Codes Correcteurs d'Erreurs
Les codes binaires linéaires **parfaits**
+ Code de Hamming,
+ Code de Golay

Marc Chaumont

November 12, 2008

Plan

Définition

Rappel : la borne de Hamming pour un code linéaire est $\sum_{i=0}^{t} \binom{n}{i} \leq 2^{n-k}$. Si $d_{min} = 3, t = 1$ on a alors : $1 + n \leq 2^{n-k}$.

Code de Hamming

Les **codes de Hamming** $[n, k, d_{min}]$ sont des codes de distance $d_{min} = 3$, $t = 1$, tels que la borne de Hamming est atteinte : $n = 2^{n-k} - 1$. Ce sont donc des codes parfaits. Les codes de Hamming sont donc des codes $[2^{n-k} - 1, k, 3]$. Plus généralement en posant $m = n - k$ on les note $[2^m - 1, 2^m - 1 - m, 3]$.

Définition

Les codes de Hamming sont $[2^m - 1, 2^m - 1 - m, 3]$, la matrice de contrôle H est donc une matrice $m \times 2^m - 1$.

Code de Hamming

La matrice de contrôle (vérification) est obtenue par énumération en colonne de tous les mots de code de m bits non nuls.

Exemple du code de Hamming [7,4,3]

On a déjà vu ce code de nombreuses fois ! et bien il vérifie la borne de Hamming !

On peut remarquer que les colonnes de la matrice de vérification sont bien une énumération de $2^3 - 1 = 7$ mots $\neq 0$ représentable sur 3 bits.

Matrice de vérification de parité:

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

Un peu d'histoire ...

Le code du minitel est le code de Hamming $[128, 120, 3]$. Ce qui correspond à coder 15 octets à l'aide d'un octet supplémentaire !

Remarque : Vous êtes capable de générer la matrice H donc H_{sys} donc G_{sys} donc coder et décoder ce code de longueur 128 bits!

Le taux est de $120/128 = 0.93$.

Plan

Propriété permettant de simplifier le codage et le décodage

La matrice de vérification de parité H des codes de Hamming a toutes ces colonnes différentes. Si une erreur e survient en une position j, $0 \leq j \leq n-1$, alors le syndrome est égal à la j^{eme} colonne de H.

Soit e le vecteur erreur ajouté à un mot de code transmis sur un canal BSC tel que seule la j^{eme} composante de e vaut 1, $e_j = 1$. Soit y le vecteur reçu. Le syndrome est

$$s = yH^t = eH^t = h_j,$$

avec h_j la j^{eme} colonne de H et $0 \leq j \leq n-1$.

Décodage simplifié

L'idée est de modifier la matrice H pour que le **syndrome** passé en base 10 donne comme valeur **la position de l'erreur** dans le vecteur erreur.

Matrice adaptée

Les colonnes de la matrice H sont exprimées comme des représentations binaires de nombres entiers i compris dans l'intervalle $[1, n]$ de manière croissante. On notera H' cette nouvelle matrice.

Note : Le code associé à la matrice H' est le même que celui associé à H à des permutations de colonnes et/ou de lignes près.

Exemple du code de Hamming [7,4,3]

Matrice de vérification de parité:

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

H' est donné par les représentations binaires des entiers 1 à 7 (bits de poids faibles en partie basse de la matrice).

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

Plan

Exercice de décodage simplifié avec le code de Hamming [7,4,3]

Le mot y = (0110101) a été reçu. À partir de la matrice de contrôle H' corriger l'erreur s'il y en a une et vérifier que la correction est valide.

Correction de décodage simplifié avec le code de Hamming [7,4,3]

Plan

Code de Golay

Golay a remarqué que :

$$\sum_{i=0}^{3} \binom{23}{i} = 2^{11}$$

Rappel : borne de Hamming pour un code binaire linéaire $[n, k, d_{min}]$: $\sum_{i=0}^{t} \binom{n}{i} \leq 2^{n-k}$.

Cette égalité montre la possible existance d'un **code binaire parfait** $[n = 23, k = 23 - 11 = 12, d_{min} = 3 * 2 + 1 = 7]$.

Code de Golay

Dans son papier, Golay donne la matrice génératrice d'un tel code binaire capable de corriger jusqu'à **3 erreurs binaires** pour un mot de code binaire de **23 bits**.

Plan

Matrice génératrice

Soit A_{11} la matrice carrée 11×11 dont la première ligne est 11011100010 et les lignes suivantes les décalées circulaires successives vers la gauche de celle-ci.

Matrice génératrice du Code de Golay [23, 12, 7]

$$\Gamma = \left(I_{12} \left| \begin{array}{c} \underline{1} \\ \hline A_{11} \end{array} \right. \right) = (I_{12}\ A)$$

où $\underline{1}$ est le vecteur ligne constitué de onze "1".

Matrice de contrôle de G[23, 12, 7]

Matrice de contrôle - matrice de parité

La matrice $\Gamma = \left(I_{12} \middle| \begin{array}{c} 1 \\ \hline A_{11} \end{array} \right) = (I_{12}, A)$ du code $G(23)$ est sous forme systématique, sa matrice de contrôle (matrice de parité) est donc :

$$H = (-A^t, I_{n-k}) = (A, I_{12}).$$

Codage du code de Golay [23, 12, 7]

Le codage est basé sur une look-up table (LUT) (table de correspondance) qui contient la liste des $2^{12} = 4096$ mot de code. À chacun des 2^{12} vecteurs d'information u de 12 bits, la LUT associe un mot de code de taille 23 bits.

LUT_c :

bits d'information (12 bits)	mot de code (23 bits)
...	...

Construction de la LUT_c

- générer les 2^{12} vecteurs d'information de 12 bits (colonne de gauche du tableau),
- pour chaque vecteur d'information u calculer le mot de code associé.

Plan

Décodage du code de Golay [23, 12, 7]

Le décodage est également basé sur une look-up table (LUT) qui contient la liste des vecteur erreurs de poids inférieur ou égal à 3. A chacun des 2^{11} syndrome s de 11 bits, la LUT associe un vecteur erreur de taille 23 bits.

LUT_d :

syndrome (11 bits)	vecteur erreur (23 bits)
...	...

Construction de la LUT_d

- générer les 2^{11} vecteurs d'erreur de 11 bits,
- pour chaque vecteur d'erreur e calculer le syndrome associé s
- remplir la LUT

Note : Le mot de code $\hat{c}$ issu du décodage d'un vecteur y sera : $\hat{c} = y + LUT_d(syndrome(y))$

Remarque : Le code de Golay est un code cyclique de polynôme générateur $g(X) = X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1$. Ce que l'on verra plus tard...

Plutôt que d'utiliser des produits matriciels pour générer les mots de code et les syndrômes, on peut utiliser des produits de polynômes...

Plan

Code de Golay étendu [24, 12, 7]

Le code de Golay étendu consiste à ajouter un bit de contrôle supplémentaire par rapport au code de Golay [23, 12, 7].
Soit A_{11} la matrice carrée circulante 11×11.

Matrice génératrice du code de Golay étendu

$$\Gamma = \left(I_{12} \left| \begin{array}{c|c} 0 & \underline{1} \\ \hline \underline{1}^t & A_{11} \end{array} \right. \right) = (I_{12}\ A)$$

où $\underline{1}$ est le vecteur ligne constitué de onze "1".

Matrice de contrôle - matrice de parité du code de Golay étendu

La matrice de contrôle (matrice de parité) est :

$$H = (-A^t, I_{n-k}) = (A, I_{12}).$$