Techniques de détection & de correction des erreurs de transmission

Rushed KANAWATI

Département GTR - IUT de Villetaneuse, © 2002

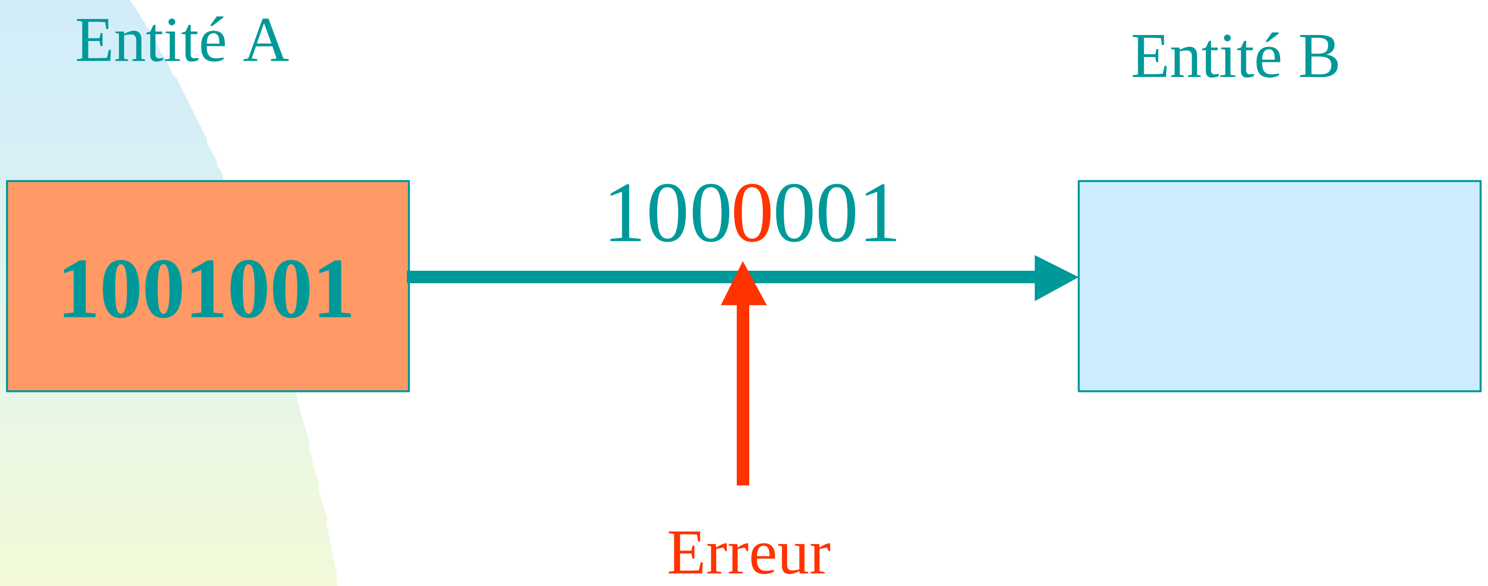
rushed.kanawati@lipn.univ-paris13.fr

Sommaire

- Problématique
- Principe de détection des erreurs
- Techniques de détection des erreurs
  - Codes de parité
  - Code polynomiale (CRC)
- Techniques de correction des erreurs
  - Codes auto-correcteurs : code de Hamming
  - Correction par demande de retransmission
- Bibliographie

Le plan de ce cours est inspiré du cours fait par B. Cousin, IFSIC, Université de Rennes

Problématique



- Comment B peut **détecter** l'occurrence d’une erreur ?
- Comment B peut **localiser** une erreur ?
- Comment B peut **corriger** une erreur ?

Approche naïve : la répétition

- Détection d'erreurs
  - Le message envoyé est constitué du double du message initial.
  - Envoyer 10010011001001 au lieu de 1001001
  - Le récepteur détecte une erreur si les exemplaires ne sont pas identiques.
- Auto-correction
  - Le message envoyé est constitué du triple du message initial.
  - Envoyer 100100110010011001001 au lieu de 1001001
  - Le message correcte correspond aux 2 exemples identiques.

Quelques remarques

- La détection et la correction des erreurs nécessitent d'introduire de la **redondance** dans les messages transmis.
- Certaines erreurs ne peuvent pas être détectées
  - *Exemple : la même erreur sur les deux exemplaires*
- Certaines erreurs détectées ne peuvent pas être corrigées
  - *Exemple : Une erreur différente sur au moins deux exemplaires.*
- Certaines erreurs sont mal corrigées
  - *une même erreur sur deux exemplaires simultanément*
- L'auto-correction nécessite plus de redondance que la simple détection.

Détection des erreurs : Code de parité

- La parité peut être paire ou impaire.
- Pour une parité paire (impair), on protège une séquence de k bits par l'ajout de r bits de sorte que le nombre de bits ayant la valeur 1 soit pair (impair)

Lettre	Code ASCII	(parité paire)	(parité impaire)
G	1110001	11100010	11100011
T	0100001	01000010	01000011
R	0100101	01001011	01001010

Ce code détecte les erreurs en nombre impair.
Pas de correction automatique.

R. Kanawati, Cours réseaux, IUT de Villetaneuse, département GTR, 1er année, 2002-2003

Détection des erreurs : Code polynomial

- A toute séquence de bits on associe un polynôme
  - $U = <u_0, u_1, u_2, \ldots, u_n> \Leftrightarrow U(x) = u_0 + u_1 .x + u_2 .x^2 + \ldots + u_n .x^n$
  - $1001001 \Leftrightarrow X^6 + X^3 + 1$
- Les séquences envoyés (codés) doivent être un multiple d'un polynôme g(x) dit **polynôme générateur**.
- **Le polynôme g(x) est connu à l'avance par l'émetteur et le récepteur.**

Procédure de codage

- Soit P(X) le polynôme associé à la séquence de bits à protéger.
- Soit g(x) le polynôme générateur de degré k .
- Les calculs sont faits dans le corps Z/2Z
  - 1+1=0; X+X=0; X=-X
- On calcule P'(X) = P(X).X^k
  - Ceci équivaut à un décalage de P(X), de k positions vers la gauche.
- On divise P'(X) par g(x).
  - P'(X)=Q(X).g(X)+R(X)
- Le message envoyé est : P'(X) +R(X)
- P'(X)+R(X) = Q(X).g(X) est multiple de g(X)

Procédure de décodage

- Soit M(X) le message reçu.
- On divise M(X) par g(X)
  - Si le reste de division est **non nul** alors : détection d'une erreur.
  - Sinon (reste de division nul) il y a une forte probabilité que la transmission est correcte.

Exemple

- Soit la séquence 1101 à envoyer
- $g(x) = x^3+x+1$
- $P(x)=x^3+x^2+1$
- $P'(x)=P(x).x^3=x^6+x^5+x^3$

$$
\begin{array}{r|l}
x^6+x^5+x^3 & x^3+x+1 \\
\underline{x^6+x^4+x^3} & \overline{x^3+x^2+x+1} \\
x^5+x^4 & \\
\underline{x^5+x^3+x^2} & \\
x^4+x^3+x^2 & \\
\underline{x^4+x^2+x} & \\
\mathbf{x^3+x} & \\
x^3+x+1 &
\end{array}
$$

$\rightarrow$ $R(x)=1$ $\rightarrow$ **Message envoyé : 1101001**

Caractéristique du code polynomiale

- La qualité de la protection dépend du choix du polynôme générateur g(x).
- On démontre par exemple (voir TD 03) que si :
  - g(x) comporte au moins 2 termes alors les erreurs simples sont détectables.
  - si g(x) a un facteur irréductible de trois termes alors les erreurs doubles sont détectables
  - g(x) est multiple de x+1 alors les erreurs en nombre impair sont détectables.

Correction des erreurs

- Deux approches :
  - Utilisation de code auto-correcteurs
    - Exemple : code de Hamming
  - Correction par retransmission
    - Si détection d'une erreur alors demander à l'émetteur de renvoyer le même message.

Code de Hamming

- La **distance de Hamming** entre deux séquences binaires de même taille est égale au nombre de bits de rang identique par lesquels elles différent.
- Exemple : d(1**10**0110, 1**01**0110) = 2
- Soit un code composé de N mot valides.
- La distance de Hamming de ce code est définie comme la distance minimale qui sépare deux mots valides du code.
- Exemple : le code :

C= [000000, 001110,010101,011011,100011,101101] a une distance de Hamming = 3

- Un code avec une distance d détecte d-1 erreurs et corrige k erreurs où d=2K+1

Correction par retransmission

- L’émetteur conserve une copie des données qu’il envoie.
- Le récepteur applique une méthode de détection des erreurs.
- Le récepteur informe l’émetteur de la bonne (resp. mauvaise) réception en lui retournant un paquet spécifique : **acquittement** positif (resp. négatif)
- Dans le cas d’un acquittement négatif, l’émetteur doit renvoi le paquet erroné.
- Un **temporisateur** bornant la durée d’attente des acquittements est nécessaire pour assurer la correction du mécanisme lors des pertes de paquets de données.
- L’identification des paquets (de données et d’acquittement) est nécessaire pour assurer la correction du mécanisme lors des pertes d’acquittement.

Pour en savoir plus

- K. Lahèche, **Les codes en informatique : codes détecteurs et correcteurs d'erreurs**, Hermès,1995.
- R. Dapoigny, **Les transmissions dans les réseaux informatiques,** Support IUT, gaëtan morin éditeur 1999. Chapitre 5.
- A. Tanenbaum, **Réseaux**, InterEditions, 1997.