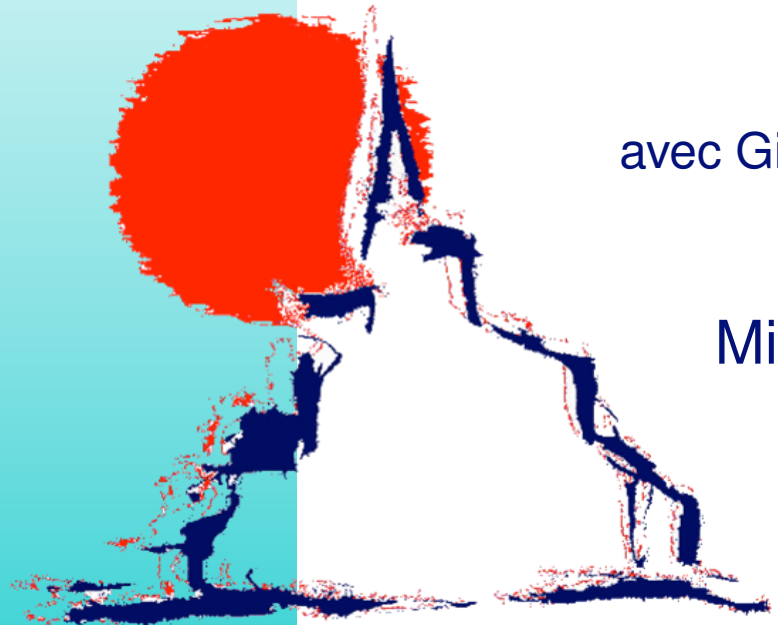
MITSUBISHI ELECTRIC
Changes for the Better

Réseaux Entiers et codes LDPC non binaires



Nicola di Pietro

avec Gilles Zémor, Joseph J. Boutros et Loïc Brunel

Mitsubishi Electric R&D Centre Europe

Institut de Mathématiques de Bordeaux

Institut de Mathématiques
Université de Bordeaux

Sommaire

MITSUBISHI ELECTRIC
Changes for the Better

Réseaux

MITSUBISHI ELECTRIC
Changes for the Better

Définition

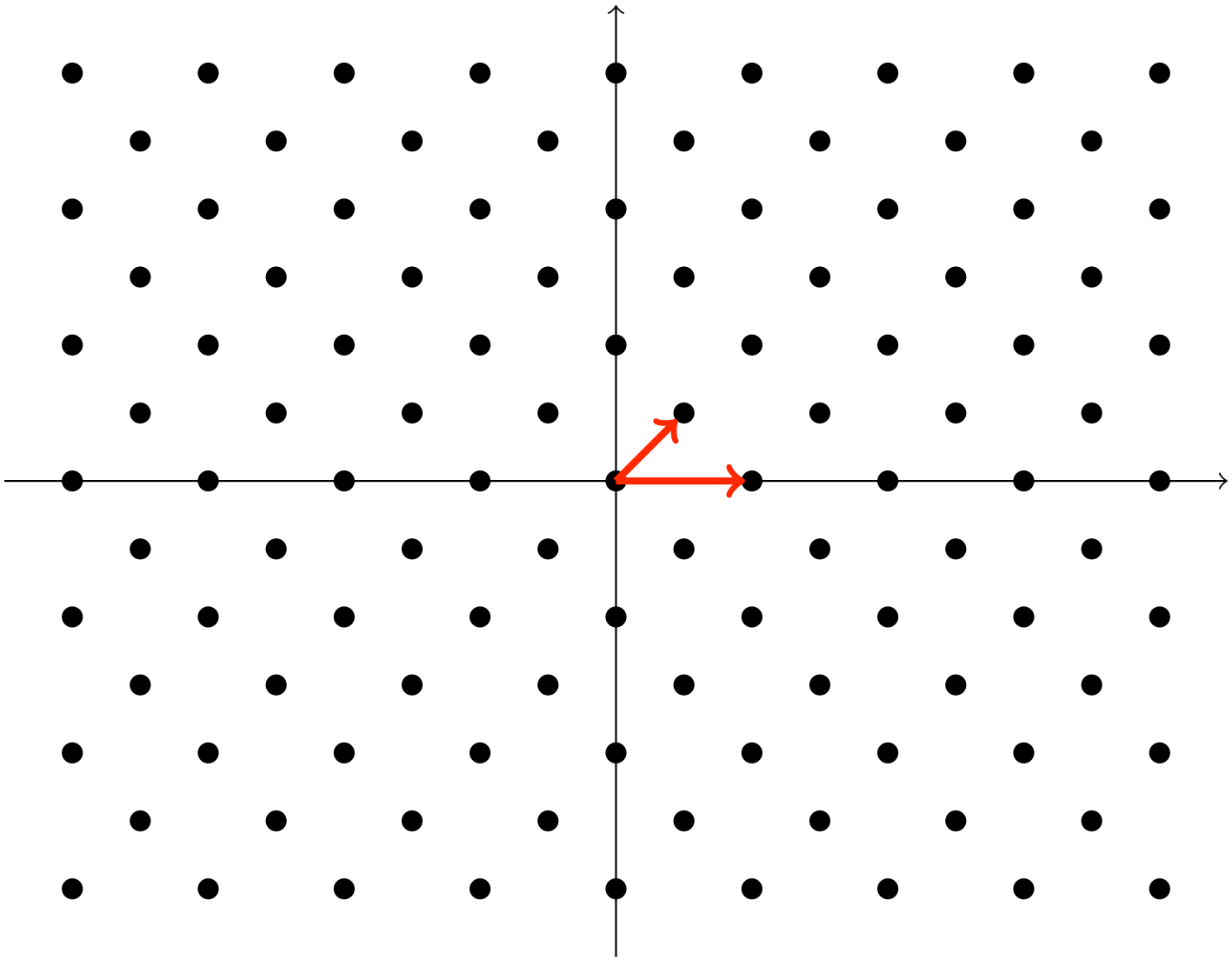
Un réseau (n-dimensionnel) est un sous-groupe additif discret de $\mathbb{R}^n$.

Un réseau $\Lambda \subseteq \mathbb{R}^n$ est identifié par une base $\{b_1, \ldots, b_n\}$, $b_i \in \mathbb{R}^n$.

$$\Lambda = \mathbb{Z}^n G, \quad \text{où les lignes de } G \text{ sont les } b_i\text{'s.}$$

- Le volume de Λ est $\mathrm{vol}(\Lambda) := |\det(G)|$.
- Pour tout $x = (x_1, \ldots, x_n) \in \Lambda$, $||x|| = \sqrt{x_1^2 + \ldots + x_n^2}$.
- La distance euclidienne minimale est $d_{\min}(\Lambda) := \min_{x \in \Lambda \setminus \{0\}} ||x||$.

Exemple bidimensionnel



La Construction A voir Conway, Sloane, *SPLAG*, 1988

MITSUBISHI ELECTRIC
Changes for the Better

Les ingrédients :

La Construction A voir Conway, Sloane, *SPLAG*, 1988

Les ingrédients :

- Soit L un réseau de petite dimension.
  (p. ex. $L = \mathbb{Z}$ ou $L = \mathbb{Z}[i] \cong \mathbb{Z}^2$)

La Construction A voir Conway, Sloane, *SPLAG*, 1988

MITSUBISHI ELECTRIC
Changes for the Better

Les ingrédients :

- Soit L un réseau de petite dimension.
  (p. ex. $L = \mathbb{Z}$ ou $L = \mathbb{Z}[i] \cong \mathbb{Z}^2$)

- Soit p un nombre premier et L' un sous-réseau de L tel que

$$\boxed{L/L' \cong \mathbb{F}_p}$$

(p. ex. $L' = p\mathbb{Z}$ ou $L' = (a+ib)\mathbb{Z}[i]$ avec $a^2 + b^2 = p$)

La Construction A voir Conway, Sloane, *SPLAG*, 1988

MITSUBISHI ELECTRIC
Changes for the Better

Les ingrédients :

- Soit L un réseau de petite dimension.
  (p. ex. $L = \mathbb{Z}$ ou $L = \mathbb{Z}[i] \cong \mathbb{Z}^2$)

- Soit p un nombre premier et L' un sous-réseau de L tel que

$$\boxed{L/L' \cong \mathbb{F}_p}$$

  (p. ex. $L' = p\mathbb{Z}$ ou $L' = (a+ib)\mathbb{Z}[i]$ avec $a^2 + b^2 = p$)

- Soit $\Pi : L^\ell \to (L/L')^\ell$ la projection naturelle.

La Construction A voir Conway, Sloane, *SPLAG*, 1988

MITSUBISHI ELECTRIC
Changes for the Better

Les ingrédients :

- Soit L un réseau de petite dimension.
  (p. ex. $L = \mathbb{Z}$ ou $L = \mathbb{Z}[i] \cong \mathbb{Z}^2$)

- Soit p un nombre premier et L' un sous-réseau de L tel que

$$\boxed{L/L' \cong \mathbb{F}_p}$$

  (p. ex. $L' = p\mathbb{Z}$ ou $L' = (a+ib)\mathbb{Z}[i]$ avec $a^2 + b^2 = p$)

- Soit $\Pi : L^\ell \to (L/L')^\ell$ la projection naturelle.
- Soit $C = C[\ell, k]_p \subseteq \mathbb{F}_p$ un code p-aire linéaire.

La Construction A voir Conway, Sloane, *SPLAG*, 1988

MITSUBISHI ELECTRIC
Changes for the Better

Définition

Un réseau obtenu par construction A est

$$\Lambda = \{x \in L^\ell \mid \Pi(x) \in C\}.$$

(N'oubliez pas : $\Pi : L^\ell \to (L/L')^\ell \cong \mathbb{F}_p^\ell$).

La Construction A voir Conway, Sloane, *SPLAG*, 1988

MITSUBISHI ELECTRIC
Changes for the Better

Exemple 1

Cas $(L, L') = (\mathbb{Z}, p\mathbb{Z})$, $\ell = n$:

$$G = \begin{pmatrix} \mathbb{1}_k & \Phi(B) \\ 0 & p\mathbb{1}_{n-k} \end{pmatrix}.$$

- $(\mathbb{1}_k \; B)$ est une matrice génératrice $k \times n$ pour C.
- $\Phi : \mathbb{F}_p \hookrightarrow \{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\} \subseteq \mathbb{Z}$.
- $\Lambda = \{x \in \mathbb{Z}^n \mid (x \mod p) \in C\} = \Phi(C) + p\mathbb{Z}^n$.

La Construction A voir Conway, Sloane, *SPLAG*, 1988

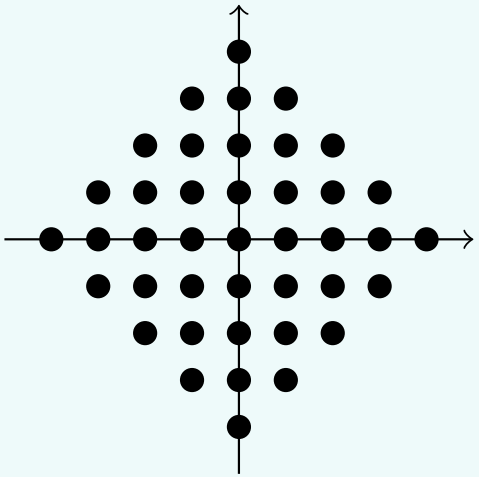
MITSUBISHI ELECTRIC
Changes for the Better

Exemple 2

Cas $(L, L') = (\mathbb{Z}[i], (a+ib)\mathbb{Z}[i])$, $a^2 + b^2 = p$, $\ell = \frac{n}{2}$:

$$G = \begin{pmatrix} \mathbb{1}_k & \Phi(B) \\ 0 & (a+ib)\mathbb{1}_{\frac{n}{2}-k} \end{pmatrix}.$$

- $(\mathbb{1}_k \; B)$ est une matrice génératrice $k \times \frac{n}{2}$ pour C.
- $\Phi : \mathbb{F}_p \hookrightarrow \mathbb{Z}[i]$.
- $\Lambda = \Phi(C) + (a+ib)\mathbb{Z}[i]^{\frac{n}{2}}$



Un exemple de $\Phi : \mathbb{F}_{41} \hookrightarrow \mathbb{Z}[i]$.

Les Réseaux LDA et le canal Gaussian

Décoder un réseau est algorithmiquement très coûteux.

Idée : adapter le décodage LDPC aux réseaux.

Définition

Un réseau LDA Λ est un réseau obtenu par construction A à partir d'un code LDPC p-aire $C \subseteq \mathbb{F}_p^n$.

Les Réseaux LDA et le canal Gaussian

Décoder un réseau est algorithmiquement très coûteux.

Idée : adapter le décodage LDPC aux réseaux.

Définition

Un réseau LDA Λ est un réseau obtenu par construction A à partir d'un code LDPC p-aire $C \subseteq \mathbb{F}_p^n$.

Le canal AWGN

1. Message non codé : $z \in \mathbb{Z}^n$.
2. Message codé : $x = zG \in \Lambda$.
3. Sortie du canal : $y = x + \eta$, où $\eta_i \sim \mathcal{N}(0, \sigma^2)$.
4. Le décodeur doit obtenir x à partir de y. En suite, $z = xG^{-1}$.

Décodage des réseaux LDA (construction p-aire)

MITSUBISHI ELECTRIC
Changes for the Better

- Pour des grandes dimensions ($n \geq 200$), nous devons utiliser un décodage itératif.
  Complexité : linéaire en n, proportionnelle à p^2.

- $x \in \Lambda$, nous avons $x = c + ps$, $\exists\ c \in C,\ s \in \mathbb{Z}^n$.

- Coordonnée par coordonnée, le décodage est basé sur

$$\mathrm{APP}(x_i) = p(x_i|C, y) \propto p(x_i|y_i) \times p(x_i|C, y \setminus \{y_i\}).$$

- $p(x_i|y_i) \propto \exp\left(-\frac{(y_i - x_i)^2}{2\sigma^2}\right)$ peut être évaluée à l'intérieur d'une fenêtre W centrée en y_i et d'amplitude limitée.

Décodage des réseaux LDA (construction p-aire)

- Pour le décodage du code LDPC :

$$p(c_i|y_i) \approx \sum_{x_i \in W \mid x_i \equiv c_i} p(x_i|y_i).$$

- Si $|\{x_i \in W \mid x_i \equiv c_i\}| = \mu$,

$$p(x_i|C, y \setminus \{y_i\}) \approx \frac{1}{\mu} p(c_i|C, y \setminus \{y_i\}).$$

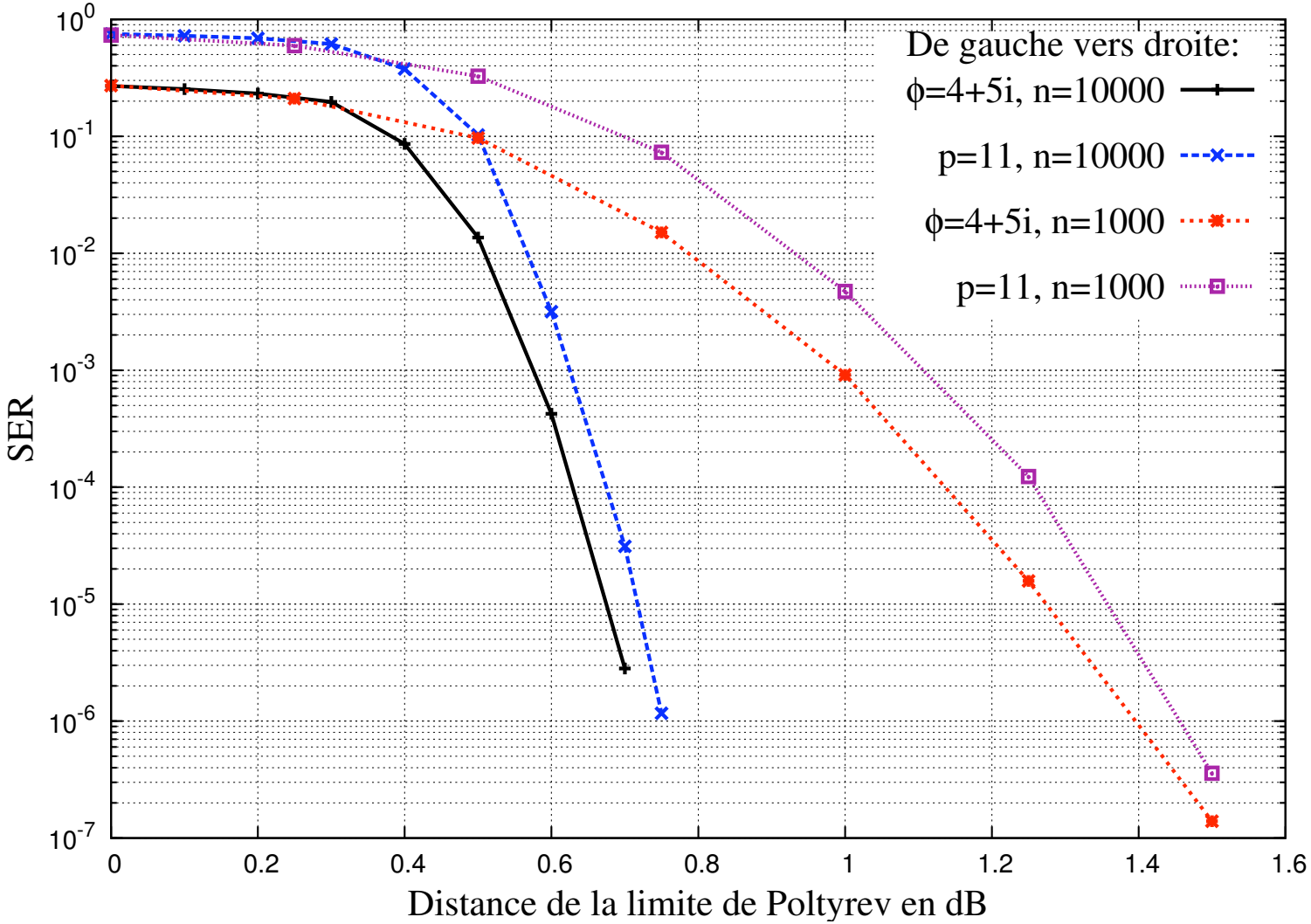
- Le décodage d'un nœud de parité du code LDPC est fait par l'algorithme «forward-backward» sur le trellis des syndromes (Bahl, Cocke, Jelinek, and Raviv, 1974).

Capacité du canal AWGN

- Capacité du canal : $\frac{1}{2}\log(1+\mathrm{SNR})$.
- Mais : nous décodons le réseau infini («*lattice decoding*») :
  - $\rightarrow$ le décodeur peut rendre n'importe quel point du réseau ;
  - $\rightarrow$ c.-à-d., le décodeur ne considère pas la région de «shaping».
- Plus de capacité traditionnelle.
- Poltyrev (1994) définit une capacité généralisée, qui se traduit en :

Bruit maximal : $\boxed{\sigma^2_{max} = \frac{\mathrm{vol}(\Lambda)^{\frac{2}{n}}}{2\pi e}}$

Performances



Conclusion : LDA et les autres familles

MITSUBISHI ELECTRIC
Changes for the Better

Concurrents des LDA :

1. Réseaux LDLC, par Sommer, Feder, and Shalvi, 2006-2008.
2. Réseaux LDPC, par Sadeghi, Banihashemi, Panario, 2004-2006.
3. Réseaux Turbo, par Sakzad, Sadeghi, Panario, 2010-2011.

	$\subseteq \mathbb{Z}^n$	Perf.	Codes embriqués	Complexité
LDPC	Oui	-	m pour $p = 2^m$	Ok pour m petit
LDLC	No	+	1	Implém. plus difficile
Turbo	Oui	+	m pour $p = 2^m$	Ok pour m petit
LDA	Oui	+	1	Ok

The end

MITSUBISHI ELECTRIC
Changes for the Better

Merci de votre attention !