MAP, Typical Set Decoding & Magnetization Enumerator in LDPC codes

David Saad

Jort van Mourik and Yoshiyuki Kabashima†

†Tokyo Inst. of Technology, Japan

NEURAL COMPUTING
NCRG
RESEARCH GROUP

Aston University, Birmingham, UK.

Contributions by Renato Vicente and
Tatsuto Murayama† are acknowledged

Outline

- We first introduce LDPC error correcting codes.

- Analysis of these codes is carried out using methods of statistical physics, exploring their theoretical and practical limits.

- Studying the entropy of the solutions we provide a link between MAP, MPM and typical set decoding results.

- Finally, we will briefly mention related work in this area.

The General Framework

- The message is a, possibly sparse, N dimensional Boolean (binary) vector $\boldsymbol{\xi}$.

- Encoded to an M dimensional Boolean (binary) vector and transmitted through a noisy channel. Here, we focus on binary symmetric channel (BSC).

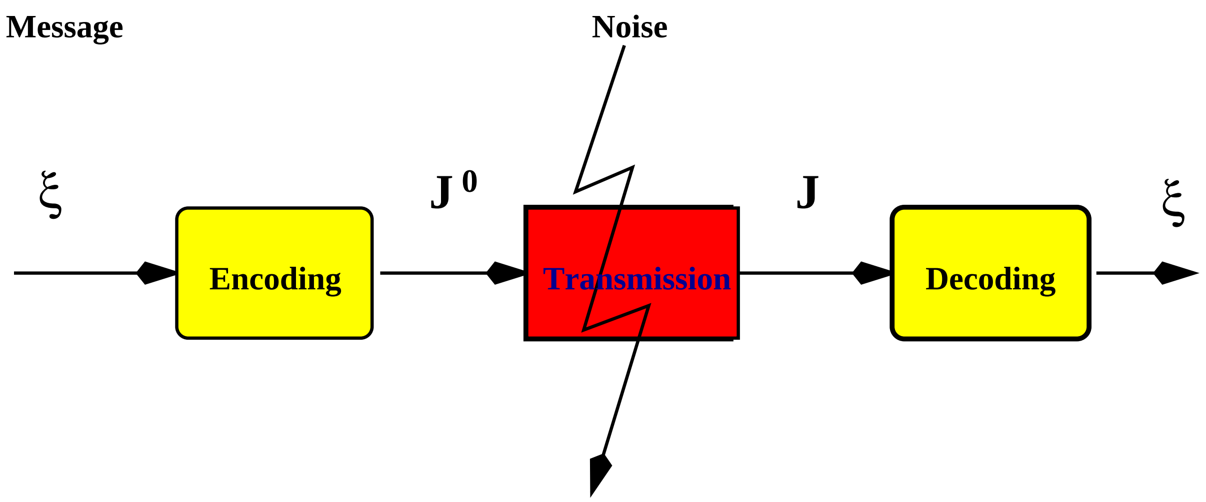
- The received massage $\boldsymbol{J} = \boldsymbol{J}^0 + \zeta$ (mod 2) is decoded to retrieve $\boldsymbol{\xi}$.

- The code rate is $R = N/M$.

- Error-free communication is theoretically possible below Shannon's bound

$$R_c = 1 + p \log_2 p + (1-p) \log_2 (1-p),$$

which has never been achieved.



Gallager/MN Codes

- Discovered by Gallager (1962) and MacKay-Neal (1996).

- Gallager's code - Construct two sparse matrices A and B of dimensionality $(M-N)\times N$ and $(M-N)\times(M-N)$ respectively.

- MN code -Construct two sparse matrices A and B of dimensionality $M\times N$ and $M\times M$ respectively.

- The matrix A has K non-zero (unit) elements per row and C per column, B has L per row/column.

$$A = \begin{array}{c} \\ M \left\{ \vphantom{\begin{pmatrix} 1\\0\\0\\0\\ \vdots \end{pmatrix}} \right. \\ \end{array} \begin{array}{c} N \\ \overbrace{\begin{pmatrix} 1 & 0 & \cdots \\ 0 & 1 & \cdots \\ 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & & \ddots \end{pmatrix}} \\ K \end{array} \begin{array}{c} \\ \downarrow C \\ \\ \end{array}, \quad B = \begin{array}{c} \\ M \left\{ \vphantom{\begin{pmatrix} 1\\0\\0\\0\\ \vdots \end{pmatrix}} \right. \\ \end{array} \begin{array}{c} M \\ \overbrace{\begin{pmatrix} 1 & 0 & 0 & 1 & \cdots \\ 0 & 0 & 1 & 0 & \cdots \\ 0 & 0 & 0 & 1 & \cdots \\ 0 & 1 & 0 & 0 & \cdots \\ \vdots & \vdots & & & \ddots \end{pmatrix}} \\ L \end{array} \begin{array}{c} \\ \downarrow L \\ \\ \end{array}.$$

In Gallager's code we may refer to $\mathcal{A} = [\boldsymbol{A} \mid \boldsymbol{B}]$ and $K+L$ only.

Gallager's Code

Encoding

$$\underbrace{\boldsymbol{J}^{\boldsymbol{0}}}_{\in\{0,1\}^M} = \boldsymbol{G}^{\boldsymbol{T}} \underbrace{\boldsymbol{\xi}}_{\in\{0,1\}^N} \pmod 2.$$

The (dense) generator matrix is

$$\boldsymbol{G} = [\boldsymbol{I} \mid \boldsymbol{B}^{-1}\boldsymbol{A}] \pmod 2.$$

The received vector takes the form

$$\boldsymbol{J} = \boldsymbol{G}^{\boldsymbol{T}}\boldsymbol{\xi} + \boldsymbol{\zeta} \pmod 2.$$

Decoding

$$\boldsymbol{z} = \mathcal{A}\boldsymbol{J} = \underbrace{\mathcal{A}\boldsymbol{G}^{\boldsymbol{T}}\boldsymbol{\xi}}_{=0} + \mathcal{A}\boldsymbol{\zeta} \pmod 2,$$

$\mathcal{A} = [\boldsymbol{A} \mid \boldsymbol{B}]$ sparse $M \times M$ binary matrix.

The problem: $\boldsymbol{z} = \mathcal{A}\boldsymbol{\tau} \pmod 2$.

- MPM – $\widehat{\zeta}_j = \text{argmax}\ P(\tau_j \mid \boldsymbol{z})$
minimises $p_b = 1 - \frac{1}{M} \sum_{j=1}^{M} \delta[\widehat{\zeta}_j; \zeta_j]$.

- MAP – $\widehat{\boldsymbol{\zeta}} = \text{argmax}\ P(\boldsymbol{\tau} \mid \boldsymbol{z})$ minimises p_B.

Statistical Physics

- Mapping from Boolean to binary variables

$$\{0, 1, +\} \rightarrow \{1, -1, \times\} \, .$$

- We look for the conditional probability

Gallager

$$P(\boldsymbol{\tau} \mid \boldsymbol{z}) = \frac{1}{\mathcal{Z}} \, \delta\left(\boldsymbol{z}; \mathcal{A}\boldsymbol{\tau}\right) \underbrace{P(\boldsymbol{\tau})}_{prior}$$

- Can be represented as

$$P(\tau \mid z) = \frac{1}{\mathcal{Z}} \exp\left[-\beta\mathcal{H}(\tau; z)\right]$$

and

Statistical Physics - Gallager

- The ground state of the Hamiltonian

$$\mathcal{H} = \lim_{\gamma\to\infty} \gamma \sum_{\sigma} \mathcal{D}_\sigma \, \delta\left[-1 \; ; \; \mathcal{J}_\sigma \prod_{j\in\sigma} \tau_j\right] - F_\tau \sum_{j=1}^{M} \tau_j ,$$

corresponds to the Bayes-optimal estimate of the noise (binary representation).

- The tensor product $\mathcal{D}_\sigma \mathcal{J}_\sigma$, where $\mathcal{J}_\sigma = \prod_{j\in\sigma} \zeta_j$ and $\mathcal{D}_\sigma = 0, 1$ is the binary equivalent of $[A|B]\ \zeta$.

- $F_\tau = (1/2) \ln[(1-p)/p]$ is the prior knowledges about the noise .

The Free Energy

• One can then calculate the free energy

$$\frac{1}{M}\langle \ln \mathcal{Z}\rangle_{\{\mathcal{D},\zeta\}}\,;\,\mathcal{Z}(\mathcal{D},\zeta) = \mathrm{Tr}_{\{\boldsymbol{\tau}\}}\exp\left[-\beta\mathcal{H}\right]$$

using methods from statistical mechanics of diluted systems (replica method).

• The choice of $1/T = \beta = 1$ is finite temperature decoding (Nishimori's condition) - MPM.

• Averages give rise to an infinite set of order parameters. Using the replica symmetric ansatz we obtain saddle-point equations.

• Solutions to these equations (numerical or analytical) indicate the phase of the system:

– Ferro solution ($m = 1$): Perfect decoding
– Para solution ($m = 0$): Catastrophic failure
– Sub-optimal ferro solution ($m < 1$): failure

where $m = \frac{1}{M}\sum_{i=1}^{M}\zeta_i\tau_i$

Alternative Method - Gallager

- The Hamiltonian can also be represented as

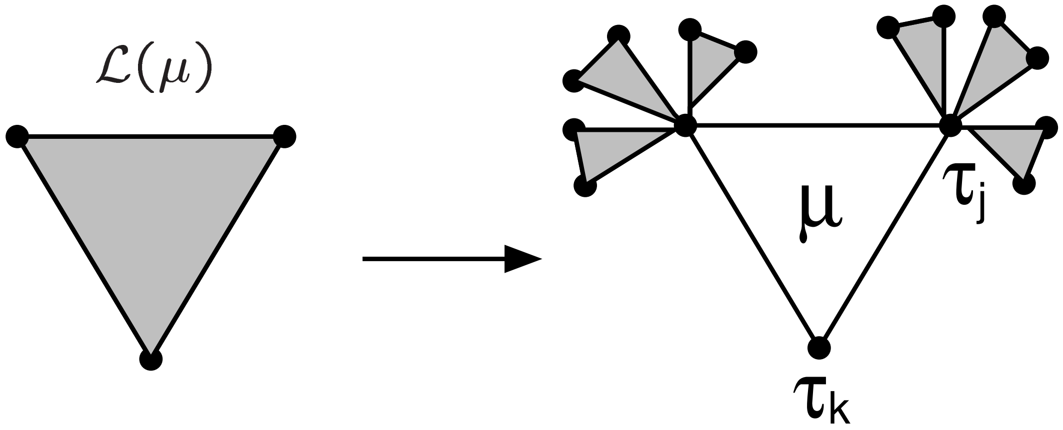
$$\mathcal{H} = -\lim_{\gamma\to\infty} \gamma \sum_{\mu=1}^{M-N} \left(z_\mu \prod_{j\in\mathcal{L}(\mu)} \tau_j - 1 \right) - \underbrace{F}_{prior} \sum_{j=1}^{M} \tau_j$$

- To estimate $\widehat{\zeta}_j$ we examine the local magnetization

$$\widehat{\zeta}_j = \mathrm{sign}(m_j) \qquad \underbrace{m_j}_{\text{local mag}} = \langle \tau_j \rangle$$

$$\overline{p_b} = \frac{1}{2} - \frac{1}{2} \underbrace{\left[\frac{1}{M} \sum_{j=1}^{M} \widehat{\zeta}_j \zeta_j \right]_{A,\zeta}}_{=m}$$

Husimi Cactus



- One constructs the recursion relations

$$P_{\mu k}(\tau_k) = \frac{1}{\mathcal{N}} P(\tau_k) \sum_{\{\tau_j\}} P(z_\mu \mid \{\tau_j\}, \tau_k) \prod_{\nu \in \mathcal{M}(j) \setminus \mu} \prod_{j \in \mathcal{L}(\mu) \setminus k} P_{\nu j}(\tau_j)$$

- A set of recursive equations is then derived

$$P_n(x) = \int \prod_{l=1}^{C-1} d\widehat{x}_l \, \widehat{P}_{n-1}(\widehat{x}_l) \left\langle \delta \left[x - \beta F \zeta - \sum_{l=1}^{C-1} \widehat{x}_l \right] \right\rangle_\zeta$$

$$\widehat{P}_{n-1}(\widehat{x}) = \int \prod_{j=1}^{K-1} dx_j \, P_{n-1}(x_j) \, \delta \left[\widehat{x} - \text{atanh} \left(\prod_{j=1}^{K-1} \tanh(x_j) \right) \right]$$

$P_n(x)$, $\widehat{P}_n(\widehat{x})$ are the n-th generation distribution of effective fields.

- The free energy is also calculated.

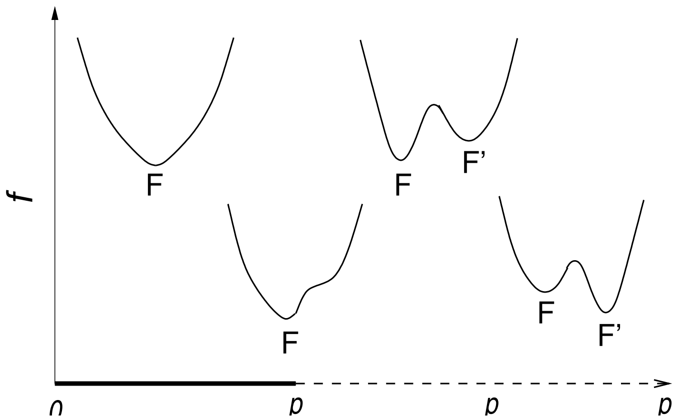
Solutions - Gallager

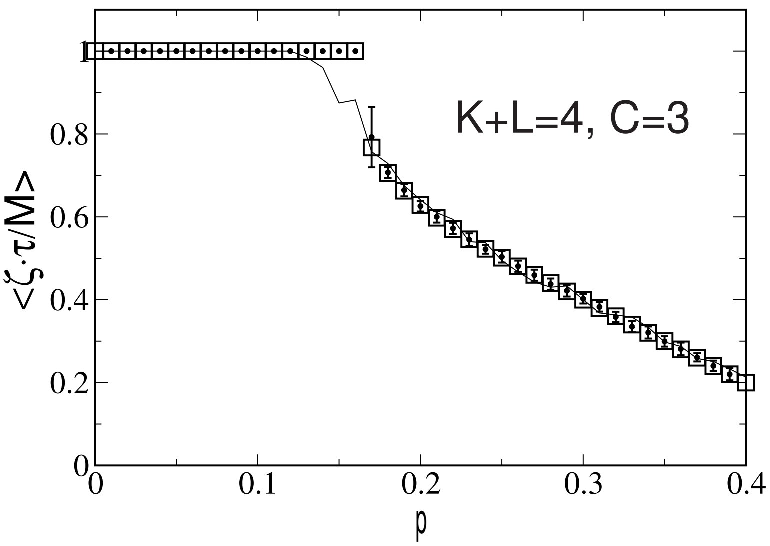
• Solutions to these equations (numerical or analytical) indicate the phase of the system:

– Ferro solution ($m = 1$): Perfect decoding

– Sub-optimal ferro solution ($m < 1$): failure

where $m = \frac{1}{M} \sum_{j=1}^{M} \widehat{\zeta}_j \zeta_j$

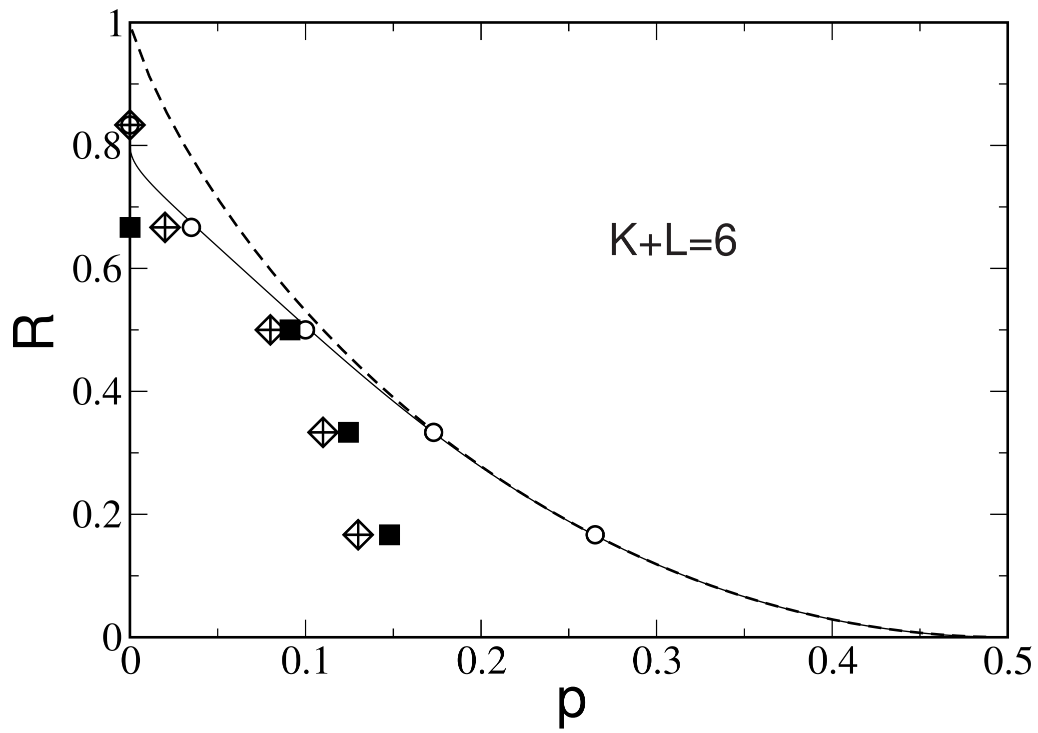




Theoretical and Practical Limits

Independently of the decoding method we identify:

- Theoretical limits - thermodynamical transition
- Practical limits - spinodal point



Decoding

• To examine different decoding methods within this framework we calculate the entropy.

• The magnetization enumerator $\mathcal{M}(m)$ can be calculated from the Hamiltonian

$$\mathcal{H} = - \lim_{\gamma\to\infty} \gamma \sum_{\sigma} \mathcal{D}_\sigma \, \delta\left[-1 \; ; \; \mathcal{J}_\sigma \prod_{j\in\sigma} \tau_j\right] ,$$

by forcing the constraint $\delta\left(\frac{1}{M}\sum_{j=1}^{M} \tau_j - m\right)$.

• To calculate the weight enumerator $\mathcal{W}(\omega)$ we use $\delta\left(\frac{1}{M}\sum_{j=1}^{M} \zeta_j \tau_j - \omega\right)$.

• The entropies can be calculated using the
replica method - $\frac{1}{M}\left\langle \ln \mathcal{Z} \right\rangle_{\{\mathcal{D},\zeta\}}$
or
annealed approximation - $\frac{1}{M} \ln \left\langle \mathcal{Z} \right\rangle_{\{\mathcal{D},\zeta\}}$.

Weight & Magnetization Enumerators

• Weight enumerator - independent of ζ after gauging, annealed approximation = replica result

$$\mathcal{W}(m) = \mathcal{M}_a(m)|_{p=0} = \mathcal{M}_q(m)|_{p=0} \ .$$

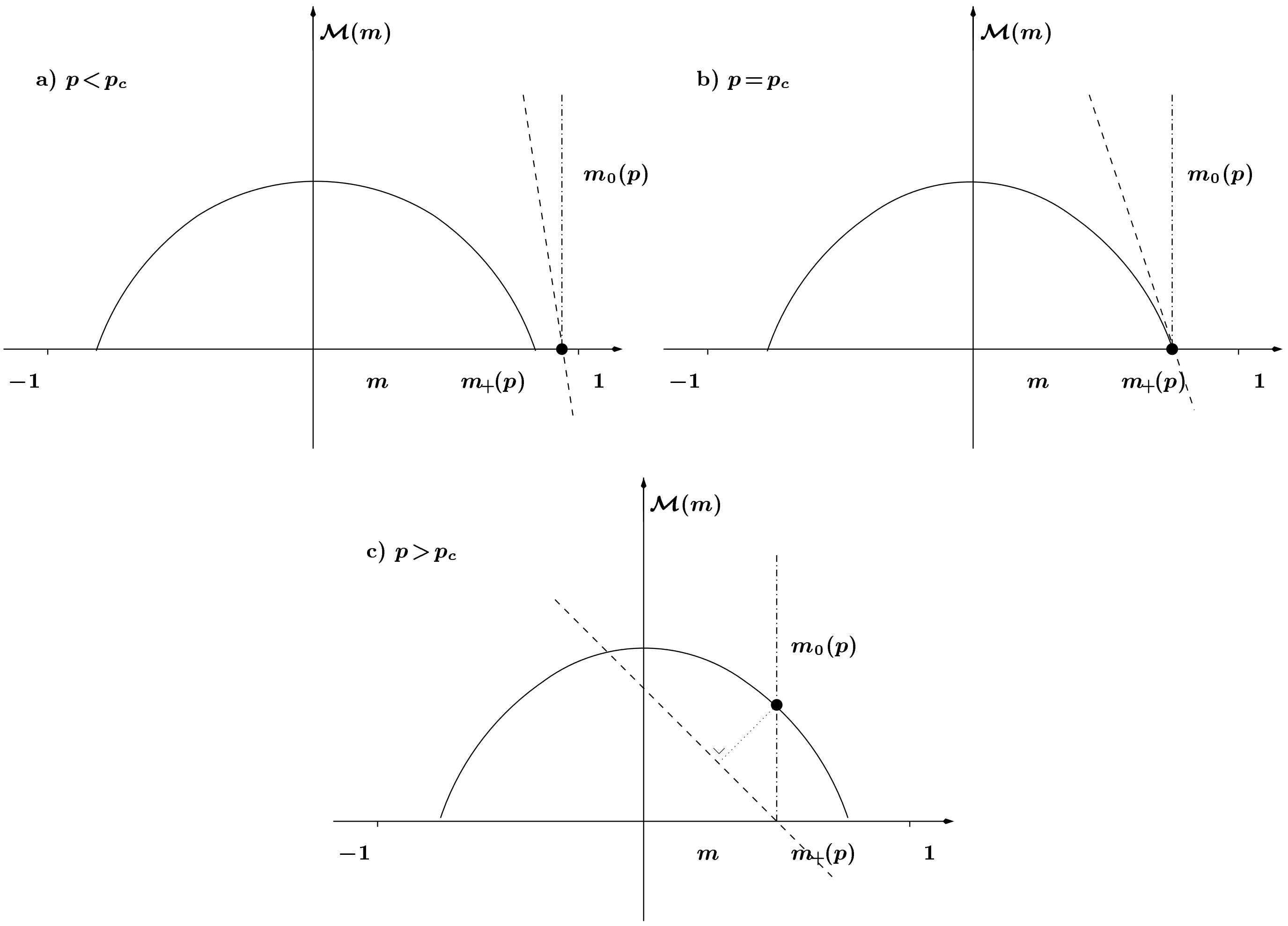
• Magnetization enumerator $\mathcal{M}(m)$ - different results for annealed approximation/replica method.

• Maximum likelihood (MAP) decoding - selects solution with highest magnetization.

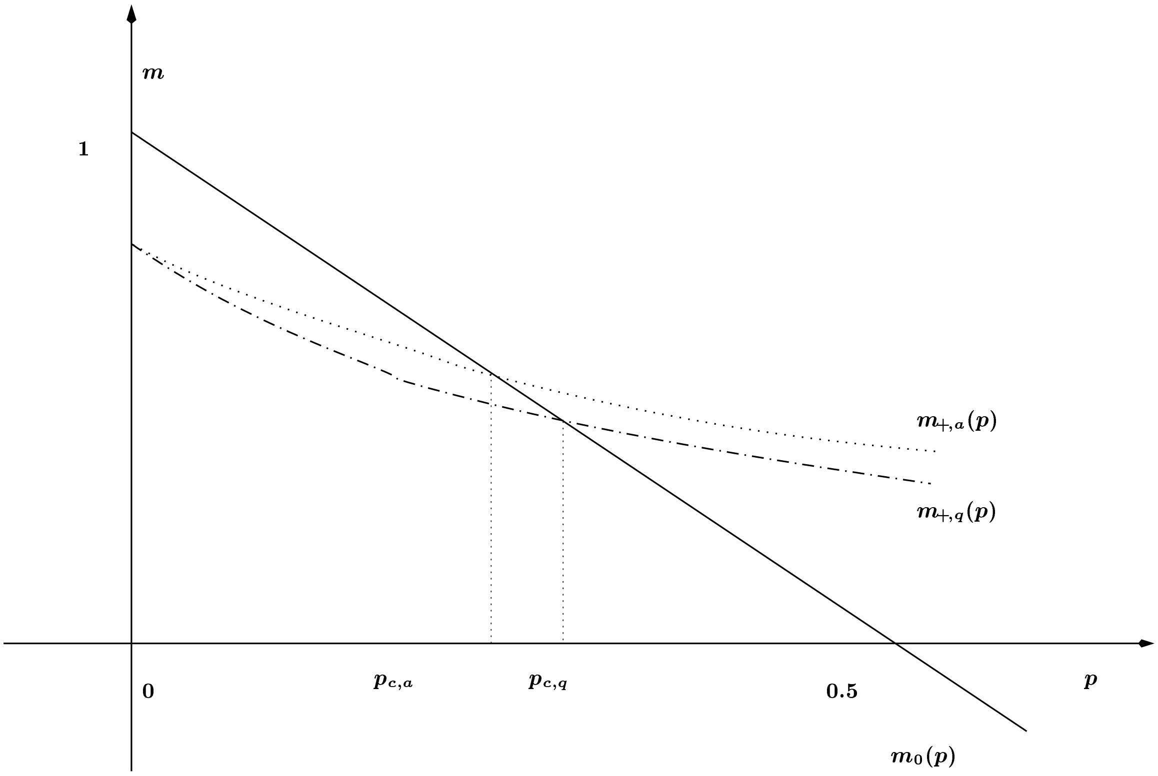
• Typical pairs decoding - selecting a (single) vector from typical set.

• Finite temperature (MPM) decoding - energy term $-Fm$ added, solution chosen by minimizing the free energy.

Entropy and decoding



Critical noise level



(K, C)	$(6, 3)$	$(5, 3)$	$(6, 4)$	$(4, 3)$
Code rate	$1/2$	$2/5$	$1/3$	$1/4$
IT ($\mathcal{W}_a$)	0.0915	0.129	0.170	0.205
SP	0.0990	0.136	0.173	0.209
$p_{c,a}$ ($\mathcal{M}_a$)	0.031	0.066	0.162	0.195
$p_{c,q}$ ($\mathcal{M}_q$)	0.0998	0.1365	0.1725	0.2095
Shannon	0.109	0.145	0.174	0.214

Summary

• Gallager codes saturate Shannon's bound only for $K+L \to \infty$, suboptimal perfect decoding is feasible for all configurations (MN theoretically saturate Shannon's bound for finite K, L, perfect decoding is feasible only in specific configurations).

• We have provided an intuitive explanation to the difference between MAP and MPM decoding based on the magnetization enumerator $\mathcal{M}(m)$.

• Critical noise levels for typical pair, MAP and MPM decoding must coincide.

• We have recently studied typical set decoding in LDPC and currently calculate the reliability exponent directly.

http://www.ncrg.aston.ac.uk