TD Réseau Les codes correcteurs et les codes détecteurs

Claude Duvallet

Matrise Informatique Année 2003-2004

Présentation (1)

Pourquoi ?

- Des canaux de transmission imparfait entraînant des erreurs lors des échanges de données.
- Probabilité d'erreur sur une ligne téléphonique : $P=10^{-4}$ (cela peut même atteindre 10^{-7}).
- ⇒ 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 (trame) à transmettre est augmentée par une autre suite de bit dite de redondance ou de contrôle.
 - Pour chaque suite de k bits transmis, on ajoute r bits. On dit alors que l'on utilise un code C(n,k) avec n=k+r.

Présentation (2)

- Principe général (suite) :
 - À la réception, on effectue l'opération inverse et les bits ajoutés permettent d'effectuer des contrôles à l'arrivée.
- Il existe deux catégories de code :
 - 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):
 - un code détecteur d'erreurs.

Le code de Hamming (1)

- Structure d'un mode de code de Hamming
 - \blacksquare les m bits du message à transmettre et les n bits de contrôle de parité.
 - In 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 coefficient d'efficacité de 4/7=57 %,
 - un mot de code 15 11 a un coefficient d'efficacité de 11/15 = 73 %,
 - un mot de code 31 26 a un coefficient 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	C 1	C0
)

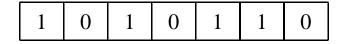
Le code de Hamming (2)

- 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'erreur 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.
- Exercice: y a-t-il une erreur dans le mot suivant?

1	0	1	0	1	1	0
---	---	---	---	---	---	---

Le code de Hamming (3)

Exercice (Correction)



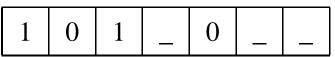
- C_2' vaut 1 + 0 + 1 + 0 = 0 (bits d'indice 7, 6, 5 et 4).
- C'_1 vaut 1+0+1+1=1 (bits d'indice 7, 6, 3 et 2).
- C'_0 vaut 1+1+1+0=1 (bits d'indice 7, 5, 3 et 1).
- $\Rightarrow C_2'C_1'C_0'$ vaut 011, c'est à dire 3 en base 10. Il y a donc une erreur à l'indice 3 du mot.

Le code de Hamming (4)

- Émission pour un contrôle de parité pair.
 - $ightharpoonup C_2$ est calculé par rapport aux bits d'indice 7, 6, 5 et sa valeur 4.
 - $ightharpoonup C_1$ est calculé par rapport aux bits d'indice 7, 6, 3 et 2.
 - $lue{C}_0$ est calculé par rapport aux bits d'indice 7, 5, 3 et 1.
- On souhaite envoyer le message 1010, compléter le mot de Hamming correspondant :

1	0	1		0	_	_
---	---	---	--	---	---	---

Le code de Hamming (5)



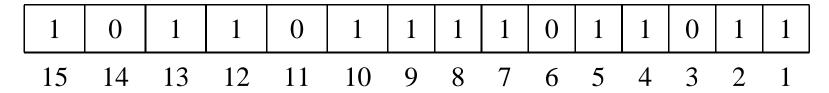
■ C2 vaut 0 pour pouvoir rendre pair 1 + 0 + 1 (les bits d'indices 7, 6, 5)

C1 vaut 1 pour pouvoir rendre pair 1 + 0 + 0 (les bits d'indices 7, 6, 3)

C0 vaut 0 pour pouvoir rendre pair 1 + 1 + 0 (les bits d'indice 7, 5, 3)

Le code de Hamming (6)

Soit un mot de Hamming de longueur 15



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

Le code de Hamming (7)

Les bits de contrôle de parité sont en position 2^i

D10	D9	D8	D7	D6	D5	D4	C3	D3	D2	D1	C2	D0	C 1	C0
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

- Les bits de contrôle : 1111
- Le message reçu : 10110111010
- Les bits de contrôle de réception vont être : $C_3'C_2'C_1'C_0'$
 - Si C'_0 vaut 1, les valeurs possibles sont (0001, 0011, 0101, 0111, 1001, 1011, 1101, 1111) soit (1, 3, 5, 7, 9, 11, 13, 15).
 - Si C_1' vaut 1, les valeurs possibles sont (0010, 0011, 0110, 0111, 1001, 1010, 1011, 1111) soit (2, 3, 6, 7, 10, 11, 14, 15).
 - Si C_2' vaut 1, les valeurs possibles sont (0100, 0101, 0110, 0111, 1100, 1101, 1110, 1111) soit (4, 5, 6, 7, 12, 13, 14, 15).
 - Si C_3' vaut 1, les valeurs possibles sont (1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111) soit (8, 9, 10, 11, 12, 13, 14, 15).

Le code de Hamming (8)

- Dans le message considéré on a :
 - $C_0'=1+0+1+1+1+0+1+1=0$
 - $C_1'=1+0+0+1+1+0+0+1=0$
 - $C_2'=1+1+0+1+1+1+0+1=0$
 - $C_3'=1+1+1+0+1+1+0+1=0$
- $\Rightarrow C_3'C_2'C_1'C_0'$ vaut 0000. Il n'y a donc pas d'erreur dans le message reçu.

Le CRC (1)

- Représentation sous forme polynomiale des suites de bits à transmettre :
 - $M = m_1 m_2 ... m_n$
 - \Rightarrow représentée par le polynôme $I(x) = m_n + m_{n-1}x + ... + m_1x^{n-1}$
- **Exemple**:
 - La suite 11000101 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 = $x^{16} + x^{15} + x^2 + 1$
 - Arr 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 (2)

■ En émission :

on ajoute au message à émettre un code contrôle tel le polynôme correspondant au message plus le code de contrôle soit divisible par le polynôme générateur.

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 nulle.

Le CRC (3)

■ 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 (4)

Exemple d'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	0	1	1	0						
	0	0	0	1	1	1	1	0			
				1	0	1	1	0			
				0	1	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 (5)

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	0	1	1	0						
	0	0	0	1	1	1	1	1			
				1	0	1	1	0			
				0	1	0	0	1	1		
					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 nulle, il n'y a donc pas d'erreur.

Le CRC (6)

Exercices:

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 : 1111000101010, 1100010101010, sont-ils corrects ?

Le CRC (7)

■ Correction : quel CRC à ajouter avant d'émettre le message 1111011101 ?

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

Le CRC est donc 1100 et le mot à transmettre 1111011101 1100 Année 2003-200

Le CRC (8)

■ Correction : quel CRC à ajouter avant d'émettre le message 1111011101 ?

x^{13}	x^{12}	x^{11}	x^{10}		x^8	x^7	x^6		x^4			x^4	$+x^2$	+x
x^{13}		x^{11}	x^{10}											
	x^{12}				x^8	x^7	x^6		x^4			x^9	+x ⁸	$+x^{6}$
	x^{12}		x^{10}	x^9								$+x^{5}$	$+x^3$	$+x^2$
			x^{10}	x^9	x^8	x^7	x^6		x^4			+x		
			x^{10}		x^8	x^7								
				x^9			x^6		x^4					
				x^9		x^7	x^6							
						x^7			x^4					
						x^7		x^5	x^4					
								x^5						
								x^5		x^3	x^2			
										x^3	x^2			

Année 2003-2004 – p.19/22

Le CRC (9)

■ Correction : quel CRC à ajouter avant d'émettre le message 1100010101 ?

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

Le CRC est donc 1000 et le mot à transmettre 1100010101 1000.

Le CRC (10)

Correction : le message reçu 1111000101010 est-il correct ?

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

Le reste est nul \Rightarrow il n'y a pas d'erreur dans le mot transmis. Année 2003-2004 – p.21/22

Le CRC (11)

Correction : le message reçu 11000101010110 est-il correct ?

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

Le reste est $1110 \Rightarrow il$ y a une erreur dans le mot transmis.