Introduction au Codage Canal

Mostafa Belkasmi

2012-2013 **ENSIAS**

Plan

- Introduction
- Codes en bloc Linéaires
- Codes Cycliques

Introduction

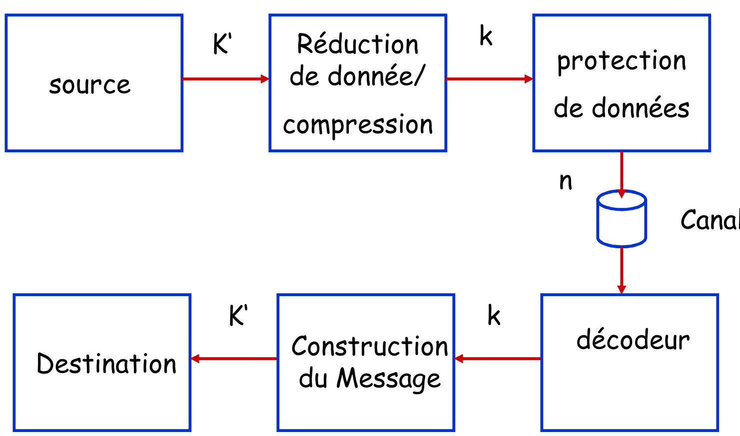
- Applications des Codes Correcteurs d'erreurs

photos Satellite

Réseaux radio mobile

Compact Disks

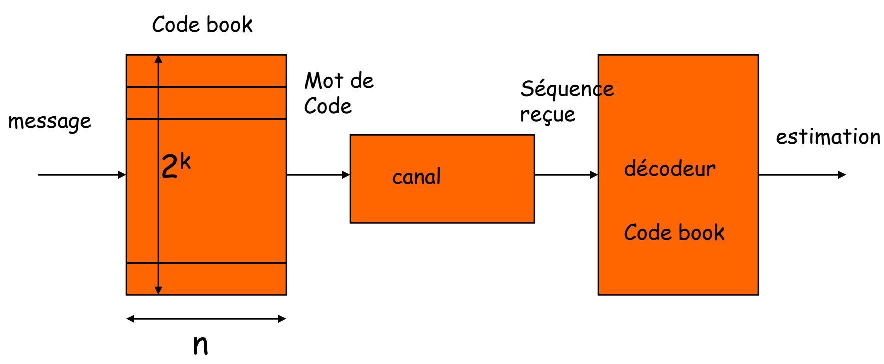
Modèle du système de communication



Codage

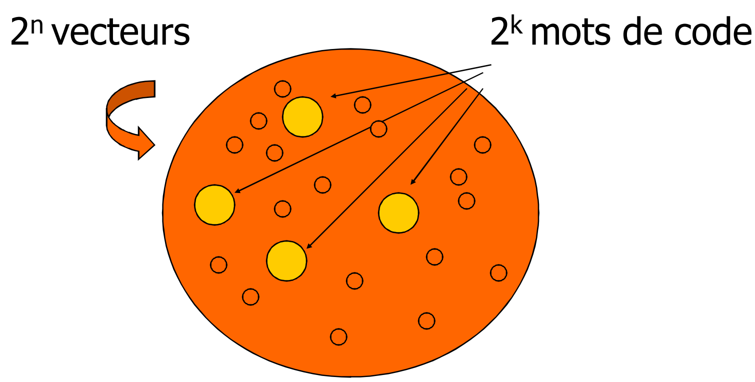
- Remplacer un message de k bits d'information par un unique mot de n bits, dit ***mot de code***
- L'ensemble des 2^k mots de code est appelé un ***CODE***

Code avec un taux k/n



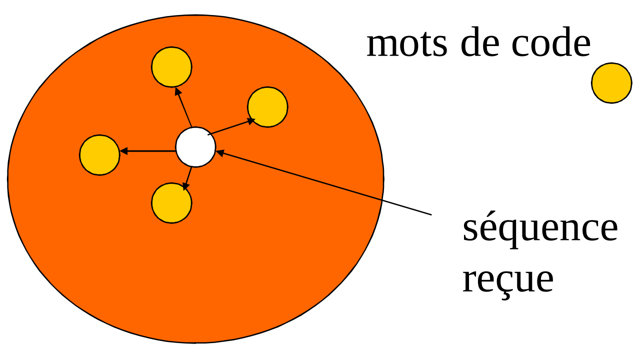
Il y a en totalité 2^k mots de code de longueur n

Une vue d'ensemble



Décodeur

- Comparer la séquence reçue avec tous les mots de code possibles



- Choisir le mot de code avec nb minimum de différences ('Plus Probable')

Exemple

- Mots de code : 0 0 0 0 0   0 1 0 1 1   1 0 1 0 1   1 1 1 1 0
- Reçu :   0 0 0 1 1
- Différence : 0 0 0 1 1   0 1 0 0 0   1 0 1 1 0   1 1 1 0 1
- Meilleure supposition : 0 1 0 1 1

une seule différence

Quelques problèmes se posent

- Mapping entre messages et mots de code
  - génération des mots de code (assez différent les uns les autres) → Construction de codes
  - Emmagasinage du code book (2^k mots de code, longueur n) → Codage
- Décodage
  - Comparer une séquence reçue avec tous les mots de code

Définitions

- Distance de Hamming entre x et y est
  $d_H := d(x, y) =$ nb de positions où $x_i \neq y_i$
- La distance minimale d'un code C est
  $d_{min} = \min \{ d(x, y) \mid x \in C, y \in C, x \neq y\}$
- Poids de Hamming d'un vecteur x est
  - $w(x) := d(x, 0) =$ nb de positions où $x_i \neq 0$

Exemple

- *distance de Hamming* d(1001, 0111) = 3
- *distance minimale* (101, 011, 110) = 2
- *Poids de Hamming* w(0110101) = 4

Hamming (Bell-lab,1950) → les codes de Hamming.

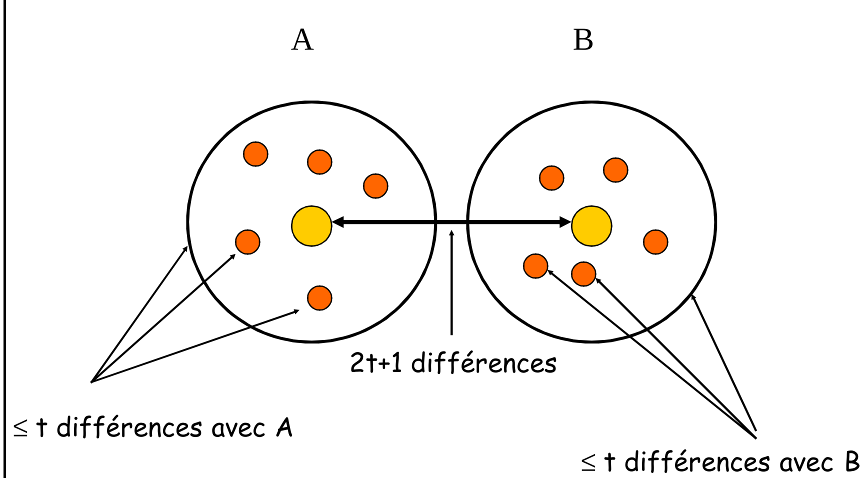
Performance

Un code avec une distance minimale d_{min} est capable de détecter 2t erreurs si

$$d_{min} \geq 2\,t + 1.$$

Ce code est aussi capable de corriger t erreurs

Illustration



Codes Linéaires

Code binaire est dit linéaire ssi

- La somme modulo-2 composante à composante de deux mots de code est aussi un mot de code.

Par conséquent le mot plein de zéro est un mot de code.

Générateur de Code Linéaire

- Les mots de code sont
  - des combinaisons linéaires des lignes d'une matrice génératrice binaire *G* de dimensions k, n
  - G doit être de rang k !
- Exemple: Considérons k = 3, n = 6.
- matrice génératrice

$$G = \boxed{\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{array}}$$

(1,0,1)G = (0, 0, 1, 0, 1, 1)

Codes Systématiques

La matrice G est de la forme :

$G = [\ I_k\ P\ ]$;

$$G = \boxed{\begin{matrix} 1\ 0\ 0 \mid 1\ 1\ 0 \\ 0\ 1\ 0 \mid 1\ 0\ 1 \\ 0\ 0\ 1 \mid 0\ 1\ 1 \end{matrix}}$$

$k = 3$, $n = 6$

Le code engendré est
- linéaire, systématique
- admet une distance minimale 3.
- le taux du code est 3/6.

Exemple (optimum)

- Code à parité simple $d_{min} = 2$, $k = n-1$

$$G = \quad [\ I_{n-1}\ P\ ] = \boxed{\begin{matrix} 100 & \cdots & 0 & 1 \\ 0100 & \cdots & 0 & 1 \\ & \cdots & & \\ 00 & \cdots & 01 & 1 \end{matrix}}$$

Tous les mots de code ont un poids pair !

Exemple (optimum)

- Code à répétition : $d_{min} = n$, $k = 1$

- G = [1 1 ••• 1]

Exemple de code de Hamming

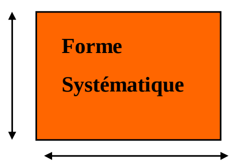
$$G = \begin{pmatrix} 1000 & 110 \\ 0100 & 101 \\ 0010 & 011 \\ 0001 & 111 \end{pmatrix}$$

Paramètres du code (n=7, k=4, dmin=3)

Codes Equivalents

- Toute matrice génératrice d'un code linéaire peut être mise sous une forme systématique

- G_{sys} = k



n

Outil : Les opérations élémentaires sur les lignes et les colonnes de la matrice

Propriété

- L'ensemble des **distances** entre paires de mots de code
- est le même que celui des distances relativement au mot nul.

- **En effet:**
  $d(x, y) = d(x \oplus x, z = y \oplus x) = d(0, z)$,

- par linéarité z est aussi un mot de code.

Ainsi !

La **détermination** de la distance minimale d'un code est équivalente à

la **détermination** du poids de Hamming minimum des mots de code.

La complexité de cette opération est proportionnelle au nb de mots de code

Exemple

- Considérons le code suivant :
  - 00000
  - 01101
  - 10011
  - 11110

La distance minimale est égale au poids minimum (= 3)

Détection par syndrome

Soit $G = [\ I_k\ P\ ]$ alors on construit $H^T = \begin{pmatrix} P \\ I_{n-k} \end{pmatrix}$

Pour tous mot de code $c = xG$, $cH^T = xGH^T = 0$

Ainsi, pour un vecteur reçu bruité ($r = c \oplus e$) :

$$\begin{aligned} r H^T &= (c \oplus e) H^T = c H^T \oplus e H^T \\ &= e H^T \\ &=: S \end{aligned}$$

Exemple

$G = \begin{matrix} 100\ 110 \\ 010\ 101 \\ 001\ 011 \end{matrix}$

$H^T = \begin{matrix} 110 \\ 101 \\ 011 \\ 100 \\ 010 \\ 001 \end{matrix}$

$x = 1\ 0\ 1$

$c = 1\ 0\ 1\ 1\ 0\ 1$

$c\ H^T = 0\ 0\ 0$

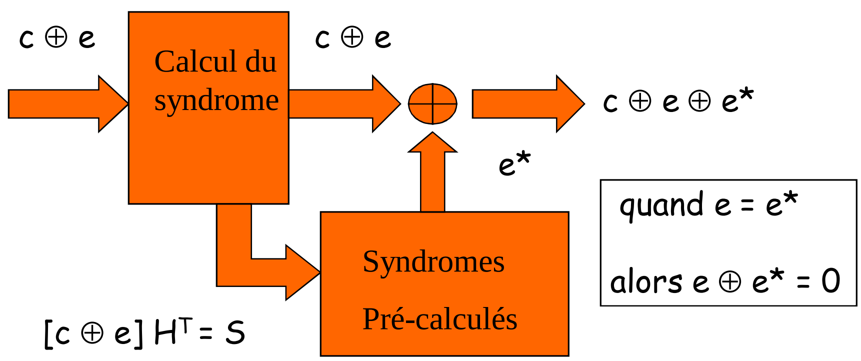
$e = 0\ 1\ 0\ 0\ 0\ 0$

$c \oplus e = 1\ 1\ 1\ 1\ 0\ 1$

$[c \oplus e]\ H^T = S = 1\ 0\ 1$

- La matrice H est dite matrice de parité

Architecture du détecteur (Correcteur)



Codes Cycliques CRC

Soit a = $(a_0\ a_1, \ldots, a_{k-1})$ k bits d'information

il peut être représenté par $A(X) = a_0+a_1X + \ldots + a_{k-1} X^{k-1}$

le polynôme générateur $g(X) = g_0+g_1X + \ldots + g_{n-k} X^{n-k}$.

le mot de code (le polynôme) à transmettre est (***procédure de codage***) :

$C(X) = X^{n-k} A(X) \bmod g(X) + X^{n-k} A(X)$

Noter que $C(X) \bmod g(X) \equiv 0$, ainsi $C(X)$ est un multiple de $g(X)$.

Procédure de détection

Supposons que nous recevons le polynôme R(X) = C(X) + E(X)

où E(X) est un polynôme d'erreur binaire
i.e. un vecteur erreur (1,0,0,1,0) $\rightarrow$ E(X) =1+ X^3

Le décodeur calcule S(X)=R(X) mod g(X) - si S(X) = 0 → 'pas d'erreur détectée' - si S(X) <> 0, alors une erreur est détectée.

Le polynôme R(X) mod g(X) = 0 ssi E(X) est un multiple de g(X).

Codes cycliques -Correction

- Codes BCH (Bose-Chaudhuri-Hocquenghem)
- Codes de Reed –Solomon

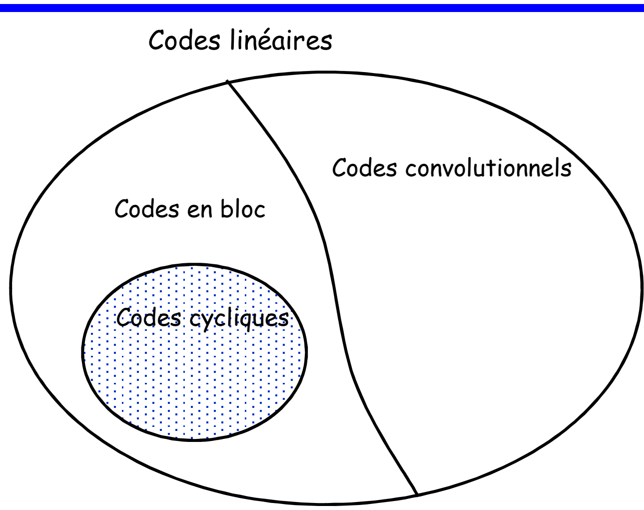
- Codes cycliques construit de manière systématique permettant de corriger au moins *t* erreurs dans un bloc de *n* symboles.
- Les symboles sont dans un corps finis GF(q)

- Algorithme de Berlekamp pour le décodage.

Applications des codes

- Codes détecteurs d'erreurs → ARQ (Automatic Repeat reQuest)
- Codes Correcteurs d'erreurs → FEC (Forward Error Correction)
- Systèmes hybrides → HARQ : Hybrid ARQ
- Erasure Codes (AL-FEC codes)

Codes correcteurs



Travaux d'actualité

- Turbo codes (Berrou et al, 1993)
- Décodage itératif : Turbo décodage, Belief Propagation, Message Passing,…
- Codes LDPC (Galager, Mackay 1995)
- Turbo Product Codes (Pyndiah et al.1994)
- Fountain codes (Luby et al., 1997)
- Network Coding (Routage +Codage)