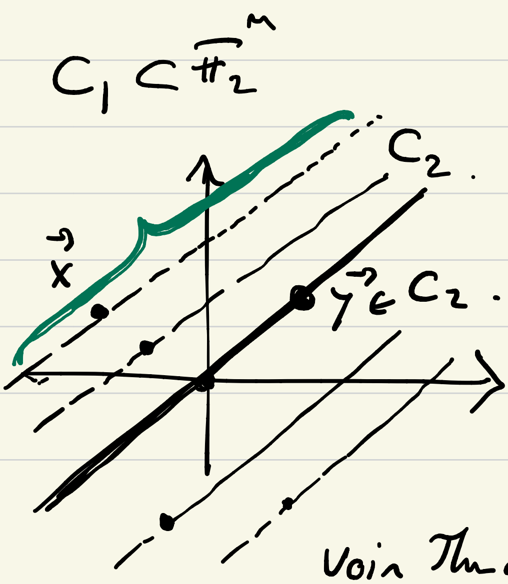
Codes de Calderbank - Steane et Shor.

- Codes quantique qui utilisent deux codes classiques C_1 et C_2 pour corriger bit flips et phase flip.

- <u>Hyp</u> :
  - C_1 et C_2 sous esp. de $\mathbb{F}_2^n$.
  - $\dim C_1 = k_1$ et $\dim C_2 = k_2$.
  - $k_2 \leq k_1$ et aussi $C_2 \subset C_1$.
  - $C_2^\perp$ et C_1 corrigent t erreurs de type classique (bit flips).

(rappel : s. esp vect $\perp C_2$. $\dim C_2^\perp = n - k_2$).

<u>Remarque</u> : $C_2 \subset C_1$ en fait C_2 est aussi un sous groupe de C_1 pour la loi $\oplus$ (addition mod 2).



classes d'équivalences C_1 / C_2.

$\vec{x} \in C_1 : \{ \vec{x} + \vec{y} \text{ avec } \vec{y} \in C_2 \}$.

$$\text{Card } |C_1/C_2| = \frac{|C_1|}{|C_2|} = \frac{2^{k_1}}{2^{k_2}} = 2^{k_1 - k_2}$$

Voir Thm de Lagrange.

Le code CSS exploite cette structure de groupe :

- Mots de code de CSS :

$\vec{x} \in C_1$: $\underbrace{|\vec{x}+C_2\rangle}_{\substack{\text{ket qui est une superposition de tous les kets} \\ \text{de la classe équivalence de } C_2}} \equiv \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y} \in C_2} |\vec{x}+\vec{y}\rangle.$

n qubits

$\in (\mathbb{C}^2)^{\otimes n}$

- Code CSS est en fait l'espace d'Hilbert construit en faisant des superpositions de tous les états de la forme $|\vec{x}+C_2\rangle$ ou $\vec{x} \in C_1/C_2$.

ces états sont $\perp$.

$$\langle \vec{x}'+C_2 | \vec{x}+C_2\rangle$$

$$= \frac{1}{|C_2|} \sum_{\substack{\vec{y} \in C_2 \\ \vec{y}' \in C_2}} \overbrace{\langle \vec{x}'+\vec{y}' | \vec{x}+\vec{y}\rangle}^{0.} = 0.$$

les deux classes d'équiv ne $\cap$ pas $\Rightarrow$ $\vec{x}'+\vec{y}'$ et $\vec{x}+\vec{y}$ ne sont pas $\perp$ ~~$\neq$~~

pr se vaut 0.

- $CSS(C_1, C_2)$; $\dim(CSS(C_1, C_2)) = \frac{|C_1|}{|C_2|} = 2^{k_1 - k_2}$.

$CSS(C_1, C_2)$ sous espace de $(\mathbb{C}^2)^{\otimes n}$.

* Code possède longueur n ; dim $2^{k_1 - k_2}$.

* On va voir qu'il corrige t erreurs si C_1 et $C_2^\perp$ corrigent t erreurs classique. → type bit-phase flip.

<u>Code de Shor</u> : longueur $n = 9$, dim 2. ($|0\rangle_S$ et $|1\rangle_S$.).

corrige 1 erreur.

*. Nous allons supposer que l'état est corrompu avec t erreurs de $\underbrace{\text{type bit}}_{\vec{e}_1}$ et phase $\underbrace{\text{flip}}_{\vec{e}_2}$.

$\vec{e}_1$: 1 si le bit i a un flip, 0 sinon

$\vec{e}_2$: 1 si le bit i phase flip, 0 sinon.

$\vec{x} + C_2$.

- $$|\psi\rangle_{\text{parfait}} = \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y} \in C_2} |\vec{x} + \vec{y}\rangle.$$

- $$|\psi\rangle'_{\text{corrompu}} = \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y} \in C_2} (-1)^{(\vec{x}+\vec{y})\cdot \vec{e}_2} |\vec{x}+\vec{y}+\vec{e}_1\rangle$$

* Pour corriger il faut détecter les bits et phase flip et nous allons stocker ces erreurs $\Longrightarrow$ Ajouter bits auxiliaires
<u>Ancilla Bits</u>.

$$\boxed{|\psi\rangle' \otimes |0_m\rangle \otimes |0_m\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y} \in C_2} (-1)^{(\vec{x}+\vec{y})\cdot\vec{e}_2} |\vec{x}+\vec{y}+\vec{e}_1\rangle \otimes |0_m\rangle \otimes |0\rangle_m}$$

Détection et la correction des bits flips.

- implémenter de façon unitaire la matrice de parité du code C_1. H_1. $\left| \begin{array}{l} H_1 \vec{x} = 0 \\ \text{si } \vec{x} \in C_1. \end{array}\right.$

$$U_1 \, |\underbrace{\vec{x} + \vec{y} + \vec{e}_1}_{\text{bits de controle.}}\rangle \otimes |0_m\rangle \otimes |0_m\rangle$$

$$\equiv |\vec{x}+\vec{y}+\vec{e}_1\rangle \otimes |\overbrace{H_1(\vec{x}+\vec{y}+\vec{e}_1)}^{H_1 \vec{e}_1 \cdot}\rangle \otimes |0_m\rangle$$

car $\vec{x}+\vec{y} \in C_1$

stockés du résultat de $H_1(\vec{x}+\vec{y}+\vec{e}_1)$.

$$\boxed{U_f \, |a\rangle \otimes |b\rangle = |a\rangle \otimes |b \oplus f(a)\rangle.}$$

on a vu cela souvent

(ici f est l'application linéaire H_1.).

- $U_1 |\psi\rangle \otimes |0\rangle_m \otimes |0\rangle_m$

$$= \left\{ \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y} \in C_2} (-1)^{(\vec{x}+\vec{y}) \cdot \vec{e}_2} \, |\vec{x}+\vec{y}+\vec{e}_1\rangle \right\} \otimes |\underbrace{H_1 \vec{e}_1}\rangle \otimes |0_m\rangle.$$

état de la base computationelle

Même que le différent.

→ Observés $|H_1 \vec{e}_1\rangle$. Connaissez $\underbrace{H_1 \vec{e}_1}_{\text{syndrome classique.}} = \vec{s}_1$

Si C_1 est capable de corriger t erreurs et que $\underbrace{|\vec{e}_1|}_{\text{poids de Hamming.}} \leq t$ ce veut dire que vous pouvez trouver un unique $\vec{e}_1$.

→ <u>Correction d'erreur</u> en <u>appliquant la matrice unitaire</u>

$$U_{1,\text{corr}} = \prod_{\substack{i \in \text{comp non} \\ \text{nulle de } \vec{e}_1}} X_i \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

$$U_{1,\text{corr}}\, U_1 |\psi\rangle' \otimes |0\rangle_m \otimes |0\rangle_m =$$

$$\frac{1}{\sqrt{|C_2|}} \sum_{\vec{y} \in C_2} \underline{\underline{(-1)^{(\vec{x}+\vec{y})\cdot\vec{e}_2}}} |\vec{x}+\vec{y}\rangle \otimes |H_1 \vec{e}\rangle \otimes |\underline{0}\rangle.$$

↳ encore phase flips à corriger

Détection et correction des phases flip :

étape préliminaire : chg de base, $H^{\otimes m}$.

$$H^{\otimes m} U_{1,corr} U_1 |\psi\rangle' \otimes |0\rangle_m \otimes |0\rangle_m$$

$$= \frac{1}{2^{m/2}} \frac{1}{\sqrt{|C_2|}} \sum_{\vec{z}} \sum_{\vec{y} \in C_2} (-1)^{\vec{z}\cdot(\vec{x}+\vec{y})} (-1)^{(\vec{x}+\vec{y})\cdot\vec{e}_2} |\vec{z}\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |0_m\rangle.$$

$$H |x_i + y_i\rangle = \frac{1}{\sqrt{2}} \sum_{z_i = 0,1} (-1)^{z_i(x_i+y_i)} |z_i\rangle.$$

$$\vec{z} \to \vec{z} + \vec{e}_2 \in \mathbb{F}_2^m.$$

$$= \frac{1}{2^{m/2}} \frac{1}{\sqrt{|C_2|}} \sum_{\vec{z}} \sum_{\vec{y} \in C_2} (-1)^{\vec{z}\cdot(\vec{x}+\vec{y})} |\vec{z} + \vec{e}_2\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |0_m\rangle.$$

$$(\vec{z} + \vec{e}_2)\cdot(\vec{x}+\vec{y}) + (\vec{x}+\vec{y})\cdot\vec{e}_2$$

$$= \vec{z}\cdot(\vec{x}+\vec{y}) \quad \text{mod } 2.$$

$$\sum_{\vec{y} \in C_2} (-1)^{\vec{z}\cdot\vec{y}} = \begin{cases} |C_2| \checkmark & \vec{z} \in C_2^{\perp} \\ 0. & \vec{z} \notin C_2^{\perp} \end{cases}$$

L'état obtenu est :

$$\frac{1}{\underbrace{\sqrt{|C_2^{\perp}|}}} \sum_{\vec{z} \in C_2^{\perp}} (-1)^{\vec{z}\cdot\vec{x}} \, |\underline{\vec{z}+\vec{e}_2}\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |0_m\rangle.$$

$$\left(\frac{1}{2^{m/2}} \frac{|C_2| \checkmark}{\sqrt{|C_2|}} = \frac{1}{2^{\frac{m-k_2}{2}}} = \frac{1}{\sqrt{|C_2^{\perp}|}}. \right)$$ parenthèse de calcul.

- Maintenant nous sommes prêts à détecter l'erreur $\vec{e}_2$ comme avant $\boxed{U_2}$ qui implémente $H_2^{\perp}$ qui est la matrice de parité de $C_2^{\perp}$.

$$\frac{1}{\sqrt{|C_2^{\perp}|}} \sum_{\vec{z} \in C_2^{\perp}} (-1)^{\vec{z}\cdot\vec{x}} \, |\vec{z}+\vec{e}_2\rangle \otimes |H_1 \vec{e}_1\rangle \otimes \underbrace{|H_2^{\perp}(\vec{z}+\vec{e}_2)\rangle}_{|H_2^{\perp}\vec{e}_2\rangle}.$$

Mesurer $\underbrace{|H_2^\perp \vec{e}_2\rangle}_{\text{ds la base computationelle}}$ et connaître $H_2^\perp \vec{e}_2 = \vec{S}_2$.

Si $C_2^\perp$ corrige t erreurs et que $|\vec{e}_2| \leq t$.
alors vous connaissez $\vec{e}_2$.

<u>Correction d'erreur en appliquant l'unitaire</u>

$$U_{2,corr} = \prod_{\substack{i \in \text{comp} \\ \text{non nulle de} \\ \vec{e}_2}} X_i$$

Finalement vous obtenez l'état

$$\boxed{\begin{aligned} & U_{2,corr}\, U_2\, H^{\otimes n}\, U_{1,corr}\, U_1\, |\psi\rangle \otimes |0_n\rangle \otimes |0_n\rangle \\ &= \frac{1}{\sqrt{|C_2^\perp|}} \sum_{\vec{z} \in C_2^\perp} (-1)^{\vec{z}\cdot\vec{x}}\, |\vec{z}\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp \vec{e}_2\rangle \end{aligned}}$$

$$\boxed{H^{\otimes n} |\vec{z}\rangle.}$$

Finalement revenons ds le base originale

$$H^{\otimes n}\, U_{2,corr}\, U_2\, H^{\otimes n}\, U_{1,corr}\, U_1\, |\psi\rangle \otimes |0\rangle_m \otimes |0\rangle_m .$$

$$H^{\otimes n} |\vec{z}\rangle = \sum_{\vec{y} \in \mathbb{F}_2^n} (-1)^{\vec{z}\cdot\vec{y}} |\vec{y}\rangle .$$

$$\left(H|z_i\rangle = \frac{1}{\sqrt{2}} \sum (-1)^{z_i y_i} |y_i\rangle \right)$$

$$\left(\sum_{\vec{z} \in C_2^{\perp}} (-1)^{\vec{z}\cdot\vec{y}} \right) = \begin{cases} |C_2^{\perp}| & \vec{y} \in (C_2^{\perp})^{\perp} = C_2 \\ 0 & \vec{y} \notin C_2 . \end{cases}$$

En mettant tout cela ensemble :

$$H^{\otimes n} U_{2,corr} U_2 H^{\otimes n} U_{1,corr} U_1 |\psi\rangle' \otimes |0_m\rangle \otimes |0_m\rangle$$

$$\underset{\substack{\uparrow \\ \text{après} \\ \text{calcul.}}}{=} \underbrace{\left(\frac{1}{\sqrt{|C_2|}} \sum_{\vec{y} \in C_2} |\vec{x} + \vec{y}\rangle \right)} \otimes |\underline{H_1 \vec{e}_1}\rangle \otimes |\underline{H_2 \vec{e}_2}\rangle.$$

état parfait non corrompu. $\underline{|\psi\rangle_{parfait}}$.

QED correction des t erreurs est possible avec le code $CSS(C_1, C_2)$. $\blacksquare$

<u>Conclure</u> : Tout ce procédé de correction + détection peut être implémenté avec un circuit quantique.

$\blacksquare$