TD 2 - Les codes correcteurs et les codes détecteurs d'erreurs

Claude Duvallet

Université du Havre
UFR Sciences et Techniques
25 rue Philippe Lebon - BP 540
76058 LE HAVRE CEDEX
Claude.Duvallet@gmail.com

Présentation (1/2)

- Pourquoi ces codes ?
  - Des canaux de transmission imparfaits entraînant des erreurs lors des échanges de données.
  - Probabilité d'erreur sur une ligne téléphonique : P=10^{-7} (cela peut même atteindre 10^{-4}).

  $\Rightarrow$ Utilisation de méthodes de détection des erreurs et éventuellement de correction des erreurs.
- Méthodes mises en place au niveau de la couche 2 OSI : liaison de données.
- Principe général :
  - Chaque suite de bits (une trame) à transmettre est augmentée par une autre suite de bits dite de redondance ou de contrôle.
  - Pour chaque suite de k bits transmise, on ajoute r bits. On dit alors que l'on utilise un code $C(n,k)$ avec $n = k + r$.
  - À la réception, on effectue l'opération inverse et les bits ajoutés permettent d'effectuer des contrôles à l'arrivée.

Présentation (2/2)

- Il existe deux catégories de codes :
  - les codes détecteurs d'erreurs,
  - les codes correcteurs d'erreurs.
- Le code de Hamming : un code détecteur et correcteur d'erreurs.
- Le CRC (Cycle Redundancy Check) : uniquement un code détecteur d'erreurs mais extrêment fiable.

Le Code de Hamming

Le code de Hamming : Principe général

- Structure d'un mode de code de Hamming
  - les m bits du message à transmettre et les n bits de contrôle de parité.
  - longueur totale : $2^n - 1$
  - longueur du messages : $m = (2^n - 1) - n$

  $\Rightarrow$ on parle de code $x - y$ où $x = n + m$ et $y = m$.
- Exemple de code de Hamming :
  - un mot de code $7 - 4$ a un cœfficient d'efficacité de 4/7 = 57 %,
  - un mot de code $15 - 11$ a un cœfficient d'efficacité de 11/15 = 73 %,
  - un mot de code $31 - 26$ a un cœfficient d'efficacité de 26/31 = 83 %,
- Les bits de contrôle de parité C_i sont en position 2^i pour i=0,1,2,...
- Les bits du message D_j occupe le reste du message.

D3	D2	D1	C2	D0	C1	C0
7	6	5	4	3	2	1

Le code de Hamming : Retrouver une erreur

- Retrouver l'erreur dans un mot de Hamming
  - Si les bits de contrôle de réception $C_2^{'} C_1^{'} C_0^{'}$ valent 0, il n'y a pas d'erreurs sinon la valeur des bits de contrôle indique la position de l'erreur entre 1 et 7.
    - Si $C_0^{'}$ vaut 1, les valeurs possibles de $C_2^{'} C_1^{'} C_0^{'}$ sont 001, 011, 101, 111, c'est-à-dire 1, 3, 5, 7.
    - Si $C_1^{'}$ vaut 1, les valeurs possibles de $C_2^{'} C_1^{'} C_0^{'}$ sont 010, 011, 110, 111, c'est-à-dire 2, 3, 6, 7.
    - Si $C_2^{'}$ vaut 1, les valeurs possibles de $C_2^{'} C_1^{'} C_0^{'}$ sont 100, 101, 110, 111, c'est-à-dire 4, 5, 6, 7.

  $\Rightarrow$ Il s'agit là des positions possibles pour une erreur.

Le code de Hamming : Calcul d'un code de parité pair

- Émission pour un contrôle de parité pair.
  - C_0 est calculé par rapport aux bits d'indice 7, 5, 3 et sa valeur 1.
  - C_1 est calculé par rapport aux bits d'indice 7, 6, 3 et sa valeur 2.
  - C_2 est calculé par rapport aux bits d'indice 7, 6, 5 et sa valeur 4.
- On souhaite envoyer le message 1010, compléter le mot de Hamming correspondant :

1	0	1	_	0	_	_
7	6	5	4	3	2	1

Le code de Hamming : Calcul d'un code de parité pair

1	0	1	_	0	_	_
7	6	5	4	3	2	1

- C_2 vaut 0 pour pouvoir rendre pair $1+0+1$ (les bits d'indices 7, 6, 5)

1	0	1	**0**	0	_	_
7	6	5	4	3	2	1

- C_1 vaut 1 pour pouvoir rendre pair $1+0+0$ (les bits d'indices 7, 6, 3)

1	0	1	**0**	0	**1**	_
7	6	5	4	3	2	1

- C_0 vaut 0 pour pouvoir rendre pair $1+1+0$ (les bits d'indices 7, 5, 3)

1	0	1	**0**	0	**1**	**0**
7	6	5	4	3	2	1

Le code de Hamming : Exercices 1 et 2

- Exercice 1 : On veut envoyer le mot `1011`, quels bits, je doit lui adjoindre et quelle séquence je transmettrai alors ?
- Exercice 2 : Y-a-t-il une erreur dans le mot suivant ? 1101101

Le code de Hamming : Exercice 3

- Exercice 3
  - Soit un mot de Hamming de longueur 15

1	0	1	1	0	1	1	1	1	0	1	1	0	1	1
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

  - Quels sont les bits de contrôle de parité ?
  - Quel est le message reçu ?
  - Est-ce que le message reçu correspond au message transmis ?
  - Si oui, quel a été le message transmis ?

Le CRC - Code Cyclique de Redondance

Le CRC : principe général

- Représentation sous forme polynomiale des suites de bits à transmettre :
  - M $= m_1 m_2 ... m_n$
  - $\Rightarrow$ représentée par le polynôme $I(x) = m_n + m_{n-1}x + ... + m_1 x^{n-1}$
- Exemple :
  - La suite 1100101 est représentée par le polynôme $x^6 + x^5 + 0x^4 + 0x^3 + x^2 + 0x + 1 = x^6 + x^5 + x^2 + 1$
- Utilisation de polynômes générateurs possédant des propriétés mathématiques particulières :
  - CRC-12 = $x^{12} + x^{11} + x^3 + x^2 + x + 1$
  - CRC-16 = $x^{16} + x^{15} + x^2 + 1$
  - CRC-CCITT = $x^{16} + x^{12} + x^5 + 1$
  - CRC-32 = $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x + 1$

Le CRC : émission/réception d'un CRC

- En émission :
  - on ajoute au message à émettre un code de contrôle tel que le polynôme correspondant au message plus le code de contrôle soit divisible par le polynôme générateur choisi.
- En réception :
  - Le message reçu qui contient les données et le CRC doit être divisible par le polynôme générateur.
  - On vérifie donc par une division euclidienne en base 2 que le reste de la division est nul.

Le CRC : émission

- Émission d'un mot :
  - On choisit un polynôme générateur puis on le transforme en un mot binaire.
  - Exemple : avec le polynôme générateur $x^4 + x^2 + x$, on obtient `10110`.
  - On ajoute m zéros au mot binaire à transmettre où m est le degré du polynôme générateur.
  - Exemple : on souhaite transmettre le mot `11100111` en utilisant le polynôme générateur $x^4 + x^2 + x$, on obtient alors `111001110000`.
  - On va ajouter itérativement à ce mot, le mot correspondant au polynôme générateur jusqu'à ce que le mot obtenu soit inférieur au polynôme générateur. Ce mot obtenu correspond au CRC à ajouter au mot avant de l'émettre.
  - On effectue donc une division euclidienne dans laquelle on ne tient pas compte du quotient.

Le CRC : exemple

- Exemple du calcul du CRC avant émission d'un mot :

1	1	1	0	0	1	1	1	0	0	0	0
1	0	1	1	0							
0	1	0	1	0	1	1	1	0	0	0	0
	1	0	1	1	0						
	0	0	0	1	1	1	1	0	0	0	0
				1	0	1	1	0			
				0	1	0	0	0	0	0	0
					1	0	1	1	0		
					0	0	1	1	0	0	0
							1	0	1	1	0
							0	1	1	1	0

  - Le CRC est donc `1110` et le mot à transmettre `11100111 1110`.

Le CRC : vérification

- Vérification du mot à la réception d'un mot :

1	1	1	0	0	1	1	1	1	1	1	0
1	0	1	1	0							
0	1	0	1	0	1	1	1	1	1	1	0
	1	0	1	1	0						
	0	0	0	1	1	1	1	1	1	1	0
				1	0	1	1	0			
				0	1	0	0	1	1	1	0
					1	0	1	1	0		
					0	0	1	0	1	1	0
							1	0	1	1	0
							0	0	0	0	0

- Le reste de la division est nul, il n'y a donc pas d'erreurs.

Le CRC : exercice

- Exercice :

  On utilisera le polynôme générateur $x^4 + x^2 + x$.

  1. On souhaite transmettre le message suivant :`1111011101`, quel sera le CRC à ajouter ?
  2. Même question avec le mot `1100010101`.
  3. Je viens de recevoir les messages suivants : `111100010101`0, `110001010101`10, sont-ils corrects ?