Codes Correcteurs d'Erreurs
Les codes cycliques

Marc Chaumont

November 12, 2008

Plan

Définition

- Un **polynôme** à coefficients dans $\mathbb{F}_2$ est une fonction de la forme $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$ avec $\forall i \in \{0, ..., n\}, a_i \in \mathbb{F}_2$;
- Si $a_n \neq 0$, l'entier n est appelé le **degré** du polynôme P et noté $deg(P)$;
- Les entiers a_i sont appelés les coefficients de P ;

Dans $\mathbb{F}_2, (a+b)^2 = a^2 + b^2$.

Division Euclidienne

Division polynomiale

Soit P_1 et P_2 deux polynômes à coefficients dans $\mathbb{F}_2$. Il existe deux polynômes à coefficients dans $\mathbb{F}_2$, Q et R, uniques, tels que $P_1 = P_2 \times Q + R$ et $deg(R) < deg(P_2)$.

Q est appelé le **quotient** de la division euclidienne de P_1 par P_2.
R est appelé le **reste** de la division euclidienne de P_1 par P_2.

Plan

Code Cycliques

Code Cycliques

Soit C l'ensemble des mots de code d'un code $[n, k, d_{min}]$. Le code est dit **cyclique** si l'ensemble des mots du code est **stable** par **décalage circulaire**.

Dit autrement

Si l'on dispose d'une fonction σ de permutation circulaire telle que $\sigma(c_1, c_2, ..., c_n) = c_n, c_1, c_2, ..., c_{n-1}$, un code C est cyclique si $\forall c \in C, \sigma(c) \in C$

Les codes cycliques

Quelques codes cycliques ...

- Les codes de répétitions pures $[n, k, .]$ sont cyliques,
- Les codes par bit de parité est cyclique,
- Le code de Hamming $[7, 4, 3]$ est cyclique; et plus généralement certains codes de Hamming,
- Certains codes simplexes $[2^k - 1, k, 2^{k-1}]$ (Les colonnes de la matrice génératrice sont une énumération de $\mathbb{F}_2^k$ excepté le vecteur nul)

Les codes cycliques

Code cycliques engendré par un mot

(l'image d')Un **code cyclique engendré** par un mot $m \in \{0,1\}^n$ est composé du vecteur nul ainsi que de tous les vecteurs obtenables par décalage circulaire de m.

Exercice :

- Quel est le code linéaire (en bloc) cyclique engendré par 111 ?

Correction :

Générateur d'un code cyclique

Générateur d'un code cyclique

Soit C (l'image d') un **code cyclique** [n, k, .]
Il existe un **unique polynôme** $g(X) = a_0 + a_1X + a_2X^2 + ... + a_{n-k}X^{n-k}$ avec $a_{n-k} = 1$ tel que :

- $g(X)$ est un diviseur de $X^n + 1$,
- C est le code cyclique engendré par $m = a_0a_1...a_{n-k}0...0$ (Il y a $k-1$ zéros en fin de m),
- Les mots $m = a_0a_1...a_{n-k}0...0$; $\sigma(m) = 0a_0a_1...a_{n-k}0...0$; ...; $\sigma(m)^{k-1} = 0...0a_0a_1...a_{n-k}$ forment une base de C. La matrice génératrice de C est donc donnée par :

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{n-k} & 0 & 0 & \dots & \dots & 0 \\ 0 & a_0 & \dots & a_{n-k-1} & a_{n-k} & 0 & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & a_0 & a_1 & \dots & \dots & a_{n-k} \end{pmatrix}$$

Polynôme générateur

Représentation polynomiale

Soit $m = a_0 a_1 \ldots a_n$ un mot de longueur n. On appelle **représentation polynomiale** de m le polynôme $a_0 + a_1 X + \ldots + a_n X^n$.

Remarque 1 : Dorénavant, on identifiera systématiquement un mot avec sa représentation polynomiale.

Polynôme générateur

Soit C un code **cyclique** $[n, k, d_{min}]$. On appelle polynôme générateur de C le polynôme $g(X)$ défini par le théorème précédement.

Remarque 1 : Dorénavant, on identifiera systématiquement un code cyclique par son polynôme générateur.

Exemple de polynôme générateur

- Le polynôme générateur du code de répétition pure [n, 1, .] est $1 + X + X^2 ... + X^{n-1}$
- Le polynôme générateur du code par bit de parité [n, n-1, .] est $1 + X$
- **Les** polynômes générateurs du code de Hamming [7, 4, 3] sont $1 + X + X^3$ et $1 + X^2 + X^3$.

Remarque sur l'occupation mémoire des différentes catégories de codes en blocs

- Les codes **en blocs quelconques** nécessitent de désigner les 2^k mots de codes ainsi que la fonction de codage,
- Les codes **en blocs linéaires quelconques** sont décrits par leur matrice génératrice de dimension $n \times k$.
- Les codes **en blocs cycliques** sont décrits par un polynôme composé de $n - k$ coefficients.

Plan

Codage

Codage

Soit C un code cyclique de polynôme générateur g(X). Soit u un mot de source de représentation polynomiale $P_u(X)$. Le mot image correspondant (c'est-a-dire le mot de code correpondant) a pour représentation polynomiale $P_u(X) \times g(X)$.

Plan

Exercice

Soit le polynôme générateur $g(X) = 1 + X + X^3$.

1. Donner le **mot de code** du mot issu du codage de $u = 1101$,
2. Donner la **matrice génératrice G** associée au polynôme générateur,
3. Vérifier que le mot de code obtenu par $u \times G$ est le même que celui obtenu en question 1.

Correction

Correction

Plan

Détection d'erreurs

Détection d'erreurs

Un mot c est **un mot de code** si et seulement si sa **représentation polynomiale** est **divisible** par le **polynôme générateur** $g(X)$ (le reste de la division par g(X) doit être nul).

Exercice : Détection d'erreurs

Soit le polynôme générateur $g(X) = 1 + X + X^3$ du code de Hamming C[7, 4, 3]. Le mot 1010001 est-il un mot de code ?

Exercice : Correction

Remarque

On vient de voir à travers les exercices qu'il est possible

- de générer un code correcteur par multiplication par le polynome générateur,
- et qu'il est posible de détecter une erreur par division par le polynôme générateur.

Décodage

Matrice de contrôle

La matrice de contrôle associée à la matrice génératrice G (cf. transparent précédent) est :

$$H = \begin{pmatrix} b_k & b_{k-1} & \dots & b_0 & 0 & \dots & 0 \\ 0 & b_k & b_{k-1} & \dots & b_0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & b_k & b_{k-1} & \dots & b_0 \end{pmatrix}$$

avec $h(X) = b_0 + b_1 X + \dots + b_k X^k$ le polynôme défini par :

$$h(X) = \frac{X^n + 1}{g(X)}.$$

Syndrome

Syndrome

Soit r un mot reçu de représentation polynomiale $r(X) = c(X) + e(X)$, où $c(X)$ est un mot de code en représentation polynomiale, et $e(X)$ est l'erreur en représentation polynomiale. Le syndrôme en représentation polynomiale est :

$$s(X) = r(X) \ mod \ g(X) = e(X) \ mod \ g(X)$$

Le calcul du syndrome en représentation polynomiale est :

- rapide (division de polynôme),
- quand la capacité de décodage t est faible (Hamming, Golay) il est peu couteux calculatoirement de remonter l'erreur $e(X)$.

Plan

Exercice

Soit le polynôme générateur $g(X) = 1 + X + X^3$ du code de Hamming C[7,4, 3].

1. Donner le polynôme permettant d'obtenir la matrice de contrôle,
2. puis donner la matrice de contrôle,
3. enfin, le mot 1010001 est-il un mot de code ?

Correction

Correction

Plan

Ce que l'on n'a pas vu...

- Les codes cycliques de longueur impaire, BCH (Bose, Ray-Chaudhuri, Hocquenghem),
- Les codes cycliques non-binaires : Code de Reed-Solomon,
- Les codes de Reed-Muller,
- Les probabilité d'erreurs pour le canal binaire symetrique (BSC), pour le canal de bruit additif banc gaussien (AWGN), pour le canal plat à effacement de Rayleigh ...
- les effacements, ...
- les turbos codes ...