Nicolas Sendrier

Majeure d'informatique

Introduction à la théorie de l'information

Cours n°7

Codes correcteurs d'erreurs

Code en bloc – Distance de Hamming

Soit A un alphabet, par exemple $A = \{0, 1\}$. Soit A^n l'ensemble des mots de longueur n. La *distance de Hamming* entre deux éléments $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ de A^n est définie par

$$d_H(x, y) = |\{x_i \neq y_i \mid i = 1, \ldots, n\}|$$

Le poids de Hamming de x est défini par $w_H(x) = d_H(x, 0)$.

Un code (correcteur d'erreur) en bloc est un sous-espace métrique non vide de A^n. La distance minimale d'un code $\mathcal{C}$ est l'entier

$$d(\mathcal{C}) = \min_{x \neq y | x, y \in \mathcal{C}} d_H(x, y)$$

Le taux de transmission du code $\mathcal{C}$ est défini par

$$R = \frac{\log_q M}{n}$$

où $M = |\mathcal{C}|$ et $q = |A|$.

Décodeur à vraisemblance maximale

Soit un canal de communication (A, B, Π). Soit $\mathcal{C}$ un code de longueur n sur A.

Définition Un *algorithme de décodage* de $\mathcal{C}$ est une procédure qui à tout élément de B^n associe un mot de $\mathcal{C}$ ou qui échoue (symbole ∞).

$$\begin{array}{rccc} \varphi : & B^n & \to & \mathcal{C} \cup \{\infty\} \\ & y & \mapsto & \varphi(y) \end{array}$$

Définition Un algorithme de décodage φ de $\mathcal{C}$ est dit à *vraisemblance maximale* si pour tout $y \in B^n$, le mot $x = \varphi(y)$ est dans $\mathcal{C}$ et réalise le maximum de la probabilité $P(\text{“}x \text{ émis”} \mid \text{“}y \text{ reçu”})$.

Canal q-aire symétrique

Canal fortement symétrique (A, B, Π) avec $A = B$, $|A| = q$ et

$$P_{B|A}(b|a) = \begin{cases} 1-p & \text{si } a = b \\ \frac{p}{q-1} & \text{si } a \neq b \end{cases} \qquad \begin{cases} p & \text{probabilité d'erreur} \\ \frac{p}{q-1} & \text{probabilité de transition} \end{cases}$$

Proposition Dans un canal q-aire symétrique sans mémoire de probabilité de transition $< 1/q$, si la loi d'émission des mots de code est uniforme, le mot $x \in \mathcal{C}$ le plus probablement émis connaissant le mot reçu $y \in A^n$ est un mot réalisant le minimum de $d_H(x, y)$.

Preuve : $$P(x \mid y) = \frac{P(y)}{P(x)} \left(\frac{p}{q-1}\right)^{d_H(x,y)} (1-p)^{n-d_H(x,y)}$$

$\Rightarrow$ dans les hypothèses de l'énoncé la meilleure stratégie de décodage consiste trouver le mot de code le plus proche du mot reçu pour la distance de Hamming.

Distance minimale – Décodage

Soit $\mathcal{C}$ un code de distance minimale d.

– Deux boules de rayon $(d-1)/2$ centrées en deux mots de code distincts sont disjointes.
  $\Rightarrow$ un code de distance minimale d peut corriger $\lfloor (d-1)/2 \rfloor$ erreurs

– Toute boule de rayon $d-1$ centrée en un mot de code ne contient aucun autre mot de code.
  $\Rightarrow$ un code de distance minimale d peut détecter $d-1$ erreurs

Performances

Définition Un algorithme de décodage φ d'un code $\mathcal{C}$ est dit *borné par t* si pour tout $x \in \mathcal{C}$

$$d_H(x, y) \leq t \Rightarrow \varphi(y) = x$$

Si la réciproque est vraie, l'algorithme est dit *strictement borné*.

Tout code de distance minimale d possède un algorithme de décodage borné par $\lfloor (d-1)/2 \rfloor$. C'est aussi la meilleure valeur possible.

Proposition La probabilité de transmission correcte d'un mot à travers un canal de probabilité d'erreur p décodé à l'aide d'un algorithme strictement borné par t vaut

$$\sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}$$

Codes linéaires

Lorsque l'alphabet est un corps fini (par exemple $A = \mathbf{F}_2 = \{0, 1\}$) l'espace de Hamming A^n est un espace vectoriel.

Définition Un code en bloc linéaire de longueur n sur $\mathbf{F}_q$ (le corps fini à q élément) est un sous-espace vectoriel de $\mathbf{F}_q^n$.

Nous parlerons de code $[n, k]_q$ si le code est de dimension k et de code $[n, k, d]_q$ si sa distance minimale est d. Un code $\mathcal{C}[n, k]_q$ peut se caractériser par

– sa matrice génératrice G (de taille $k \times n$ sur $\mathbf{F}_q$) :

$$\mathcal{C} = \left\{(u_1, \ldots, u_k)G \mid (u_1, \ldots, u_k) \in \mathbf{F}_q^k\right\}$$

Les lignes de G forment une base de $\mathcal{C}$.

– ou sa matrice de parité H (de taille $(n-k) \times n$ sur $\mathbf{F}_q$) :

$$\mathcal{C} = \left\{(x_1, \ldots, x_n) \in \mathbf{F}_q^n \mid H(x_1, \ldots, x_n)^T = 0\right\}$$

Les lignes de H forment une base de l'orthogonal de $\mathcal{C}$.

Codes linéaires – Propriétés

Proposition Pour tout code linéaire $\mathcal{C}$

$$\min_{x \neq y | x,y \in \mathcal{C}} d_H(x,y) = \min_{x \neq 0 | x \in \mathcal{C}} w_H(x)$$

(la distance minimale est égale au poids minimal)

Proposition Soit $\mathcal{C}$ un code de matrice de parité H

$$\left(\begin{array}{c} \mathcal{C} \text{ de distance} \\ \text{minimale } d \end{array} \right) \Leftrightarrow \left(\begin{array}{c} d-1 \text{ colonnes quelconques} \\ \text{de } H \text{ sont libres} \end{array} \right)$$

Proposition **(Borne de Singleton)**
Pour tout code $[n,k,d]$ nous avons $d \leq n - k + 1$.

Existence de bon codes – Borne de Varshamov-Gilbert

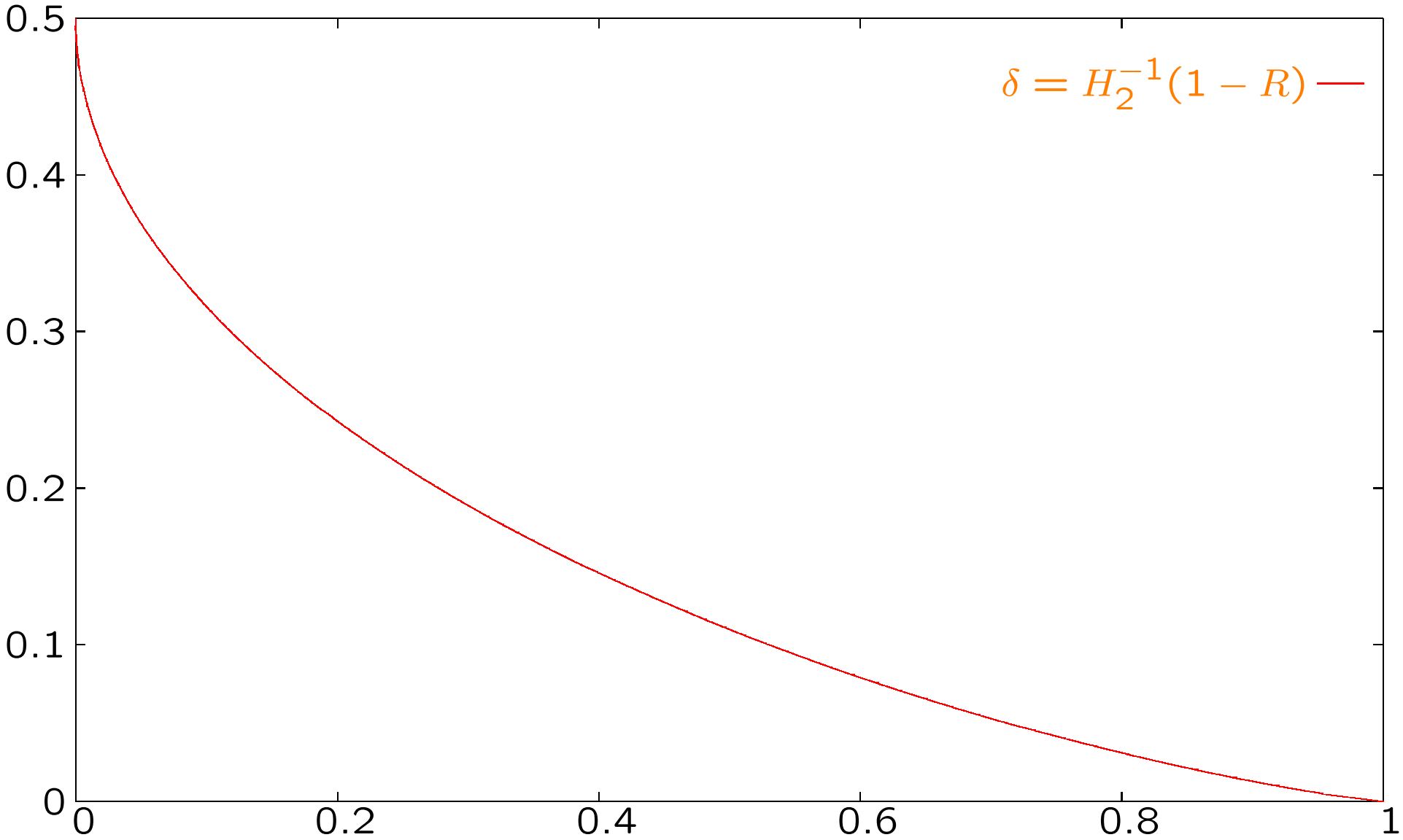
Theorème (Borne de Varshamov-Gilbert)

$$\sum_{i=0}^{d-2}(q-1)^i\binom{n-1}{i} < q^{n-k} \Rightarrow \begin{pmatrix}\text{il existe un}\\ \text{code } [n,k,d]_q\end{pmatrix}$$

Theorème (Borne de Varshamov-Gilbert asymptotique)
Soit $0 \leq \delta \leq (q-1)/q$. Pour tout $0 \leq R < 1 - H_q(\delta)$ il existe une infinité de codes $[n,k,d]_q$ tels que $d \geq \delta n$ et $k \geq Rn$.

$$(H_q(x) = -x\log_q\frac{x}{q-1} - (1-x)\log_q(1-x) \text{ est la fonction d'entropie } q\text{-aire})$$

Varshamov-Gilbert – Cas binaire



Codes linéaires – Décodage par syndrome

À toute matrice de parité H de $\mathcal{C}$ on associe le syndrome

$$\begin{array}{rccc} S_H : & \mathbf{F}_q^n & \to & \mathbf{F}_q^{n-k} \\ & y & \mapsto & S_H(y) = Hy^T \end{array}$$

Nous noterons $S_H^{-1}(s) = \{y \in \mathbf{F}_q^n \mid S_H(y) = s\}$. Nous avons $S_H^{-1}(0) = \mathcal{C}$, et de façon générale

$$S_H^{-1}(Hy^T) = y + \mathcal{C} = \{y + x \mid x \in \mathcal{C}\}$$

Pour tout $s \in \mathbf{F}_q^{n-k}$, notons $L_H(s)$ un mot de poids minimal de $S_H^{-1}(s)$.

Proposition Le décodeur $y \mapsto y - L_H(Hy^T)$ est à vraisemblance maximale.

Décodage par tableau standard : mettre $L(s)$ en table (précalcul).

Décodage algébrique : calculer $L(s)$ pour certaines valeur de s.

Exemple

Code de Hamming de longueur 7 (et dimension 4). Matrice de parité :

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Pour un mot reçu $y \in \mathbf{F}_2^7$, il y a 8 syndromes possibles

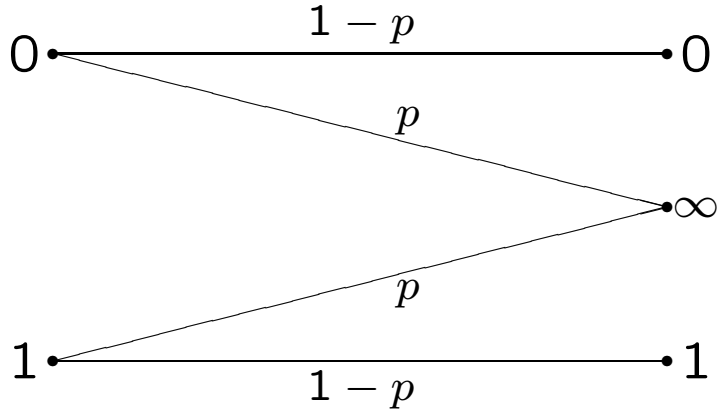
$$Hy^T \in \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\},$$

le premier correspond à un mot de code les autres à une erreur respectivement en position 1, 2, . . . , 7.

$\Rightarrow$ tout mot de l'espace de Hamming $\{0,1\}^n$ s'écrit $x + e$ avec x dans le code et e de poids au plus 1 (code parfait).

Correction d'effacements

Un effacement est une « erreur localisée », c'est-à-dire que les symboles sont transmis à travers le canal suivant :



Pour tout code de distance minimale d, il existe un algorithme de décodage corrigeant $d-1$ effacements.

$\Rightarrow$ un effacement est « deux fois plus facile » à corriger qu'une erreur.

Proposition Pour tout code de distance minimale d, il existe un algorithme de décodage corrigeant ν erreurs et ρ effacements ssi

$$2\nu + \rho < d$$

Codes concaténés

Il sont construit à partir de deux codes :

- le code interne $\mathcal{B}[n,k]$ sur $\{0,1\}$ (généralement)
  codeur : $\psi : \{0,1\}^k \to \mathcal{B} \subset \{0,1\}^n$.
- le code externe $\mathcal{E}[N,K]$ sur A avec $|A| = |\mathcal{B}|$ $(= 2^k)$
  codeur : $\Psi : A^K \to \mathcal{E} \subset A^N$.

Codage :

$$\begin{array}{ccccccc} A^K & \xrightarrow{\Psi} & A^N & \xrightarrow{\psi} & \{0,1\}^{nN} \\ (u_1,\ldots,u_K) & \longmapsto & (x_1,\ldots,x_N) & \longmapsto & \psi(x_1) \,\|\, \ldots \,\|\, \psi(x_N) \end{array}$$

(on identifie A et $\{0,1\}^k$)

Codes concaténés – Décodage

Le mot reçu est de la forme

$$\underbrace{(y_{1,1},\ldots,y_{1,n})}_{y_1} \parallel \underbrace{(y_{2,1},\ldots,y_{2,n})}_{y_2} \parallel \cdots \parallel \underbrace{(y_{N,1},\ldots,y_{N,n})}_{y_N}$$

Chacun des N bloc est décodé indépendemment à l'aide d'un décodeur de $\mathcal{B}$:

$$\begin{array}{rccc} \varphi & : & \{0,1\} & \to & \mathcal{B}\cup\{\infty\} \\ & & y_i & \mapsto & z_i \end{array}$$

Chaque lettre du mot $(z_1,\ldots,z_N)$ peut être identifiée avec un symbole de A ou bien avec un effacement (symbole ∞). L'ensemble est ensuite décodé à l'aide d'un décodeur d'erreurs et d'effacements du code externe $\mathcal{E}$.

$\Rightarrow$ Il n'est pas forcément optimal d'utiliser le code interne au maximum de sa capacité de décodage, il existe un optimum entre le nombre d'erreurs et le nombre d'effacements produits par le décodeur interne.