

Reconstruction de familles de codes

Application aux codes cycliques

Christophe Chabot

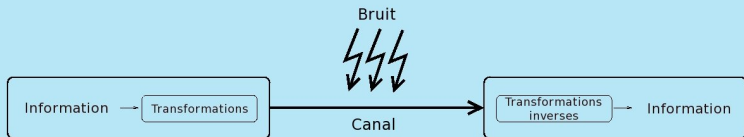
Université de Limoges - XLIM - DMI - PI2C
INRIA Rocquencourt - Projet CODES

Séminaire PI2C - Limoges - 15/01/2008

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.

Reconstruction d'un code aléatoire

Problème : (Réduction de rang)

Etant donnés $X \in M_{M,n}(\mathbb{F}_2)$, $k \in \mathbb{N}$ et $\omega \in \mathbb{N}$,
peut-on trouver $E \in M_{M,n}(\mathbb{F}_2)$ telle que :

- $\text{rg}(X + E) \leq k$
- $w_H(E) \leq \omega$

→ problème *NP-complet* (A. Valembois).

Reconstruction d'un code aléatoire

Sans bruit :

$$(h_0, \dots, h_{n-1}) \left(\begin{array}{|c|c|c|c|} \hline & & & \\ \hline x_1 & x_2 & \dots & \dots & x_M \\ \hline \end{array} \right)$$
$$(0 , 0 , \dots , 0)$$

Reconstruction d'un code aléatoire

Avec bruit :

$$(h_0, \dots, h_{n-1}) \left(\begin{array}{|c|c|c|c|} \hline & & & \\ \hline x_1 & x_2 & \dots & \dots & x_M \\ \hline \end{array} \right)$$

$$(0 , 1 , \dots , 0)$$

→ recherche de mots de poids faible (*Canteaut-Chabaud*).

Reconstruction d'un code aléatoire

Résultats expérimentaux :

Code	Longueur	p	Temps
LDPC	100	0.01	1s
LDPC	100	0.02	30s
LDPC	100	0.03	6min
LDPC	250	0.005	10min
LDPC	1000	0.001	1h
LDPC	1000	0.002	>12h
aléatoire	100	0.005	1s
aléatoire	100	0.01	1s
aléatoire	100	0.02	10min

→ $n = 10000$, $p = 10^{-3}$.

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. $C \subset C_0$?)

Sans bruit pour $x \in \mathbb{F}_2^n$, $P(\langle h, x \rangle = 1) = \frac{1}{2}$
 pour $c \in h^\perp$, $P(\langle h, c \rangle = 1) = 0$

Avec bruit pour $x \in \mathbb{F}_2^n$, $P(\langle h, x + \mathbf{e} \rangle = 1) = \frac{1}{2}$
 pour $c \in h^\perp$, $P(\langle h, c + \mathbf{e} \rangle = 1)$ est petite.

→ 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 :

Définition :

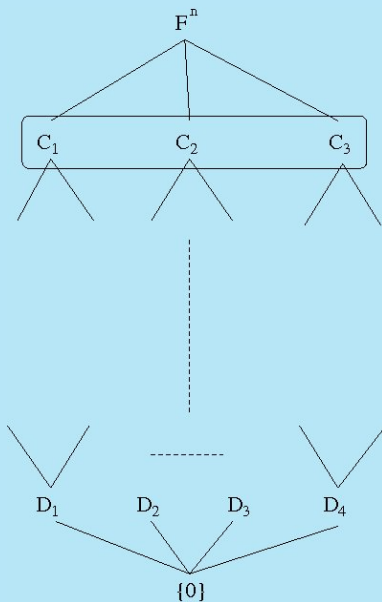
Un élément $C \in \mathcal{C}$ est dit maximal si : dès que l'on a $C \subsetneq D$ et $D \in \mathcal{C}$, alors $D = \mathbb{F}^n$.

Soit $\mathcal{C}_{max} := \{C_1, \dots, C_r\}$ 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} : $\mathcal{C} = \bigsqcup_{I \in \mathcal{P}(\{1, \dots, r\})} \mathcal{C}_I$

Codes maximaux

Principe :

Si $C \in \mathcal{C}$,

- on calcule $I(C)$ (revient à vérifier si $C \subset C_i$, $i = 1, \dots, r$)
- on construit $\mathcal{C}' := \mathcal{C}_{I(C)}$

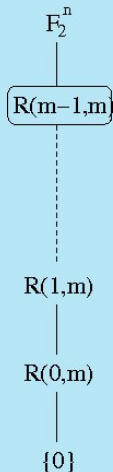
et finalement, C appartient à la sous-famille \mathcal{C}' .

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

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

Reconstruction

Résultats expérimentaux :

Longueur n	$\#C_{max}$ r	Erreur p	Temps Cluzeau	Temps Notre algo.
123	8	0.01	≤ 1 s	≤ 1 s
123	8	0.02	7 min	3 s
511	59	0.001	≤ 1 s	≤ 1 s
511	59	0.002	≥ 10 min	1 s
511	59	0.005		14 s
1011	34	0.001	≥ 10 min	2 s
1011	34	0.002		9 s
1011	34	0.003		66 s

- Algo codes cycliques en *Magma*.
- Algo de *M. Cluzeau* en *C*.

Codes quasi-cycliques

Approche algébrique

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

- C est stable par σ^ℓ .
- $C \subset \mathbb{F}_q^{n=\ell m} \longleftrightarrow C' \subset (\mathbb{F}_q^\ell)^m =: \mathbb{A}^m$.
- 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 τ 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 $\mathbb{F}_q^{\ell m}$ ($C \subset \mathbb{A}^m$).

Définition :

- $\Omega(f) := \{x \in \mathbb{A}^m / f.x = 0\}$ (\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 $M[X]/\langle X^m - 1 \rangle$).

Codes quasi-cycliques

Propriétés

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, $\Omega(Ann(C)) \neq C$.
- $\dim_{\mathbb{F}_q}(\Omega(f)) = \ell \deg(f)$.
- $Ann(\Omega(f)) = \langle f \rangle$.
- $\Omega(f) = Q \cdot \mathbb{A}^m$.
- $\Omega(f)^\perp = \Omega({}^t Q^*) = {}^t f^* \cdot \mathbb{A}^m$.

Codes quasi-cycliques

Codes maximaux

Soient :

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

Propriétés :

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

Questions :

Éléments maximaux de \mathcal{C}' et \mathcal{C} ?

Conclusion

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

Merci de votre attention.