Théorie et codage de l'information

Les codes de Hamming et les codes cycliques

- Chapitre 6 (suite et fin)-

Les codes de Hamming

Principe

La distance minimale d'un code linéaire $\mathcal{L}$ est le plus petit nombre de colonnes linéairement dépendantes dans sa matrice de test $\mathbf{H}$. Pour un $[n, k, 3]$-code, aucune colonne de $\mathbf{H}$ n'est multiple d'une autre.

Construction

Les codes de Hamming sont des $[n, k, 3]$-codes construits ainsi :

1. choix d'un vecteur-colonne c_1 non-nul dans $(\mathbf{F}_q)^r$
2. choix d'un vecteur-colonne c_2 dans $(\mathbf{F}_q)^r - \{\alpha.c_1 : \alpha \in \mathbf{F}_q^\star\}$
3. réitération jusqu'à ce qu'il n'y ait plus de c_i non-nul

Les codes de Hamming

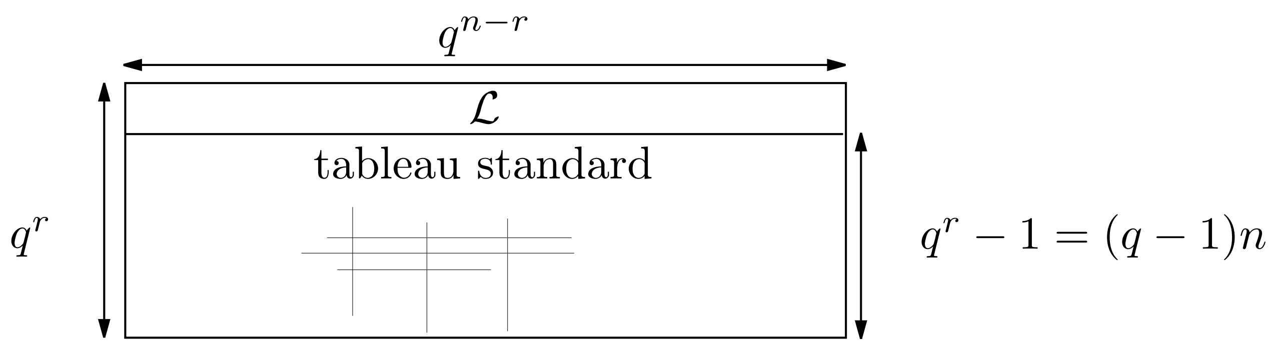
Intérêts

Notations

Un $[n,k,d]$-code de Hamming q-aire d'ordre r, noté $\mathcal{H}_q(r)$, est tel que :

$$n = (q^r - 1)/(q-1) \quad ; \quad k = n - r \quad ; \quad d = 3$$

Décodage des codes de Hamming



On constate que $(q-1)n$ représente aussi le nombre d'erreurs possibles de poids 1 !

$\triangleright$ le syndrome de e_i est donc égal à la $i^{\text{ème}}$ colonne de $\mathbf{H}$.

Décodage des codes de Hamming $\mathcal{H}_2(r)$

Exemple

Les colonnes de la matrice de contrôle $\mathbf{H}$ sont simplement les représentations binaires des $2^r - 1$ premiers nombres positifs non-nuls.

$\triangleright$ syndrome = position de l'erreur à corriger

Exemple : $\mathcal{H}_2(3)$

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

En supposant qu'une unique erreur s'est produite à la position 3, ce qui correspond au vecteur d'erreur donné par $e_3 = 0010000$, le syndrome du mot reçu est égal à $e_3\mathbf{H}^\top = 011$. Ce nombre donne la position de l'erreur.

Décodage des codes de Hamming $\mathcal{H}_3(r)$

Exemple

Comme pour $\mathcal{H}_2(r)$, on choisit les colonnes de $\mathbf{H}$ comme l'expression des premiers nombres dans une base ternaire, en s'assurant que la première composante non-nulle de ces nombres est 1.

Exemple : $\mathcal{H}_3(3)$

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

Si une erreur apparaît à la position i, le vecteur d'erreur est de la forme $\alpha\, e_i$, avec $\alpha \in \{1, 2\}$. Le syndrome résultant $\alpha\, e_i \mathbf{H}^\top$.

$\triangleright$ on détermine la position de l'erreur et la correction à apporter.

Principe des codes cycliques

Définition

Les codes cycliques $\mathcal{C}$ constituent l'une des classes les plus importantes parmi les codes linéaires.

Définition 1. *Un code $\mathcal{C}$ est dit cyclique s'il est linéaire et s'il vérifie la propriété suivante :*

$$(c_0 \ldots c_{n-1}) \in \mathcal{C} \iff (c_{n-1} c_0 \ldots c_{n-2}) \in \mathcal{C}.$$

La permutation circulaire des composantes est appelée *shift*. On peut dire que $(c_{n-1} c_0 \ldots c_{n-2})$ est le shift de $(c_0 \ldots c_{n-1})$.

Principe des codes cycliques

Exemples

Les codes suivants sont des exemples de codes cycliques, qui ne présentent pas tous un intérêt pratique :

- $\{0\}$ et $(\mathbf{F}_q)^n$
- $\mathcal{C} = \{000, 101, 011, 110\}$
- Soit $\mathcal{C}$ le code dont la matrice génératrice est définie par

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{array}{l} \longrightarrow \quad \mathbf{G}^{(1)} \\ \longrightarrow \quad \mathbf{G}^{(2)} \\ \longrightarrow \quad \mathbf{G}^{(3)} \end{array}$$

Représentation polynômiale

Intérêt

Il est commode d'utiliser la représentation polynômiale suivante :

$$(c_0 c_1 \ldots c_{n-1}) \longleftrightarrow m(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}.$$

En effet, le polynôme associé au mot shifté $(c_{n-1} c_0 \ldots c_{n-2})$ est celui que l'on obtient en évaluant $x.m(x)$ modulo $(x^n - 1)$:

$$\begin{aligned} c_{n-1} + c_0 x + \ldots + c_{n-2} x^{n-1} &= x(c_0 + \cdots + c_{n-1} x^{n-1}) - c_{n-1}(x^n - 1) \\ &\equiv x.m(x) \text{ modulo } (x^n - 1). \end{aligned}$$

Représentation polynômiale

Cadre algébrique

Définition 2. *Soit* $\mathbf{F}_q$ *un corps fini et soit* n *un entier non-nul. On appelle représentation polynômiale de* $(\mathbf{F}_q)^n$ *l'application*

$$\theta : (\mathbf{F}_q)^n \longrightarrow \mathbf{F}_q[x]/ < x^n - 1 >$$

telle que $\theta(c_0 c_1 \ldots c_{n-1}) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$.

Définition 3. *On appelle représentation polynômiale de* $\mathcal{C}$ *l'ensemble des représentations polynômiales des mots de* $\mathcal{C}$*, que l'on note* $\theta(\mathcal{C})$.

Exemple

Si $\mathcal{C} = \{000, 101, 011, 110\}$, alors $\theta(\mathcal{C}) = \{0, 1 + x^2, x + x^2, 1 + x\}$ où 0 désigne ici le polynôme nul.

Structure algébrique de $\theta(\mathcal{C})$

Codes cycliques et idéaux

La définition d'un code cyclique nous amène directement à :

Théorème 1. *Le code $\mathcal{C}$ est cyclique si et seulement si $\mathcal{C}$ est un sous-espace vectoriel de $(\mathbf{F}_q)^n$ et si tout multiple modulo $(x^n - 1)$ d'un polynôme de $\theta(\mathcal{C})$ est aussi un polynôme de $\theta(\mathcal{C})$.*

En se rappelant de la définition d'un *idéal bilatère*, on obtient :

Théorème 2. *Soit $\mathcal{C}$ un code linéaire de longueur n sur $\mathbf{F}_q$. Alors $\mathcal{C}$ est un code cyclique si et seulement si sa représentation polynômiale est un idéal bilatère de l'anneau $\mathbf{F}_q[x]/ < x^n - 1 >$.*

Structure algébrique de $\theta(\mathcal{C})$

Polynôme générateur

Après avoir montré que tout idéal de l'anneau $\mathbf{F}_q[x]/ < x^n - 1 >$ est engendré par un même polynôme, dit *polynôme générateur*, on montre :

Théorème 3. *Chaque code cyclique $\mathcal{C}$ de longueur n sur $\mathbf{F}_q$, et non réduit à l'élément nul, possède un polynôme générateur unitaire et un seul qui est diviseur de $(x^n - 1)$ dans $\mathbf{F}_q[x]$.*

Exemple

Soit $\mathcal{C}$ le code cyclique tel que :

$$\theta(\mathcal{C}) = \{0, 1 + x, x + x^2, 1 + x^2\}.$$

On constate que le polynôme $(1 + x)$ est le polynôme générateur de $\mathcal{C}$.

Structure algébrique de $\theta(\mathcal{C})$

Polynôme générateur

Il est maintenant possible d'exhiber tous les codes cycliques de longueur n grâce à la recherche de tous les diviseurs de $(x^n - 1)$.

Le résultat suivant permet ensuite de trouver les mots du codes :

Théorème 4. *Soit $\mathcal{C}$ un code cyclique de longueur n et $g(x)$ son polynôme générateur tel que* $\mathrm{d}^\circ(g) = t$*. La famille suivante*

$$\{g(x), x.g(x), \ldots, x^{n-t-1}.g(x)\}$$

est une base de $\theta(\mathcal{C})$ et la dimension du code est $n - t$.

Construction d'un code cyclique

Exemple

On veut construire un code cyclique de longueur 7 sur $\mathbf{F}_2$. On montre que $(x^7 - 1) = (x-1)(x^3+x+1)(x^3+x^2+1)$, ce qui nous conduit à :

$$
\begin{aligned}
\mathcal{C}_0 : \quad g_0(x) &= x^7 - 1 \equiv 0 \\
\mathcal{C}_1 : \quad g_1(x) &= x - 1 \\
\mathcal{C}_2 : \quad g_2(x) &= x^3 + x + 1 \\
\mathcal{C}_3 : \quad g_3(x) &= x^3 + x^2 + 1 \\
\mathcal{C}_4 : \quad g_4(x) &= g_1(x).g_2(x) = x^4 + x^3 + x^2 + 1 \\
\mathcal{C}_5 : \quad g_5(x) &= g_1(x).g_3(x) = x^4 + x^2 + x + 1 \\
\mathcal{C}_6 : \quad g_6(x) &= g_2(x).g_3(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
\end{aligned}
$$

Matrice génératrice

Construction à partir du polynôme générateur

La famille $\{g(x), x.g(x), \ldots, x^{n-t-1}.g(x)\}$ est une base de $\theta(\mathcal{C})$. Il suffit donc de choisir les mots associés à cette base pour construire $\mathbf{G}$.

Théorème 5. *Soit $g(x) = g_0 + g_1 x + \ldots + g_t x^t$ le polynôme générateur d'un code cyclique $\mathcal{C}$ de longueur n sur $\mathbf{F}_q$. La matrice $\mathbf{G}$ constituée de $n-t$ lignes et n colonnes suivante est génératrice.*

$$\mathbf{G} = \begin{pmatrix} g_0 & g_1 & \ldots & g_t & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & 0 & g_t & \ldots & 0 \\ & & \ldots & & \ldots & & \\ 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_t \end{pmatrix}.$$

Matrice génératrice

Exemple

Considérons le code cyclique $\mathcal{C}$ de $(\mathbf{F}_2)^7$ engendré par le polynôme générateur $g(x) = 1 + x^2 + x^3$. D'après le théorème précédent, une matrice génératrice de ce code est donnée par :

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Chaque ligne de $\mathbf{G}$ peut être obtenue par un shift de la précédente.

Matrice de contrôle

Définition du polynôme de contrôle

On définit un polynôme de contrôle ainsi :

Définition 4. *Soit $\mathcal{C}$ un $[n, k]$-code cyclique de polynôme générateur $g(x)$. Le polynôme $h(x)$ vérifiant $g(x).h(x) = (x^n - 1)$ est dit polynôme de contrôle.*

On peut montrer le résultat suivant :

Théorème 6. *Soit $\mathcal{C}$ un $[n, k]$-code cyclique dont le polynôme de contrôle est $h(x)$. On a la relation suivante :*

$$p(x) \in \theta(\mathcal{C}) \Leftrightarrow p(x).h(x) = 0.$$

Matrice de contrôle

Construction à partir du polynôme de contrôle

Déterminons maintenant l'expression de la matrice de contrôle à partir du polynôme de contrôle.

Théorème 7. *Soit $\mathcal{C}$ un $[n,k,d]$-code cyclique de polynôme de contrôle $h(x) = h_0 + h_1 x + \ldots + h_k x^k$. La matrice* $\mathbf{H}$ *suivante est une matrice de test de $\mathcal{C}$:*

$$\mathbf{H} = \begin{pmatrix} h_k & h_{k-1} & \ldots & h_0 & 0 & \ldots & 0 \\ 0 & h_k & h_{k-1} & \ldots & h_0 & \ldots & 0 \\ & & \ldots & & \ldots & & \\ 0 & \ldots & 0 & h_k & h_{k-1} & \ldots & h_0 \end{pmatrix}.$$