Codes protographes et distance minimale

Tarik Benaddi

23/03/2015, Toulouse

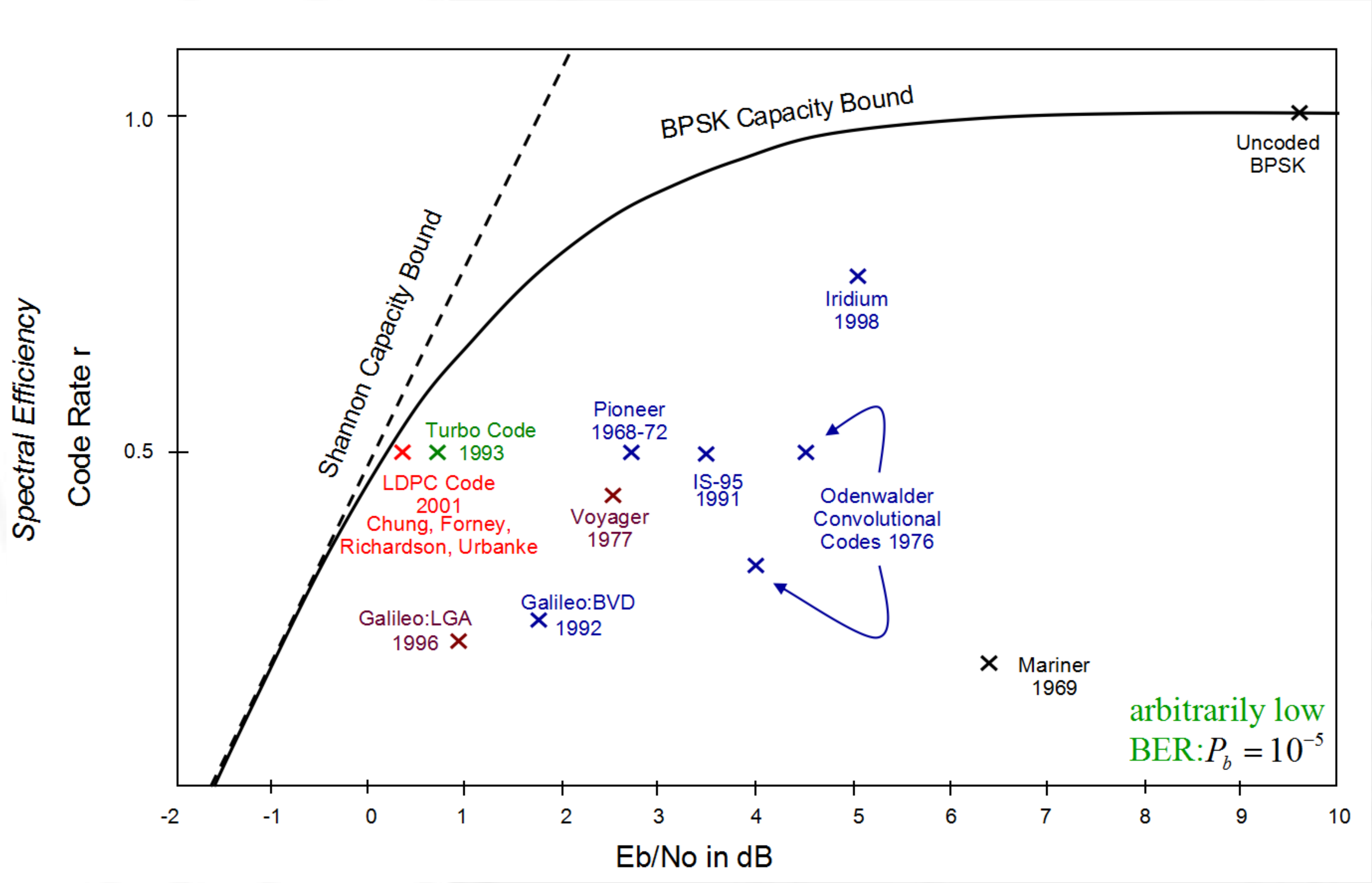
Sommaire

- Codes LDPC
- Protographe
- Distance minimale

LDPC – brève histoire

- 1963: Gallager
- 1993: Berrou et Glavieux
- 1995: MacKay et Niel
- 2001: Richardson, Urbanke, Shokrollahi …

LDPC - performances



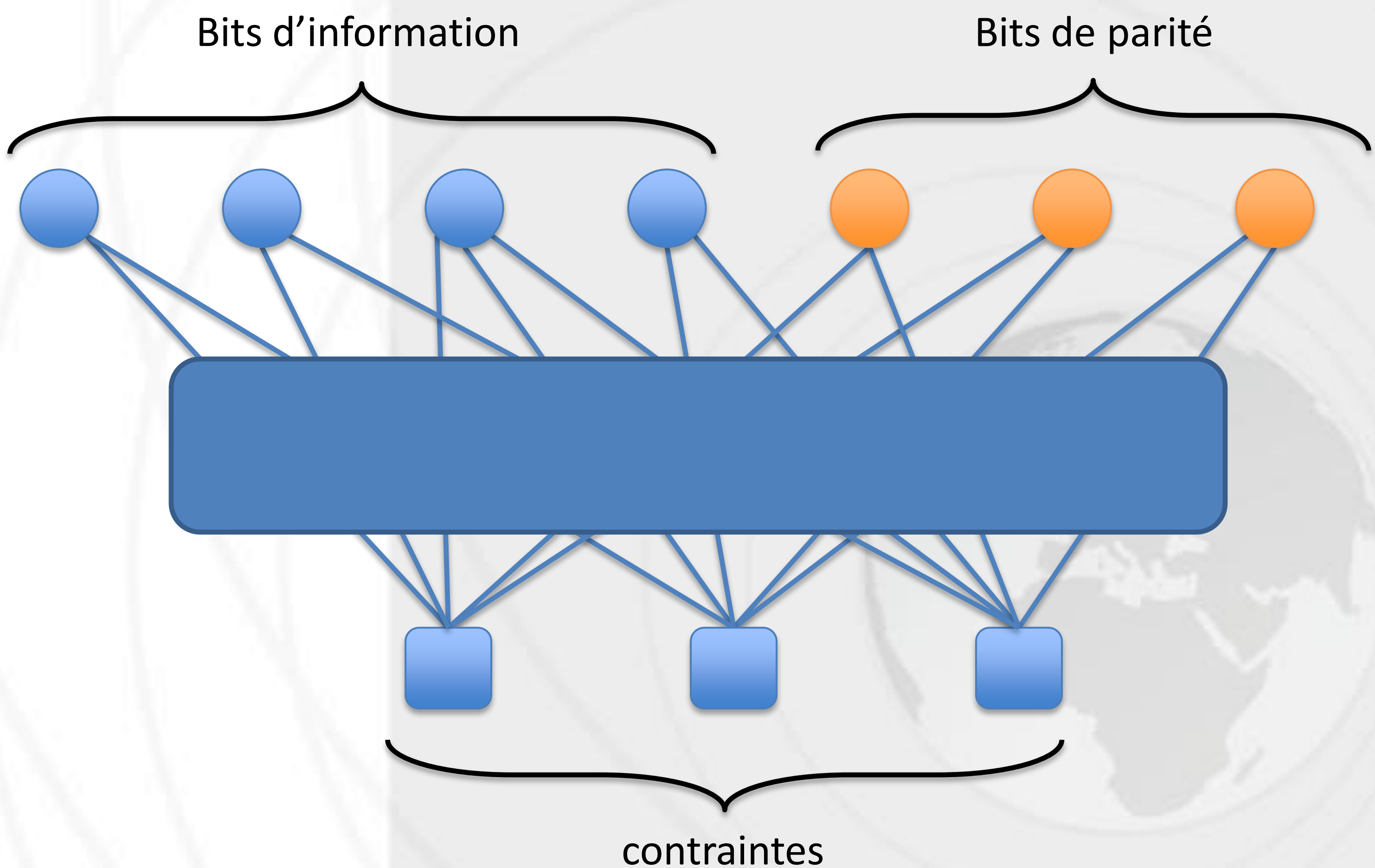
LDPC - introduction

$$H=\begin{pmatrix} & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & \end{pmatrix}$$

$$Hc^T = 0$$

LDPC binaire, GF(2)

LDPC - introduction



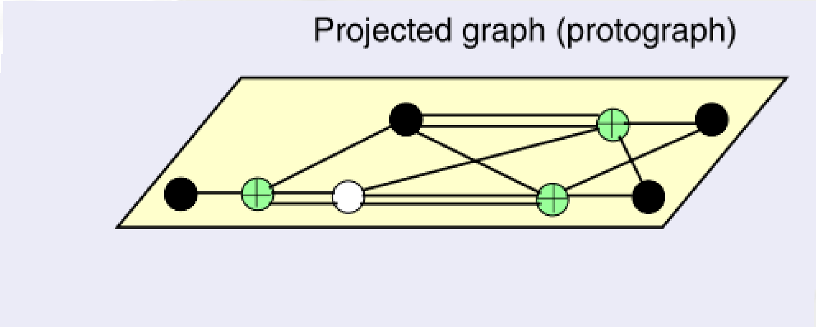
LDPC - application

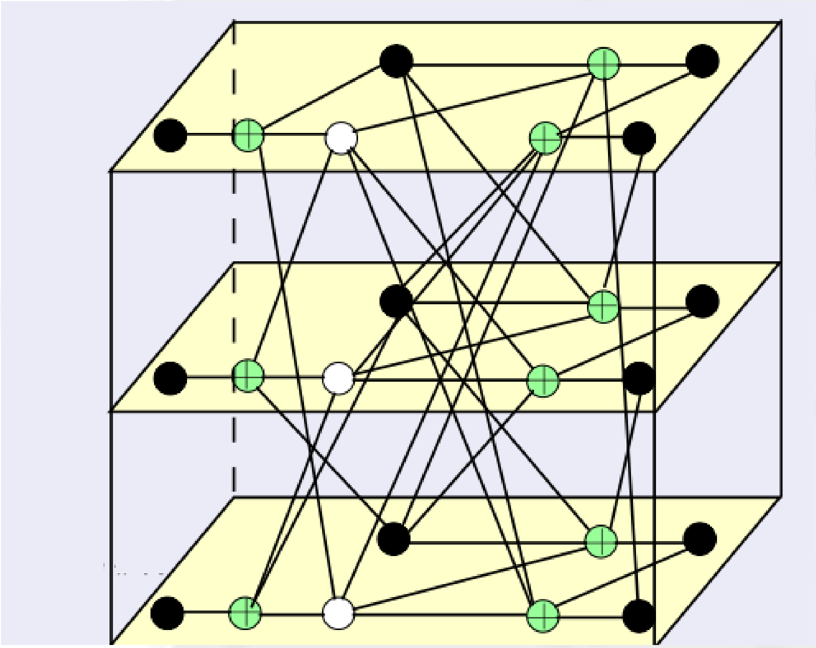
- WiMAX
- CCSDS
- 802.11n
- DVB-S2
- Stockage
- Communication optique

Protographe - introduction

- 2004: Jeremy Thorpe
- Petite matrice de parité
- stockage/parallélisme/encodage/étude
- Copy&permute

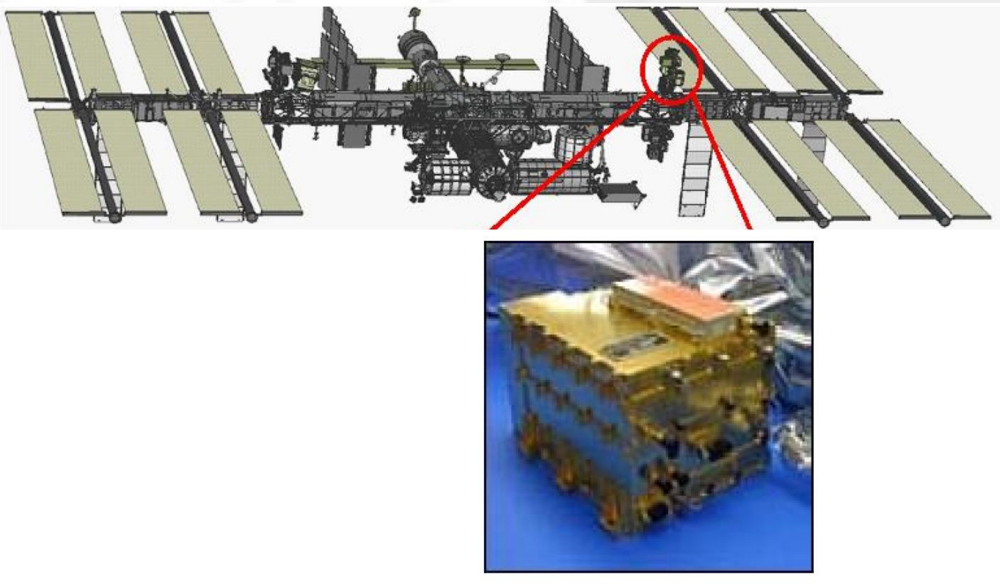
Protographe - introduction





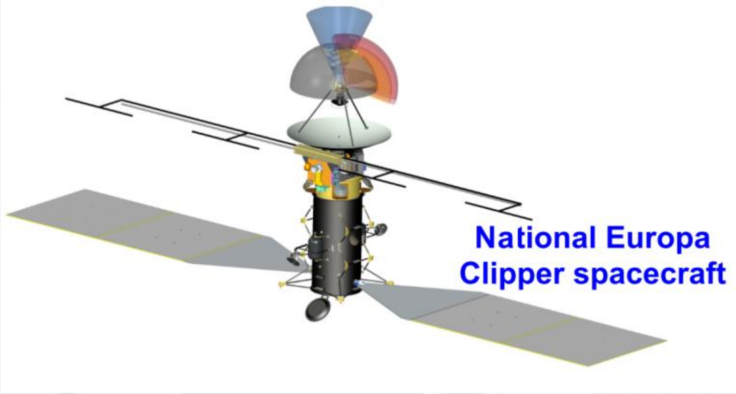
Protographe - application

- Quasi cyclique codes

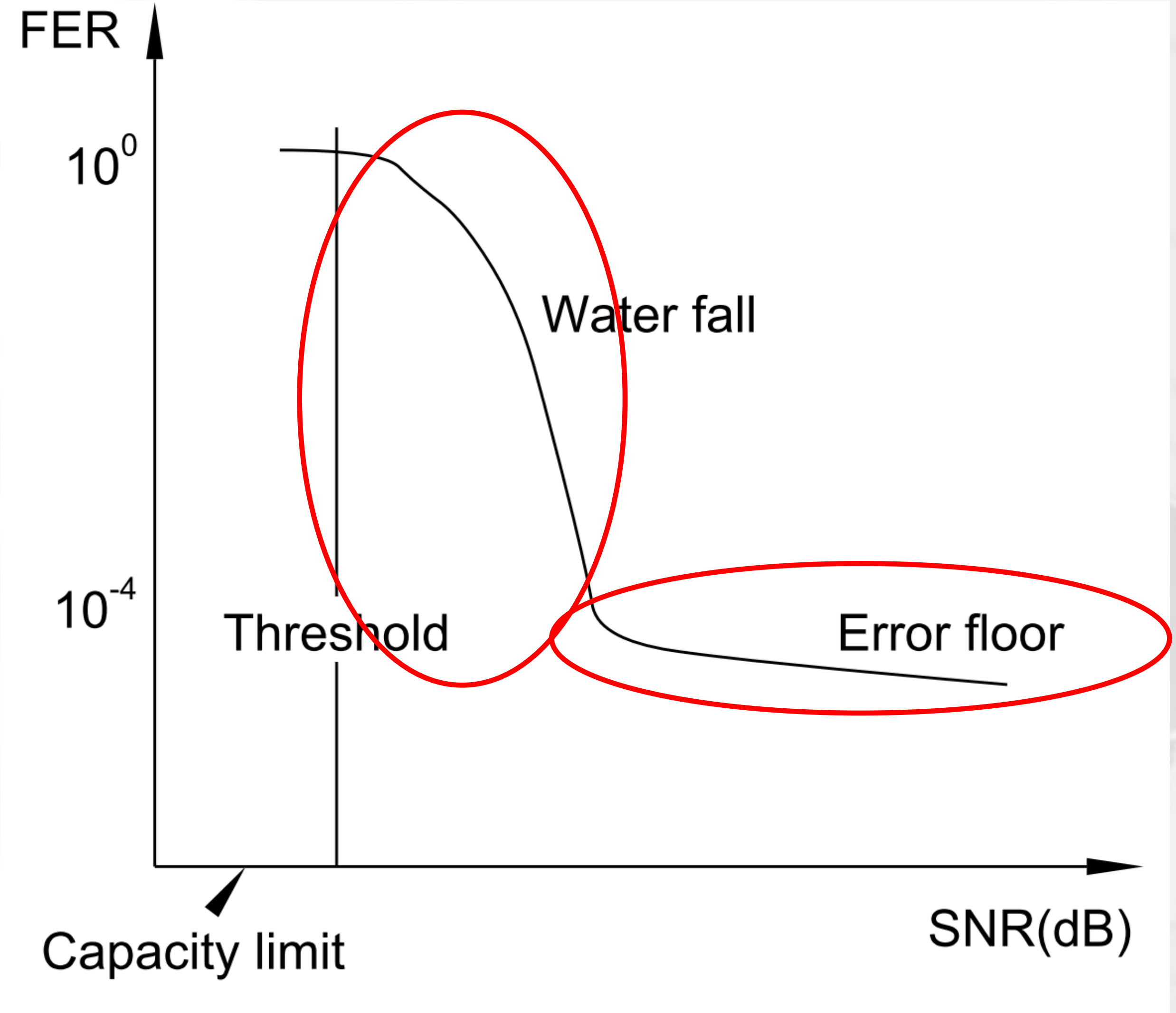


2012

2018, Jupiter



Protographe - régions



Protographe - régions

- Décodage itératif

$$P_{cw} \leq \sum_{w=d_{\min}}^{N} A_w P_w$$

$$P_w = Q\left(\frac{d_{\mathrm{E}}}{2\sigma}\right) = Q\left(\sqrt{\frac{2wRE_b}{N_0}}\right).$$

Protographe - régions

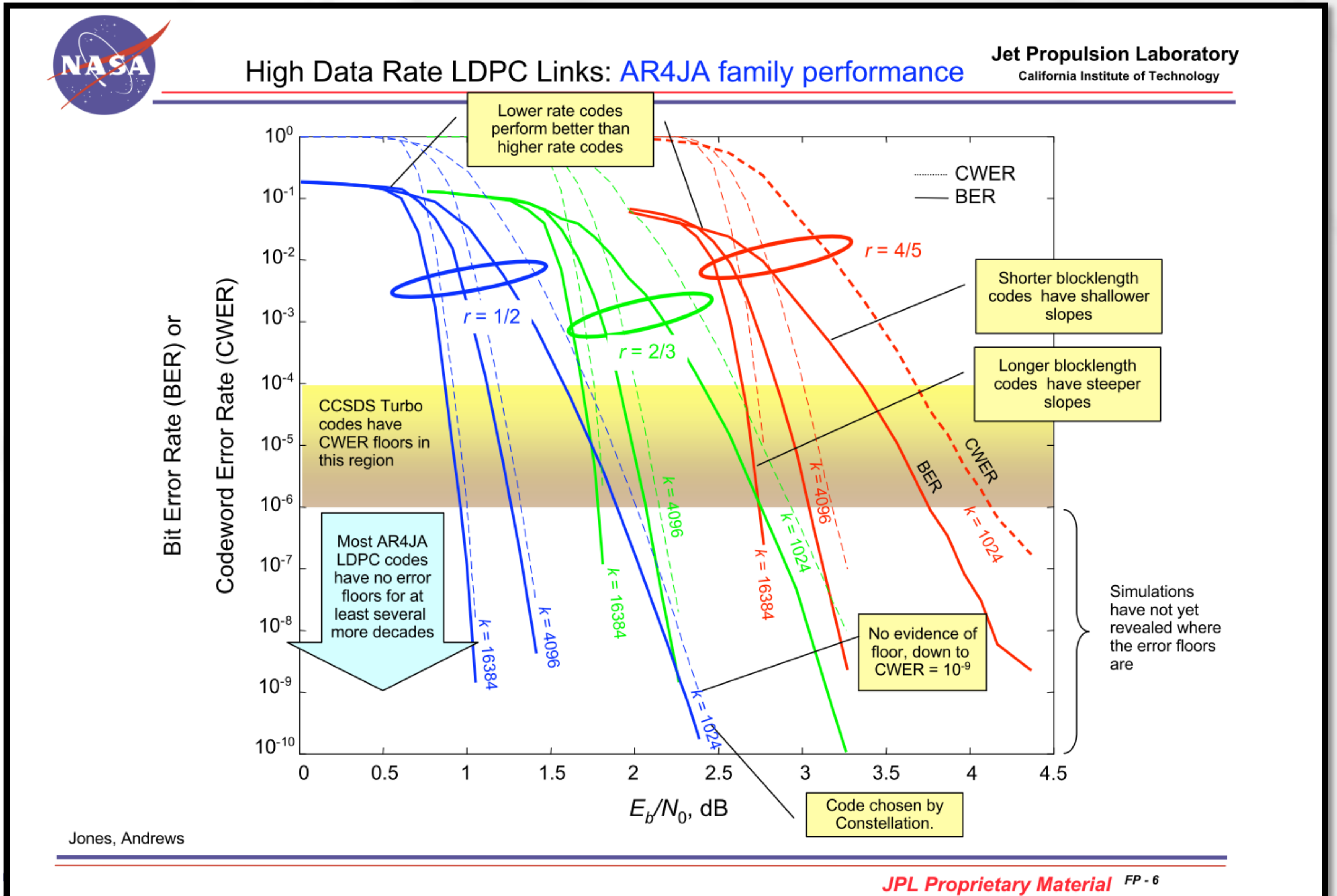
- Gallager (ML): $A_w \leq f(n)e^{nr(\delta)}$

$$A_w \simeq 0 \text{ for large } n \text{ when } r(\delta) < 0$$

$$A_{\lfloor n\delta_{\min} \rfloor} \simeq 0 \text{ and } A_{\lfloor n\delta_{\min} \rfloor + 1} > 0$$

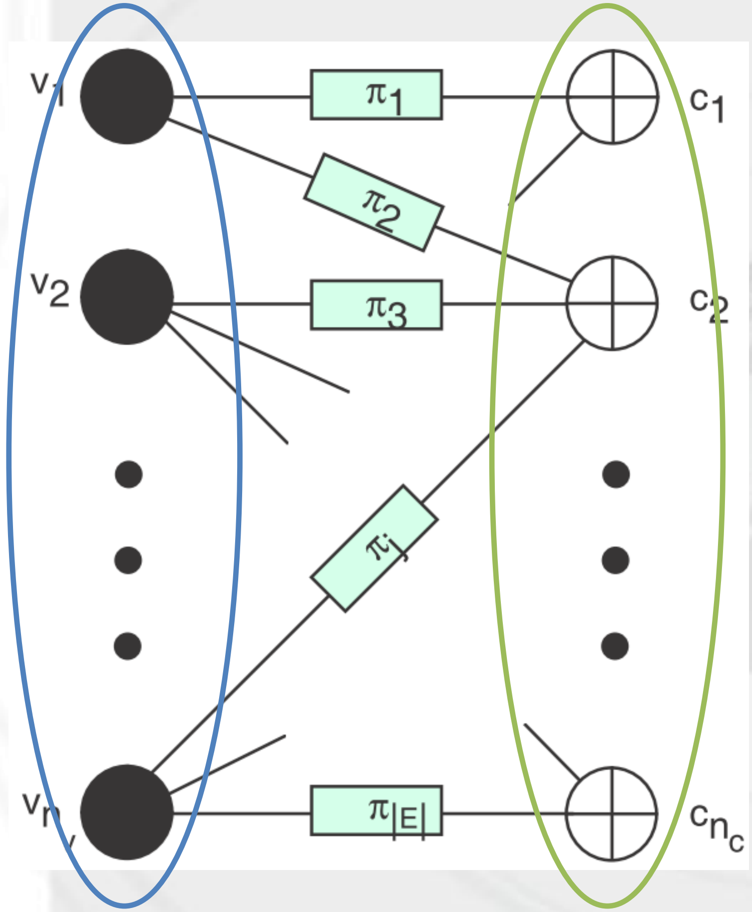
$$d_{\min} = w_{\min} \simeq n\delta_{\min}$$

Protographe - régions

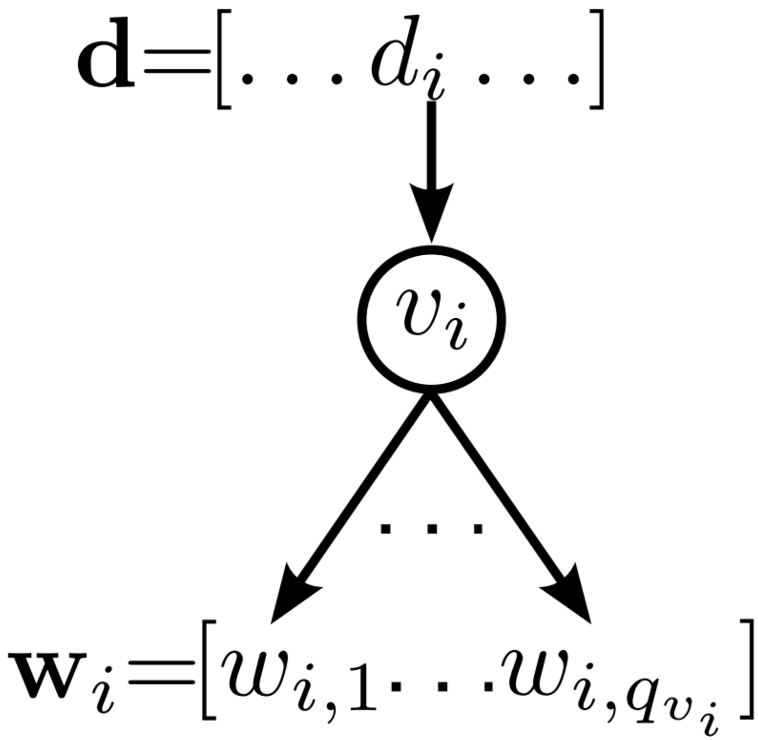


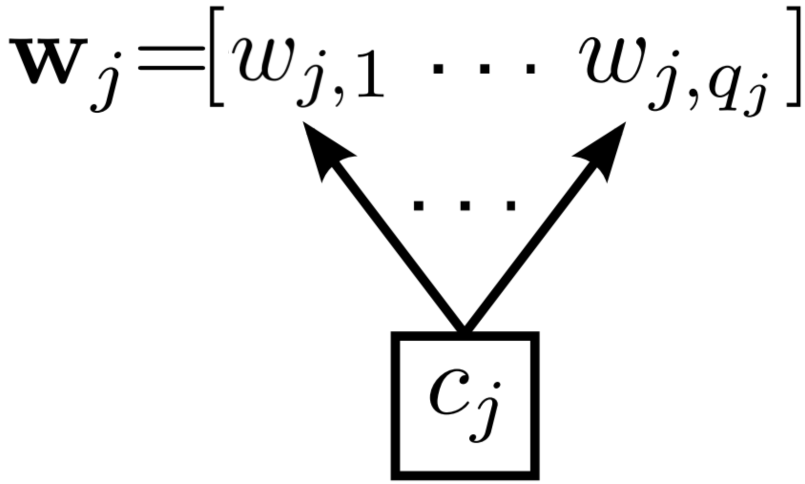
Protographe – dmin

- Entrelacement aléatoire



Protographe - dmin



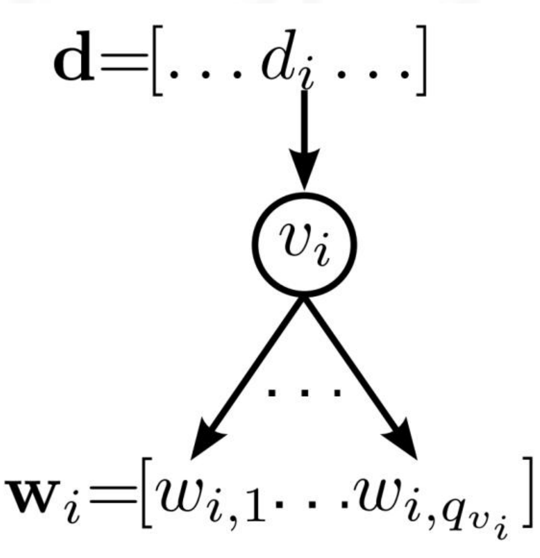


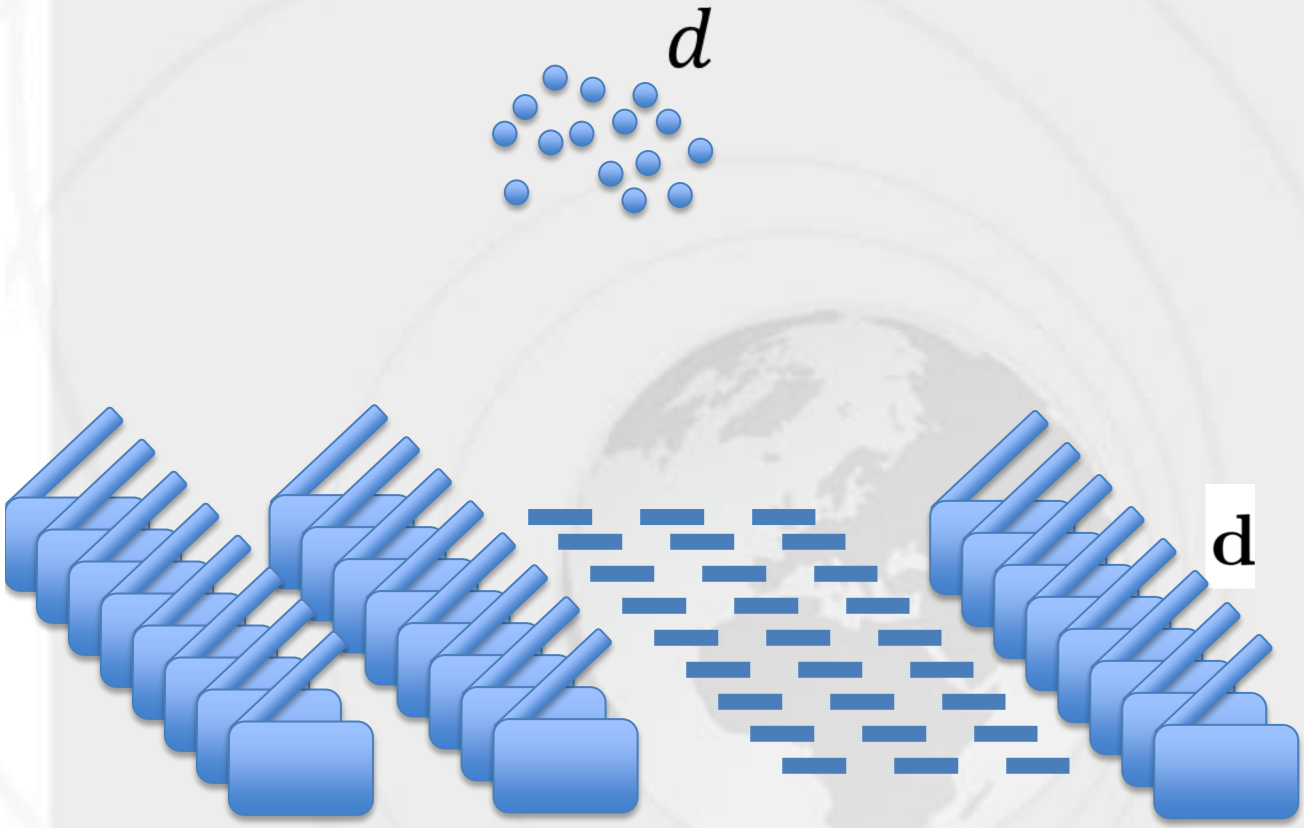
$$0 \leq d_i \leq N$$

$$A(\boldsymbol{d}) = \frac{\prod_{j=1}^{n_c} A^{c_j}(\boldsymbol{w}_j)}{\prod_{i=1}^{n_v} \binom{N}{d_i}^{q_{v_i}-1}}$$

Protographe - dmin

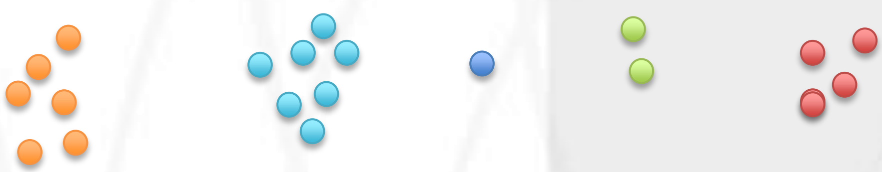
- VNs

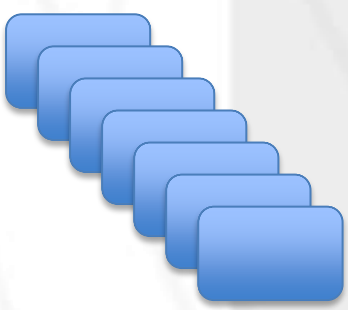


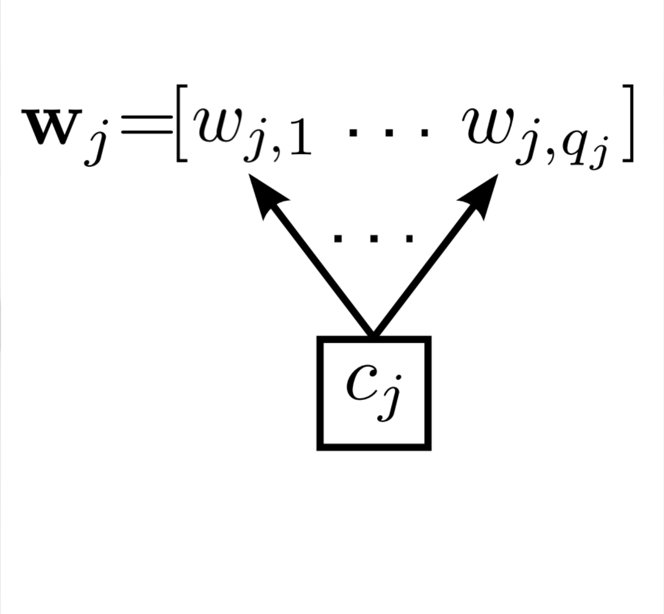


Protographe - dmin

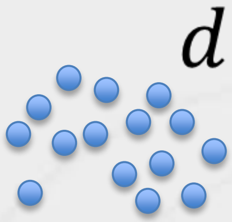
- CNs

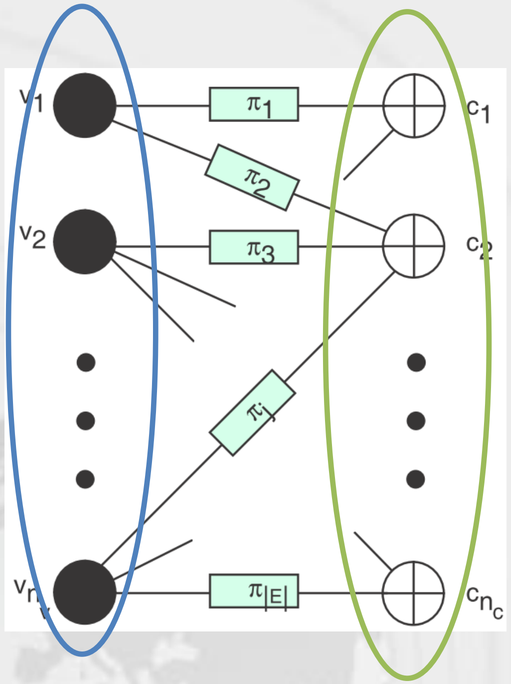






Protographe - dmin





$$A_d = \sum_{\{d_i / v_i \in \Omega_t\}} \sum_{\{d_k / v_k \in \Omega_p\}} A(\boldsymbol{d})$$

$$A(\boldsymbol{d}) = \frac{\prod_{j=1}^{n_c} A^{c_j}(\boldsymbol{w}_j)}{\prod_{i=1}^{n_v} \binom{N}{d_i}^{q_{v_i}-1}}$$

TéSA
Telecommunications for Space and Aeronautics

Protographe - dmin

$$\log A(\boldsymbol{d}) = \sum_{j=1}^{n_c} \log A^{c_j}(\boldsymbol{w}_j) - \sum_{i=1}^{n_v} (q_{v_i} - 1) \log \binom{N}{d_i}$$

$$A(\boldsymbol{d}) = \frac{\prod_{j=1}^{n_c} A^{c_j}(\boldsymbol{w}_j)}{\prod_{i=1}^{n_v} \binom{N}{d_i}^{q_{v_i}-1}}$$

Protographe - dmin

$$\log A(\boldsymbol{d}) = \sum_{j=1}^{n_c} \log A^{c_j}(\boldsymbol{w}_j) - \sum_{i=1}^{n_v} (q_{v_i} - 1) \log \binom{N}{d_i}$$

$$\delta_i = d_i / N \qquad \log \binom{N}{d_i} \approx N.H(\delta_i) \qquad \forall N$$

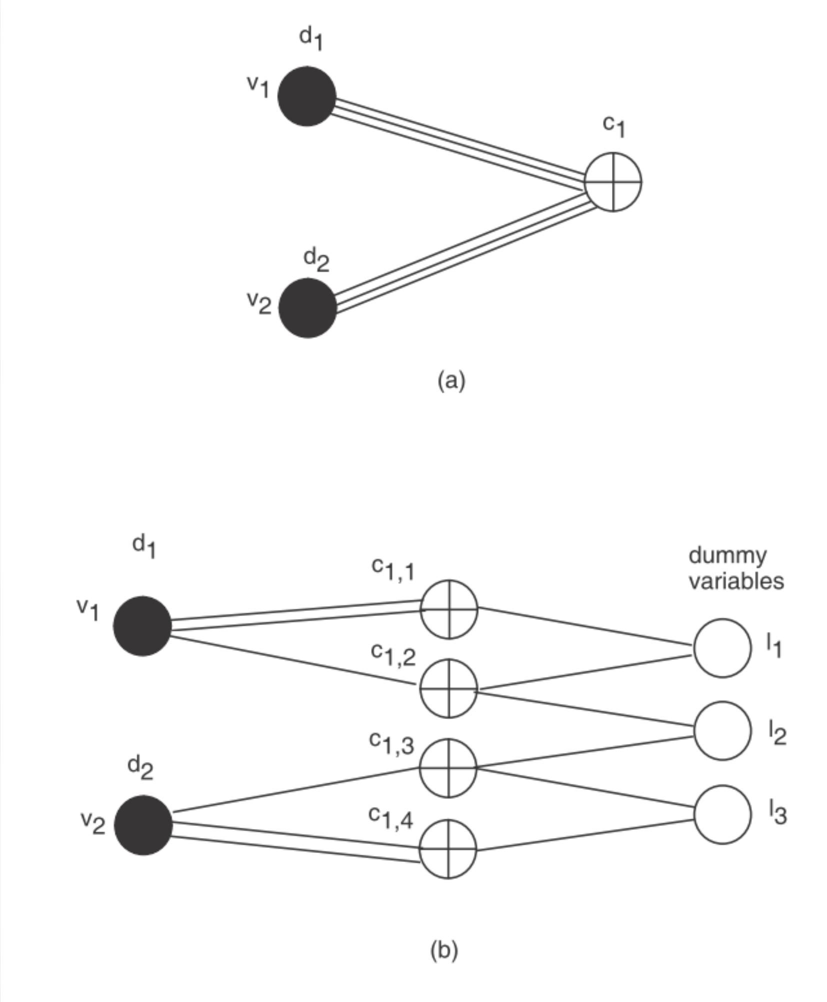
Protographe - dmin

$$\log A(\boldsymbol{d}) = \sum_{j=1}^{n_c} \log A^{c_j}(\boldsymbol{w}_j) - \sum_{i=1}^{n_v} (q_{v_i} - 1) \log \binom{N}{d_i}$$

- 2006: Divsalar (degré 3)
- Theorème multinomial

Protographe - dmin

- Check splitting:



Protographe - dmin

- CN de degré 4:

$$A^{c}_{w_1,w_2,w_3,w_4} = \sum_{l=1}^{N} \frac{A_{w_1,w_2,l} A_{w_3,w_4,l}}{\binom{N}{l}}$$

- Complexité: degré, N, CN généralisé…

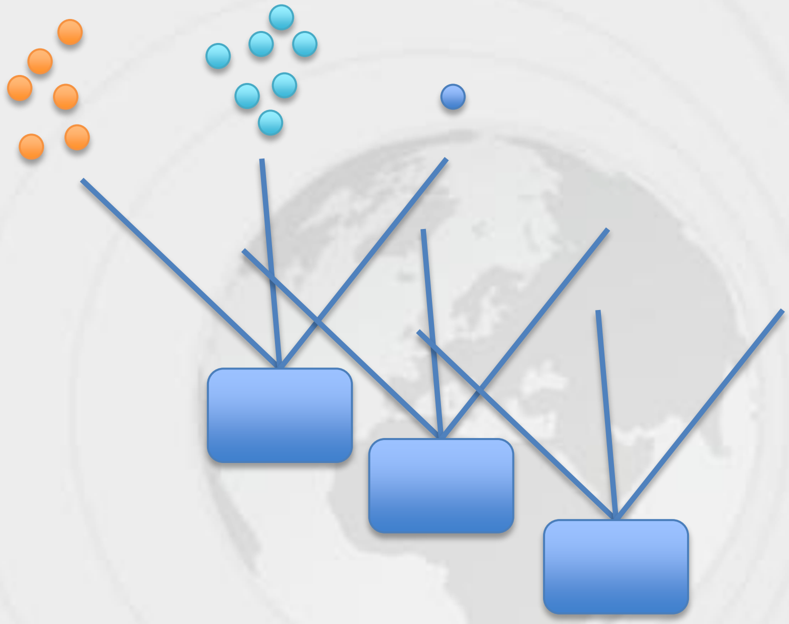
Protographe - dmin

- 2009: Abu Surra

$$M^c = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

$$w = M^c . n$$

$$\sum_{i=1}^{4} n_i = N$$



Protographe - dmin

$$A^c(\boldsymbol{w}) = \sum_{\{\boldsymbol{n}\}} C(N;\boldsymbol{n})$$

$$\begin{cases} \boldsymbol{w} = \boldsymbol{M}^c.\boldsymbol{n} \\ \sum_{i=1}^{K} n_i = N \end{cases}$$

$$\log\left(A^c(\boldsymbol{w})\right) = \log\left(\sum_{\{\boldsymbol{n}\}} C(N;\boldsymbol{n})\right)$$
$$= \max_{\{\boldsymbol{n}\}}{}^{*}\left(\log C(N;\boldsymbol{n})\right)$$

$$\max{}^{*}(x,y) = \max(x,y) + \log\left(1 + e^{-|x-y|}\right)$$

$$\log\left(A^c(\boldsymbol{w})\right) = \max_{\{\boldsymbol{n}\}}\left(\log C(N;\boldsymbol{n})\right)$$

Protographe - dmin

- $$\log C(N;\boldsymbol{n}) \approx N.H(\frac{n_1}{N},\ldots,\frac{n_K}{N})$$

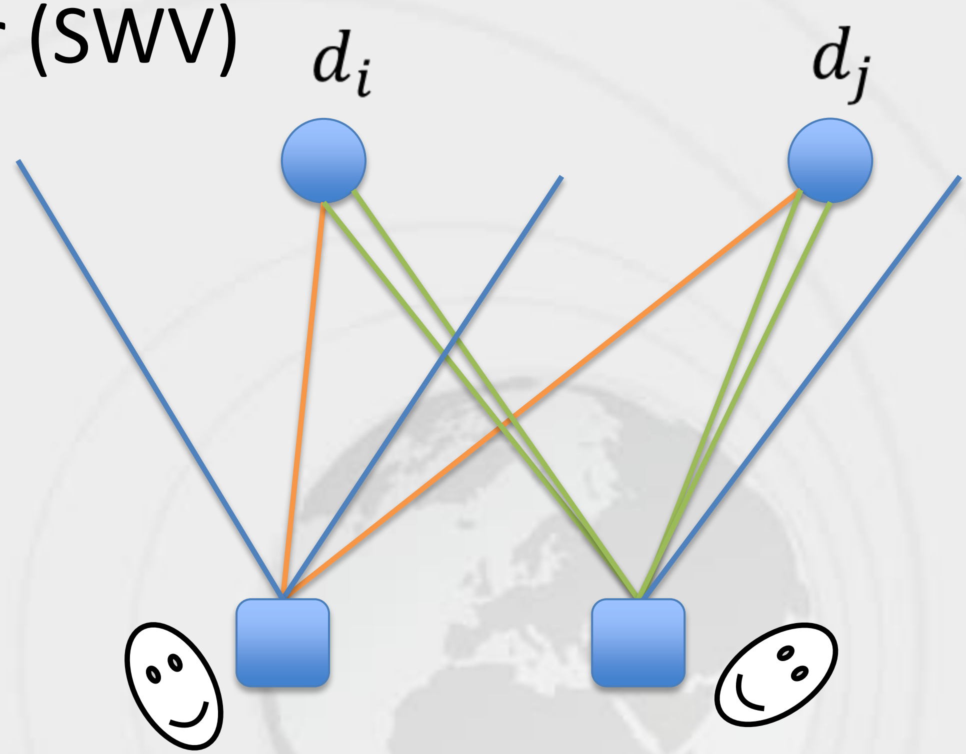
$$\log\left(A^c(\boldsymbol{w})\right) = N \max_{\{\boldsymbol{n}\}}\left(H(\frac{n_1}{N},\ldots,\frac{n_K}{N})\right)$$

$$a^c\left(\boldsymbol{\delta}\right) = \limsup_{N\to\infty}\frac{\log\left(A^c(\boldsymbol{w})\right)}{N} \approx \max_{\{\boldsymbol{p}\}}\left(H(p_1,\ldots,p_K)\right)$$

$$p_i = \frac{n_i}{N} \qquad \boldsymbol{\delta} = \boldsymbol{M}^c.\boldsymbol{p} \qquad \|\boldsymbol{p}\|_1 = 1$$

Protographe - dmin

- Subset weight vector (SWV)



Conjoncture:
Le maximum est atteint quand les proportions $\{p_i\}$ des mots de code qui ont le même SWV sont égales.

$$a^c(\boldsymbol{\delta}) = \limsup_{N \to \infty} \frac{\log(A^c(\boldsymbol{w}))}{N} \approx \max_{\{\boldsymbol{p}\}} \Big(H(p_1, \ldots, p_K) \Big)$$

Protographe - dmin

$$
\begin{aligned}
\underset{x}{\text{maximize}} \quad & H(\boldsymbol{x}) \\
\text{subject to:} \quad & \boldsymbol{M}^c.\boldsymbol{x} = \boldsymbol{\delta} \\
& \sum_{i=0}^{K} x_i = 1 \\
& x_i \in \{\frac{k}{N} / k \in [\![0, N]\!]\}, \quad \forall i \in [\![1, K]\!]
\end{aligned}
$$

- Goulot d’étranglement:
  - grand N (entropie)
  - grand degré

Protographe - dmin

$$0 \leq n_k \leq \min\{ \min_{\{j:\ m_{kj}=1\}} \{w_j\}, \min_{\{j:\ m_{kj}=0\}} \{N - w_j\}\} \leq N$$

Protographe - dmin

$$\mathscr{L} = \{\frac{k}{N} / k \in [\![0, N]\!]\}$$

$\mathscr{L}^K$ is dense in $[0,1]^K$

$\boldsymbol{y}$ in $[0,1]^K$

$\boldsymbol{x}_N$ in $\mathscr{L}^K$ such that $\boldsymbol{x}_N \xrightarrow[N\to\infty]{\|\cdot\|_2} \boldsymbol{y}$

$$\boldsymbol{x}_N = \left(\frac{\lfloor N y_i \rfloor}{N}\right)_{1\leq i\leq K}$$

Protographe - dmin

$$\boldsymbol{y}^{opt} = (y_i^{opt})_{1 \leq i \leq K}$$

$$\boldsymbol{x}_N^{opt}$$

$$\mathscr{L}^K$$

$$\forall \varepsilon \geq 0, \exists N_0 \in \mathbb{N}, \forall N \geq N_0,$$
$$\begin{cases} \|\boldsymbol{x}_N^{opt} - \boldsymbol{y}^{opt}\|_2 \leq \varepsilon \\ |H(\boldsymbol{x}_N^{opt}) - H(\boldsymbol{y}^{opt})| \leq \varepsilon \\ \|\boldsymbol{M}^c.\boldsymbol{x}_N^{opt} - \boldsymbol{b}\|_2 \leq \varepsilon \end{cases}$$

Protographe - dmin

$$\begin{aligned} \underset{x}{\text{maximize}} \quad & H(\boldsymbol{y}) \\ \text{subject to:} \quad & \boldsymbol{M}^c.\boldsymbol{y} = \boldsymbol{b} \\ & \boldsymbol{y} \in [0,1]^K \end{aligned}$$

- Point initial

$$\boldsymbol{M}^c.\boldsymbol{y} = \boldsymbol{b}$$

$$[0,1]^K$$

Protographe - dmin

- Pseudo inverse

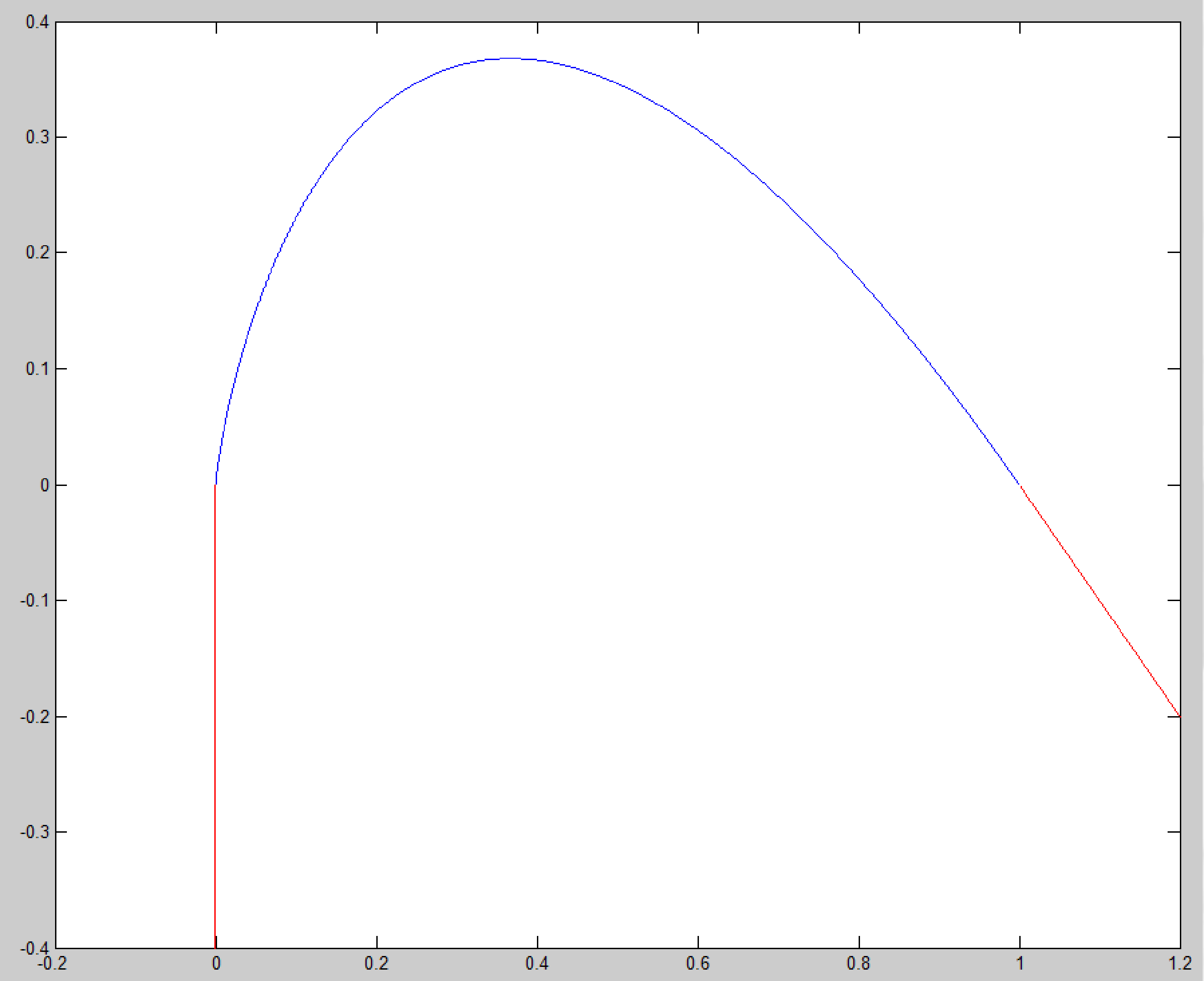
$$\boldsymbol{y}_0 = \boldsymbol{M}^{c+}\boldsymbol{b}$$

- Pas unique + valeur de **b**

K

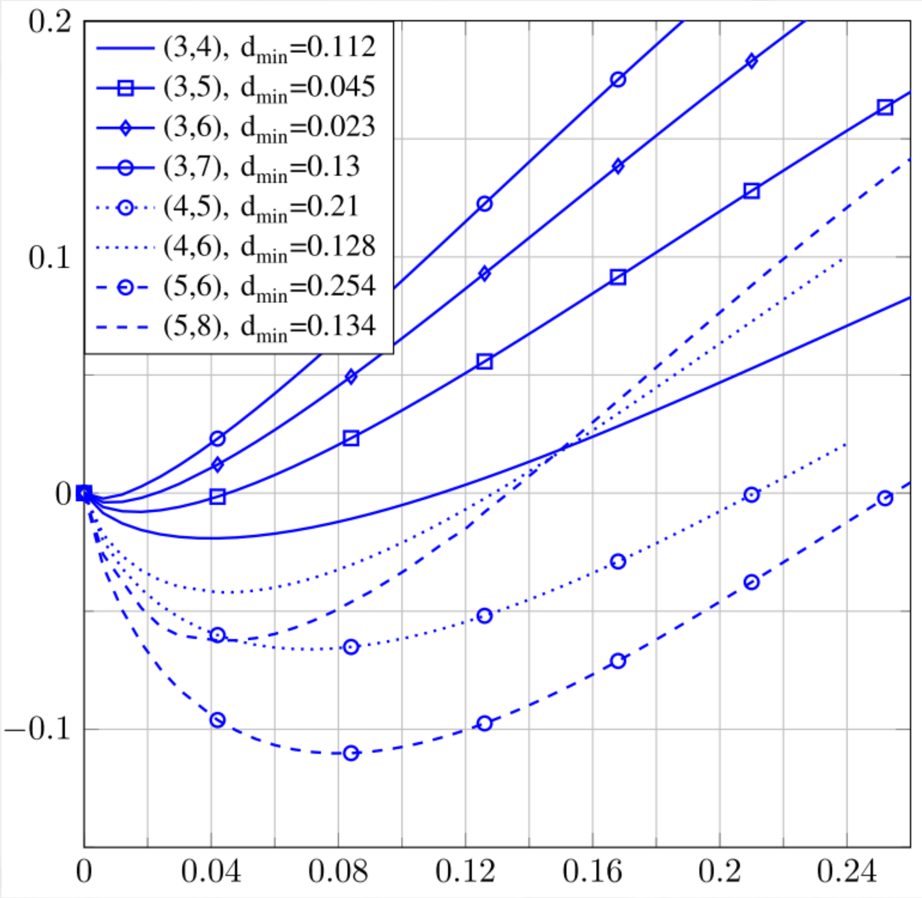
$$[0, 1]^K$$

Protographe - dmin



Protographe - résultats

Ensemble	δ_{min}
$(3,4)$	0.112 [1]
$(3,5)$	0.045 [1]
$(3,6)$	0.023 [1]
$(3,7)$	0.0129
$(3,8)$	0.0081
$(3,9)$	0.0054
$(3,12)$	0.0021
$(4,5)$	0.210 [1]
$(4,6)$	0.128 [1]
$(4,8)$	0.063 [1]
$(4,10)$	0.037
$(4,12)$	0.024
$(5,6)$	0.254 [1]
$(5,8)$	0.136
$(5,10)$	0.084



Merci