Plan

Finite-Length Performance of Regular LDPC Ensembles over $GF(2^m)$

Iryna Andriyanova*
joint work with K. Kasai†

*ETIS Lab, ENSEA / Univ. Cergy-Pontoise / CNRS, Cergy, France

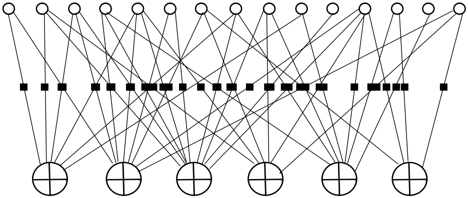
†Tokyo Institute of Technology, Tokyo, Japan

Jan 14, 2010

Motivation

- Non-binary sparse-graph codes :
  - iterative threshold - unimodal function of alphabet size q ; not necessarily improves [Rathi&Urbanke]
  - however, examples of a good finite-length performance in the literature, e.g. [Davey&Mackay], [Hu], [Zhou et al], [Andriyanova&Tillich]
- Moderate codelengths applications
- Does the finite-length iterative performance improve with q ?

Non-binary LDPC Codes



$\circ$ symbol $\in \mathbb{F}_q$

$\blacksquare$ $f : \mathbb{F}_q \leftrightarrow \mathbb{F}_q$

$\oplus$ $\sum_i \alpha_i x_i = 0,\ \alpha_i \in \mathbb{F}_q^*$

Our case :

- (c, d) regular codes : $\circ$ of degree c, $\oplus$ of degree d
- binary codelength n
- $q = 2^m$
- ensemble over GL - f : linear bijective mappings
- transmission channel - $BEC(\epsilon)$

Main Result : Slope of the Error Curve

The average block erasure rate

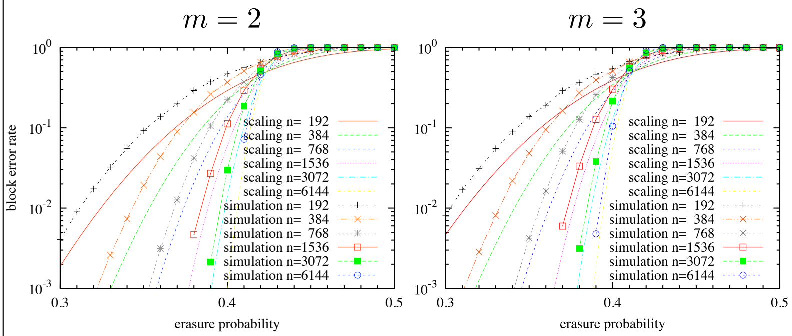
$$\bar{P}_{block}(\epsilon) = Q\left(\sqrt{n}\frac{\epsilon^* - \epsilon}{\alpha}\right) + o(n),$$

with the scaling parameter α

$$\alpha = \frac{\partial^2 \epsilon(x)}{\partial x^2}|_* \lim_{\epsilon \to \epsilon^*} \sqrt{\frac{\xi}{c} \frac{x - x^*}{1 - \gamma \lambda_2}},$$

where $\gamma = (c-1)(d-1)$, $\epsilon(x)$ - EXIT-like curve, (ϵ^*, x^*) - critical point, λ_2 and ξ are related to the evolution matrix M.

Example : $(3, 6)$ Codes



Demonstration of the Main Result

Assumption : Gaussian distribution for the channel random variable H given the decoding state X^*

H = fraction of unknown bits in cwd

X^* = probability vector for messages $\circ \rightarrow \oplus$ at the critical point ϵ^*

Our calculation

- Part I : relation of the variance σ^2 of H with a variance $\mathcal{V}$
- Part II : computation of $\mathcal{V}$

Part I

1. EXIT-like curve $\epsilon(x)$:
   $\{(x,\epsilon) : x = 1 - X(0),\ (x,\epsilon)$ is a fixed point of DE$\}$;
   $\epsilon(x)$ is regular
2. Taylor expansion of $\epsilon(x)$ around x^* :

$$\Delta\epsilon = \frac{\partial^2\epsilon}{\partial x^2}|_* \Delta x(x - x^*)$$

3. $\sigma^2 = \mathbb{E}[(\Delta\epsilon)^2]$, hence

$$\sigma^2 = \frac{\alpha^2}{n} = \frac{1}{nc}\left(\frac{\partial^2\epsilon(x)}{\partial x^2}|_*\right)^2 \lim_{\epsilon\to\epsilon^*}(x - x^*)^2\mathcal{V}$$

with

$$\mathcal{V} := \lim_{n\to\infty}\frac{\mathbb{E}[N_{known} - \mathbb{E}[N_{known}]]^2}{nc}$$

Remarks to Parts I and II

– σ^2 through EXIT-like curves : [Ezri et al]

– $\mathcal{V}$ through evolution of cond. probabilities : [Amraoui et al], [Ezri et al]

– calculation of $\mathcal{V}$ using statistics of known messages

Part II

1. Fix l, consider the computation tree $\mathcal{T}$ of a chosen root.

$$\mathcal{V}^{(l)} = \mathcal{V}_{\substack{\rightarrow\\ \rightarrow}}^{(l)} + \mathcal{V}_{\substack{\rightarrow\\ \leftarrow}}^{(l)} + \mathcal{V}_{\substack{\leftarrow\\ \leftarrow}}^{(l)} + \mathcal{V}_{\substack{\leftarrow\\ \rightarrow}}^{(l)}$$

2. $\mathcal{V}_{\substack{\leftarrow\\ \leftarrow}}^{(l)} + \mathcal{V}_{\substack{\leftarrow\\ \rightarrow}}^{(l)} \rightarrow 0$ and $\mathcal{V}_{\substack{\rightarrow\\ \rightarrow}}^{(l)} = o(\mathcal{V}_{\substack{\rightarrow\\ \leftarrow}}^{(l)})$ close to ϵ^*
3. $\mathcal{V} = \lim_{l\rightarrow\infty} \mathcal{V}_{\substack{\rightarrow\\ \leftarrow}}^{(l)}$ and hence

$$\mathcal{V} = (c-1)\sum_{i=1}^{\infty} \gamma^i [\underline{q}^T M^i \underline{p} - X(0)^2],$$

where $\underline{q}$, $\underline{p}$ - cond. prob. vectors,
M - matrix of evolution of cond. prob. at one stage of $\mathcal{T}$

Part II (cont'd)

Let $\lambda_1 > \lambda_2 > \ldots > \lambda_s$ be eigenvalues of M. Assuming the multiplicity 1 for λ_1, multiplicity 2 for λ_2 and multiplicity 1 for others, by eigenvalue decomposition

$$M^i \underline{p} = i c_2^{(1)} \lambda_2^{i-1} \underline{e}_j^{(2)} + \sum_{j=1}^{s} \sum_{k=1}^{a_j} c_j^{(k)} \lambda_j^i \underline{e}_j^{(k)}.$$

As $c_1^{(1)} \lambda_1^i \underline{q}^T \underline{e}_1^{(1)} = X(0)^2$,

$$\begin{aligned} \mathcal{V} &= \frac{c_2^{(1)}(c-1)\gamma}{(1-\gamma\lambda_2)^2} \underline{q}^T \underline{e}_2^{(2)} + O\left(\frac{1}{1-\gamma\lambda_2}\right) \\ &= \frac{\xi}{(1-\gamma\lambda_2)^2} + O\left(\frac{1}{1-\gamma\lambda_2}\right) \end{aligned}$$

for $\xi = c_2^{(1)}(c-1)\gamma \underline{q}^T \underline{e}_2^{(2)}$

Reminder

We obtained

$$P_{block}(\epsilon) = Q\left(\sqrt{n}\frac{\epsilon^* - \epsilon}{\alpha}\right) + o(n)$$

with the scaling coefficient

$$\alpha = \frac{\partial^2 \epsilon(x)}{\partial x^2}|_* \lim_{\epsilon \to \epsilon^*}(x - x^*)\sqrt{\frac{\mathcal{V}}{c}},$$

while

$$\mathcal{V} = \frac{\xi}{(1-\gamma\lambda_2)^2} + O\left(\frac{1}{1-\gamma\lambda_2}\right).$$

More Examples

$(3,6)$ LDPC :

m	ϵ^*	α
1	0.4294	0.559
2	0.4235	0.591
3	0.4122	0.598

$(4,6)$ LDPC :

m	ϵ^*	α
1	0.5061	0.561
2	0.4843	0.609

Discussion

1)

One needs to find code families for which α improves with m and/or design conditions which would improve α for larger m.

2)

The analysis of 2-regular ensembles is needed.