Sécurité des Réseaux

Jean-Yves Antoine

LI - Université François Rabelais de Tours

Jean-Yves.Antoine AT univ-tours.fr

UNIVERSITÉ FRANÇOIS - RABELAIS TOURS

Sécurité des réseaux

Codes correcteurs de paquets d'erreurs

Paquets d'erreurs

Définition

- **Paquet d'erreur d'étendue L** : vecteur d'erreur dont les seules composantes non nulles sont comprises dans L bits successifs
  Exemple 0000010010110000 0 L =7
- **Représentation polynomiale** : $e(X) = X^k.e'(X)$ avec e'(X) polynôme de degré égal à L-1

  Exemple $E(X) = X^5. (1 + X + X^3 + X^6)$

Utilisation et hypothèses statistiques

- Sucession d'erreurs non aléatoire : événements non indépendants
- Disque compact (poussières, rayures), GSM, satellites

Erreurs indépendantes

Décodage par maximum de vraissemblance : le vecteur d'erreur le plus probable est celui de poids minimal

Tableau standard : chaque lasse latérale a pour tête de liste le vecteur d'erreur de poids minimal

Syndrôme : identifique pour tous les mots d'une classe donnée

Paquets d'erreurs

Décodage par maximum de vraissemblance : le vecteur d'erreur le plus probable est celui présentant un paquet d'étendue minimale

Exemples	0100 0100	2 erreurs mais étendue 5
	0011 0100	3 erreurs mais étendue 4

Tableau standard : chaque lasse latérale a pour tête de liste un vecteur de motif d'étendue minimale

Syndrôme : non applicable

Correction d'un paquet d'erreurs

Un code linéaire peut corriger des paquets d'étendue L si tous les motifs d'erreur d'étendue L sont dans des classes linéaires distinctes

Soit un code linéaire de dimension m et de longueur n, alors sa capacité L de correction de paquets d'erreurs est limitée par :

$$L_{max} \leq n - m$$

Exemple $G = \begin{pmatrix} 10\ 011 \\ 01\ 111 \end{pmatrix}$

- Mots de code
- Tableau standard pour correction classique et de paquets d'erreurs
- Décodage de (11010)

Entrelacement

Idée

Réduire l'influence d'un paquet d'erreur sur les mots transmis.

Principe

Codage classique : transmission à la suite de mots de longueur n

$$(m_{11}\ m_{12}\ ...\ m_{1n})\ (m_{21}\ m_{22}\ ...\ m_{2n})\ ...\ (m_{t1}\ m_{t2}\ ...\ m_{tn})$$

Entrelacement de profondeur t : répartition bits sur n mots de longueur t

$$(m_{11}\ m_{21}\ ...\ m_{t1})\ (m_{12}\ m_{22}\ ...\ m_{t2})\ ...\ (m_{1n}\ m_{2n}\ ...\ m_{tn})$$

Intérêt

Paquets d'erreurs répartis surdifférents mots envoyés : plus de mots concernés, mais erreur par mot limitée

Propriétés

Soit C un code linéaire de dimension *m* et de longueur *n* capable de corriger des paquets d'erreurs d'étendue *L*.

Le code entrelacé construit sur C et de profonteur *t* est capable de corriger des paquets d'erreurs de longueur *Lt*.

Application (exemple)

- support de transmisision : paquets d'erreur d'étendue L au maximum
- un code classique 1-correcteur entrelacé avec une profondeur L permet de gérer directement cette situation

Entrelacement avec retard

Principe

Envoi par entrelacement avec **retard r** de t mots codés

$(m_{11}\ m_{12}\ \dots\ m_{1n})\ (m_{21}\ m_{22}\ \dots\ m_{2n})\ \dots\ (m_{t1}\ m_{t2}\ \dots\ m_{tn})$

Matrice d'entrelacement

$$
\begin{array}{cccccccccccccccc}
m_{11} & m_{21} & m_{31} & \dots & m_{t1} & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & m_{12} & m_{22} & m_{32} & \dots & m_{t2} & \dots & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & m_{13} & m_{23} & m_{33} & \dots & m_{t3} & \dots & 0 & 0 \\
 & & & & & & & & & & & & & \\
 & & & & & & & & & \dots & 0 & 0 & 0 & m_{1n}\ m_{2n}\ \dots\ m_{tn}
\end{array}
$$

Transmission colonne par colonne : r.(n-1) + t mots de n bits

Entrelacement avec retard

Propriétés

Soit C un code linéaire de longueur *n* capable de corriger des paquets d'erreurs d'étendue *L*.

Le code entrelacé construit sur C avec un retard *r* est capacble de corriger des paquets d'erreurs de longueur $L(r.n + 1)$.

Exemple $G = \begin{pmatrix} 100011 \\ 010101 \\ 001110 \end{pmatrix}$

- Mots à transmettre : (100), (010), (111), (010) (100), (111)
- Codage G entrelacé de profondeur 3
- Codage G entrelacé avec retard de 1

Entrelacement croisé

Idée

Croisement de deux codes : un code pour détecter le paquet d'erreur, l'autre pour le corriger

Principe

- Code C1 (dimension m_1, longueur n_1, d_1-détecteur)
- Code C2 (dimension m_2, longueur n_2, d_2-détecteur)

codage

- Codage par C1 des messages
- Entrelacement avec une profondeur m_2
- Codage par C2 des mots obtenus par entrelacement
- Eventuellement, entrelacement du résultat avec une profondeur t

Entrelacement croisé

Propriétés

Soit deux codes C1 et C2 tq :

- Code C1 (dimension m_1, longueur n_1, d_1-détecteur)
- Code C2 (dimension m_2, longueur n_2, d_2-détecteur)

On construit un code par entrelacement croisé de C1 et C2 de profondeur $t \leq d_1 - 1$. Alors, tous les paquets d'erreurs d'étendue au plus $t \cdot (d_2 - 1)$ seront décodés convenablement si chaque mot transmis est affecté au pire par un seul paquet d'erreur.

Exemple

$$G1 = \begin{pmatrix} 1000\ 1110 \\ 0100\ 1101 \\ 0010\ 1011 \\ 0001\ 0111 \end{pmatrix} \qquad G2 = \begin{pmatrix} 100\ 110 \\ 010\ 101 \\ 001\ 011 \end{pmatrix}$$

- Transmettre (1000) (1100) (1010) avec entrelacement de profondeur 3
- Décodage si erreur sur les 6 premiers symboles reçus

Conclusion

Codes étudiés dans ce cours

- **Réseaux informatiques** codes cycliques non primitifs CRC
- **Minitel** code de Hamming étendu
- **Disque compact** (CD audio) code CIRC *(Reed-Salomon à entrelacement croisé)*
- **CD-ROM** code CIRC + 2nd code plus élaboré

Codes convolutifs

Transmission bit à bit sans paquets

- **GSM** code cyclique CRC + code convolutif
- **UMTS** turbo-codes convolutifs
- **Satellite** code Golay étendu + coce convolutif (*Planetary Standard*)