Correction d'erreurs de transmission

Théophile Cailliau

Sommaire

Définition

Pour un alphabet Σ, un **mot fini** de longueur n est un élément de Σ^n. On notera $\boldsymbol{a} = a_1 a_2 \cdots a_n$ le mot $(a_1, \cdots, a_n)$. Un **mot binaire** est un mot sur l'alphabet $\boldsymbol{F}_2$ (on note ses éléments 0 et 1).

On note $\mathbf{0} = 0 \cdots 0$ et $\mathbf{1} = 1 \cdots 1$

Code

Définition

Un **(n, M)-code** C sur l'alphabet Σ de cardinal q est une partie $C \subseteq \Sigma^n$ de cardinal M. On dit que M est sa dimension. On dit qu'il est q-aire s'il est l'image d'une application injective $E : \Sigma^k \longrightarrow \Sigma^n$. Dans ce cas, $M = k$

En pratique, on prendra toujours pour Σ le corps fini à q éléments $\boldsymbol{F}_q$

Distance de Hamming

Définition

Le poids d'un mot $\boldsymbol{u}$ est définit par

$$w(\boldsymbol{u}) := d(\boldsymbol{y}, \boldsymbol{0})$$

pour $d : \boldsymbol{F}_q^n \times \boldsymbol{F}_q^n \to \boldsymbol{R}_+^\star$

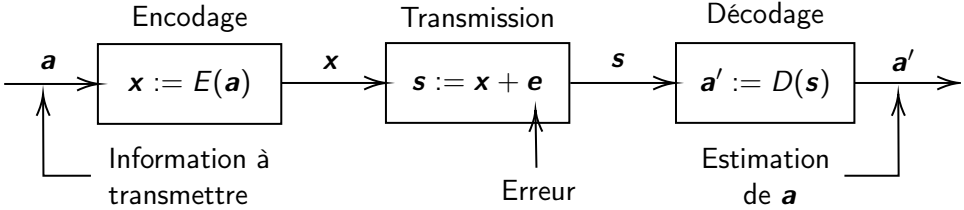
Une distance souvent utilisée est la distance de Hamming :

Propriété-Définition

On définit la **distance de Hamming** sur $\boldsymbol{F}_q^n$ de la manière suivante : pour $\boldsymbol{a} = a_1 \cdots a_n$ et $\boldsymbol{b} = b_1 \cdots b_n$ des mots de $\boldsymbol{F}_q^n$,

$$d(\boldsymbol{a}, \boldsymbol{b}) := \#\{i \in [\![1, n]\!] \mid a_i \neq b_i\}$$

Principe des codes correcteurs



- $E : \boldsymbol{F}_q^k \longrightarrow C \subseteq \boldsymbol{F}_q^n$ est la fonction d'encodage
- $D : \boldsymbol{F}_q^n \longrightarrow \boldsymbol{F}_q^k$ est la fonction de décodage

Encodage et Décodage

Définition

Soit E une application injective associée à un (n, k)-code q-aire C. Alors E est une fonction d'encodage. Pour u un mot de longueur k, $E(\boldsymbol{u})$ est le mot codé associé à $\boldsymbol{u}$.
Une fonction $D : \boldsymbol{F}_q^n \longrightarrow \boldsymbol{F}_q^k$ est une fonction de décodage si $D \circ E = \mathrm{Id}$.

L'injectivité de E garantit l'existence d'une fonction de décodage.

Codes e-correcteurs

Définition

La **distance minimale** d'un (n, k)-code $C \subseteq \boldsymbol{F}_q^n$ est la valeur

$$d(C) := \min\{d(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x}, \boldsymbol{y} \in C, \boldsymbol{x} \neq \boldsymbol{y}\}$$

On dira alors que C est un (n, M, d)-code, où $d = d(C)$.

Définition

Un (n, k, d)-code est e-correcteur si pour tout $\boldsymbol{y} \in \boldsymbol{F}_q^n$, il existe au plus un mot $\boldsymbol{x}$ de C tel que $d(\boldsymbol{x}, \boldsymbol{y}) \leq e$

L'utilisation d'un tel code garantit que si l'erreur $\boldsymbol{e}$ ajoutée lors de la transmission est telle que $w(\boldsymbol{e}) \leq e$, alors on pourra retrouver le mot d'origine

Définition

Un $(n, k, 2e+1)$-code C est dit **parfait** si on a

$$\forall \boldsymbol{x} \in \boldsymbol{F}_q^n, \exists ! \boldsymbol{y} \in C, d(\boldsymbol{x}, \boldsymbol{y}) \leq e$$

Cela revient à dire que chaque mot de $\boldsymbol{F}_q^n$ admet un unique décodage pour le code C

Exemple : Code de répétition

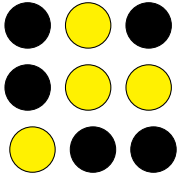


Figure – Donnée à transmettre

Exemple : Code de répétition

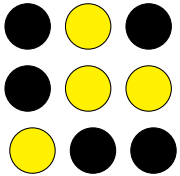


Figure – Donnée à transmettre

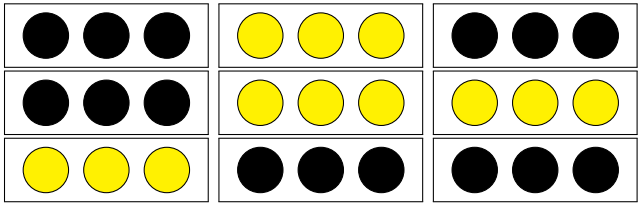


Figure – Information codée

Exemple : Code de répétition

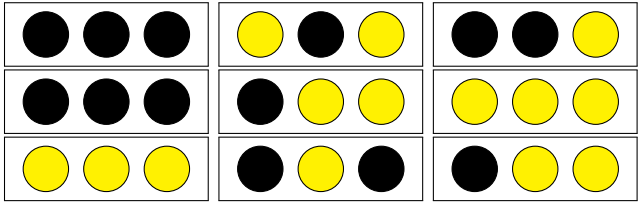


Figure – Information reçue

Exemple : Code de répétition

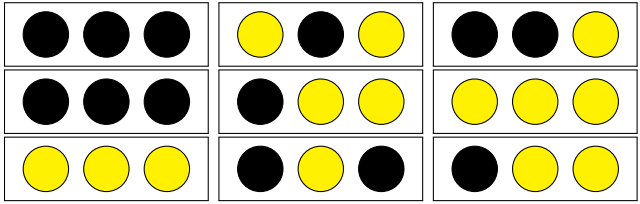


Figure – Information reçue

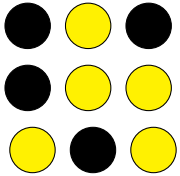


Figure – Estimation du message d'origine

Pistes

- Codes linéaires et cycliques
- Codes convolutionnels