CODES CORRECTEURS

I] Pourquoi ?

Perturbations dues à l'environnement / systèmes de transmission
↳ ajout d'un signal aléatoire ("bruit")
↳ solutions physiques, mais aussi numériques.

II] Principe :

Ajout de bits de contrôle ou de redondance au codage existant.

$$\left.\begin{array}{l} s = s_1 \dots s_k \\ \phi(s) = s'_1 \dots s'_{k+n} \end{array}\right\} \quad \phi \text{ injective, } \mathrm{Im}\,\phi \subset \{0;1\}^{k+n} \text{ et } |\mathrm{Im}\,\phi| = 2^k$$

↳ détection d'une erreur : test d'appartenance à $\mathrm{Im}\,\phi$
↳ On choisit ϕ pour détecter le $\oplus$ d'erreurs possible et à moindre coût.
↳ Deux possibilités de correction : par retransmission ou directe.

Ex : Redondance totale, bit de parité

III] Définitions :

Codage systématique : découpage en blocs de k chiffres, puis codage de chaque bloc en ajoutant n bits de contrôle.

↳ $\left\{\begin{array}{ll} m = k+n & \text{longueur du code} \\ R = k/m & \text{rendement du code} \end{array}\right.$ se note $C(m,k)$

Ex : Redond. totale, $C(m, \frac{m}{2})$, $R = \frac{1}{2}$. Parité, $C(m, m-1)$, $R = \frac{m-1}{m}$

Code t-détecteur / correcteur : Code qui permet de détecter / corriger toutes portant sur t chiffres au moins sur un bloc de n chiffres.

Ex : Redond. totale et Parité sont 1-détecteur et 0-correcteurs.

(nuls)

Poids de Hamming : Avec $X = X_1 \dots X_n$, $w(X)$ est $|\{X_i \neq 0\}|$

Distance de Hamming : Avec $\begin{cases} X = X_1 \dots X_n \\ Y = Y_1 \dots Y_n \end{cases}$, $d(X,Y) = w(X-Y)$.

Il s'agit du nombre d'éléments différents entre X et Y. → caractérise le nombre d'erreurs

Code parfait : code qui corrige toute erreur détectée.

IV Correction :

n mot émis, n' mot reçu.

$(C$ détecte une erreur$) \iff (n' \notin C)$

pour pouvoir corriger, n doit être l'unique mot de C le plus proche de n'.

Donc $\forall X \in C, X \neq n, d(X,n') > d(n,n')$.

↳ **Ptéo :** Avec $B_t(X) = \{Y \in V^n / d(X,Y) \leq t\}$:

$(n'$ peut être corrigé$) \iff ((B_{d(n,n')}(n') \cap C) = \{n\})$

donc $(C$ est t-correcteur$) \iff (\forall X \in V^n, |B_t(X) \cap C| = 1)$

Donc la capacité de correction est liée à la distance minimale entre deux éléments de C : $\delta(C) = \min_{(X_1,X_2) \in C, X_1 \neq X_2} d(X_1,X_2)$

↳ **Ptéo :**

$$\begin{aligned} & (\forall X \in V^n, |\{Y \in C / d(X,Y) \leq t\}| \leq 1) \\ \iff & (\forall (X,Y) \in C, X \neq Y, B_t(X) \cap B_t(Y) = \emptyset) \\ \iff & (\forall (X,Y) \in C, X \neq Y, d(X,Y) > 2t) \\ \iff & (\delta(C) > 2t) \end{aligned}$$

$(C$ est t-correcteur$)$

Thm : Un code $C(n,R)$ est t-parfait $\iff$ ($\{B_t(X), X \in C\}$ forme une partition de V^n)

V] Code linéaire :

Code dont les mots sont obtenus après transfo linéaire des bits du mot initial. ↳ sous-espace vect de V^n, de dim k

↳ caractérisé par une matrice génératrice G : $XG=Y$

Ppté: Soit $C(n,k)$ linéaire et $d = \min_{Y\in C, Y\neq 0} w(Y)$

Alors $\delta(C) = d$ et C est $(d-1)$ détecteur et $(\frac{d-1}{2})$ correcteur. noté $CC(n,k,d)$.

THM : borne de singleton : $d \leq n-k+1$

G s'exprime de manière générale sous la forme $G=(R\ L)$, $\begin{cases} R\in GL_k(\mathbb{R}) \\ L\in \mathcal{M}_{k,n}(\mathbb{R}) \end{cases}$

↳ Après permutat° des colonnes, on se ramène à $G'=(I_k, T)$ appelée matrice génératrice normalisée / canonique de C. Alors C' est systématique et $XG' = (X\ XT)$

Détection d'erreurs :

On définit la matrice de contrôle H par $H=(T^T I_n)$. Alors $\forall Y\in C,\ HY=0$.

↳ HY sert à détecter une erreur

↳ On pose $E = Y_{erreur} - Y_{correct}$. Alors E est l'unique mot de w minimal et vérifie $HE = HY_{erreur}$.

↳ Pour corriger : on calcule HY_{err}, et on trouve une colonne de H. En l'appelant e_j, on a juste à modifier le j-ième bit de Y_{err} pour retrouver $Y_{correct}$. (⚠ marche si une seule erreur)