Codes Correcteurs d'erreurs en Inf Quant.

- important pour protéger qubits
  1) pour les protocoles de communication.
  2) pour réaliser le calcul quantique.
- idée générale : introduire redondance dans les états quantiques.
  ↳ Eliminer les erreurs en reconstruire l'état quant original.

On pourrait objecter de la façon suivante :

(*) • En codage classique l'inf est digitalisée.
⟹ les erreurs sont discrètes (bit flips).
⟹ correction d'erreur.

(**) • Cas classique : on observe le signal direct avant de corriger l'erreur.

Mais Cas Quantique (*) et (**) Non triviaux.

états quant $\alpha|0\rangle + \beta|1\rangle$
forment un continuum $\alpha, \beta \in \mathbb{C}^2$.
Correction d'erreur si continuum.

Car d'une mesure détruire l'état quant.
⟹ "perd toute l'information"

<u>Remarquablement</u> : passer outre ces objections. (Shor).

en un mot : Nature "discrète" de la MQ se manifeste et essentiellement on peut en fait regarder l'inf quantique et plusieurs type d'erreurs comme état digitales.

#.

<u>Plan</u> : (1) Rappel sur les codes correcteurs d'erreur classique.
(ex Hamming, ect...).

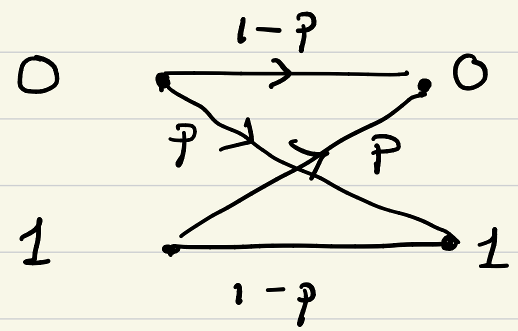
2) Introduire la façon de contourner (*) et (**) avec un code de Répétition Quantique.
"Mauvais code"

3) Code de Rép Quantique ⇝ $\boxed{\text{Code de Shor}}$
traiter des erreurs : bit flip / phase flip.

4) Généralisation → $\boxed{\text{Code CSS}}$
Calderbank - Shor - Steane

① Rappel sur notions élémentaires de codage classique

\# Imaginons un modèle de bruit BSC
"binary symmetric channel"



$0 < p < \frac{1}{2}$.

\# Code de répétition : $\underbrace{0}$ ⇝ $\underbrace{000}$

$\underbrace{1}_{\text{bits d'information}}$ ⇝ $\underbrace{1\,1\,1}_{\text{mots de code}}$.

Transmet un "0" ⇝ Envoyer le mot de code "000"

Recevoir	000	pas d'erreur
	100 010 001	une erreur
	110 101 011	deux erreurs
	111	3 trois erreurs

Décoder si $0 < p \ll \frac{1}{2}$

Règle de Majorité.

000 ⇝ 000
100 ⇝ 000
010 ⇝ 000
001 ⇝ 000

Bon pour 1 erreur au plus

Mauvais 2 ou 3 erreurs

110 ⇝ 111
101 ⇝ 111
011 ⇝ 111
111 ⇝ 111

erreur de décodage

Probabilité de faire une erreur de décodage :

= prob d'avoir 2 ou 3 bits flips.

$$= 3\,p \cdot p \cdot (1-p) + p^3 = 3p^2 - 2p^3.$$

avec $0 < p << \frac{1}{2}$ prob petite $O(p^2)$.

$$\boxed{\text{en fait } 3p^2 - 2p^3 < p \text{ pour tout } 0 < p < \tfrac{1}{2}}$$

Prob de mal décoder avec le code de Répétition et le décodage par règle de majorité

est plus petite

que si vous n'utilisiez pas de code de rép.

#.

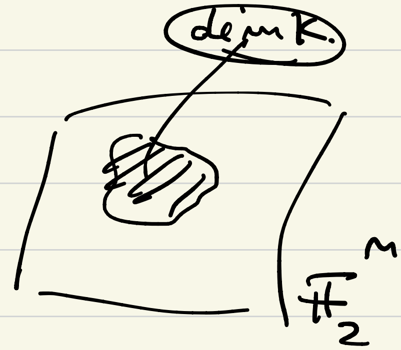
Définitions formelles sur les codes classiques :

Déf Un code linéaire est s-esp vect de dim K de l'esp vect $\mathbb{F}_2^n$.

Code de longueur n et de dimension K.

$\#$(des mots de code) $=$ Card du s-esp vect de dim K

$= 2^K$.



Matrice Génératrice

$$G : \mathbb{F}_2^K \longrightarrow \mathbb{F}_2^n \qquad n > K.$$

$$\vec{u} \longmapsto G\vec{u} = \vec{x}.$$

$$\begin{pmatrix} u_1 \\ \vdots \\ u_K \end{pmatrix} \qquad\qquad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

vect des bits d'information

2^K vect.

$[u_1 \cdots u_K]$

2^K Mots de code de longueur n.

$[x_1 \cdots x_n]$.

mot de code transmis.

$$\boxed{\dim \operatorname{Im}(G) = K = \operatorname{Rank}(G)}$$

$(n > k)$.

- En général on choisit G de dim $\underline{\underline{n}} \times \underline{\underline{k}}$.

avec un <u>rang k</u>.

c.a.d $G = [\vec{g}_1, \vec{g}_2, \dots, \vec{g}_k]$.

k vecteurs colonnes $\vec{g}_i$ de dim n.
et sont <u>lin indépendants</u>.

- <u>Exemple du code de Répétition</u> :

$$G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$\begin{matrix} n & \times & k \\ \shortparallel & & \shortparallel \\ 3 & \times & 1 \end{matrix}.$$

<u>Mots de Code</u> $G\vec{u} = \vec{x}$

$$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \underbrace{[0]}_{\in \mathbb{F}_2} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \underbrace{\underbrace{[1]}_{\in \mathbb{F}_2}}_{\text{bits d'information}} = \underbrace{\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}}_{\text{Mots de code}}$$

Matrice de Parité H.

On décrit le code comme s-esp de $\mathbb{F}_2^n$ vu
↳ dim k.

comme le Noyau d'une matrice H.

$$\vec{x} \in \mathcal{C} \subset \mathbb{F}_2^n \quad \text{ssi} \quad H\vec{x} = 0.$$

dimension de H ? $\qquad \underbrace{(n-k)}_{\text{lignes.}} \times n.$

. on veut ici $\dim \mathcal{C} = k = \dim(\ker H)$

$$= n - \underbrace{\dim(\operatorname{Im} H)}_{\text{rang}(H)}.$$

. si $(n-k)$ lignes sont indépendantes alors
$\text{rang}(H) = n-k \implies n-(n-k) = k$. ✓.

Résumé : H $(n-k) \times n$ avec $n-k$ lignes indép

$$H = \begin{bmatrix} \vec{h}_1^{\,T} \\ \vdots \\ \vec{h}_{n-k}^{\,T} \end{bmatrix}$$ avec $\vec{h}_1 \ldots \vec{h}_{n-k}$ vect à n composantes et lin indép.

$\dim \ker H = k$.
$\dim \operatorname{Im} H = n-k$

Connection importante entre G et H :

$$\begin{cases} G\vec{u} = \vec{x} & \vec{u} \in \mathbb{F}_2^k \\ & \vec{x} \in \mathbb{F}_2^n \\ H\vec{x} = 0 & \end{cases}$$

$$\Rightarrow \underset{[(n-k)\times n]\,[n \times k]}{(H\,G)}\vec{u} = 0 \quad \forall\, \vec{u} \in \mathbb{F}_2^k$$

$$\Rightarrow \boxed{HG = 0}$$

$$\begin{bmatrix} \vec{h}_1^T \\ \vdots \\ \vec{h}_{n-k} \end{bmatrix} \begin{bmatrix} \vec{g}_1 & \cdots & \vec{g}_k \end{bmatrix} = 0.$$

- Si G est connue on peut trouver H. $\boxed{\vec{h}_i^T \vec{g}_1 = 0 \ldots \vec{h}_i^T \vec{g}_k = 0.}$
- Si H est connue on peut trouver G $\boxed{\vec{h}_1^T \vec{g}_i = 0 \ldots \vec{h}_{n-k}^T \vec{g}_i = 0}$

Exemple du code de répétition.

$$G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \qquad H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

$\vec{u} = [0]\ ,\ [1] \in \mathbb{F}_2^{1=k}.$

$\vec{x} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} , \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ vérifiez propriétés discutées.

$\mathbb{H}.$

Exemple du code de Hamming.

Fixé $r \geqslant 2$ entier. Et on considérera tout les vecteurs colonnes de dim r non nuls.

$\Rightarrow 2^r - 1$ vects comme ça

$$H = \begin{bmatrix} \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix} \quad \underbrace{r}_{n-k} \times \underbrace{2^r - 1}_{n}.$$

Matrice de Parité du Code de Hamming.

$$\begin{cases} \text{Mots de Code longueur } n = 2^{r-1}. \\ \text{dim du code } \quad k = 2^{r-1} - 1 - r. \end{cases}$$

$\boxed{\text{Matrice } H \text{ est de rang } r.}$

Hamming $\quad n = 7, \quad k = 4$

$r = 3$

$$n = 2^r - 1 = 7$$
$$k = 2^r - 1 - r = 4.$$

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

On peut calculer G et aussi tous les mots du code : $\quad H\vec{x} = \vec{0}$.

Correction d'erreur..