

# Reconstruction de codes cycliques et peut-être quasi-cycliques...

Christophe Chabot

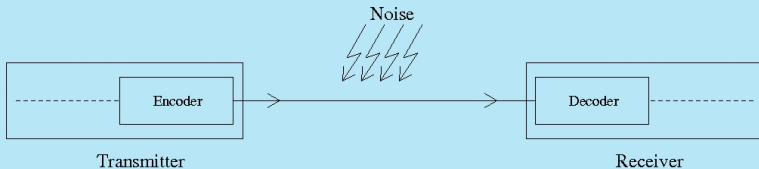
Université de Limoges - XLIM - DMI - PI2C  
INRIA Rocquencourt - Projet CODES

Séminaire AINTERCOM - 29/11/2007

# Sommaire

- 1 Introduction
- 2 Reconnaissance d'un code
- 3 Codes maximaux
- 4 Codes cycliques
  - Approche algébrique
  - Reconstruction
- 5 Codes quasi-cycliques
  - Approche algébrique
  - Perspectives
- 6 Conclusion

# Introduction



- Reconstruction de codes aléatoires :  
→ Valembois, Cluzeau, Finiasz.
- En pratique, peu de codes utilisés :
  - décodables → structure algébrique.
  - familles de codes.

## Reconnaissance d'un code

- $C$  : code en bloc linéaire de longueur  $n$ .
- $S$  : séquence de mots de  $C$  bruités.
- $C_0$  : code de longueur  $n$ .

**Question** : Est-ce que  $S$  est une séquence de mots de  $C_0$  bruités ?  
(i.e.  $C \subset C_0$  ?)

→ Revient à tester si  $S$  est composée de mots bruités du dual de  $C_0^\perp$  (i.e.  $C \subset (C_0^\perp)^\perp$ ).

## Reconnaissance d'un code

Entrée :

- $S = (x_i)_{i=1,\dots,N}$  : séquence de mots bruités de  $C$ .
- $H = (h_j)_{j=1,\dots,n-k}$  : matrice de parité de  $C_0$ .

Algorithme :

- Calculer  $N_j := \sum_{i=1}^N \langle h_j, x_i \rangle$ , pour  $j = 1, \dots, n - k$ .

Résultat :

- Si  $N_j \leq T$ , pour tout  $j = 1, \dots, n - k$ , répondre **OUI**.
- Sinon, répondre **NON**.

## Codes maximaux

Soit  $\mathcal{C}$  une famille de codes linéaires sur  $\mathbb{F}$  de longueur  $n$  contenant le code trivial  $\mathbb{F}^n$ .

L'inclusion  $\subset$  est une relation d'ordre sur  $\mathcal{C}$ . On a donc la notion d'éléments maximaux :

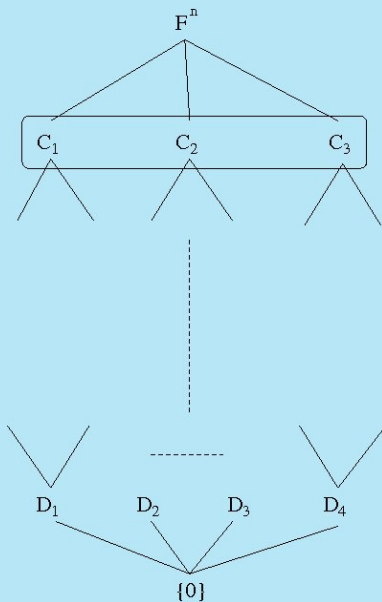
Un élément  $C \in \mathcal{C}$  est dit maximal si : dès que l'on a  $C \subsetneq D$  et  $D \in \mathcal{C}$ , alors  $D = \mathbb{F}^n$ .

Soit  $\mathcal{C}_{max} := \{C_0, \dots, C_r\}$  l'ensemble des éléments maximaux de  $(\mathcal{C}, \subset)$ .

Ainsi, pour tout  $C \in \mathcal{C}$ ,  $C \neq \mathbb{F}^n$ , il existe  $i \in \{1, \dots, r\}$  tel que

$$C \subset C_i$$

# Codes maximaux



## Codes maximaux

### Définition :

Soit  $C \in \mathcal{C}$ , on note

$$I(C) := \{i \in \{1, \dots, r\} \mid C \subset C_i\} \text{ le support de } C.$$

Et pour  $I \subset \{1, \dots, r\}$ , on note

$$\mathcal{C}_I := \{C \in \mathcal{C} \mid I(C) = I\}.$$

### Propriété :

Les  $\mathcal{C}_I$  forment une partition de  $\mathcal{C}$  :  $\mathcal{C} = \bigsqcup_{I \in \mathcal{P}(\{1, \dots, r\})} \mathcal{C}_I$

### Principe :

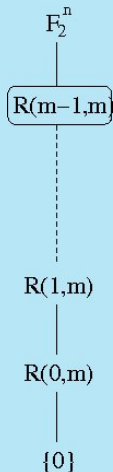
Si  $C \in \mathcal{C}$ , alors  $C$  appartient à la sous-famille  $\mathcal{C}_{I(C)}$ .

### Remarque :

Plus la sous-famille  $\mathcal{C}_{I(C)}$  est petite, mieux c'est !

## Exemple : Codes de Reed-Muller

Soit  $\mathcal{C}$  la famille des codes de *Reed-Muller* de longueur  $2^m$ .



# Codes cycliques

## Approche algébrique

**Définition :** Soit  $\mathbb{F}$  un corps de caractéristique  $p$ . Soit  $n$  un entier premier avec  $p$ . Un code cyclique de longueur  $n$  sur  $\mathbb{F}$  est un idéal de l'anneau quotient  $R_n := \mathbb{F}[X]/\langle X^n - 1 \rangle$ .

**Propriétés :** Soit  $C$  un code cyclique de longueur  $n$  sur  $\mathbb{F}$ .

- $C$  est un idéal principal de  $R_n$ .
- Il existe un unique polynôme unitaire  $g(X)$  de plus bas degré dans  $C$ .
- $C = \langle g(X) \rangle$ .
- $g(X)$  divise  $X^n - 1$ .

## Approche algébrique

On a la bijection suivante :

$$\begin{array}{ccc} \phi & : & \{\text{diviseurs de } X^n - 1\} \longrightarrow \{\text{codes cycliques de longueur } n\} \\ & & g(X) \longmapsto \langle g(X) \rangle \end{array}$$

Si on considère  $\mathcal{C}$  la famille des codes cycliques de longueur  $n$ ,

$$\mathcal{C}_{max} = \phi(\{\text{facteurs irréductibles de } X^n - 1\})$$

Si on note  $g_1(X), \dots, g_r(X)$  les facteurs irréductibles de  $X^n - 1$ , alors

$$\mathcal{C}_{max} = \{C_i := \langle g_i(X) \rangle\}_{i=1, \dots, r}$$

et pour tout  $I \in \mathcal{P}(\{1, \dots, r\})$ ,  $\mathcal{C}_I = \left\{ \bigcap_{i \in I} C_i \right\}$ .

## Reconstruction

Soit  $C$  un code cyclique de longueur  $n$ .

Soit  $S = (x_j)_{j=1,\dots,N}$  une séquence de mots bruités de  $C$ .

Pour  $i$  de 1 à  $r$ , on teste si  $S$  est une séquence de mots bruités du dual de  $C_i^\perp$ .

$$\text{Mais } C_i^\perp = \langle g_i(X) \rangle^\perp = \left\langle \left( \frac{X^n - 1}{g_i(X)} \right)^* \right\rangle =: \langle h_i(X) \rangle.$$

Il suffit donc de vérifier si  $S$  est orthogonale (au bruit près) à

$$h_i(X), X.h_i(X), \dots, X^{\deg(g)-1}.h_i(X).$$

# Codes quasi-cycliques

## Approche algébrique

Soit  $C$  un code quasi-cyclique de longueur  $n$ , d'indice  $l$  sur  $\mathbb{F}_q$ .  
Soit  $\sigma$  l'opération de shift vers la droite.

- $C$  est stable par  $\sigma^l$ .
- $C \subset \mathbb{F}_q^{n=lm} \longleftrightarrow C' \subset (\mathbb{F}_q^l)^m =: \mathbb{A}^m$ .
- $C'$  est cyclique sur  $\mathbb{A}$ .

## Codes quasi-cycliques

Soit  $M := M_{l,l}(\mathbb{F}_q)$ .

**Structure de  $M[X]$  module à gauche sur  $\mathbb{A}^m$  :**

Si on note  $\tau$  le shift à gauche sur  $\mathbb{A}^m$ ,  $X^i.c := \tau^i(c)$ .

$$\begin{aligned}
 M[X] \times \mathbb{A}^m &\longrightarrow \mathbb{A}^m \\
 (P(X), c) &\longmapsto P.c := \sum_{i=0}^{\deg(P)} p_i \tau^i(c) \\
 &= \left( \sum_{i=0}^{\deg(P)} p_i c_{i+j} \right)_{j=0, \dots, m-1}
 \end{aligned}$$

où  $P(X) = \sum_{i=0}^{\deg(P)} p_i X^i$  et  $c = (c_0, \dots, c_{m-1})$

# Codes quasi-cycliques

## Propriétés

Soient  $f \in M[X]/\langle X^m - 1 \rangle$ ,  $C$  un sous-e.v. de  $\mathbb{F}_q^{lm}$  ( $C \subset \mathbb{A}^m$ ).

On note :

- $\Omega(f) := \{x \in \mathbb{A}^m / f.x = 0\}$  ( $\mathbb{F}_q$ -espace vectoriel).
- $Ann(C) := \{P \in M[X]/\langle X^m - 1 \rangle / P.x = 0, \forall x \in C\}$ .  
(idéal à gauche de  $M[X]/\langle X^m - 1 \rangle$ ).

**Résultats principaux :**

Soient  $f, Q \in M[X]/\langle X^m - 1 \rangle$  réversibles tels que  $fQ = X^m - 1$ .

- $Ann(C)$  n'est pas forcément principal.
- En général,  $\Omega(Ann(C)) \neq C$ .
- $\dim_{\mathbb{F}_q}(\Omega(f)) = l \deg(f)$ .
- $Ann(\Omega(f)) = \langle f \rangle$ .
- $\Omega(f) = Q.\mathbb{A}^m$ .
- $\Omega(f)^\perp = \Omega({}^t Q^*)$ .

# Codes quasi-cycliques

## Codes maximaux

Soient :

- $\mathcal{C} := \{\text{codes } l\text{-quasi cycliques de longueur } lm\}$ .
- $\mathcal{C}' := \{C \in \mathcal{C} / \exists f \text{ diviseur à gauche réversible de } X^m - 1, C \subset \Omega(f)\}$ .
- $\mathcal{C}'' := \{\Omega(f)/f \text{ diviseur à gauche réversible de } X^m - 1\}$ .

Propriétés :

- $\mathcal{C}'' \subset \mathcal{C}' \subset \mathcal{C}$ .
- Si  $l \geq 2$ ,  $\mathcal{C}'' \neq \mathcal{C}'$ .
- $\mathcal{C}''_{\max} = \{\Omega(f)/\nexists g = af, g \text{ diviseur à gauche de } X^m - 1\}$ .

Questions :

- Éléments maximaux de  $\mathcal{C}'$  et  $\mathcal{C}$  ?
- $\mathcal{C}' \subsetneq \mathcal{C}$  ?

# Conclusion

- Reconstruction → Reconstruction par familles.
- Méthode utilisant la notion de “base”.
- Recherche exhaustive → Recherche sur la base.  
exponentiel → linéaire
- Problème : permutations.