Fabien DONIUS, Nicolas GRILL, Chérine KAMEL, Selim MILED - Ing1 Gr4

ANALYSE MATHEMATIQUE
HAMMING (7,4,3)

Projet CCE

On ne corrige pas les correcteurs

Les codes correcteurs d'erreur

ECOLE CENTRALE D'ELECTRONIQUE

ece

GROUPE ECE

Le code de Hamming est un code correcteur d'erreur généré par un polynôme générateur appelé $\mathrm{H(z)}$.

I. Génération de la matrice génératrice

La matrice génératrice du code est générée par le polynôme générateur suivant :

$$\mathrm{H(z)} = \mathrm{z}^3 + \mathrm{z} + 1$$

La matrice génératrice est obtenue en effectuant la division euclidienne de ce polynôme par les différents polynômes de transmission ne contenant qu'un seul 1.

Par exemple :

$0001 ==> 1$

$1000 ==> \mathrm{z}^3$

Ces quatre polynômes sont ensuite multipliés par le terme de plus haut degré du polynôme générateur.

Les lignes de la matrice génératrice nous sont données par les coefficients des polynômes de la manière suivante :

Message	Polynôme	Dénominateur	Quotient de la division par H(z)	Reste	Ligne de la génératrice
1000	z^3	$z^3 \times z^3 = z^6$	$z^3 + z + 1$	$z^2 + 1$	1000101
0100	z^2	$z^2 \times z^3 = z^5$	$z^2 + 1$	$z^2 + z + 1$	0100111
0010	$z^1 = z$	$z^1 \times z^3 = z^4$	z	$z^2 + z$	0010110
0001	$z^0 = 1$	$z^0 \times z^3 = z^3$	1	$z + 1$	0001011

Les lignes de la matrice génératrice sont obtenues en mettant d'abord les coefficients du polynôme représentant le message, puis en mettant les coefficients du reste de la division par $H(z)$

Nous obtenons ainsi la matrice génératrice suivante (que nous appellerons G) :

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

Or, cette matrice n'est pas exploitable sous cette forme, nous devons donc la transposer. Nous obtenons donc :

$$\mathrm{G^T} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

La matrice de parité H est générée de la même manière que la matrice génératrice, exceptée que ses lignes sont formées des coefficients du reste de la division par $H(z)$ *puis* des coefficients du polynôme représentant le message à transmettre.

Nous obtenons la matrice suivante pour la matrice de contrôle de parité :

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

II. Codage des informations à transmettre :

Nous connaissons maintenant la matrice génératrice et la matrice de contrôle de parité

Soit p la matrice représentant les données à transmettre

$p = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$ Par exemple (on pourrait prendre autre chose en l'occurrence).

Le codage des informations à transmettre est effectué en faisant le produit matriciel $G^T \cdot p$

On pose $x = G^T \cdot p$

$$x = G^T \cdot p = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1[2] \\ 1[2] \\ 0[2] \\ 1[2] \\ 2[2] \\ 2[2] \\ 3[2] \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Ici, x représente les données effectivement transmises.

III. **Réception :**

Soit R la matrice de données reçues.

Dans le cas idéal, aucune erreur n'est apparue lors de la transmission et dans ce cas $R = x$, et il suffit de passer à l'étape du décodage.

IV. **Correction des erreurs :**

Si des erreurs sont apparues au cours de la transmission :

Soit r la matrice de données reçues (ces données ont été altérées lors de la transmission).

On pose $r = x + e_i$ où e_i désigne un vecteur unitaire de l'espace considéré (c'est-à-dire un espace à 7 dimensions).

Ainsi, nous savons que nous avons une erreur à la ie place.

Nous avons : $r = x + e_i$ et en multipliant cette expression par H, nous obtenons :

$Hr = H(x + e_i) = Hx + He_i$

x étant la matrice de données transmises, nous avons $Hx = 0\,[2]$. En effet, la matrice x

Nous supposons maintenant qu'une erreur est apparue au bit 5.

Les données idéalement reçues seraient : $r = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Avec une erreur au 5e bit, nous obtenons : $r_a = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$

Il s'agit maintenant de la trouver, puis de la corriger.

Nous avons : $z = Hr_a = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2[2] \\ 3[2] \\ 2[2] \\ 2[2] \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

La matrice $z = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ correspond à la 5e colonne de la matrice de parité. Or, nous savons que l'erreur de transmission est apparue au bit 5. La matrice z est en fait un vecteur correspondant nécessairement à la une des colonnes de la matrice de contrôle de parité H et il indique la position de l'erreur détectée.

Connaissant la position de l'erreur, la correction des erreurs peut se faire de plusieurs manières :

En additionnant 1[2] ou en appliquant l'opération Xor à l'endroit de l'erreur

En permutant 1 par 0 ou 0 par 1 à l'endroit de l'erreur

Ces deux méthodes donnent exactement le même résultat, mais il peut être utile de les connaître pour programmer le code.

V. **Décodage du message :**

Il suffit en fait de faire le cheminement inverse du codage.

Après avoir éventuellement corrigé la matrice de données reçues, nous pouvons la décoder par la matrice suivante :

Soit R une matrice telle que :

$$R = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Et $P_r = Rr = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$

VI. **Limites du code :**

Il est évident que le code de Hamming (7,4) ne peut corriger des erreurs de plusieurs bits consécutifs.

Nous allons le démontrer en effectuant une démonstration par l'absurde.

En partant de l'exemple précédent, nous allons admettre que deux bits de données ont été altérés lors de la transmission : les bits 2 et 4. Considérons maintenant que le code sera capable de corriger les deux erreurs.

Nous avons ainsi les données reçues suivantes : $r = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ (les bits 2 et 4 sont faux)

Nous effectuons le cheminement de la correction d'erreur, nous avons :

$$z = Hr = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

La matrice z ici trouvée ne correspond à aucune colonne de la matrice de contrôle de parité. La limite du code de Hamming (7,4) devient évidente : le code est incapable de corriger plus d'une erreur dans une transmission de 7 bits. Il est néanmoins capable de détecter la présence d'erreurs quand deux erreurs se produisent.

Nous pouvons tout de même remarquer que sachant que les erreurs se trouvent aux bits 2 et 4, la matrice z est la somme des colonnes 2 et 4 de la matrice ce parité.

VII. Capacité de correction du code Hamming (7,4,3) :

Le troisième paramètre du code (3) indique la distance de Hamming maximale entre deux mots de code. La distance de Hamming correspond au nombre de bits différents entre deux mots binaires (elle n'existe que si les deux mots sont de longueur égale !).

La capacité de correction du code de Hamming est donc de $\frac{3-1}{2} = 1$ erreur pour 7 bits de données.

VIII. Autre méthode de génération des matrices du code :

La méthode de génération des matrices présentées plus haut n'est pas la seule utilisée pour générer les matrices du code de Hamming (7,4,3). En voici une autre.

Soit le vecteur $d = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$ représentant les données à transmettre.

On pose le vecteur $t = \begin{pmatrix} a \\ b \\ c \\ d \\ a+b+c \\ a+b+d \\ b+c+d \end{pmatrix}$ représentant les données à transmettre (et donc encodées par la matrice génératrice).

Note : les opérations sur les trois dernières coordonnées du vecteur t sont arbitraires. N'importe quelle combinaison linéaire de a, b, c, d conviendra à condition qu'elle soit unique sur le vecteur.

Soit G la matrice génératrice recherchée. Nous savons par définition que $Gd = t$.

Nous obtenons donc la matrice génératrice suivante :

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

Dans ce cas, la construction de la matrice de parité diffère légèrement de celle expliquée plus haut. Nous pouvons d'abord remarquer deux zones distinctes dans la matrice génératrice. Les quatre premières lignes représentent la matrice identité, alors que les trois suivantes représentent les données de parité ajoutées par la matrice génératrice.

Il suffit alors de transposer la matrice génératrice puis d'inverser ces deux parties. Nous obtenons alors :

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