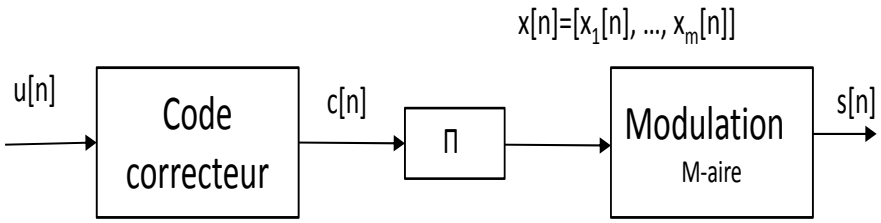
LDPC codes - Part I: principles and constructions

21 octobre 2020

Plan

Plan

Bit-interleaved coded-modulation (BICM)

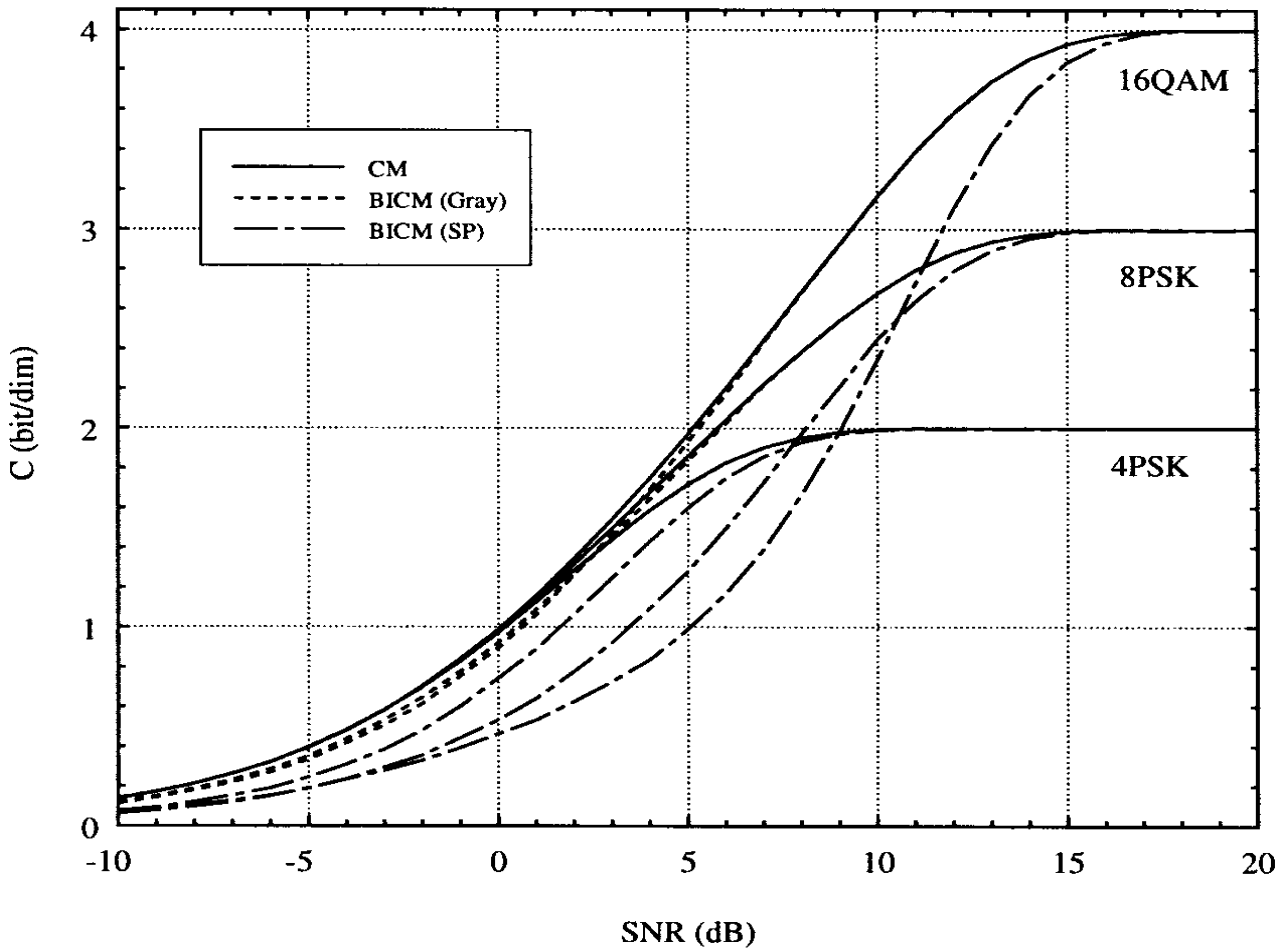


Bit-Interleaved Coded Modulation

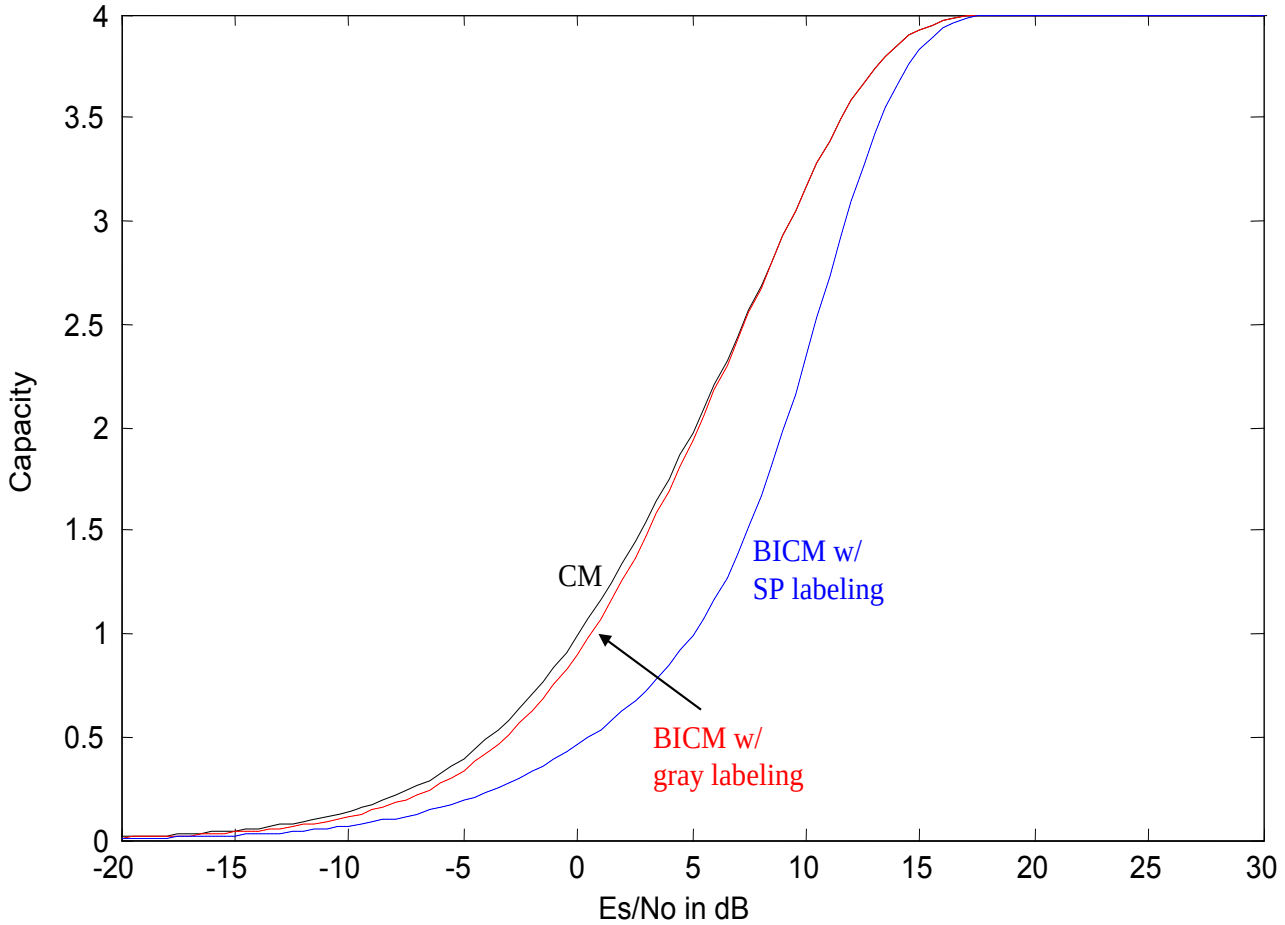
- High spectral efficiency communications systems : M-ary constellation $\mathcal{S}$ with $M = 2^m$, $m = \#\,\text{of bits}$.
- Equivalent to $\log_2(M)$ parallel channels,
- Achievable capacity depends on the mapping used :

$$C = \sum_{\ell=0}^{\log_2(M-1)} I(b_\ell; y) = m - \frac{1}{2}\sum_{k=0}^{m-1}\sum_{c=0}^{1}\mathbb{E}\left(\log_2\left(\frac{\sum_{s_i\in\mathcal{S}} p(y|s_i)}{\sum_{s_j\in\mathcal{S}_c^k} p(y|s_j)}\right)\right)$$

Bit-interleaved coded-modulation (BICM)



Bit-interleaved coded-modulation (BICM)



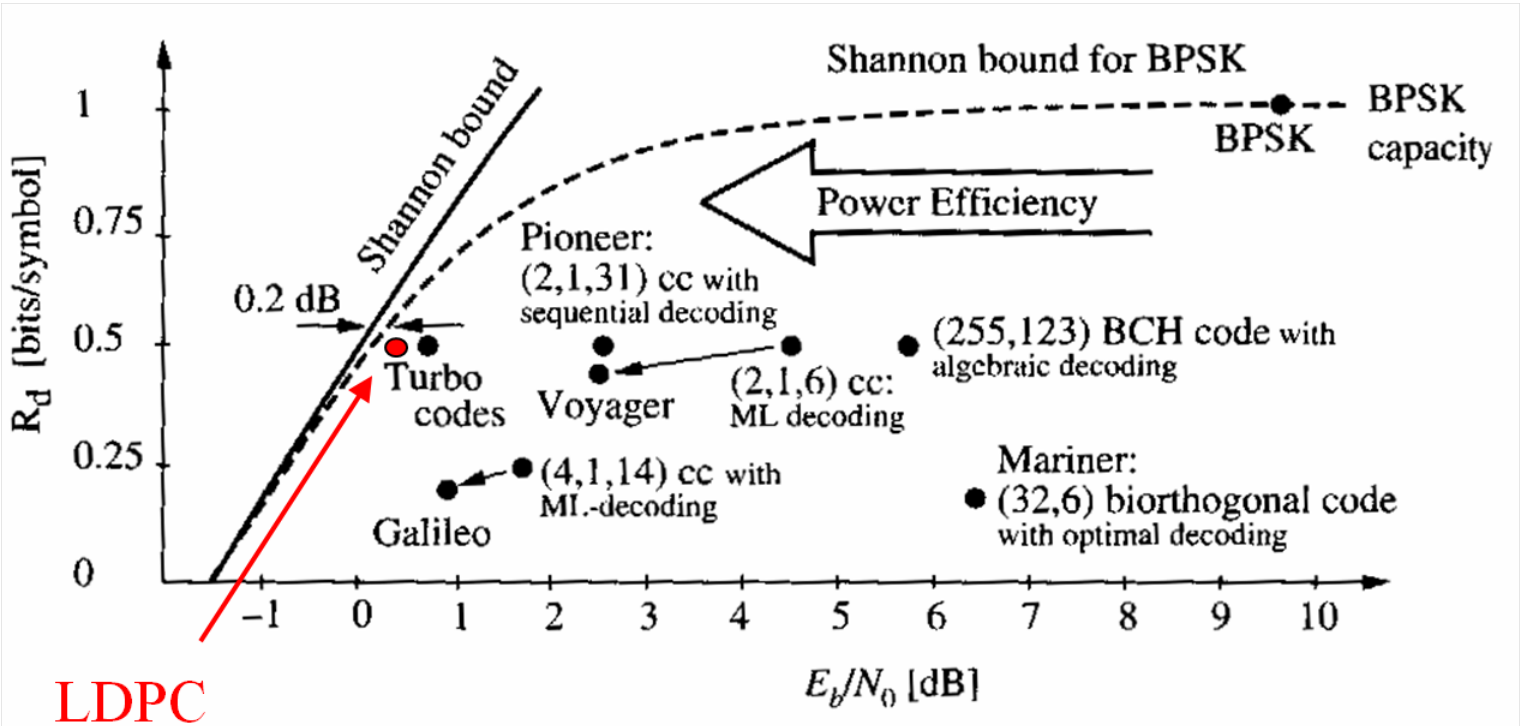
Plan

Codes LDPC

Introduction

- 1963 : Gallager, Regular LDPC codes
- 1981 : Tanner codes : codes defined on graphs.
- 1995 : MacKay, Belief propagation decoding
- 2001 : Richardson et Urbanke, Irregular LDPC.

Coding systems : a brief history



Linear bloc codes

Hamming code ($N = 7, K = 4$)

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$u = [u_1, u_2, u_3 . u_4]$$

$$c = [c_1, c_2, c_3, c_4, c_5, c_6, c_7]$$

$$u \cdot G = c$$

$$Hc^{\mathrm{T}} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Low-Density Parity-Check (LDPC)codes

Introduction

Definition

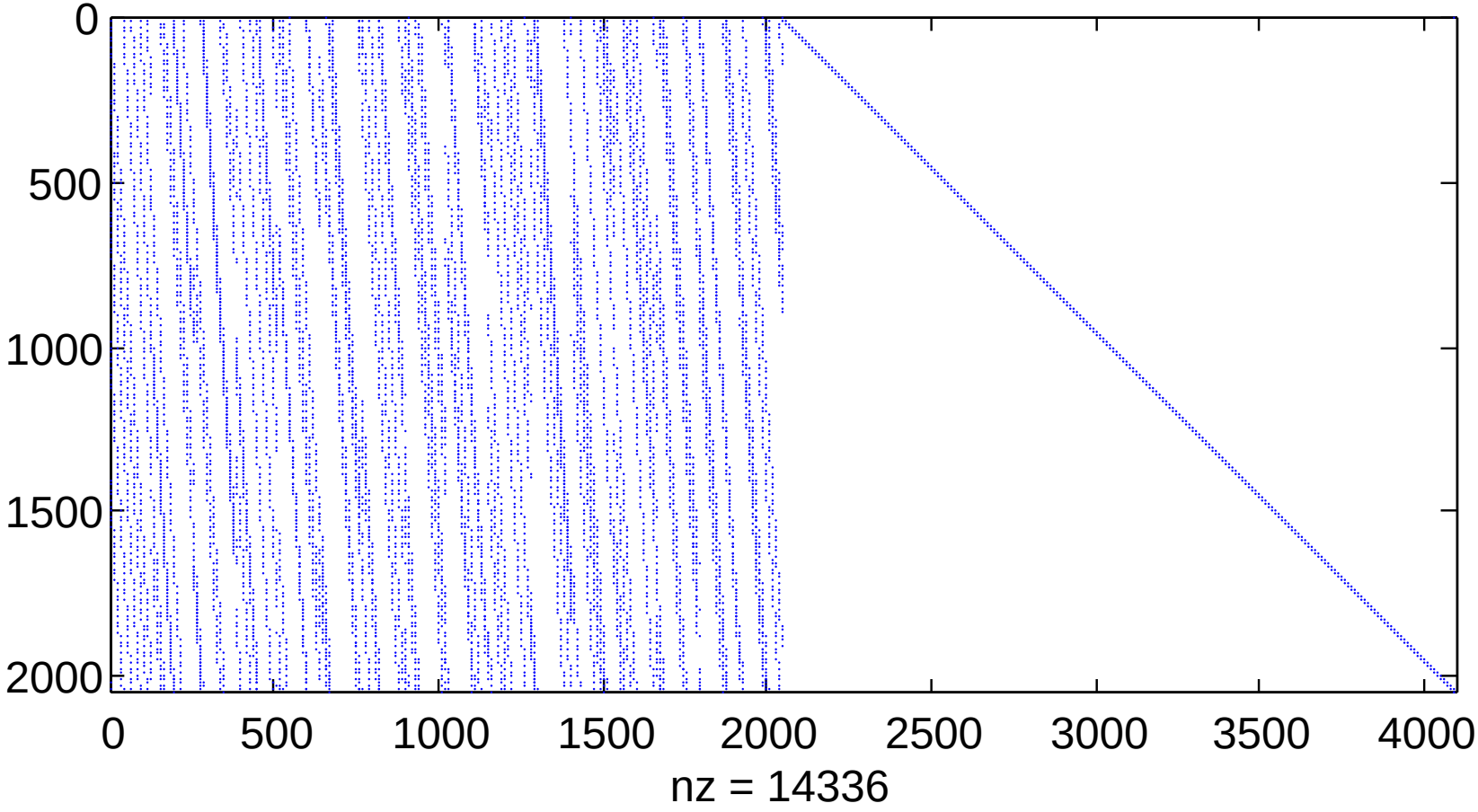
$$\mathcal{C}_H = \{\mathbf{c} \in GF(2)^{\times N} | H.\mathbf{c}^\top = \mathbf{0}\}$$

- H is the parity check matrix of size $M \times N$,
- If H is full rank : $R = K/N$ with $K = N - M$,
- Parity check equations : $\bigoplus_{j:h_{ij}\neq 0} c_j = 0, \quad \forall i = 1 \ldots M$,
- H is sparse if

$$\frac{\text{non nul element}}{N.M} \underset{N \mapsto +\infty}{\longrightarrow} 0$$

LDPC Codes

example : SIRA, N=4096



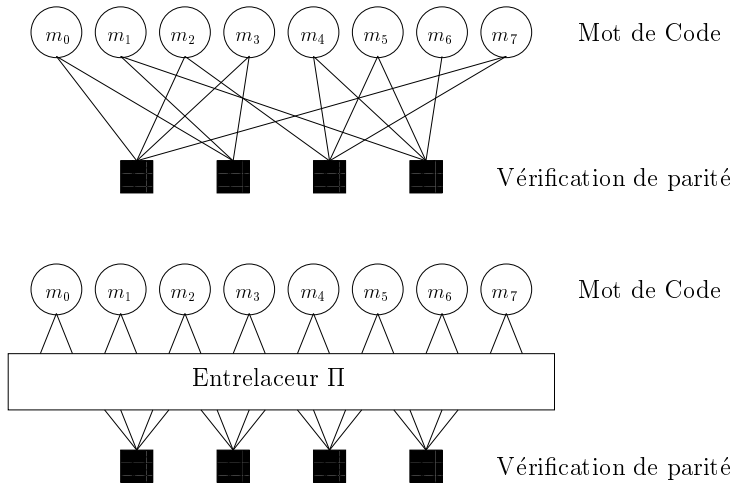
densité = 0.0017

Low-Density Parity-Check (LDPC) codes

Representation

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Parity check matrix



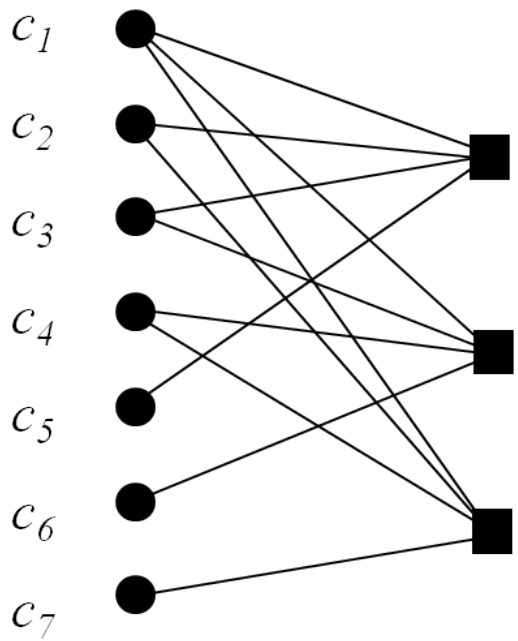
Tanner graph

Tanner Graph

- Variable/data nodes (VN) : associated with codeword bits,
- Parity check nodes (CN) : associated with parity checks,
- Edges : link between a VN and a CN. VN n is connected to CN m if $h_{mn} = 1$ in H.

LDPC Codes

Hamming code



$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$c_1 + c_2 + c_3 + c_5 = 0$$

$$c_1 + c_3 + c_4 + c_6 = 0$$

$$c_1 + c_2 + c_4 + c_7 = 0$$

LDPC Codes

Regular case

- Parameters : (d_v, d_c),
- d_v : number of $'1'$ per column,
- d_c : number of $'1'$ per row,
- $R \geq 1 - d_v/d_c$

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Code with $(2, d_c)$

LDPC Codes)

Irregular codes

- Edge perspective polynomials :

$$\lambda(x) = \sum_{i=1}^{d_v} \lambda_i x^{i-1} \quad \rho(x) = \sum_{j=2}^{d_c} \rho_j x^{j-1}$$

avec

- λ_i : proportion of edges connected to a VN of degree i,
- d_v : max degree of a VN,
- ρ_j : proportion of edges connected to a CN of degree j,
- d_c : max degree of a CN,

- Rate :

$$R \geq 1 - \frac{\sum_{j=1}^{d_c} \rho_j / j}{\sum_{i=1}^{d_v} \lambda_i / i} \tag{1}$$

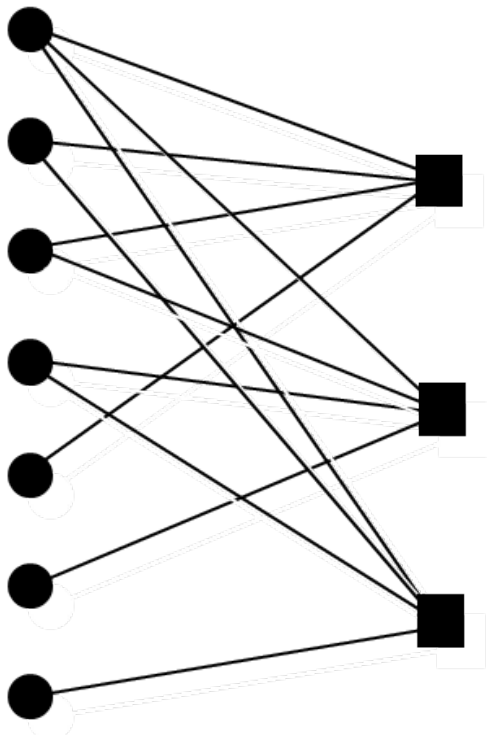
LDPC Codes

Hamming code (following)

$$\lambda(x) = \frac{1}{4} + \frac{1}{2}x + \frac{1}{4}x^2$$

$$\rho(x) = x^3$$

$$R = 1 - \frac{3}{7} = \frac{4}{7}$$



Plan

LDPC Codes

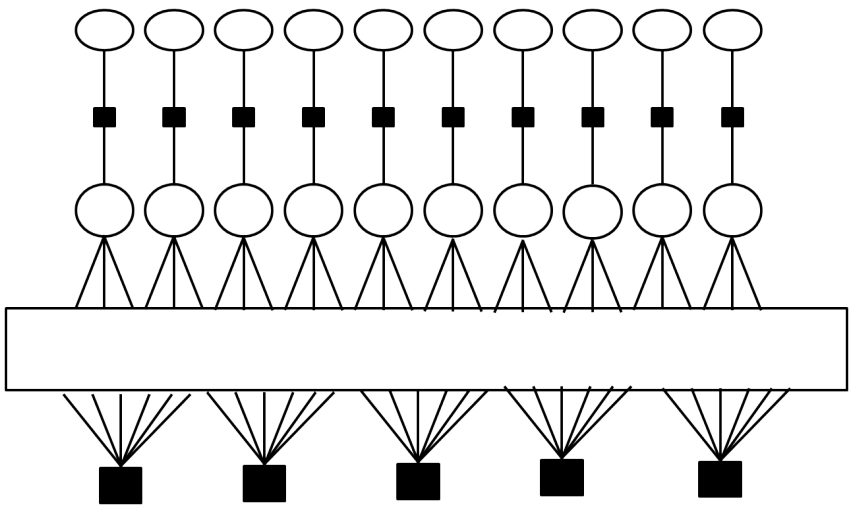
Belief Propagation, BP

Iterative decoding of LDPC codes

- ML decoding : too complex,
- Use of iterative decoding : Belief Propagation is an iterative decoding algorithm that forwards ”messages” (beliefs) between nodes of the Tanner graph along edges,
- Hypotheses : perfect interleaving
  $\Rightarrow$ messages are considered locally independent
  $\Rightarrow$ tree-like assumption enabling local Bayes rule application,
- messages are extrinsic by nature,
- Low complexity.

LDPC Codes)

BP

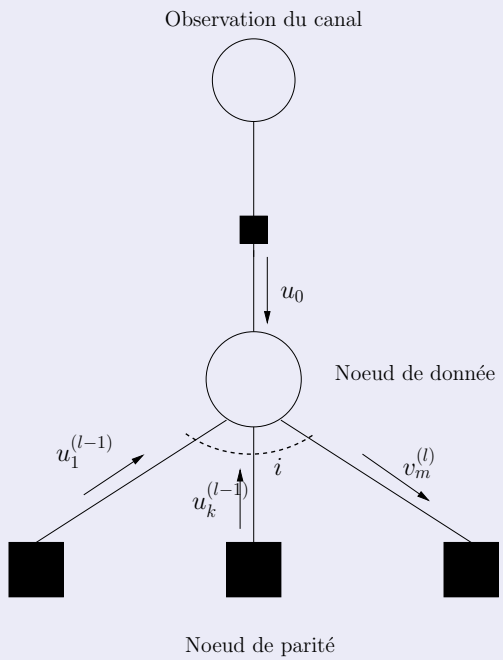


Codes Low-Density Parity-Check (LDPC)

BP

VN update

messages are LLRs $v = \log(\frac{p(c=0|\{z\})}{p(c=1|\{z\})})$



$$v_m^{(l)} = u_0 + \sum_{k=1,k\neq m}^{i} u_k^{(l-1)}, \forall m = 1 \ldots i$$

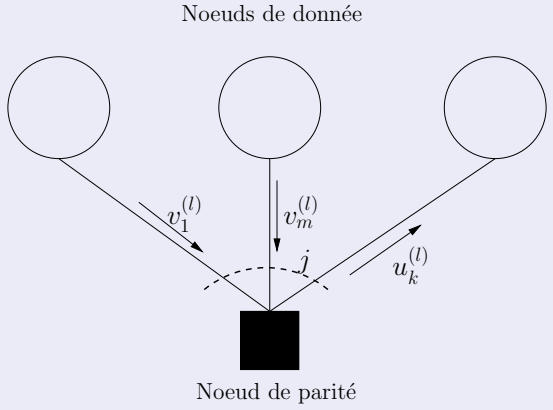
$$u_0 = \log(\frac{p(x=0|y)}{p(x=1|y)}) = \log(\frac{p(y|x=0)}{p(y|x=1)})$$

LDPC Codes

BP

CN update

$$u = log(\frac{p(c'=0|\{z'\})}{p(c'=1|\{z'\})})$$



$$\tanh \frac{u_k^{(l)}}{2} = \prod_{m=1, m\neq k}^{j} \tanh \frac{v_m^{(l)}}{2}, \forall k = 1 \ldots j$$

LDPC Codes

BP

Decoding and decision

$$v_{\text{app},n} = u_0 + \sum_{k=1}^{i} u_k^{(L)}, \forall n = 1 \dots N$$

$$\hat{m}_n = \frac{1 - \text{sign}(v_{\text{app},n})}{2}, \forall n = 1 \dots N$$

Initial messages for different binary memoryless channels

- BEC : $u_0 \in \{+\infty, -\infty, 0\}$,
- BSC : $u_0 = (-1)^{y[n]} \log(\frac{1-p}{p})$,
- Gaussian : $u_0 = \frac{2}{\sigma_b^2} y[n]$,

LDPC Codes

Simplified BP : Min-Sum

$$u_k^{(l)} = \left[\prod_{m=1, m \neq k}^{j} \operatorname{sign}(v_m^{(l)}) \right] \left[\min_{m \neq k} (|v_m^{(l)}|) \right], \forall k = 1 \ldots j$$

Scaled Min-Sum

$$u_k^{(l)} = \alpha_k^{(l)} \left[\prod_{m=1, m \neq k}^{j} \operatorname{sign}(v_m^{(l)}) \right] \left[\min_{m \neq k} (|v_m^{(l)}|) \right], \forall k = 1 \ldots j$$

$0 < \alpha < 1$ is a scaling factor.

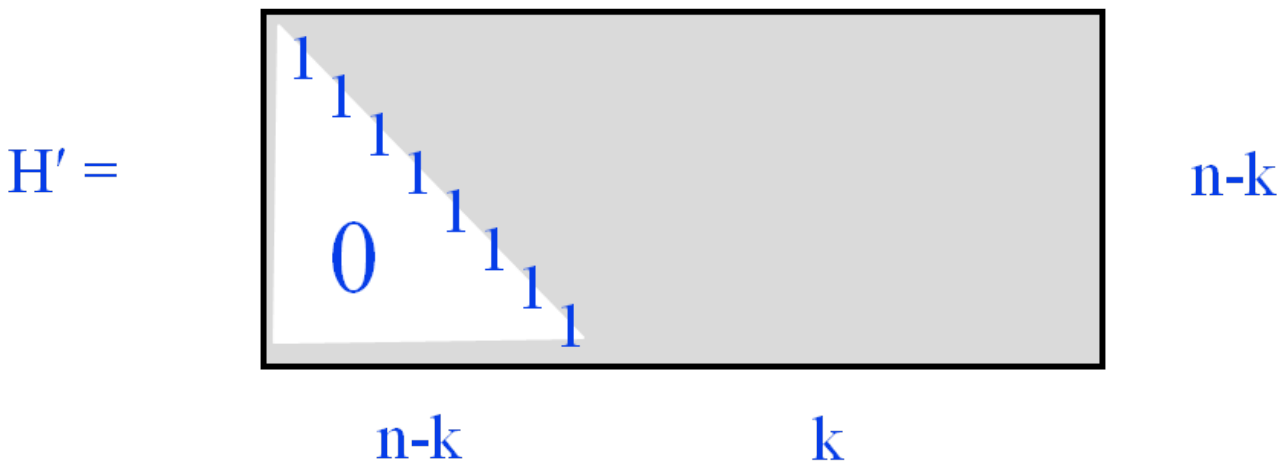
Min-Sum with offset

$$u_k^{(l)} = \left[\prod_{m=1, m \neq k}^{j} \operatorname{sign}(v_m^{(l)}) \right] \left[\max \left\{ \min_{m \neq k} (|v_m^{(l)}|) - \beta, 0 \right\} \right], \forall k = 1 \ldots j$$

$0 < \alpha < 1$.

Codes Low-Density Parity-Check (LDPC)

Encoding ?

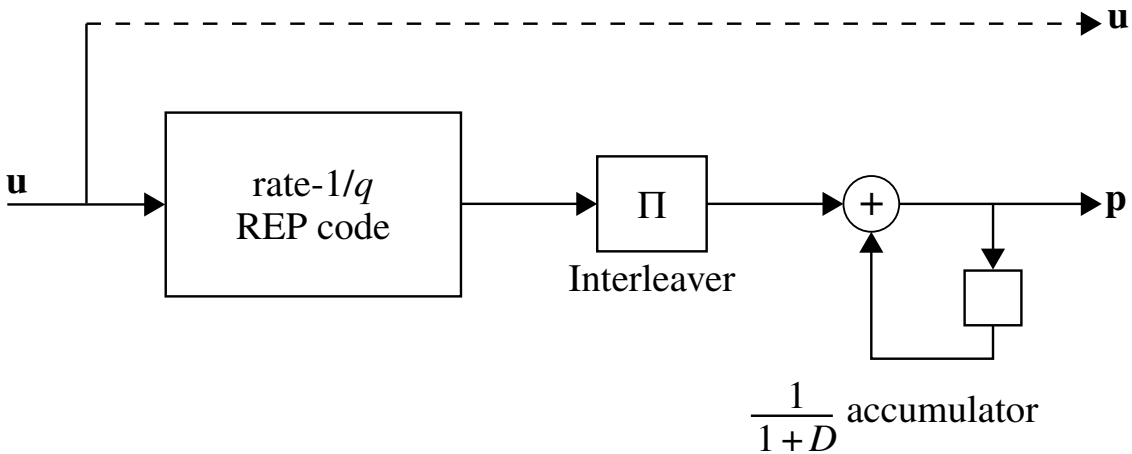


Gaussian elimination is scaling with $O(n^3)$

Plan

LDPC Codes

Repeat-Accumulate Codes

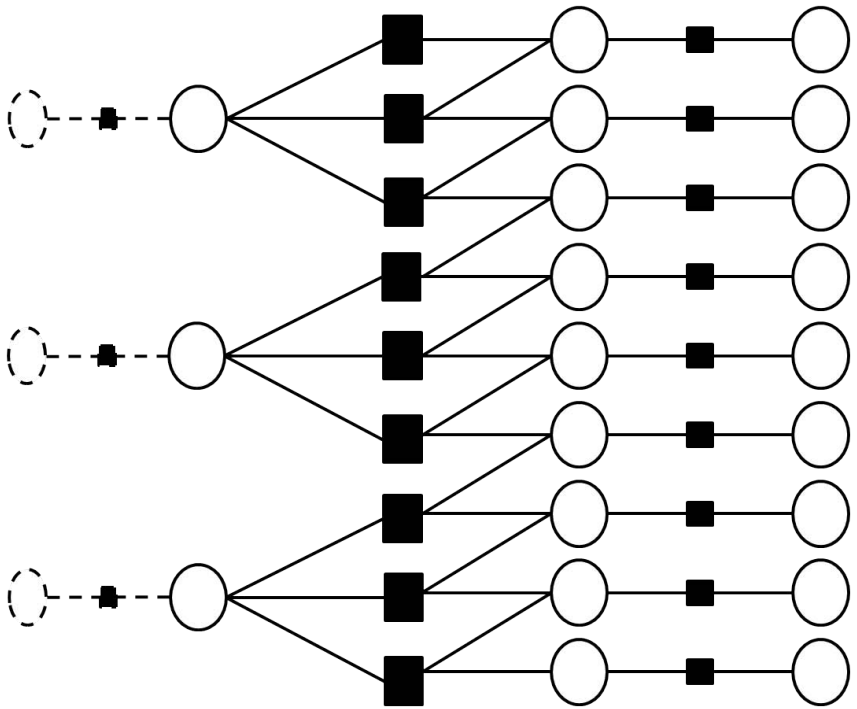


Principe

- Take K bits, repeat q times,
- Interleave,
- encode with $G_{acc}(D) = 1/(1 + D)$.

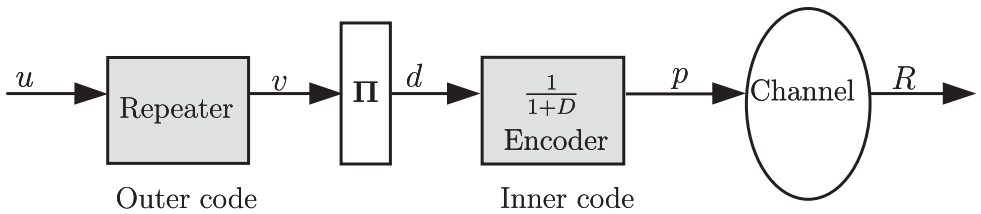
LDPC Codes

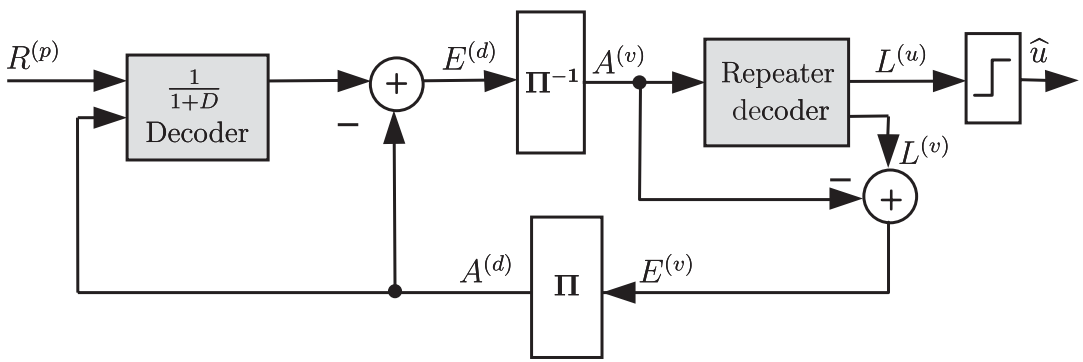
Repeat-Accumulate Codes



LDPC Codes

RA COdes as a serial concatenation



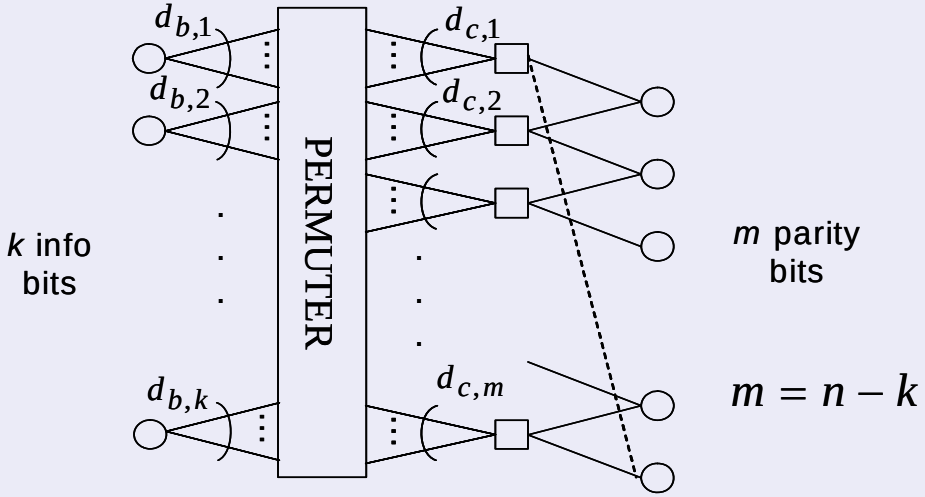


LDPC Codes

Irregular Repeat Accumulate

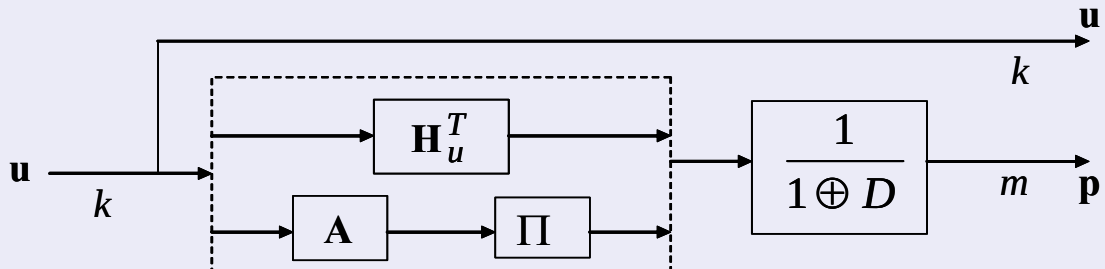
Structure

(a)



(b)

	$d_{b,i}$	$d_{c,j}$	$m = n - k$
RA	q	1	$m > k,\ m = qk$
IRA	variable	variable	$m \geq 1,\ k \geq 1$



LDPC Codes

Codes Irregular Repeat Accumulate

Principe

- k information bits are irregularly repeated,
- then *combined* (combiner),
- finally encoded by an accumulator.

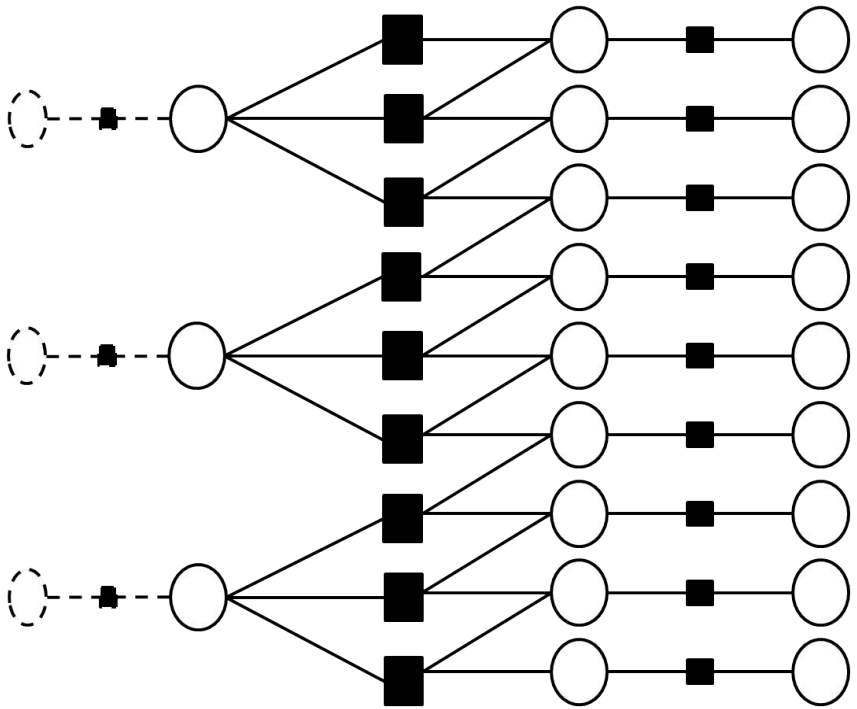
Structure

- Classical IRA : $H = [H_u H_p]$, with

$$H_p = \begin{bmatrix} 1 & & & & (1) \\ 1 & 1 & & & \\ & \ddots & \ddots & & \\ & & 1 & 1 & \\ & & & 1 & 1 \end{bmatrix}$$

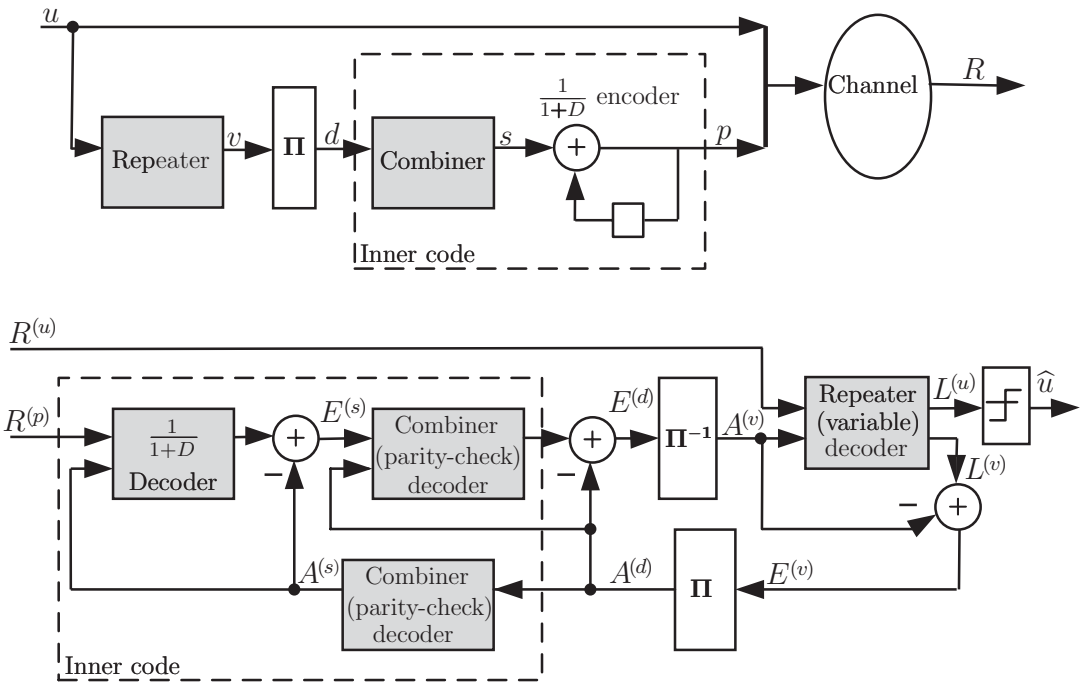
LDPC Codes

IRA codes



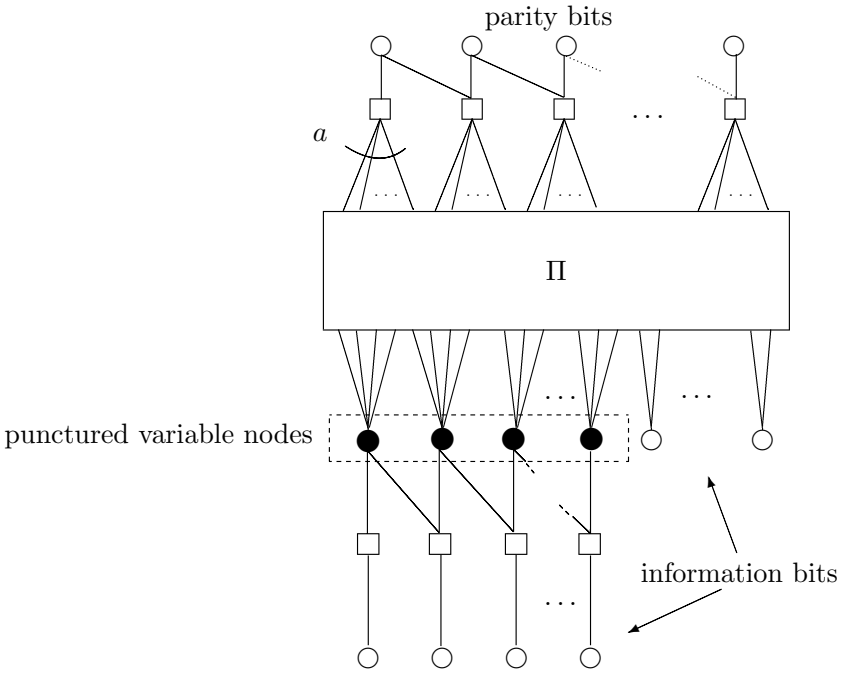
LDPC Codes

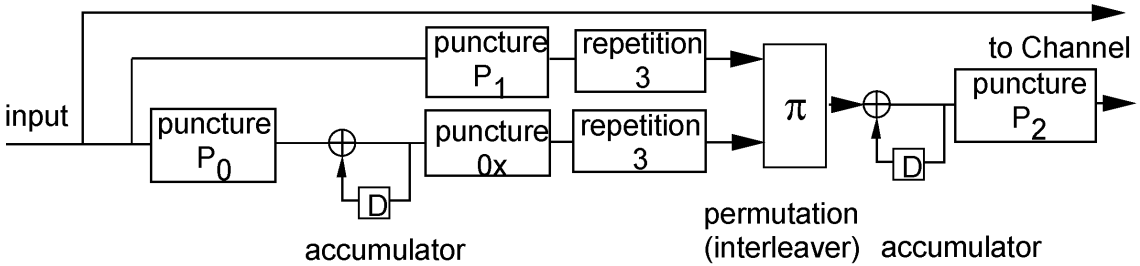
IRA codes as turbo-codes



LDPC Codes

IRA extensions





Accumulate Repeat Accumulate

Plan

LDPC Codes

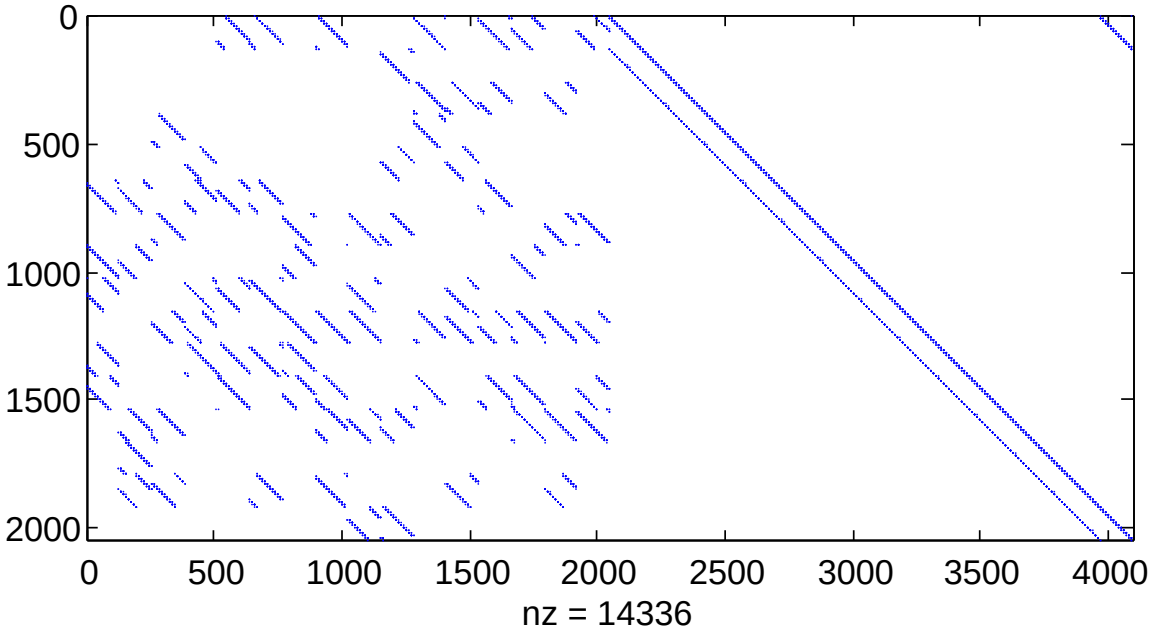
QC-LDPC : an example

$$= \left[\begin{array}{ccccc|ccccc|ccccc|ccccc} 1&0&1&0&0&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0 \\ 0&1&0&1&0&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&1&0&1&0&1&1&0&0&0&0&1&0&0&0&0&0&0&0 \\ 1&0&0&1&0&0&0&1&1&0&0&0&0&1&0&0&0&0&0&0 \\ 0&1&0&0&1&0&0&0&1&1&0&0&0&0&1&0&0&0&0&0 \\ \hline 1&1&0&0&0&0&1&0&1&0&0&0&0&0&0&1&0&0&0&0 \\ 0&1&1&0&0&0&0&1&0&1&0&0&0&0&0&0&1&0&0&0 \\ 0&0&1&1&0&1&0&0&1&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&1&1&0&1&0&0&1&0&0&0&0&0&0&0&0&1&0 \\ 1&0&0&0&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&1 \end{array}\right].$$

$$\left.\begin{array}{l} \mathbf{c} = [00110|01100|10000|00011] \\ \tilde{\mathbf{c}} = [00011|00110|01000|10001] \end{array}\right\} \text{deux mots de codes possibles}$$

LDPC Codes

Example



LDPC Codes

QC-LDPC properties

Polynomial representation

- Polynomial Matrix : generating element

$$P = \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ & & & & \ddots & \vdots \\ 0 & 0 & 1 & 0 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & 1 & 0 \\ 0 & & & & 0 & 1 \\ 1 & 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix}$$

LDPC Codes

Exemple :

$$H = \begin{pmatrix} I + P^2 & I + P^4 & I & 0 \\ I + P & P + P^3 & 0 & I \end{pmatrix}$$

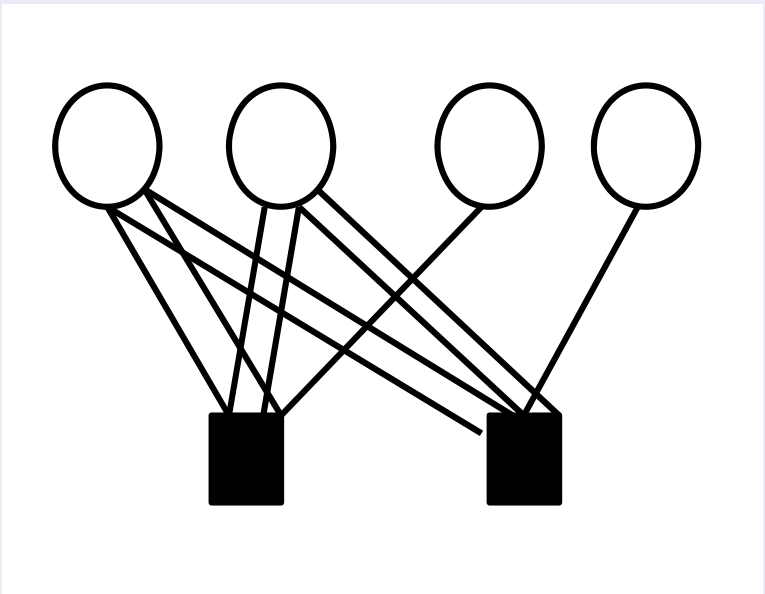
Definitions

- Base or proto matrix : number of monomials for each position of the polynomial matrix $L \times L$,
- Lift/extension order : H is obtained by"lifting" of H_B of order L.

$$H_B = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{pmatrix}$$

LDPC Codes

Protographes



protograph

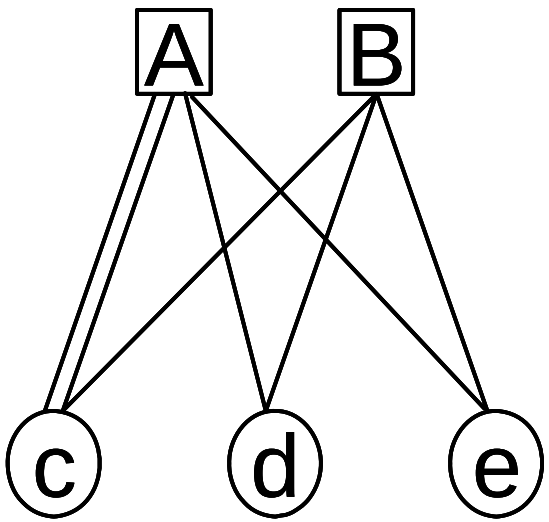
Plan

LDPC Codes

Protogrpahes

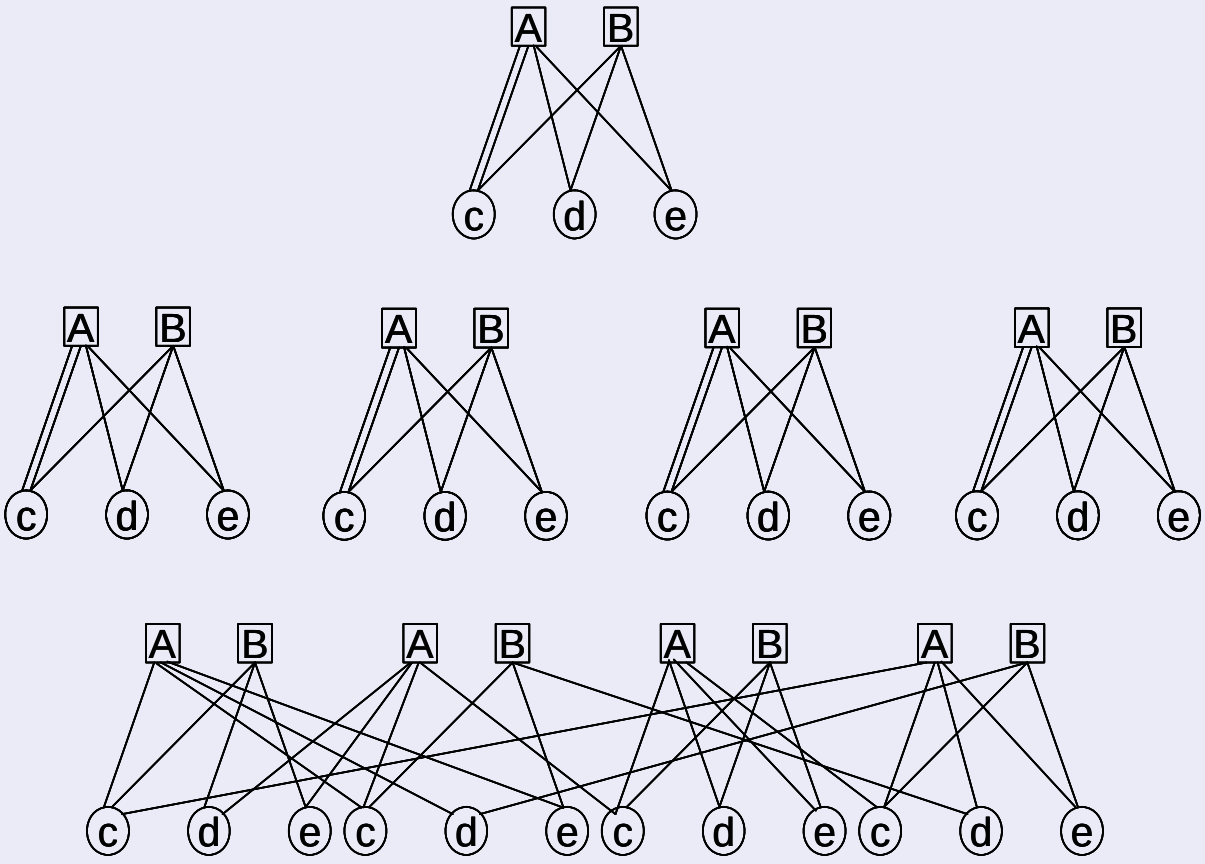
Definition

Protograph = small bipartite graph to be used for defining larger graphs with structure



Codes Low-Density Parity-Check (LDPC)

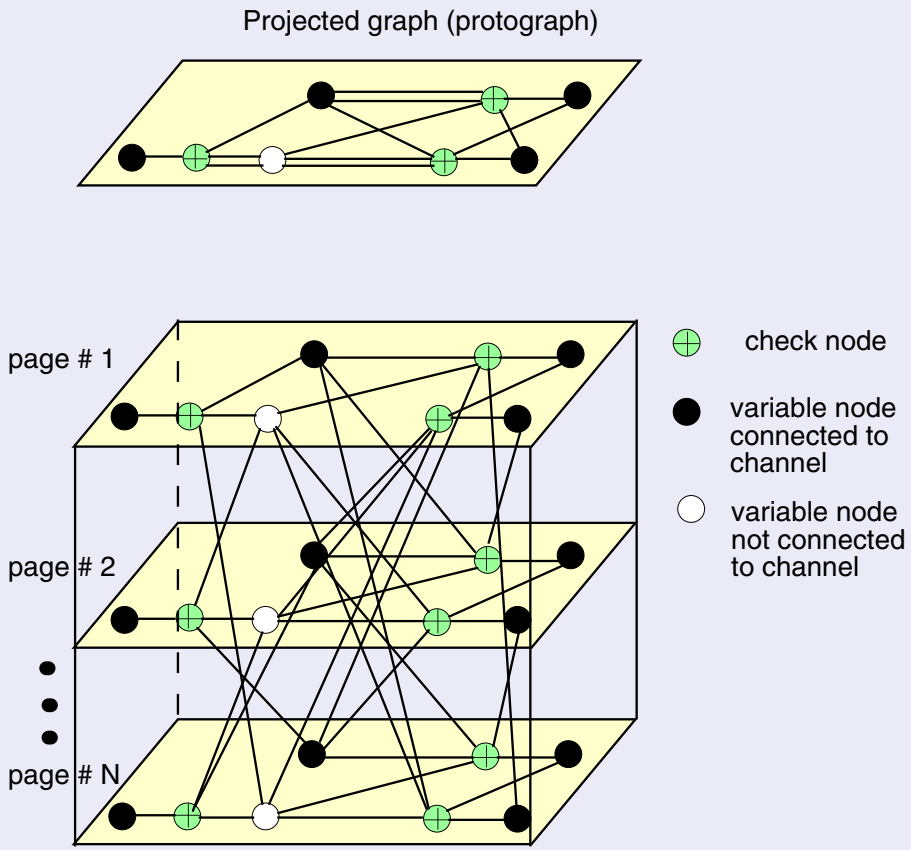
Codes basés Protographes



Copy and permute procedure

LDPC Codes

Protographs



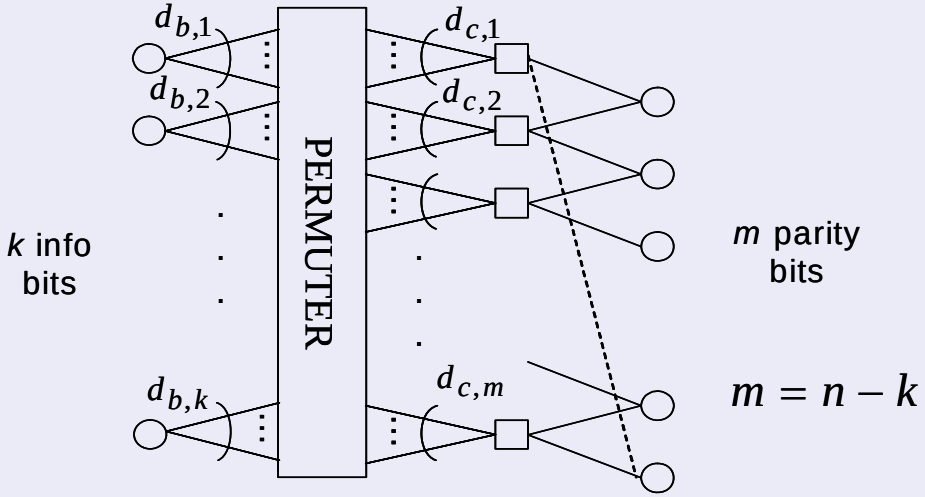
Plan

LDPC Codes

Irregular Repeat Accumulate

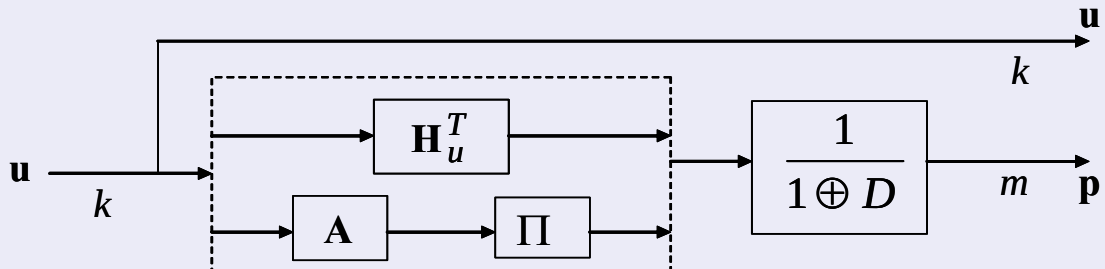
Structure

(a)



(b)

	$d_{b,i}$	$d_{c,j}$	$m = n - k$
RA	q	1	$m > k,\ m = qk$
IRA	variable	variable	$m \geq 1,\ k \geq 1$



Codes Low-Density Parity-Check (LDPC)

Codes Irregular Repeat Accumulate

- QC-IRA : $H_{QC} = [H_{u,QC} H_{p,QC}]$

$$H_{p,QC} = \begin{bmatrix} I & & & & P \\ I & I & & & \\ & \ddots & \ddots & & \\ & & I & I & \\ & & & I & I \end{bmatrix}$$

- Other possibility :

$$H_{p,QC} = \begin{bmatrix} P & I & & & \\ & I & I & & \\ I & & \ddots & \ddots & \\ & & & I & I \\ P & & & & I \end{bmatrix}$$

LDPC Codes

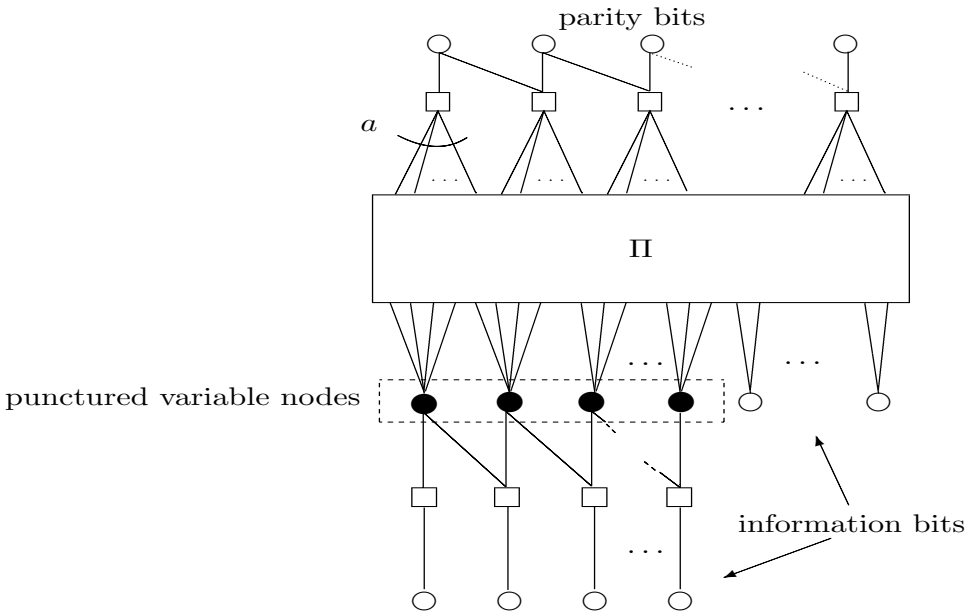
Irregular Repeat Accumulate codes

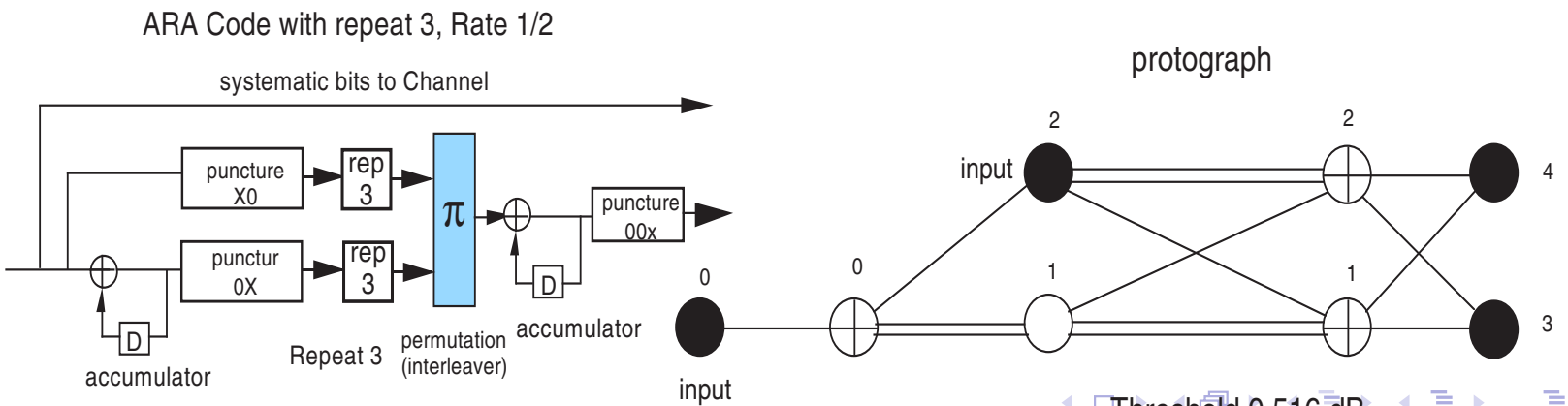
Standards

- ETSI DVB-S2 : LDPC IRA codes, $N = 64800, 16200$.
  $R = 1/4, \cdots, 9/10$.
- IEEE 802.11n et 802.16e : type QC-IRA.
- 5G : IRA codes with incremental parity.

LDPC Codes

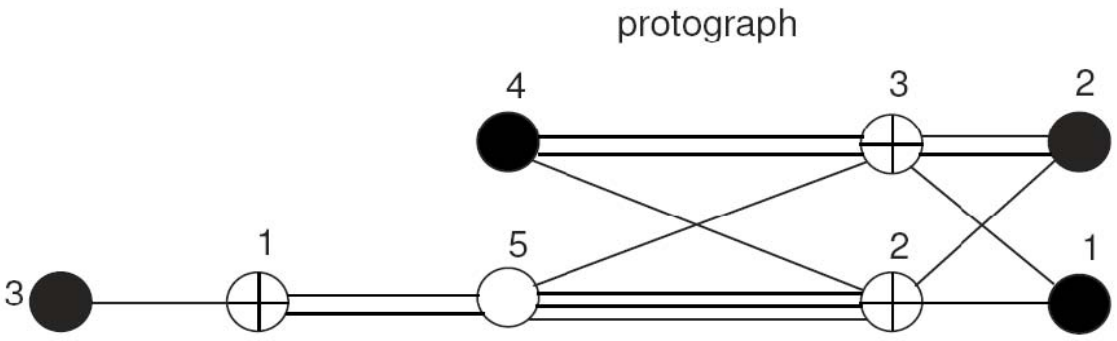
Accumulate Repeat Accumulate (ARA)

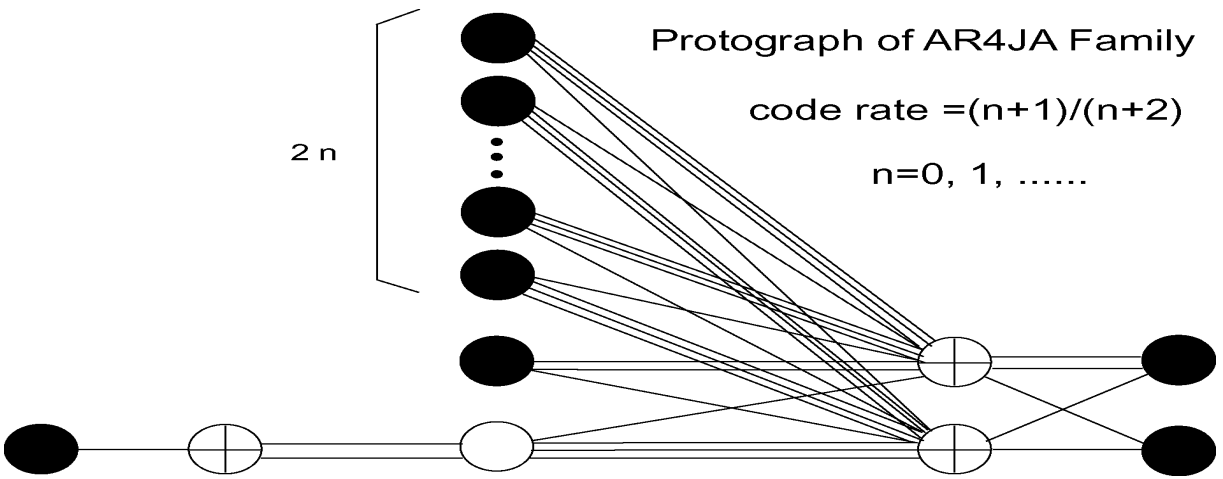




LDPC Codes

ARJA (Accumulate Repeat Jagged Accumulate) codes, CCSDS





LDPC Codes

ARJA codes : performances

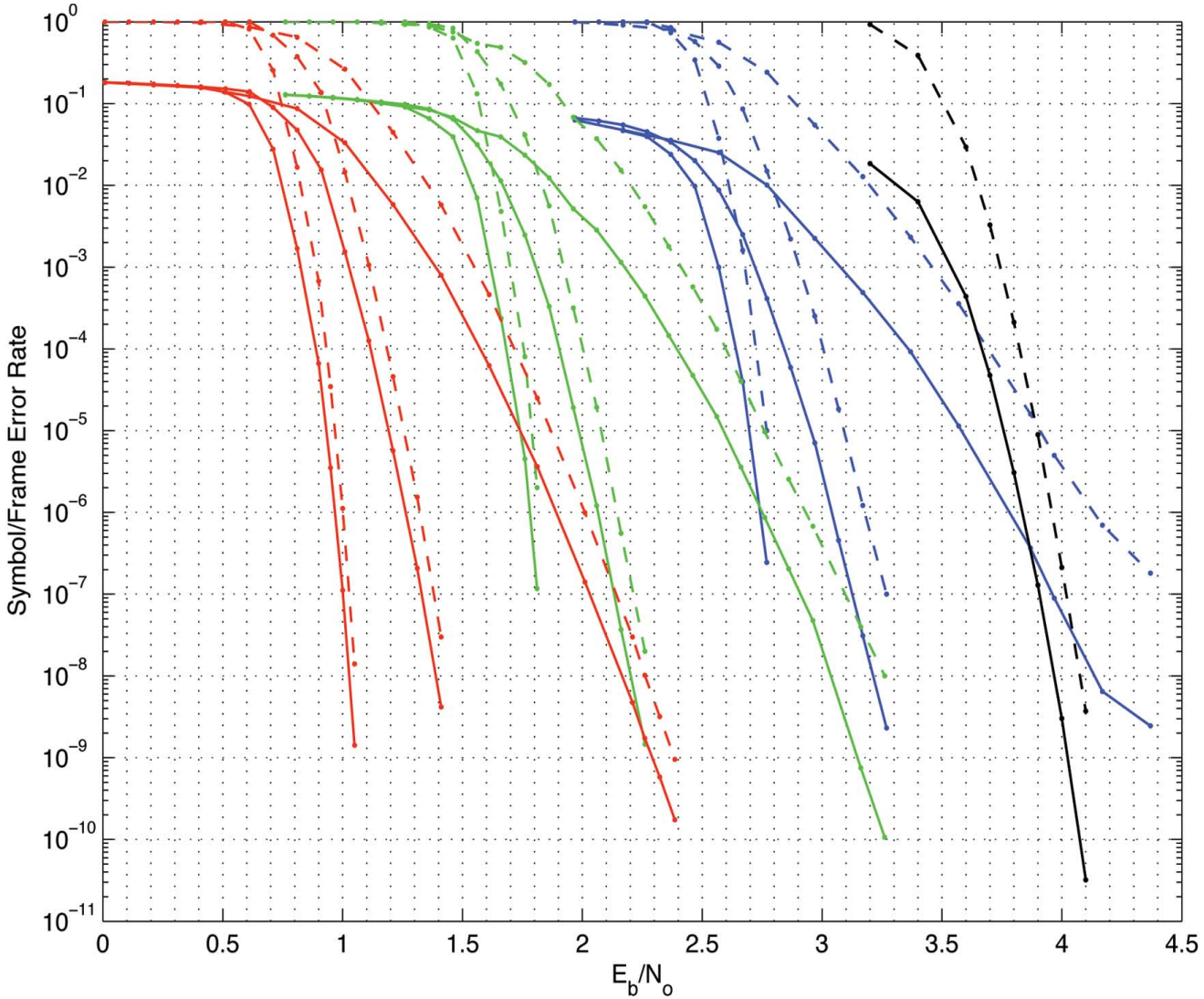
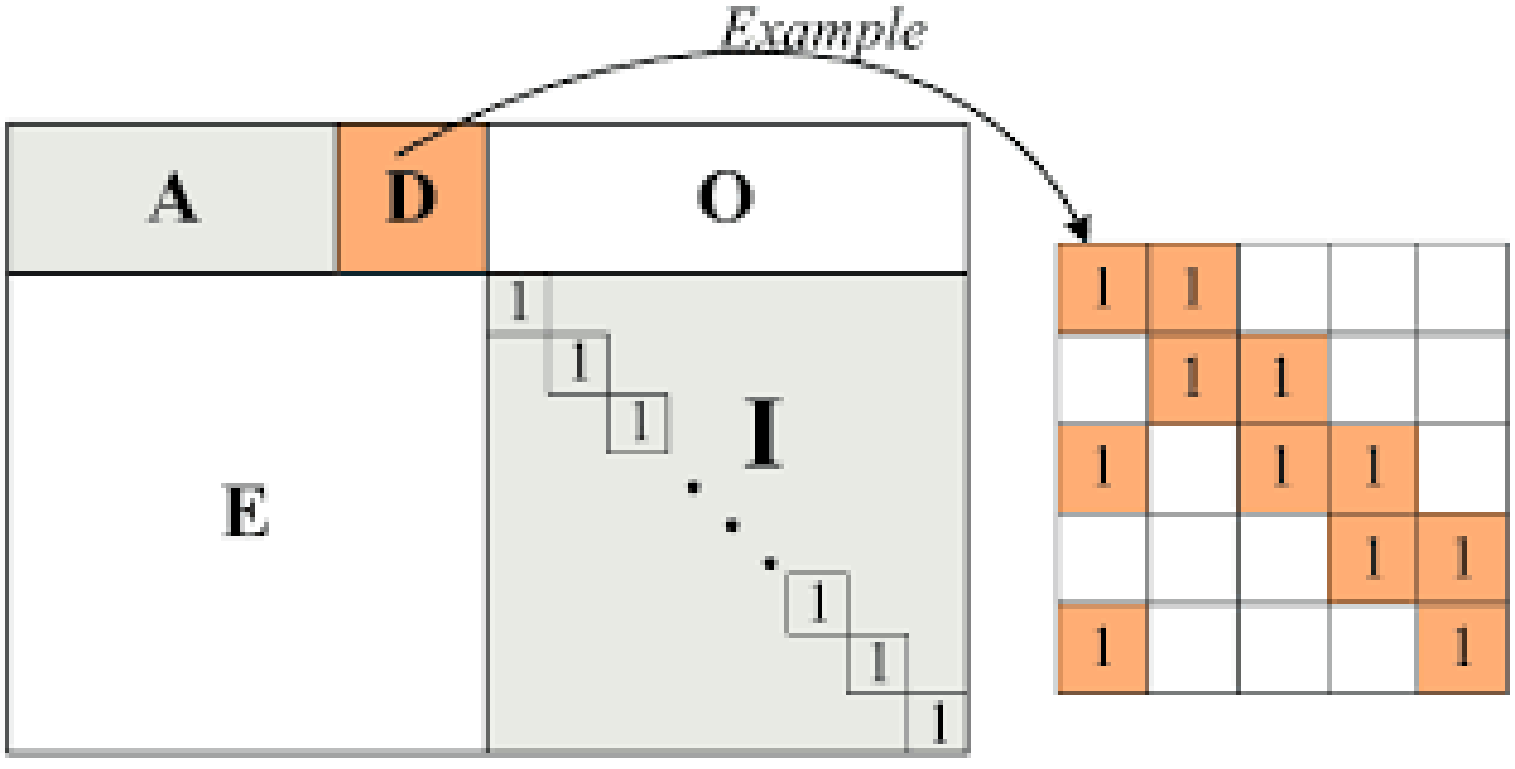


Fig. 13. *Bit error rate (solid) and codeword error rate (dashed) for nine AR4JA codes and C_2, with code rates 1/2 (red), 2/3 (green),*

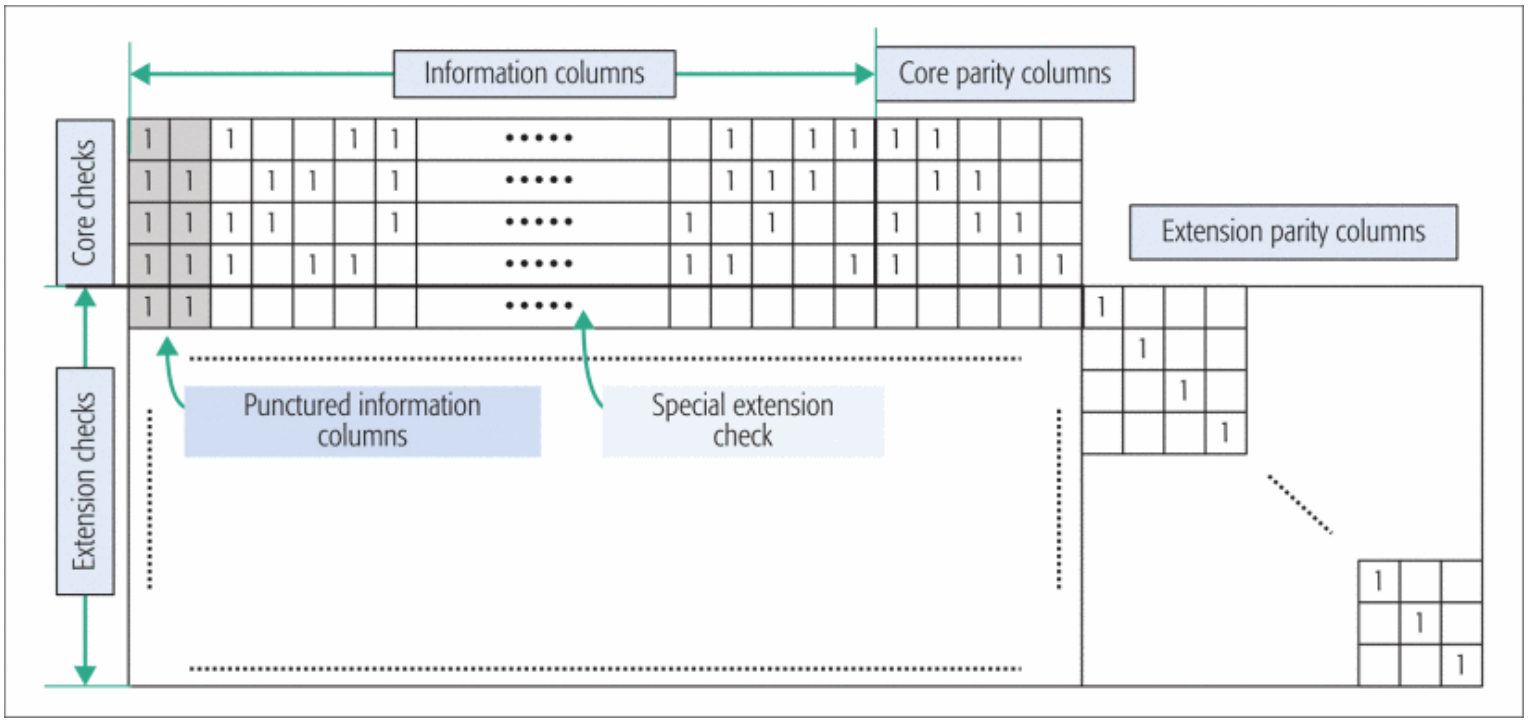
LDPC Codes

5G LDPC : Structure 1/3



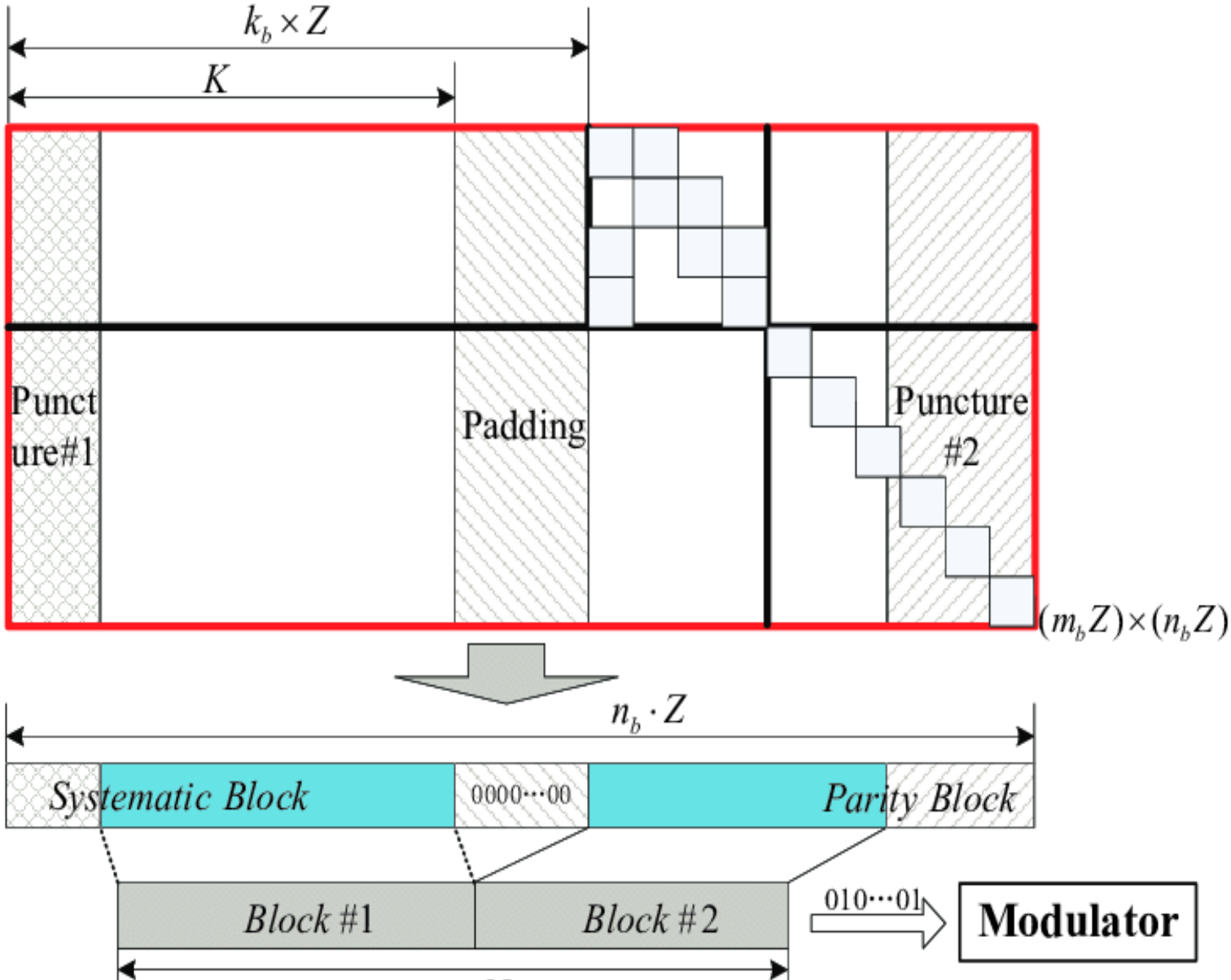
LDPC Codes

5G LDPC : Structure 2/3



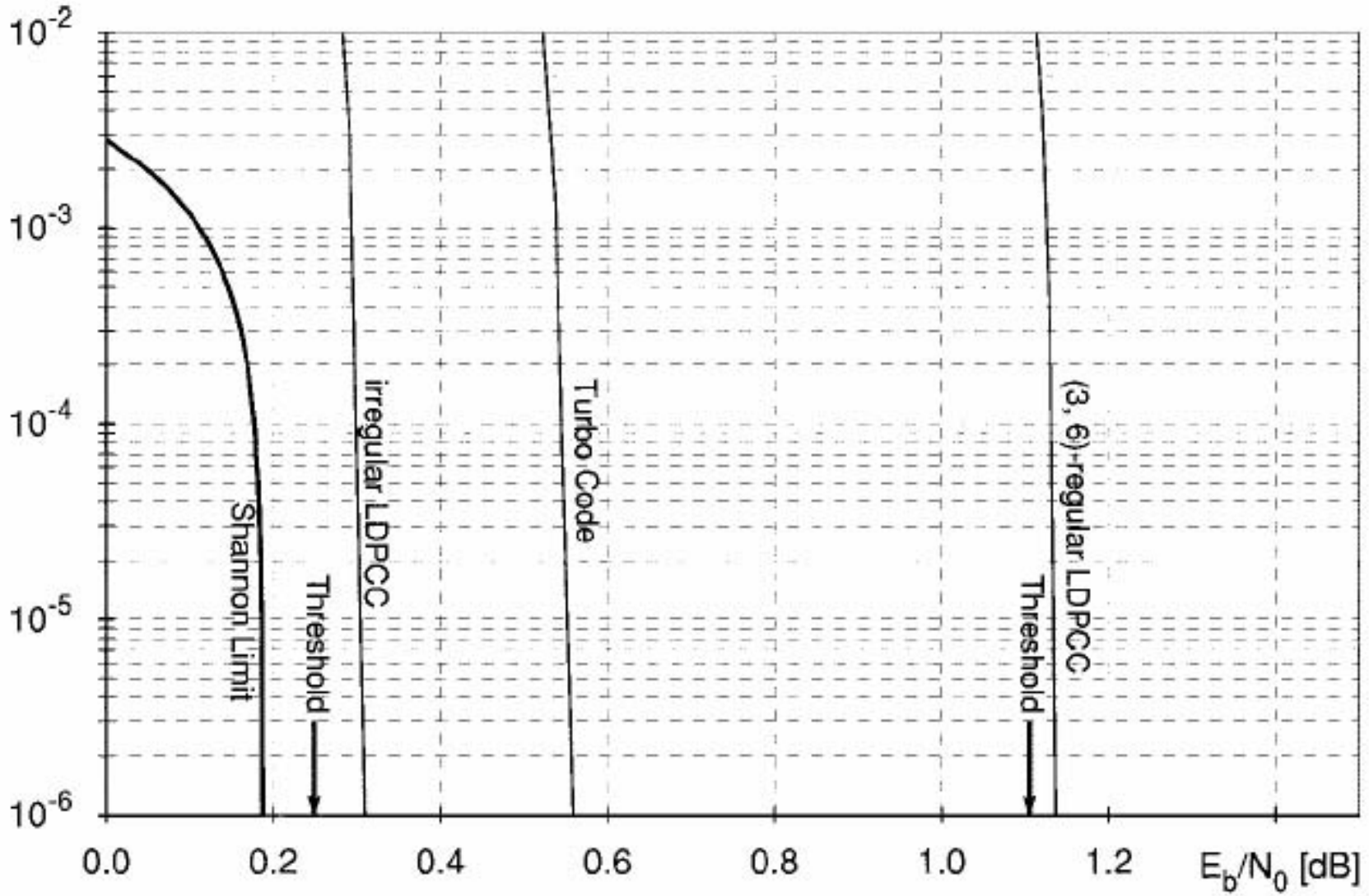
LDPC Codes

5G LDPC : Structure 3/3



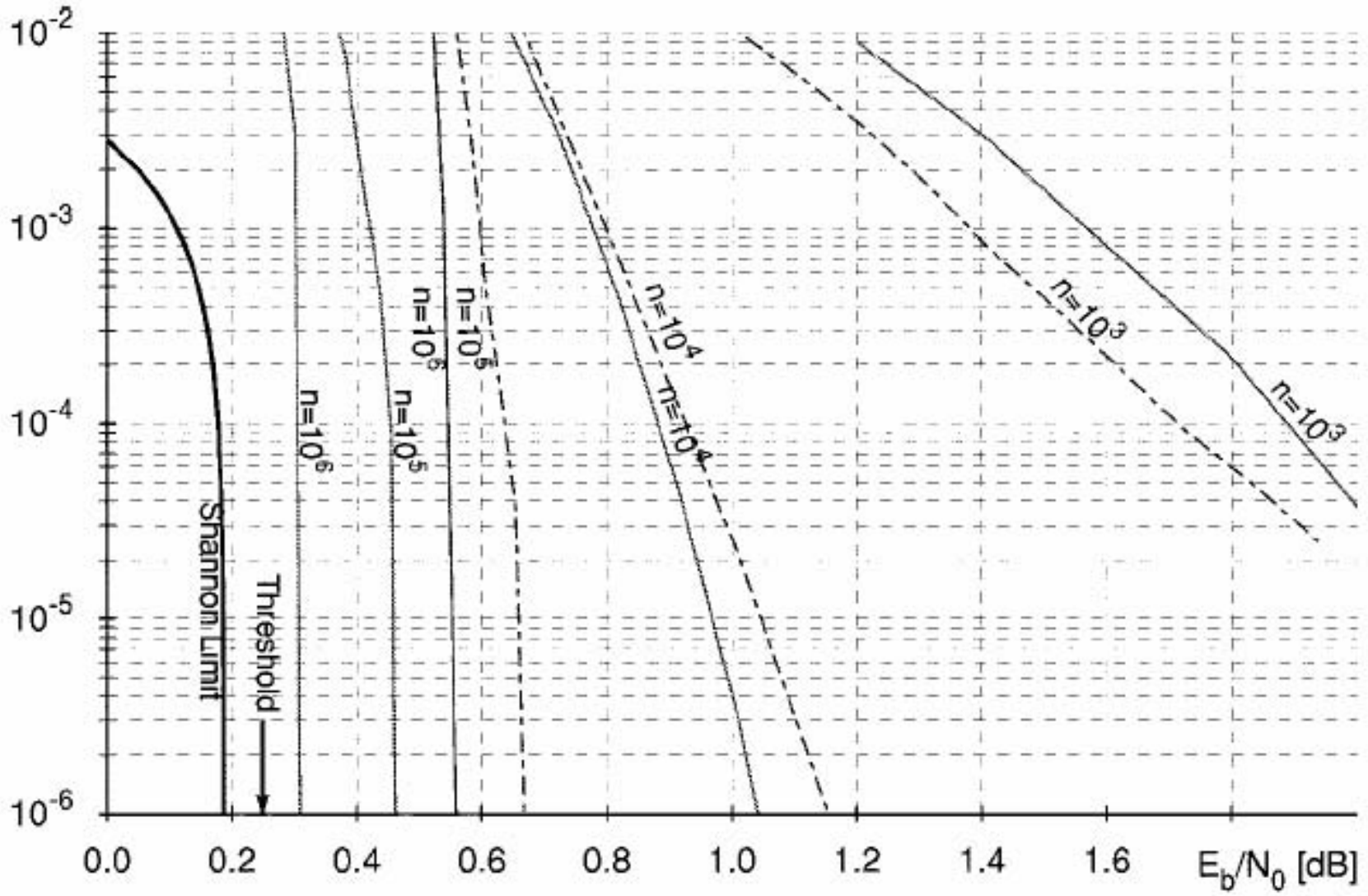
LDPC Codes

Performances



LDPC Codes

Performances



Bibliography

- W.E. Ryan, Shu Lin, *Channel codes : classical and modern*, Cambridge University Press, 2009.
- T. Richardson, R. Urbanke, *Modern coding theory*, Cambridge University Press, 2008.
- S.J. Johnson, *Iterative Error Correction : Turbo, Low-Density Parity-Check and Repeat-Accumulate Codes*, Cambridge University Press, 2010.
- Todd K. Moon, Error Control Coding : Mathematical Methods and Algorithms, Wiley, 2005.