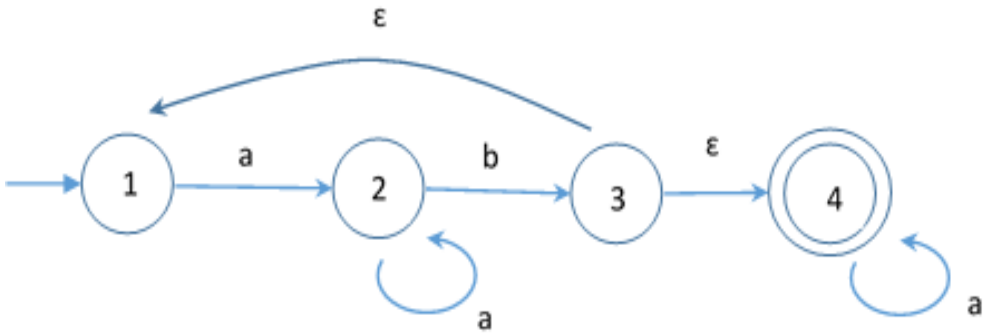
Automates – CODES (MVA004)

Codage linéaire

Par: J.SAAB



Definition:

On dit qu'un code est linéaire si pour tous m_1 et m_2 deux mots de code, la somme $m_1 \oplus m_2$ est un mot de code

⇒ LE MOT 0 EST TOUJOURS UN MOT DE CODE DANS UN CODAGE LINEAIRE

⇒ La distance de Hamming est $d = \min_i \omega(m_i)$

Un codage $f : B^k \rightarrow B^n$ est dit linéaire si f est une application linéaire

$$f(a \oplus b) = f(a) \oplus f(b)$$

Le codage de la somme deux k-blocs est la somme de leurs codes

Il suffit de coder les elements d'une base de B^k

REPRESENTATION MATRICIELLE:

- Un mot binaire de longueur k est une matrice ligne de longueur k,

$$m \in M_{1,k}(B)$$

- Une matrice generatrice d'un code $\varphi : B^k \rightarrow B^n$ est une matrice

$$G \in M_{k,n}(B)$$

- $G = (\varphi(b_i))$ avec $\{b_i\}$ est une base de B^k

Si $\varphi(b_i) = b_i a_1 \cdots a_r$ alors G sera de la forme $G = (I_k \mid P)$

Le code est dit systematique

Pour tout k-blocs b, on a $\varphi(b) = b.G$

Soit le codage systematique $G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$. On a :

$$\varphi(0\ 1\ 1) = (0\ 1\ 1).\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = (0\ 1\ 1\ 0)$$

SYNDROMES

1- Pour un codage systematique:

La matrice associee a un code lineaire systematique $G = (I_k \mid P)$

est la matrice $H = ({}^tP \mid I_r) \in M_{r,n}$

Le syndrome de m est

$m = (a_1 \cdots a_n)$ $\sigma(m) = m.{}^tH$

$$\sigma(a \oplus b) = \sigma(a) \oplus \sigma(b)$$

La matrice de controle du codage est la matrice

$$^tH = \begin{pmatrix} P \\ \hline I_r \end{pmatrix} \in M_{n,r}$$

Si $\sigma(m) = 0$ alors m est un mot de code

Decodage

1-TABLEAU DES SYNDROMES

C’est un tableau de deux colonnes:

$1^{ière}$ Colonne:	On met les 2^r mots de B^r
$2^{ième}$ Colonne:	On met dans l’ordre croissant de poids, les mots de longueur n dont les syndromes se trouvent dans la preimiere colonne

Regle de decision:

Soit R le mot recu:

1- On calcule $\sigma(R)$
2- On choisit e de la deuxieme colonne du tableau des syndromes tel que: $\sigma(R) = \sigma(e)$
3- On prend comme mot initial $C = R \oplus e$

2-Tableau standard

C’est un tableau de 2^r lignes et 2^k colonnes; chaque case est un mot de longueur n:

$1^{ière}$ ligne: On met les mots de code
$1^{ière}$ colonne et a partir de la $2^{ième}$ ligne: On place dans l’odre croissant de poids, les elements de B^n
$a_{ij} = a_{i1} \oplus a_{1j}\ ;\ \ i, j \geq 2$

REGLE DE DECISION

1- Si le mot recu est R, on localise $R = a_{ij}$ dans le tableau

2- On suppose que le mot initial est $C = a_{1j}$

Code non systematique

Obtenir h a partir de g

$H = (v_1 \cdots v_n)$ Les v_i sont des colonnes de dimension r

Les lignes de H sont independantes

$$G.{}^t(v_1 \cdots v_n) = 0$$

On a un systeme de k vecteurs qui s'experiment en fonction de r vecteurs

On choisit les r vecteurs comme une base de B^r

Transformer un code lineaire en code systematique

- Si G n'est pas sous forme canonique $G = (I \mid P)$
- On transforme G sous cette forme grâce aux operations élémentaires:

  1- On peut échanger deux lignes de G

  2- Une ligne de G peut etre remplacée par sa C.L. avec d'autres lignes

Code de Hamming

Soit le code linéaire C=[k,n,d]. Si le code C est de Hamming H(r) alors:

$$n = 2^r - 1,\ k = n - r$$

H(r) est un codage correcteur $t \geq 1$

Un codage de Hamming est parfait $C_n^0 + C_n^1 + \cdots + C_n^t = 2^r$

$H(r)$ est de Hamming, si les colonnes de H couvrent les éléments de $B^r - \{0\}$

Code dual

$$X, Y \in B^n : \quad < X, Y >= {}^t X.Y = \sum x_i.y_i$$

C=[n,k,d] un code linéaire de matrice génératrice G. Le code

dual ou orthogonal de C est $C^{\perp} = [n, r, d']$

$$C^{\perp} = \{X \in B^n / G.X = 0\}$$

Si H est la matrice associée à C alors la matrice génératrice de $C^{\perp}$ est H

$$G(C^{\perp}) = H(C) \in M_{r,n}(B)$$

$$(C^{\perp})^{\perp} = C$$

Le code C est dit auto-orthogonal si $C \subset C^{\perp}$

C=[n,k,d] un code linéaire de matrice de contrôle H, on a:

$$l < d \leq r + 1$$

l étant le nombre de colonnes linéairement indépendantes de H.

Hamming h(r), Codage et décodage

Ontenir la matrice Génératrice et la matrice de contrôle:

La seule donnée c'est r, on a un code de Hamming H(r)

Déduction:

1) $n = 2^r - 1;\ k = n - r$

2) Les colonnes de la matrice de contrôle sont formées des éléments de $B^r - \{0\}$

$$H = \begin{pmatrix} 1 & 0 & \cdots & 1 \\ 0 & 1 & & 1 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in M_{r,\,n}(B)$$

Dans un code de Hamming les bits de contrôle sont places aux positions 2^i

$$\begin{array}{ccc} B^k & \xrightarrow{\varphi} & B^n \\ (a_1 a_2 \cdots a_k) & \rightarrow & c_1 c_2 a_1 c_3 a_2 a_3 \cdots \end{array}$$

Les c_i sont les bits de contrôle placés aux position $1 = 2^0,\ 2 = 2^1, 4 = 2^2 \cdots$

Recherche de G, la matrice génératrice:

On propose deux methods:

$1^{ière}$ méthode:

On pose $G = \begin{pmatrix} C_1 & C_2 & \cdots & C_n \end{pmatrix}$, C_i est une colonne de taille k

$H.{}^tG = 0$ donne un système linéaire en C_i de r équations

On exprime les $C_1, C_2, C_4, \cdots C_{2^i} \cdots$ en fonction des k autres C_i

On donne aux k variables du 2^{nd} membre les valeurs de la base canonique de B^k

On déduit les C_i du 1^{ier} membre et parsuite on trouve G

$2^{ième}$ méthode:

$C = c_1 \cdots c_n$ un mot de code. On a $H.{}^tC = 0$

$H.{}^tC = 0$ donne un système linéaire en c_i de r équations

On exprime les bits de contrôle de C en fonction des bits d'informations

On sait que $C = (c_1 \cdots c_n) = (c_3 c_5 c_6 c_7 c_9 \cdots).G$

Le mot de code est donné par le produit de ses bits d'info par G

On obtient $G = \left(g_{ij}\right)$ par identification de $(c_1 \cdots c_n) = (c_3 c_5 c_6 c_7 c_9 \cdots).G$

Codage et décodage par H(r)

1-Codage:

Pour coder m, une chaîe de bits, on la découpe en de blocs de logueur k

Chaque bloc $a_1 \cdots a_k$ de m sera codé par $(a_1 \cdots a_k).G$

Le codage de m est suite de codages de chacun de ses k blocs

2-Décodage:

Pour décoder m, une chaîe de bits, on la découpe en de blocs de logueur n

Pour décoder le n-bloc C, ils uffit de détecter la position du bit erroneé

1) $HC = 0$ et donc C est un mot de code

2) $HC \neq 0$ et HC représente une colonne H

La position de HC dans H est la position du bit erroné de C

La correction de C sera en modifiant ce bit

Code cyclique

Un code linéaire est dit cyclique si pour tout mot de code $a_1 a_2 a_3 \cdots a_n$ le mot $a_2 a_3 \cdots a_n a_1$ est aussi un mot de code.

Si $m = a_1 \cdots a_p \cdots a_n \in B$ le deplacement de m d'ordre p est $D_m^p = a_{p+1} \cdots a_n a_1 \cdots a_p$

Dans un codage cyclique, si m est un mot de code alors tout deplacement D_m^p de m est un mot de code

Un polynôme binaire de degré k s'écrit $P(X) = a_0 X^k \oplus \cdots \oplus a_{k-1} X \oplus a_k$; les $a_i \in B$

Propriétés:

$1 - P(X) \oplus P(X) = 0$

$2 - P(X) \oplus Q(X) = R(X) \Leftrightarrow P(X) \oplus R(X) = Q(X) \Leftrightarrow Q(X) \oplus R(X) = P(X)$

$3 -$ Si $d^\circ A(X) \leq d^\circ B(X)$ alors $A(X) = B(X) \oplus Q(X) \oplus R(X)$; avec $d^\circ R < d^\circ B$

$4 -$Si $m = a_1 \cdots a_n$ est un mot de code alors $P_m(X) = a_1 X^{n-1} \oplus \cdots \oplus a_{n-1} X \oplus a_n$

est le polynôme de code de m

$5 - P_{a \oplus b}(X) = P_a(X) \oplus P_b(X)$

Code polynomial

Un code linéaire $\varphi : B^k \longrightarrow B^n$ est dit polynômial engendré par un polynôme $g(X)$ de degré r si les polynômes qui codent les éléments de B^k sont mutliples de $g(X)$.

Codages des éléments de B^k

$$a = a_1 \cdots a_k \in B^k \quad \Longrightarrow \quad i(X) = a_1 X^{k-1} \oplus \cdots \oplus a_{k-1} X \oplus a_k \quad \Longrightarrow$$

$r(X)$ est le reste de la division de $i(X).X^r$ par $g(X)$ $\Longrightarrow$

$P_a(X) = i(X).X^r + r(X)$ est le ploynôme qui code a

La matrice génératrice systèmatique associée à un code polynomial engendré par g(X) est une matrice dont les lignes représentent les mots de code associés aux éléments de base de B^k

La matrice systématique du codage engendré par $g(X)$ est équivalente à la matrice :

$$\begin{pmatrix} X^{k-1}g(X) \\ \vdots \\ Xg(X) \\ g(X) \end{pmatrix}$$

Un code polynomial engendré par g(X) est cyclique si g(X) divise $X^n \oplus 1$

Le syndrôme de $m = a_{n-1} \cdots a_1 a_0 \in B^n$ s'obtient par deux méthodes:

$$1 - P_{\sigma(m)}(X) = a_0 r_0(X) \oplus a_1 r_1(X) \oplus \cdots \oplus a_{n-1} r_{n-1}(X)$$

$r_i(X)$ est le reste de la division de X^i par $g(X)$

$2 - P_{\sigma(m)}(X)$: représente le reste de la division de $P_m(X)$ par $g(X)$