ULB UNIVERSITÉ LIBRE DE BRUXELLES

Réseaux, information et communication

Fiabilité - Débit
Théorème fondamental de Shannon
Codes correcteurs d'erreur
Codes linéaires

Yves Roggeman

FACULTÉ DES SCIENCES - DÉPARTEMENT D'INFORMATIQUE

Boulevard du Triomphe - CP212

B-1050 Bruxelles (Belgium)

Tél. : +32-2-650 5598

E-mail : **yves.roggeman@ulb.ac.be**

Année 2015–2016

ULB
UNIVERSITÉ LIBRE DE BRUXELLES
yves.roggeman@ulb.ac.be

Fiabilité

- **Code à répétition (canal binaire)**
  - **$\mathbb{P}$[erreur] par bit = p $\Rightarrow$ répéter n fois**

    Décodage par majorité : $\mathbb{P}_{err} = \sum_{k=\lceil \frac{n}{2} \rceil}^{n} \binom{n}{k} p^k (1-p)^{n-k} < \frac{(2p)^n}{n}$
  - **Fiabilité = 1 - $\mathbb{P}_{err}$**
  - **Si $\lim_{n\to\infty} \mathbb{P}err = 0$ si p < ½ (en fait p ≠ ½ suffit)**
    - Mais on ne transmet (presque) plus rien !
- **Généralisation : code correcteur**
  - **Code bloc : K(S) = K $\subset C^n$; noter x et plus K(x)**
  - **Décodage de y $\in C^n$ « reçu » (si y $\notin$ K(S)) :**
    - Maximum de vraisemblance : $y \mapsto x : \max_{x \in S} \mathbb{P}[y|x]$

Débit d'un code

- **Définition (« *information rate* »)**
  - $R(K) = \log_r|K| \,/\, L(K) = k/n$ (si $|K| = r^k$)
  - Mesure de l'efficience, du rendement
  - Faux synonyme : « bande passante »
- **Propriétés**
  - $0 \leq R(K) \leq 1$
  - $R(K) = 1 \Leftrightarrow$ Code bloc (Canal sans bruit)
- **Exemple binaire : bit de parité**
  - $R = (n-1)/n = 1 - 1/n$: $n \nearrow$, $R \nearrow 1$, mais $\mathbb{P}_{err} \nearrow 1$

yves.roggeman@ulb.ac.be

(2^d) Théorème de Shannon

- ***Shannon's Fundamental Noisy Channel Theorem***
- **Énoncé (1948)**
  - **∀ canal binaire symétrique de capacité C > 0**
    ∀ δ > 0, ∀ ε > 0, ∃ code K :

$$\mathbb{P}_{err}(K) < \varepsilon \quad \text{et } C - R(K) < \delta$$

- **Démonstration (Amiel Feinstein 1954)**
  - **Complexe ⇒ sketch :**
    - Fixer n et δ' < δ : $\log_r|K| = k = n(C-\delta') \in \mathbb{Q}$ (*i.e.* R = C-δ')
    - K = r^k mots <u>au hasard</u> parmi r^n ⇒ $\mathbb{P}_{err}(K)$= var. aléatoire
    - ∀ δ, ∀ ε, ∃ N : n > N ⇒ $E[\mathbb{P}_{err}] < \varepsilon$ (partie difficile !)
    - ⇒ ∃ K_n : $\mathbb{P}_{err}(K_n) \leq E[\mathbb{P}_{err}] < \varepsilon$

yves.roggeman@ulb.ac.be

Conséquences

- **Remarques**
  - C = lim sup accessible pour R et fiable ≈ 100 %
  - On peut y arriver « au hasard »,
    mais on ne sait pas comment (thm existence)
  - On ne connaît aucun aussi code « idéal » !
- **Inverse (Jacob Wolfowitz 1959)**
  - $\forall n, \exists \varepsilon > 0 : R(K_n) \geq C+\varepsilon \Rightarrow \lim_{n\to\infty} \mathbb{P}_{err}(K_n) = 1$
  - *i.e.* ce K est tout à fait non fiable
  - Utilise inégalité de Fano : $|X| = m$, $P_{err} = E[\mathbb{P}_{err}]$

$$H(X|Y) \leq H(P_{err}) + P_{err} \log_r(m-1)$$

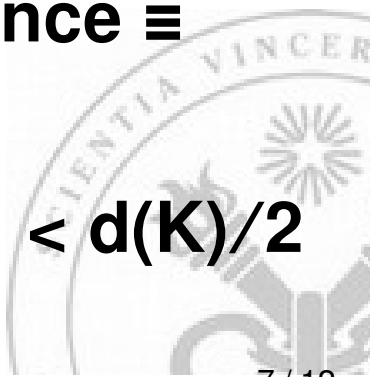
yves.roggeman@ulb.ac.be

Distance de Hamming

- **Définition (r quelconque)**
  - **$\forall$ a, b $\in C^n$: d(a, b) = # { i | $a_i \neq b_i$ }**
  - **Si r = 2 : d(a, b) = w(a $\oplus$ b) (*i.e.* poids)**
- **Propriétés**
  - **C'est une distance !**
  - **Donc : 3 propriétés :**
    - d(a, b) $\geq$ 0 ; d(a, b) = 0 $\Leftrightarrow$ a =b
    - d(a, b) = d(b, a)
    - d(a, b) + d(b, c) $\geq$ d(a, c)
  - **0 $\leq$ d(a, b) $\leq$ *n* et d(a, b) $\in \mathbb{N}$**
- **Poids de Hamming : w(a) = w(d(a, 0))**

Code détecteur ou correcteur

- **Distance minimale et poids d'un code**
  - $d = d(K) = \min \{ d(a, b) \mid a, b \in K, a \neq b \}$
  - $w(K) = \min \{ w(a) \mid a \in K, a \neq 0 \}$
- **Détecter**
  - Reçu $y \notin K \Rightarrow$ il y a eu une erreur !
  - Thm : K détecte t erreurs $\Leftrightarrow t \leq d-1 < d(K)$
- **Corriger**
  - Thm : si $p < ½$, maximum de vraisemblance $\equiv$ $y \mapsto x : d(x, y) = \min_{x \in K} d(x, y)$
  - Thm : K corrige t erreurs $\Leftrightarrow t \leq \lfloor (d-1)/2 \rfloor < d(K)/2$



Inégalités remarquables

- **Correction maximale pour code $A_r(n, d)$**
  - **Rayons de recouvrement [c] et d'empilement [s]**

    $$s \leq \lfloor (d-1)/2 \rfloor \leq (d-1)/2 \leq \lfloor d/2 \rfloor \leq c$$

  - **Corrige t erreurs : $t \leq s$**

    Au maximum : $t = s = c \Rightarrow d = 2 \cdot t+1$

- **Borne de Richard W. Hamming (1950)**

  $$|A_r(n,d)| \leqslant \frac{r^n}{V_{\lfloor (d-1)/2 \rfloor}} \quad \text{où} \quad V_t = \sum_{i=0}^{t} \binom{n}{i} (r-1)^i$$

  - **Si $|K| = r^k$: $V_{\lfloor (d-1)/2 \rfloor} \leq r^{n-k}$**

- **Borne de Richard C. Singleton (1964)**

  $$|A_r(n, d)| \leq r^{n-d+1}$$

  - **Si $|K| = r^k$: $d \leq n-k+1$**

Code linéaire

- **Propriétés / définition**
  - **C^n = E = espace vectoriel sur le corps F**
    - NB : $r = |F| = p^\beta$ où p est un nombre premier
    - Cas binaire : $r = 2$ ou $C = F_2$
  - **Code K = sous-espace de E :**
    - $a, b \in K \Rightarrow (a + b) \in K$
    - $\lambda \in F, a \in K \Rightarrow \lambda \cdot a \in K$ (pas utile si $K = F_2$)
    - $K \neq \varnothing$ ou $0 \in K$
  - **Dimensions : dim E = n, dim K = k**
  - **Paramètres : $[n, k, d]_r$**

ULB
UNIVERSITÉ LIBRE DE BRUXELLES
yves.roggeman@ulb.ac.be

Matrice génératrice, de contrôle

- **Matrice génératrice « G »**
  - **K est application linéaire <u>injective</u> :**
    - $K : F^k \rightarrow F^n : x \mapsto x \cdot G$ (NB : x = vecteur-ligne)
    - G = matrice $k \times n$ sur F, de rang k
- **Matrice de contrôle « H »**
  - **Contrôle = application de noyau K(X)**
    - Noyau : $Ker(P) = \{y \in F^n \mid P(y) = 0\}$
    - $P : F^n \rightarrow F^{n-k} : {}^{\tau}y \mapsto H \cdot {}^{\tau}y$, avec Ker(P) = K
    - H = matrice $(n-k) \times n$, de rang $(n-k)$
    - Donc : $K(F^k) = K = \{y \in F^n \mid H \cdot {}^{\tau}y = 0\}$

ULB
UNIVERSITÉ LIBRE DE BRUXELLES
yves.roggeman@ulb.ac.be

Équivalence, Forme canonique

- **Équivalence**
  - **$G' \equiv G \Leftrightarrow \exists\ U(k\times k)$ inversible : $G' = U\cdot G$**
  - **U = changement de base dans F^k**
- **Forme canonique (ou systématique)**
  - **$G = [1_k|P]$**
    - P : « parité » ou « redondance » : $y = [x|\pi]$
    - n-k dernières coordonnées = somme de contrôle
  - **$\Rightarrow$ $H = [-{}^\tau P|1_{n-k}]$ (car $G\cdot{}^\tau H = 0_{k\times(n-k)}$)**
  - **Tout code est ≡ à un code canonique :**
    - Construction du U par élimination de Gauß

Décodage par syndrome

- **Syndrome : $\sigma(y) = H \cdot {}^{\tau}y$**
  - **NB : σ = vecteur-colonne $\in F^{n-k}$**
  - **Si $y = x + \varepsilon$ où $x \in K$, alors $\sigma(y) = H \cdot {}^{\tau}\varepsilon$**
    - Si $H = [-{}^{\tau}P | 1_{n-k}]$, $y = [y_k | y_{n-k}]$, $\sigma(y) = {}^{\tau}y_{n-k} - {}^{\tau}P \cdot {}^{\tau}y_k$
    - Et $x \in K \Leftrightarrow x = [x_k | x_k \cdot P] \Leftrightarrow \sigma(x) = 0$
- **Décodage**
  - **Table : $\sigma \mapsto \varepsilon$ $\forall \sigma : d(\sigma, 0) \leq t$ [$\leq r^{n-k}$ entrées]**
  - **Décodage : $y \mapsto \sigma(y) \mapsto \varepsilon \mapsto x = y - \varepsilon$**
    - $\sigma(y) = \sigma(y') \Rightarrow d(y, y') = d(x, x') \geq d > 2 \cdot t$
    - OK si $t = c$ (= s), sinon ambiguïté pour $t < d(\sigma, 0) \leq c$
  - **Enjeu : remplacer table par algorithme**