations of Computer Science, 1992, pp. 296–303

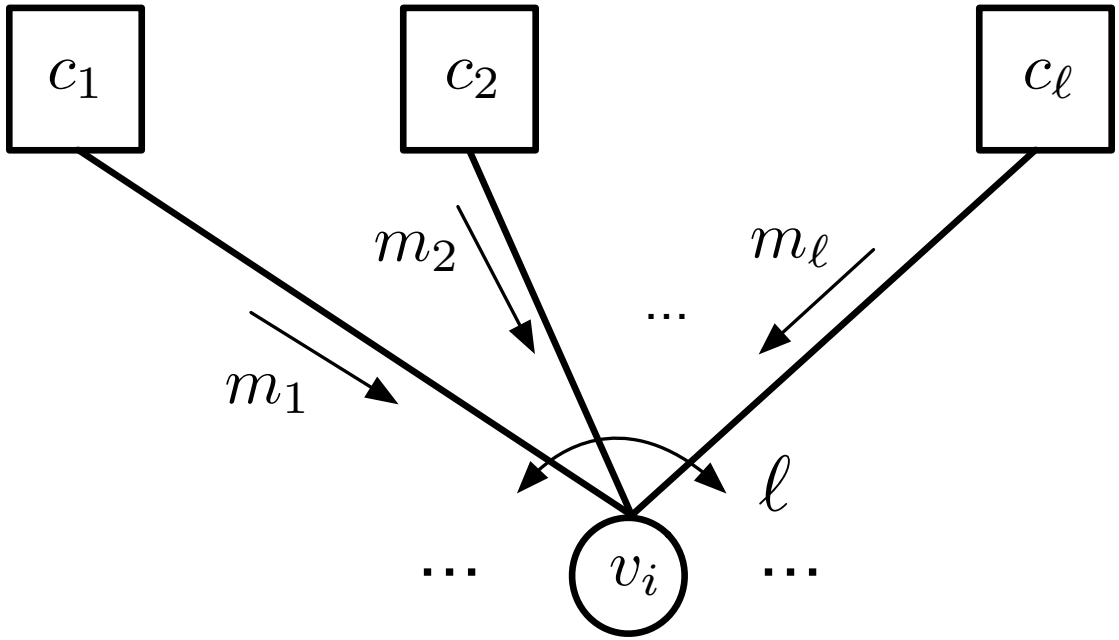
# Single threshold majority decoding algorithm

The algorithm is an iterative hard-decision decoding algorithm (generalization of bit-flipping algorithm for the binary case).

By *iteration* we mean the sequential processing of all $N$ symbols of the sequence to be decoded ($\mathbf{r} = (r_1, r_2, \ldots, r_N)$).

It is important to note, that the algorithm works with the symbols in the sequential manner. 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 proceeds to the next symbol.

# Calculation of messages




Assume the algorithm is considering the symbol $r_i$. The corresponding variable node $v_i$ is connected to $\ell$ check nodes $c_j$, $j \in \Gamma(i)$. Each of these nodes sends a message $m_{j \to i}$, $j \in \Gamma(i)$, to $v_i$.

# Calculation of messages

The messages are calculated as follows

$$m_{j\to i} = z_{i,j} - r_i, \;\; j \in \Gamma(i),$$

where $z_{i,j}$ is the value of $v_i$, such that the check node $c_j$ is satisfied ($s_j = 0$).
It is easy to check, that

$$z_{i,j} = -h_{i,j}^{-1} \left( \sum_{t\in\Phi(j), t\neq i} h_{t,j} r_t \right)$$

and thus, for $j \in \Gamma(i)$

$$m_{j\to i} = -h_{i,j}^{-1} \left( \sum_{t\in\Phi(j), t\neq i} h_{t,j} r_t \right) - r_i = -h_{i,j}^{-1} s_j.$$

# Calculation of messages

**Remark**

*We would like to point out, that a message $m_{j\to i}$ is actually an error value, sent by the check mode $c_j$. Indeed, if we replace $r_i$ with $r_i + m_{j\to i}$, then the syndrome of the $j$-th component code $(s_j)$ will become zero. If a check node is satisfied, it sends a zero message.*

# Replacement criterion

Assume the algorithm is considering the symbol $r_i$ and the messages $m_{j\to i}$, $j \in \Gamma(i)$, are calculated in accordance to the rules above.

- $A_{\max}$ – a subset of equal non-zero messages of maximal cardinality;
- $a = |A_{\max}|$
- $m$ – a value of the messages from $A_{\max}$.
- $\theta$ (threshold) – an integer such that $0 \leq \theta < \ell$ (in this section $\theta = 0$).
- $z$ – a number of zero messages.

The replacement criterion is as follows: If

$$a - z > \theta.$$

the algorithm replaces the symbol $r_i$ with $r_i + m$, syndrome is updated and the algorithm continues with the next symbol.

# Replacement criterion

**Remark**

*Note, that in accordance to the replacement criterion the syndrome weight is reduced by at least $\theta + 1$ with each change. Indeed, $a = |A_{\max}|$ unsatisfied component codes become satisfied, $z$ satisfied check nodes become unsatisfied and $a - z > \theta$.*

**Remark**

*Note, that within the section $\theta = 0$, we introduced the parameter here just for our convenience. We will use it in what follows.*

# Stopping criterion

We stop the algorithm if no changes in $\mathbf{r}$ were made during the iteration. Recall, that in accordance to the replacement criterion the syndrome weight is reduced by at least $\theta + 1$ with each change, that is why the oscillations are not possible and we do not restrict the maximal number of iterations.

# Algorithm 1

**Input:**
received sequence $\mathbf{r}$, threshold $\theta : 0 \leq \theta < \ell$
**Output:**
decoded sequence $\mathbf{c}$, failure flag $F$

**$\mathbf{S} \leftarrow \mathbf{H}\mathbf{r}^T$; $b \leftarrow 1$** ▷ Initialization
**while** $b = 1$ **do**
  $b \leftarrow 0$
  **for all** $1 \leq i \leq N$ **do**
    **for all** $j \in \Gamma(i)$ **do**
      $m_{j \to i} \leftarrow -h_{i,j}^{-1} s_j$ ▷ $s_j$ is a syndrome of a $j$-th component code
    **end for**
    $A_{\max} \leftarrow$ maximal subset of equal non-zero messages
    $a \leftarrow |A_{\max}|$; $m \leftarrow$ value from $A_{\max}$
    $z \leftarrow$ number of zero messages
    **if** $a - z > \theta$ **then**
      $r_i \leftarrow r_i + m$
      update $\mathbf{S}$
      $b \leftarrow 1$ ▷ Replacement occurred, set flag to 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**

# Known results

## Lemma (Frolov, Zyablov 2010)

*Let*

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

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

## Theorem (Frolov, Zyablov 2010)

*Let* $\mathcal{C}^*$ *be an LDPC code over GF(q), satisfying (1). If the number of errors in the received sequence*

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

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

# Outline

# Improvement in case of single threshold

## Theorem

*Let $\mathcal{C}^*$ be an LDPC code over GF(q), satisfying (1). If the number of errors in the received sequence*

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

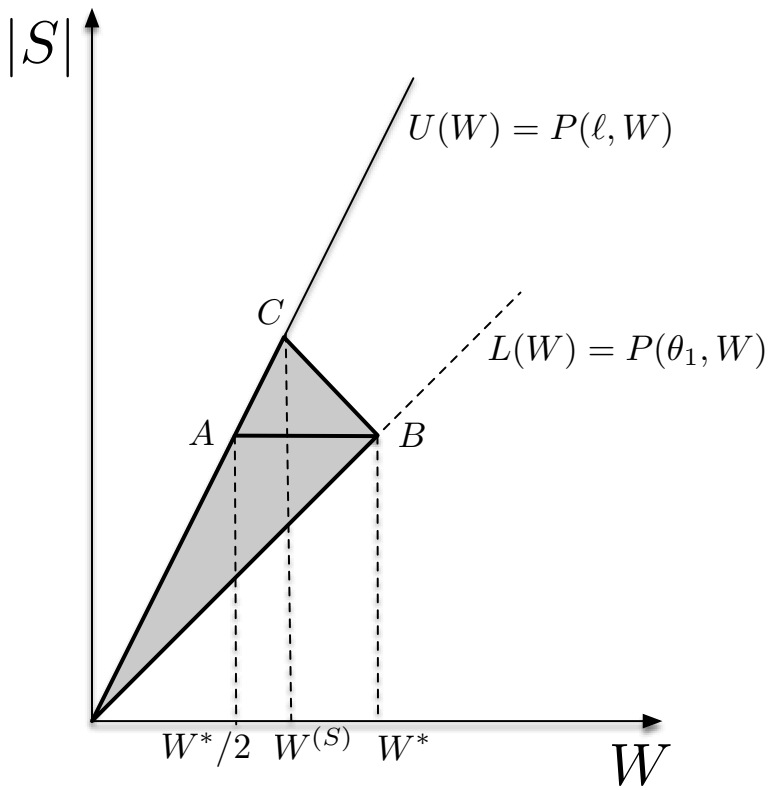
*the Algorithm 1 (with $\theta = 0$) will correct all the errors with the complexity $O(N \log N)$.*

## Corollary (Relative decoding radius, $N \to \infty$)

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

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

# Sketch of the proof




The lower estimate $L(W)$ is valid only up to $W^*$, that is why the line is dashed after the point.

Point A: $(W^*/2;\ W^*\ell/2)$

Point B: $(W^*;\ W^*\ell/2)$

Point C: $(W^{(S)};\ W^{(S)}\ell)$

# Outline

# Decoding with multiple thresholds

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

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

# Algorithm 2

**Input:**

**Input:** received sequence $\mathbf{r}$, $t$ thresholds $0 = \theta_1 < \theta_2 < \ldots < \theta_t < \ell$

**Output:**

decoded sequence $\mathbf{c}$, failure flag $F$

$\mathbf{S} \leftarrow \mathbf{H}\mathbf{r}^T$ ▷ Initialization
**for all** $0 \leq i \leq t-1$ **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**

# Multiple thresholds

**Lemma**

*Let $\theta$ be an integer, $0 \leq \theta < \ell$, let*

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

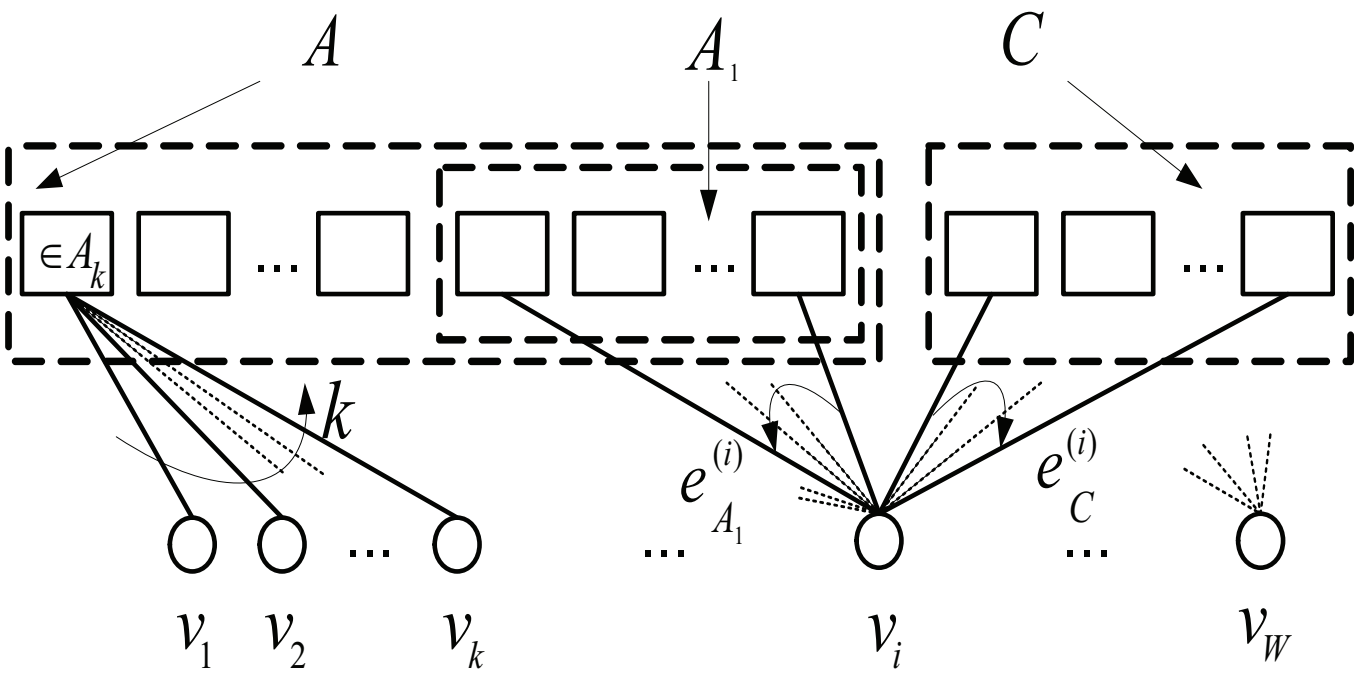
*then there exist a symbol whose replacement leads to the syndrome weight reduction by at least by $\theta + 1$.*

# Sketch of the proof

Let us introduce the following notation:

- $A$ is the set of check nodes with that detect an error ($|A| = |\mathbf{S}|$);
- $A_i$, $i = 1, \ldots, n_0$, is the subset of $A$ containing only the check nodes with precisely $i$ incoming edges ($a_i = |A_i|$);
- $A_{\geq 2} = A \backslash A_1$ is a subset of $A$ containing only check nodes with at least 2 incoming edges ($a_{\geq 2} = |A_{\geq 2}|$);
- $C$ is the set of check nodes 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 $C$.

# Sketch of the proof



# Sketch of the proof

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

If

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

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

# Sketch of the proof

In order to finish the proof we need to count the edges in the subgraph. The number of edges outgoing from $W$ erroneous symbols is $W\ell$.

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

# Sketch of the proof

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

After some transformations, we have

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

# Multiple thresholds

## Lemma

*Let $\theta$ be an integer, $0 \leq \theta < \ell$, let*

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

*then at least $\delta W$ symbols are changed by Algorithm 2 within one iteration with threshold $\theta$, where*

$$\delta = \frac{\varepsilon}{(\ell - \theta)(\ell(n_0 - 1) + 1)}.$$

# Multiple thresholds

## Theorem

*Let $\mathcal{C}^*$ be an LDPC code over GF(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*

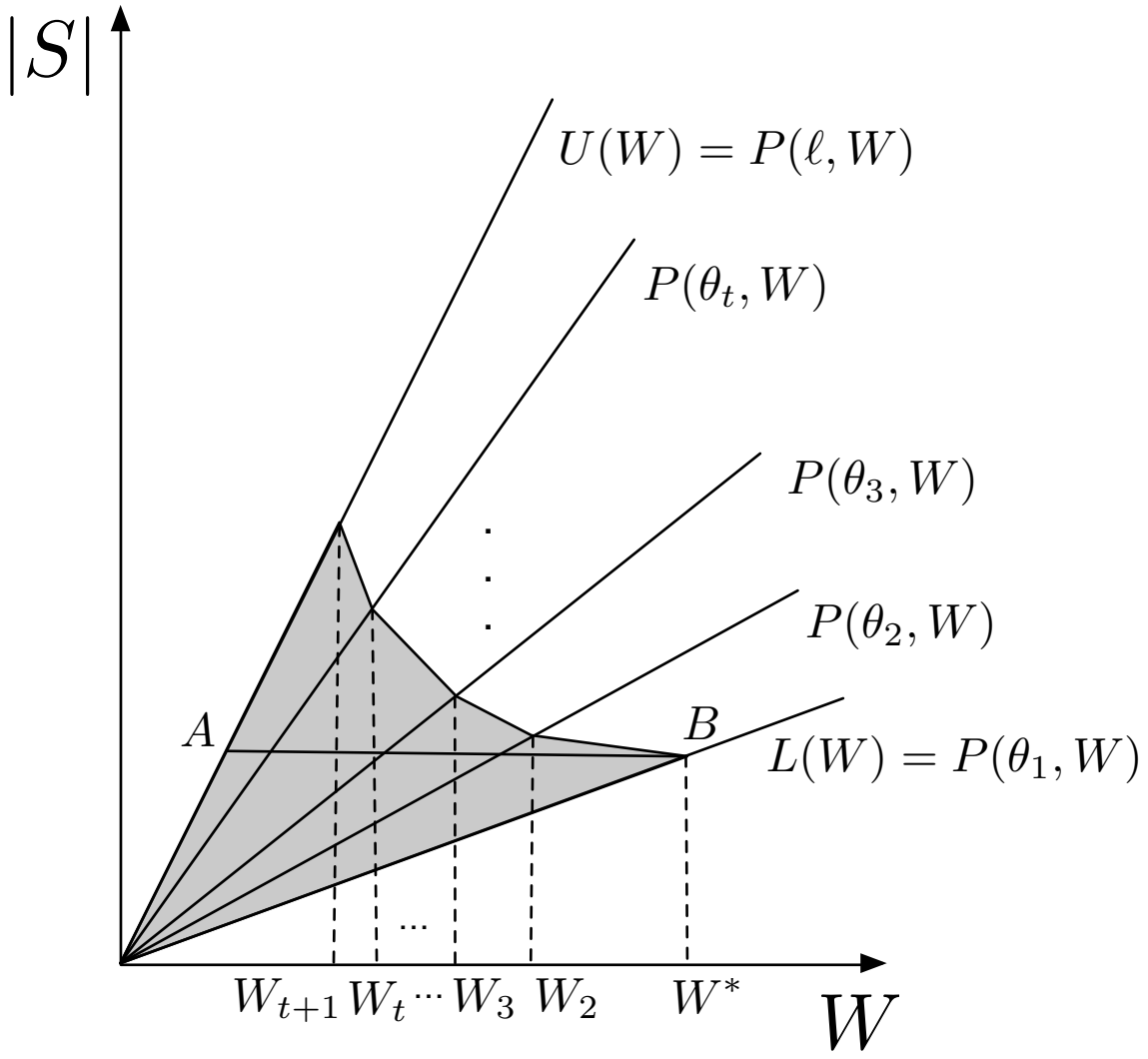
$$W \leq W_{t+1},$$

*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 $O(N \log N)$.*

# Sketch of the proof



# Decoding complexity

The complexity of an iteration is $O(N)$, so our aim is to estimate the number of iterations.

Assume the syndrome weight is $P(\theta+\varepsilon, W)$ and consider an iteration with threshold $\theta$. In accordance to Lemma $\delta W$ symbols will be changed by Algorithm 2, thus the syndrome weight will be reduced at least

$$\gamma = \frac{P(\theta+\varepsilon, W)}{P(\theta+\varepsilon, W) - \delta\theta W} = \frac{\ell+\theta+\epsilon}{\ell+\theta+\epsilon-2\delta\theta} > 1$$

times.

$$\theta_i \to \theta_i + \varepsilon, \quad i = 1, \ldots, t.$$

# Relative decoding radius

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

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

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

where

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

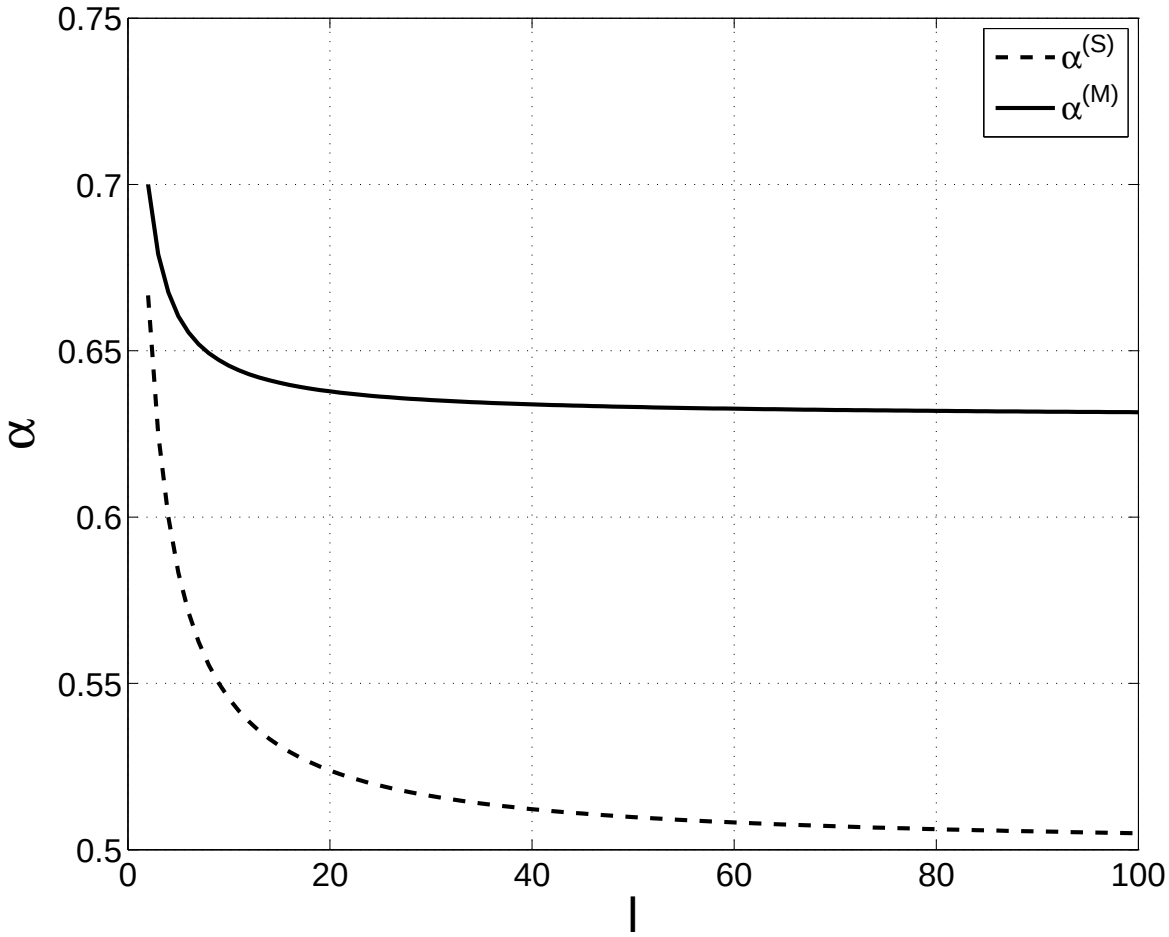
# Relative decoding radius

$$\rho = \alpha\omega^*$$

$$0.630\ldots = \sqrt[3]{\frac{1}{4}} \leq \alpha^{(M)} \leq \sqrt[3]{\frac{\ell+2}{4\ell+2}}.$$

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

# Relative decoding radius



# Outline

# q = 16

| $(\ell,\ n_0);\ R$ | $\delta$ | $\omega^*$ | $\rho^{(S)}$ | $\rho^{(M)}$ | $\rho^{(M)}/\rho^{(S)}$ |
|---|---|---|---|---|---|
| (45, 52); 0.135 | 0.6130 | 0.0103 | 0.0053 | 0.0065 | 1.226 |
| (43, 58); 0.26 | 0.4855 | 0.0095 | 0.0049 | 0.0060 | 1.224 |
| (40, 64); 0.375 | 0.3797 | 0.0085 | 0.0044 | 0.0054 | 1.227 |
| (31, 62); 0.5 | 0.2808 | 0.0072 | 0.0037 | 0.0046 | 1.243 |
| (24, 64); 0.625 | 0.1935 | 0.0053 | 0.0028 | 0.0034 | 1.214 |
| (24, 96); 0.75 | 0.1168 | 0.0033 | 0.0017 | 0.0021 | 1.235 |
| (26, 208);0.875 | 0.0507 | 0.0015 | 0.0008 | 0.0010 | 1.250 |

# q = 64

| $(\ell,\ n_0);\ R$ | $\delta$ | $\omega^*$ | $\rho^{(S)}$ | $\rho^{(M)}$ | $\rho^{(M)}/\rho^{(S)}$ |
|---|---|---|---|---|---|
| (21, 24); 0.125 | 0.7355 | 0.0156 | 0.0082 | 0.0099 | 1.207 |
| (24, 32); 0.25 | 0.5863 | 0.0131 | 0.0068 | 0.0083 | 1.221 |
| (20, 32); 0.375 | 0.4585 | 0.0104 | 0.0054 | 0.0066 | 1.222 |
| (22, 44); 0.5 | 0.3445 | 0.0081 | 0.0042 | 0.0052 | 1.238 |
| (27, 72); 0.625 | 0.2415 | 0.0059 | 0.0031 | 0.0038 | 1.226 |
| (24, 96); 0.75 | 0.1485 | 0.0037 | 0.0019 | 0.0024 | 1.263 |
| (26, 208); 0.875 | 0.0661 | 0.0017 | 0.0009 | 0.0011 | 1.222 |

# Main results

- We improved the estimate on the relative decoding radius $\rho$ for the single threshold majority decoding algorithm.
- 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 1.2 times better than the estimate for a single threshold majority decoder.
- We prove, that introducing multiple thresholds does not affect the order of decoding complexity.

Thank you for your attention!