Correction d'erreur et de la notion de syndrome.

- BSC envoit le mot $\vec{x}$; recoit $\vec{x}'$

$$\vec{x}' = \vec{x} + \vec{e}.$$

↗ vecteur d'erreur $\in \mathbb{F}_2^n$ avec comp. 1 si le bit est erroné et comp 0 si le bit est bien transmis.

$$\vec{x} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} ; \quad \vec{x}' = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \qquad \vec{e} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \leftarrow \text{erreur}.$$

- $\vec{x}' \to$ est $\vec{x}' \in \mathcal{C}$?

$$H\vec{x}' = \underbrace{H\vec{x}}_{0} + H\vec{e} = \boxed{H\vec{e}} \quad \text{syndrôme}$$

- si $H\vec{e} \neq 0$ alors $\vec{x}' \notin \mathcal{C}$ ⇝ certainement une erreur.
- si $H\vec{e} = 0$ alors $\vec{x}' \in \mathcal{C}$ ⇝ pas d'erreur $\vec{x}' = \vec{x}$ et $\vec{e} = 0$
  - ⇝ $\vec{x}' \neq \vec{x}$ et $\vec{e} \neq 0$.

Exemple du code de Hamming : $r = 3$.

$$\boxed{\begin{aligned} n &= 7 \\ k &= 4 \end{aligned}} \quad \begin{aligned} &= 2^r - 1 \\ &= 2^r - 1 - r \end{aligned}$$

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

Supposons que le vecteur d'erreur $\vec{x}' = \vec{x} + \vec{e} \in \mathbb{F}_2^7$

$$\vec{e} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad H\vec{e} = \underbrace{\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}}_{3^{\text{ie}} \text{ colonne de } H.} \neq 0.$$

Ici en calculant $H\vec{e}$ pour des erreurs $\underline{\vec{e}}$ avec <u>1 comp erronée</u> on trouve la <u>colonne correspondante de H</u>.

$\Rightarrow$ déduisez quelle comp est erronée.

$\Rightarrow$ et vous corrigez en retournant cette comp.

<u>Correction</u> : $\vec{x}' \longrightarrow \vec{x}' + \underline{\vec{e}} = \vec{x}$.

Avec Code de Hamming $(\underset{\substack{\uparrow \\ \text{longueur}}}{7}, \underset{\substack{\uparrow \\ \text{dim}}}{4})$ on corrige toujours 1 erreur.

en fait pour $\forall r \geq 3$.

2) Introduction au codage quantique.

$\uparrow$

aujourd'hui : codes de répétition.

Canal $\overbrace{\text{quantique}}^{\text{bruité}}$ ou modélisation du bruit ?

Bit-flip. $\alpha|0\rangle + \beta|1\rangle \rightarrow \boxed{\text{Bit flip}} \rightarrow \alpha|1\rangle + \beta|0\rangle$.

agit comme $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Phase flip.

$\alpha|0\rangle + \beta|1\rangle \rightarrow \boxed{\text{Phase flip}} \rightarrow \alpha|0\rangle - \beta|1\rangle$

agit comme $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

- Action de X et/ou Z est aléatoire

$(\alpha|0\rangle + \beta|1\rangle)$, $(\gamma|0\rangle + \delta|1\rangle)$, ...

survient avec prob $= p$. $0 < p < \frac{1}{2}$.

L'état quantique de sortie est aléatoire.

(Th de la "Matrice densité").

- Idée du code de répétition de longueur = 3.

$|0\rangle$ ⇝ encodé en $|0\rangle\otimes|0\rangle\otimes|0\rangle$
$= |000\rangle$

$|1\rangle$ ⇝ encodé en $|1\rangle\otimes|1\rangle\otimes|1\rangle$
$= |111\rangle$.

- en général pour transmettre $\alpha|0\rangle+\beta|1\rangle$ on fait l'encodage

$$\underbrace{\alpha|000\rangle+\beta|111\rangle}.$$ ← Bonne chose à faire

ce n'est plus un simple pr tensoriel.

⚠ pour α et β génériques état intriqué
pas un produit tensoriel.

- Pas de violation du "No-cloning Thm" car le code de répétition copie des qu-bits de la base computationnelle orthonormés. ⚠

Par contre on ne pourrait encoder
$\alpha|0\rangle+\beta|1\rangle$ comme $(\alpha|0\rangle+\beta|1\rangle)^{\otimes 3}$ $\forall\alpha,\beta$.
à cause du No-cloning.

- Bit d'information $|0\rangle$ ou $|1\rangle$ $\in \boxed{\mathbb{C}^2}$

oui non message classique. $\underbrace{\alpha|0\rangle + \beta|1\rangle}_{\text{messages quant.}}$.

- Mots de codes

$|000\rangle$; $|111\rangle$; $\alpha|000\rangle + \beta|111\rangle$.

Longueur = 3 .

vivent dans Hilbert $= (\mathbb{C}^2)^{\otimes 3}$.

en fait $\alpha|000\rangle + \beta|111\rangle$ sont dans un sous ensemble de $(\mathbb{C}^2)^{\otimes 3}$ qui est de dim 2 et avec base $\{|000\rangle, |111\rangle\}$.

dimension du code = 2.

- Imaginons la transmission du mot

$$\alpha|0\underline{0}0\rangle + \beta|1\underline{1}1\rangle.$$

et imaginons que l'on reçoive

$$\alpha|0\underline{1}0\rangle + \beta|1\underline{0}1\rangle.$$

Erreur bit-flip sur le second qubit.

Question correction d'erreur:

Mesure

a) Lire ou observer le mot reçu sans le détruire

b) Opération unitaire de correction.

Mesure : Mesurer les observables ou les matrices

$$Z_1 \otimes Z_2 \otimes \mathbb{1}. \quad \text{et} \quad \mathbb{1} \otimes Z_2 \otimes Z_3.$$

en d'autres termes on prend la base des vects propres de ces deux matrices pour faire la mesure.

#.

Remarque : $Z_1 \otimes Z_2 \otimes \mathbb{1}$ et $\mathbb{1} \otimes Z_2 \otimes Z_3$.

commutent ⇒ diag dans la m̂ base (base de mesure).

$$(Z_1 \otimes Z_2 \otimes \mathbb{1})\left(\alpha|010\rangle + \beta|101\rangle\right)$$

$$= -\alpha|010\rangle - \beta|101\rangle = (-1)\left(\alpha|010\rangle + \beta|101\rangle\right)$$

$$(\mathbb{1} \otimes Z_2 \otimes Z_3)\left(\alpha|010\rangle + \beta|101\rangle\right)$$

$$= -\left(\alpha|010\rangle + \beta|101\rangle\right).$$

- l'état vect propre de ces deux matrice avec v.p $(-1,-1)$
  ↪ aussi de la base de mesure.
  ↪ n'est pas détruit par la mesure.

- v.p $(-1,-1)$ joue le rôle de syndrome.

Autre exemple avec mot de code reçu :

$$\alpha|00\underline{1}\rangle + \beta|11\underline{0}\rangle .$$

$$(Z_1\otimes Z_2\otimes \mathbb{1})(\alpha|\underbrace{00}_{}1\rangle + \beta|\underbrace{11}_{}0\rangle) = (+1)(\alpha|001\rangle+\beta|110\rangle)$$

$$(\mathbb{1}\otimes Z_2\otimes Z_3)(\alpha|0\underset{\cdot}{0}\underset{\cdot}{1}\rangle + \beta|1\underset{\cdot}{1}\underset{\cdot}{0}\rangle) = (-1)(\alpha|001\rangle+\beta|110\rangle).$$

- A nouveau l'état n'est pas détruit par cette mesure
- v.p $(+1, -1)$ <u>syndrome</u>.

$\alpha|\underline{1}00\rangle + \beta|\underline{0}11\rangle$ ⇝ v.p $(-1, +1)$.

syndrome.

$\alpha|000\rangle + \beta|111\rangle$. ⇝ v.p $(+1, +1)$

aucune erreur

syndrome.

Resumé la situation :

Mot transmis : $\alpha|000\rangle + \beta|111\rangle$.

Mot reçus qui possèdent une erreur	syndrome par la mesure de $(Z_1\otimes Z_2\otimes \mathbb{1})$ et $(\mathbb{1}\otimes Z_2\otimes Z_3)$
$\alpha|000\rangle + \beta|111\rangle$ ✓	$(+1, +1)$ v.p.
$\alpha|100\rangle + \beta|011\rangle$ ✓	$(-1, +1)$ v.p.
$\alpha|010\rangle + \beta|101\rangle$	$(-1, -1)$ v.p
$\alpha|001\rangle + \beta|110\rangle$	$(+1, -1)$ v.p.

plus d'une erreur. Ne peut pas corriger

$\alpha|110\rangle + \beta|001\rangle$ v.p $(+1, -1)$

CORRECTION ERREUR UNIQUE AU MAX.

op unitaires

$\mathrm{Id}\otimes\mathrm{Id}\otimes\mathrm{Id}\left(\alpha|000\rangle + \beta|111\rangle\right)$. $\leftarrow$ $(+1, +1)$ pas erreur

$X_1\otimes\mathrm{Id}\otimes\mathrm{Id}\left(\alpha|100\rangle + \beta|011\rangle\right)$ $\leftarrow$ $(-1, +1)$ erreur sur 1er bit

$= \alpha|000\rangle + \beta|111\rangle$

$\mathrm{Id}\otimes X_2\otimes\mathrm{Id}$. $\leftarrow$ $(-1, -1)$ erreur sur 2ème bit

$\mathrm{Id}\otimes\mathrm{Id}\otimes X_3$. $\leftarrow$ $(+1, -1)$ erreur sur 3ème bit

Tout cela ne marche pas pour le canal phase flip.

$$\alpha|000\rangle + \beta|111\rangle \longrightarrow \alpha|000\rangle - \beta|111\rangle .$$

Néanmoins pour un canal phase flip chg de base qui nous ramène au cas précédent :

$|0\rangle \rightsquigarrow |{+}{+}{+}\rangle$ $\qquad |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ ✓

$|1\rangle \rightsquigarrow |{-}{-}{-}\rangle$ $\qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. ✓

Encodage :

$$\alpha|0\rangle + \beta|1\rangle \rightsquigarrow \alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle .$$

Mesures $\quad X_1 \otimes X_2 \otimes \mathbb{1} \quad ; \quad \mathbb{1} \otimes X_2 \otimes X_3 .$

Décodage en appliquant les **unitaires** c/

$\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1}$	pas d'erreur phaseflip
$Z_1 \otimes \mathbb{1} \otimes \mathbb{1}$	1 erreur sur 1 qubit.
$\cancel{Z} \otimes Z_2 \otimes \mathbb{1}$	" 2em qubit
$\mathbb{1} \otimes \mathbb{1} \otimes Z_3$	" 3èm qubit

// CODE DE SHOR COMBINE ENCODAGE // BIT FLIP + PHASE FLIP. //