GRENOBLE INP UGA Ensimag

École nationale supérieure d'informatique et de mathématiques appliquées

Introduction à l'Informatique Quantique

Information quantique :

Correction d'erreur quantique

Cryptographie quantique

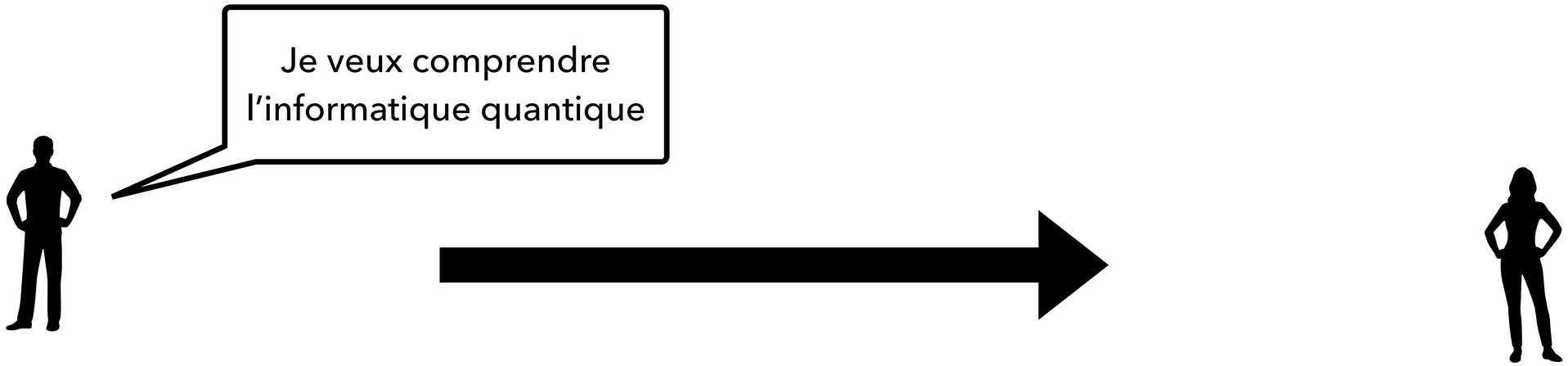
Corrélations quantiques

Mehdi Mhalla

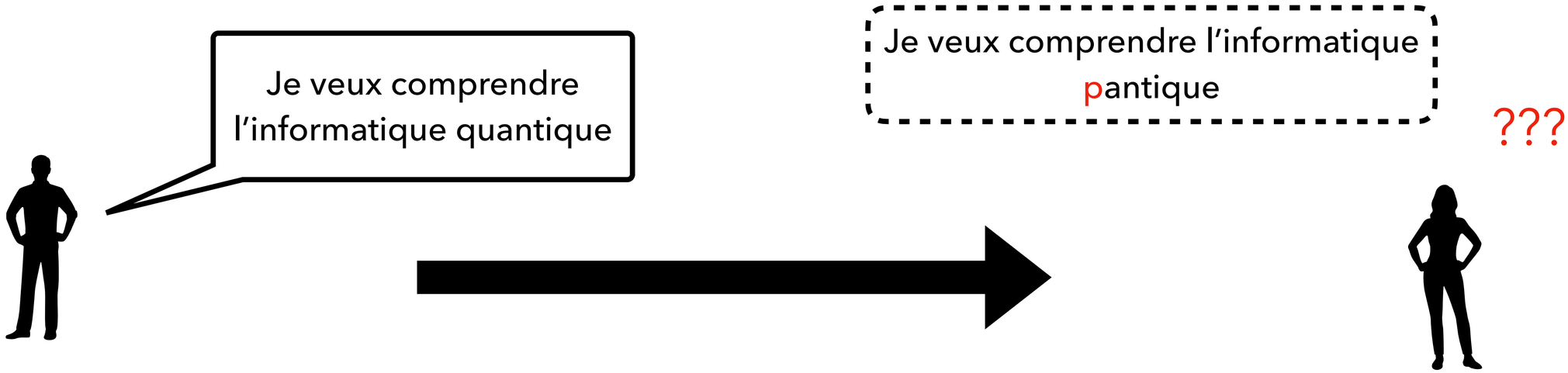
CNRS -UGA - LIG - CAPP

26 octobre, 2022

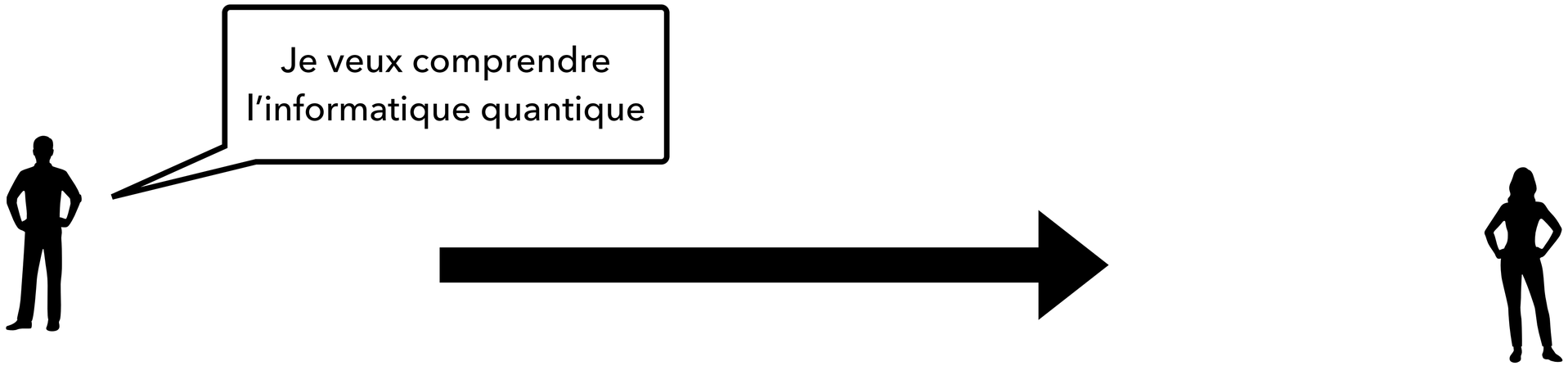
Codes correcteurs d’erreur



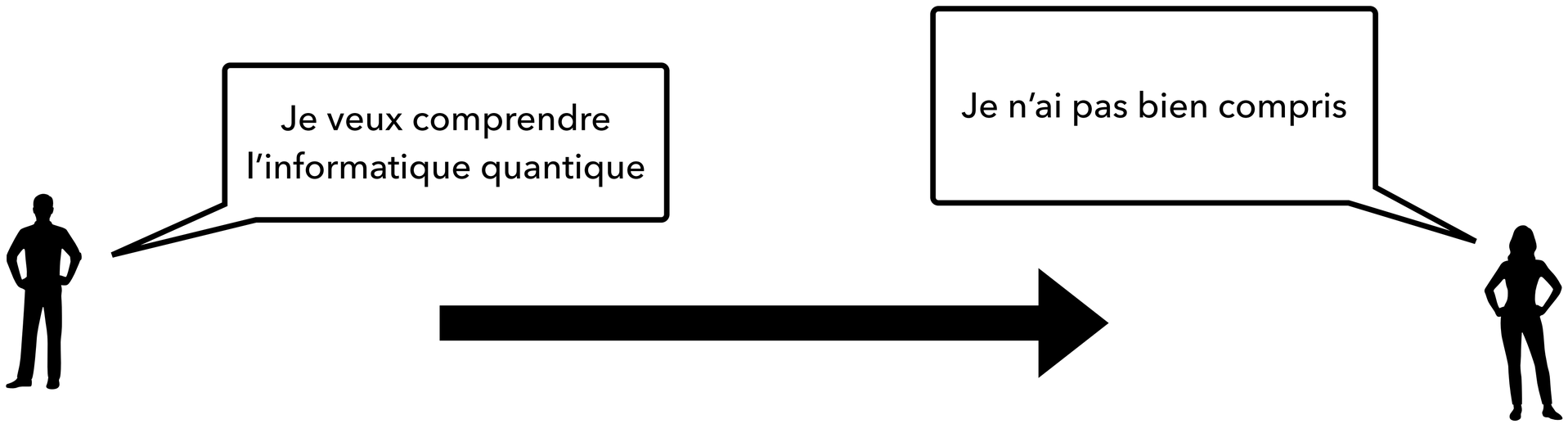
Codes correcteurs d’erreur



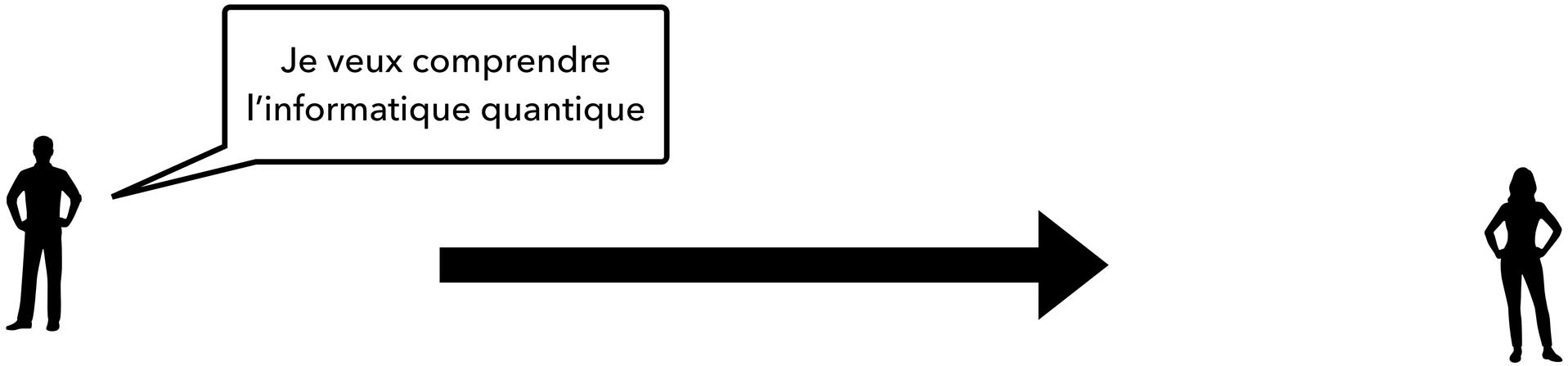
Codes correcteurs d’erreur



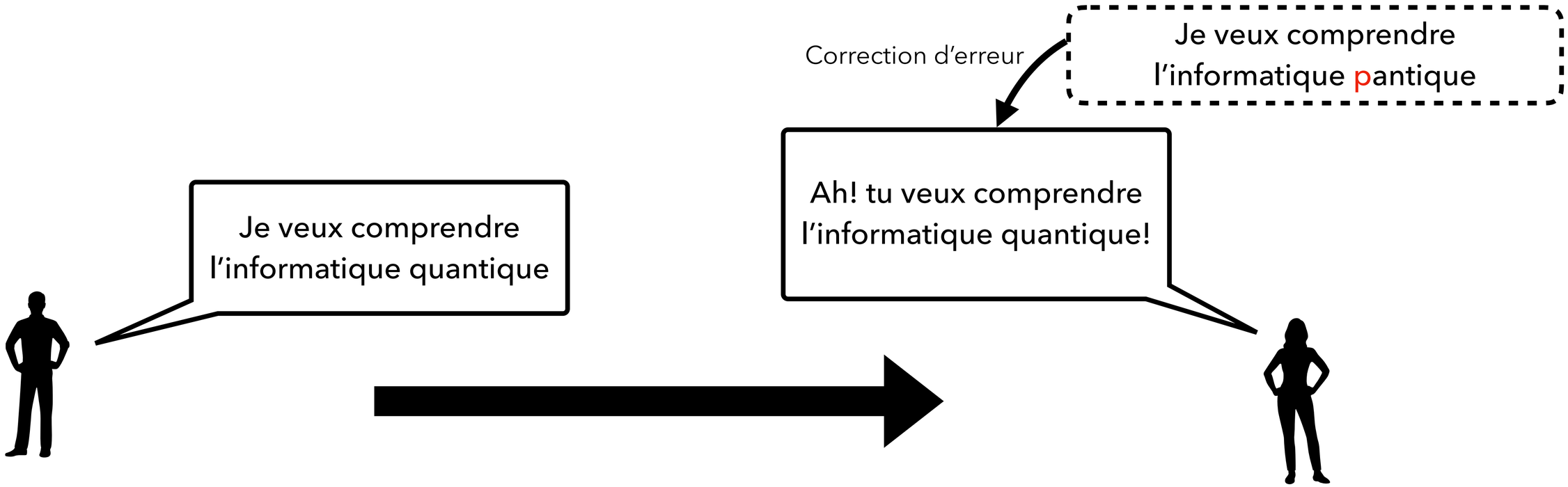
Codes correcteurs d’erreur



Codes correcteurs d’erreur

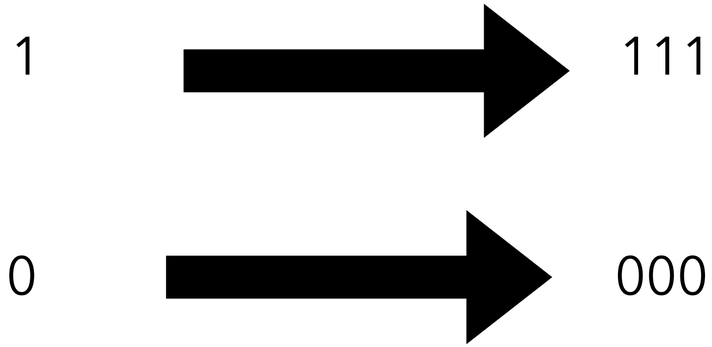


Codes correcteurs d'erreur

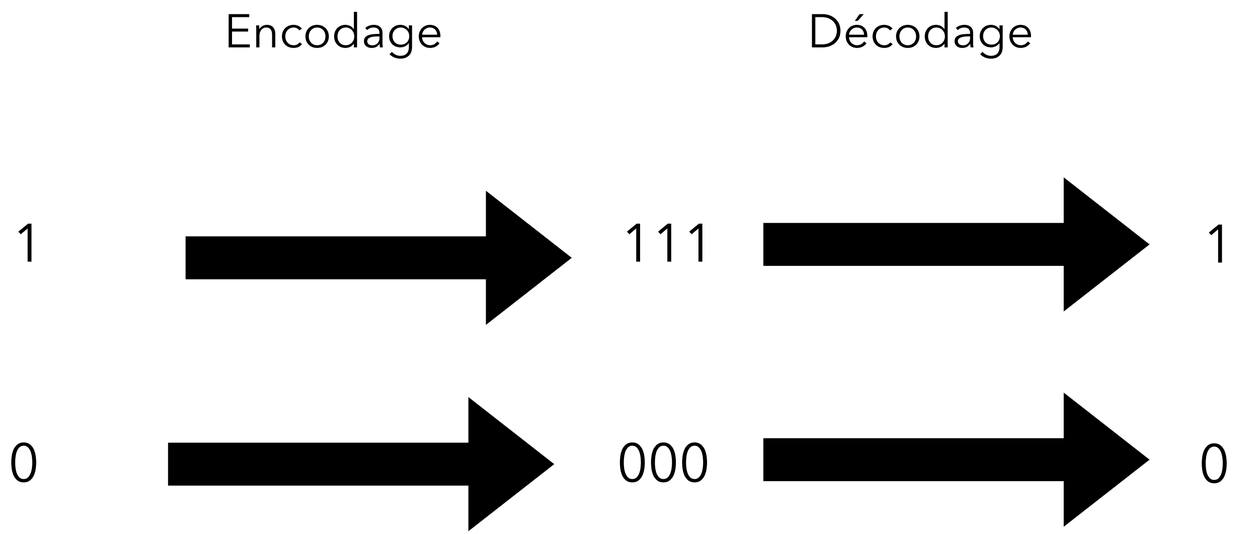


Code de Répétition

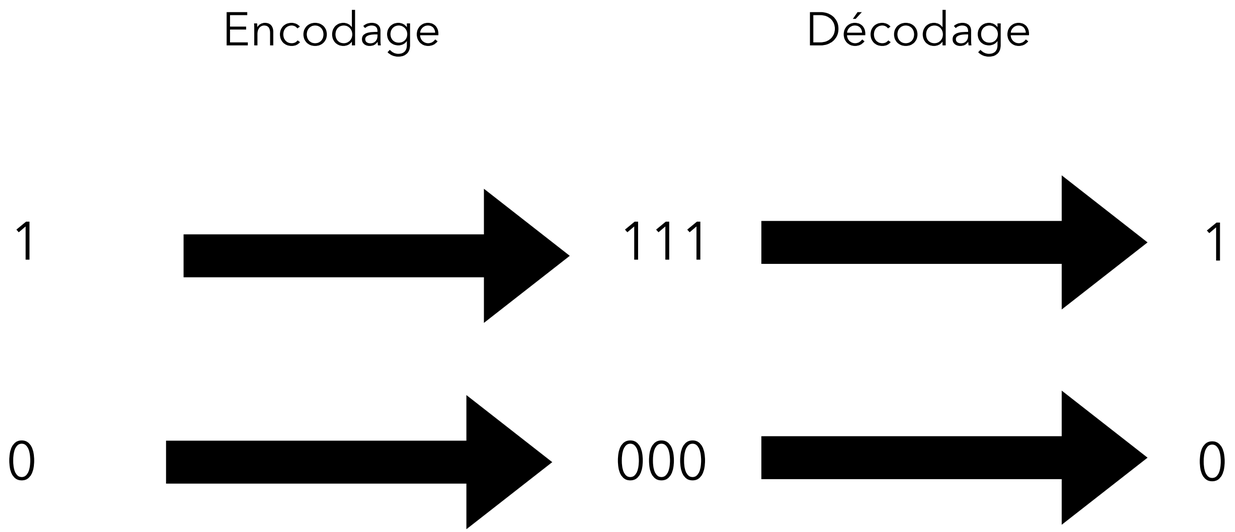
Encodage

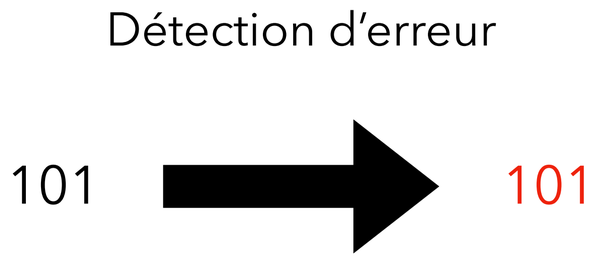


Code de Répétition



Code de Répétition



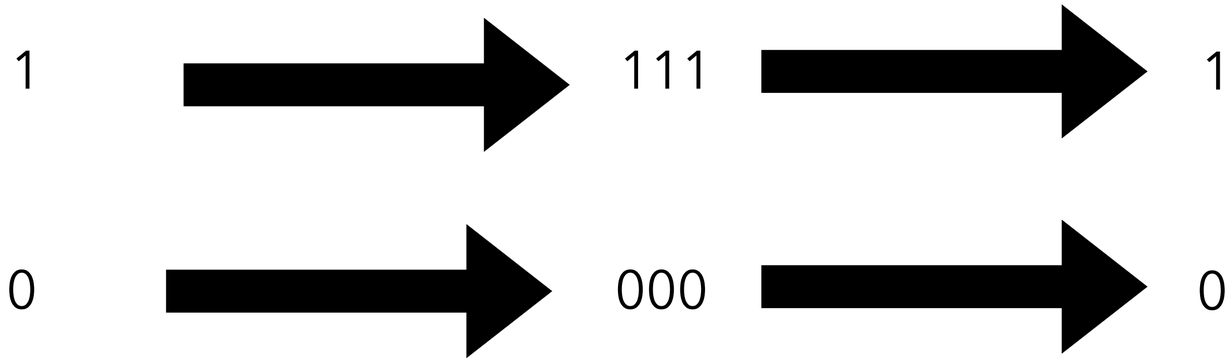


Code de Répétition

Encodage

Décodage

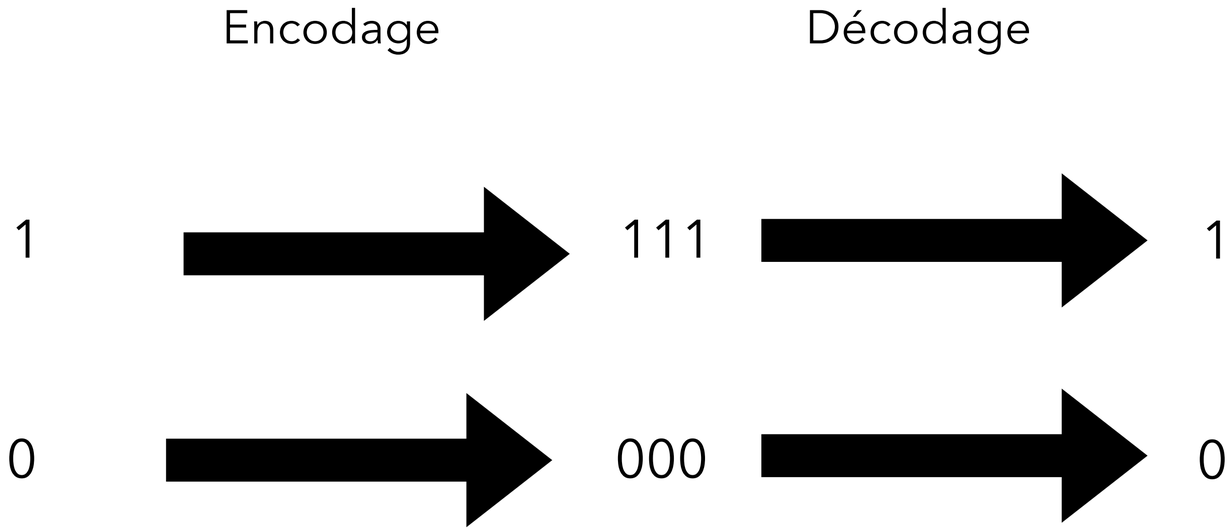
Détection d'erreur

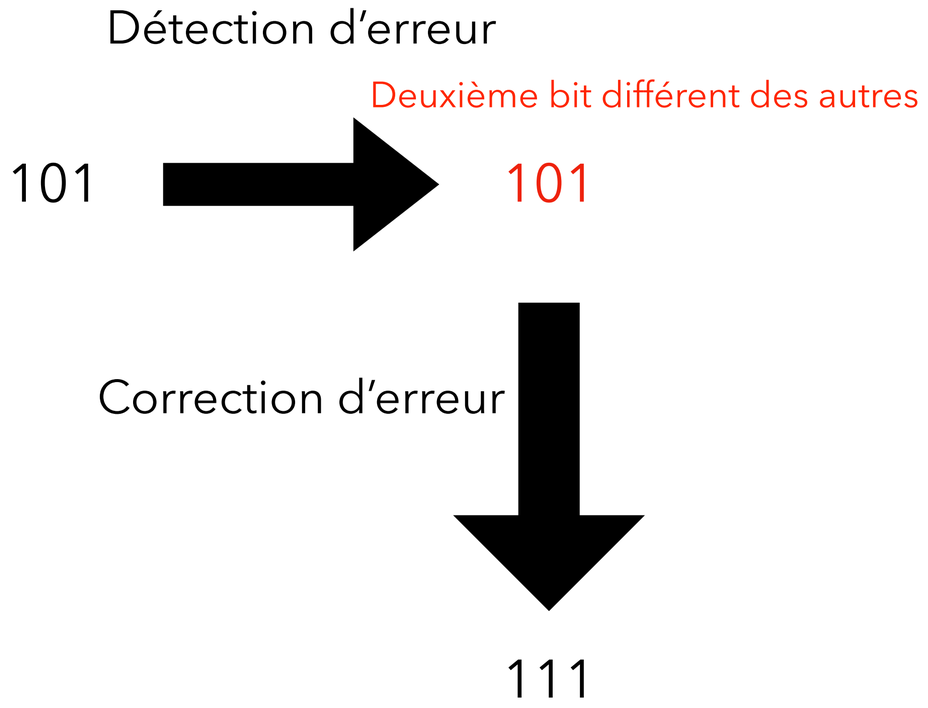


Deuxième bit différent des autres

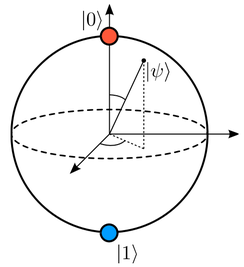
101 → 101

Code de Répétition





Codes Quantiques ?



- Erreurs continues:
  - Un état quantique pour un bit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in \mathbb{C}^2 \qquad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- No-cloning :
  - On ne peut pas copier un état quantique

Rappel : Systèmes de qubits

Système de deux qubits: produit tensoriel

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \text{ et } |\phi\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \text{ alors } |\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$$

Rappel : Systèmes de qubits

Système de deux qubits: produit tensoriel

$$|\psi\rangle = \begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix} \text{ et } |\phi\rangle = \begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix} \text{ alors } |\psi\rangle \otimes |\phi\rangle = \begin{pmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{pmatrix}$$

$$|\psi\rangle_{q_1} = \alpha_0|0\rangle_{q_1} + \alpha_1|1\rangle_{q_1} \qquad |\phi\rangle_{q_2} = \beta_0|0\rangle_{q_2} + \beta_1|1\rangle_{q_2}$$

$$|\psi\rangle_{q_1} \otimes |\phi\rangle_{q_2} = \alpha_0\beta_0|00\rangle_{q_1,q_2} + \alpha_0\beta_1|01\rangle_{q_1,q_2} + \alpha_1\beta_0|10\rangle_{q_1,q_2} + \alpha_1\beta_1|11\rangle_{q_1,q_2}$$

Rappel : Systèmes de qubits

Système de deux qubits: produit tensoriel

$|\psi\rangle = \begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix}$ et $|\phi\rangle = \begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix}$ alors $|\psi\rangle \otimes |\phi\rangle = \begin{pmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{pmatrix}$

$$|\psi\rangle_{q_1} = \alpha_0|0\rangle_{q_1} + \alpha_1|1\rangle_{q_1} \qquad |\phi\rangle_{q_2} = \beta_0|0\rangle_{q_2} + \beta_1|1\rangle_{q_2}$$

$$|\psi\rangle_{q_1} \otimes |\phi\rangle_{q_2} = \alpha_0\beta_0|00\rangle_{q_1,q_2} + \alpha_0\beta_1|01\rangle_{q_1,q_2} + \alpha_1\beta_0|10\rangle_{q_1,q_2} + \alpha_1\beta_1|11\rangle_{q_1,q_2}$$

$$\text{pour } x_1 \dots x_n \in \{0,1\}^n \text{ on note} \qquad |x_1 \dots x_n\rangle_{q_1,\dots q_n} = |x_1\rangle_{q_1} \otimes \dots \otimes |x_n\rangle_{q_n}$$

$$|\psi\rangle = \sum_{x_1 \dots x_n \in \{0,1\}^n} \alpha_{x_1\dots,x_n}|x_1 \dots x_n\rangle, \text{ with } \sum_{x_1 \dots x_n \in \{0,1\}^n} |\alpha_{x_1\dots,x_n}|^2 = 1$$

Rappel : Systèmes de qubits

Système de deux qubits: produit tensoriel

$$|\psi\rangle = \begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix} \text{ et } |\phi\rangle = \begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix} \text{ alors } |\psi\rangle \otimes |\phi\rangle = \begin{pmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{pmatrix}$$

$$|\psi\rangle_{q_1} = \alpha_0|0\rangle_{q_1} + \alpha_1|1\rangle_{q_1} \qquad |\phi\rangle_{q_2} = \beta_0|0\rangle_{q_2} + \beta_1|1\rangle_{q_2}$$

$$|\psi\rangle_{q_1} \otimes |\phi\rangle_{q_2} = \alpha_0\beta_0|00\rangle_{q_1,q_2} + \alpha_0\beta_1|01\rangle_{q_1,q_2} + \alpha_1\beta_0|10\rangle_{q_1,q_2} + \alpha_1\beta_1|11\rangle_{q_1,q_2}$$

$$\text{pour } x_1 \dots x_n \in \{0,1\}^n \text{ on note} \qquad |x_1 \dots x_n\rangle_{q_1,\dots q_n} = |x_1\rangle_{q_1} \otimes \dots \otimes |x_n\rangle_{q_n}$$

$$|\psi\rangle = \sum_{x_1 \dots x_n \in \{0,1\}^n} \alpha_{x_1\dots,x_n}|x_1 \dots x_n\rangle, \text{ with } \sum_{x_1 \dots x_n \in \{0,1\}^n} |\alpha_{x_1\dots,x_n}|^2 = 1$$

Intrication : en général ce n'est pas un produit

Corriger des bit flips

X

$$|0\rangle \mapsto |1\rangle$$

$$|1\rangle \mapsto |0\rangle$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$$

Corriger des bit flips

$$|0_L\rangle = |0\rangle_{q_1} \otimes |0\rangle_{q_2} \otimes |0\rangle_{q_3} = |000\rangle$$

X

$$|0\rangle \mapsto |1\rangle$$

$$|1\rangle \mapsto |0\rangle$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$$

Corriger des bit flips

$$|0_L\rangle = |0\rangle_{q_1} \otimes |0\rangle_{q_2} \otimes |0\rangle_{q_3} = |000\rangle$$

$$|1_L\rangle = |111\rangle$$

X

$$|0\rangle \mapsto |1\rangle$$

$$|1\rangle \mapsto |0\rangle$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$$

Corriger des bit flips

$$|0_L\rangle = |0\rangle_{q_1} \otimes |0\rangle_{q_2} \otimes |0\rangle_{q_3} = |000\rangle$$

$$|1_L\rangle = |111\rangle$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow |\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle$$

X

$$|0\rangle \mapsto |1\rangle$$

$$|1\rangle \mapsto |0\rangle$$

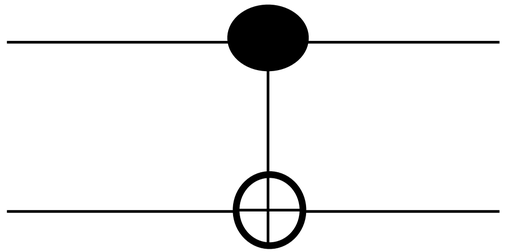
$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$$

Corriger des bit flips

$$|0_L\rangle = |0\rangle_{q_1} \otimes |0\rangle_{q_2} \otimes |0\rangle_{q_3} = |000\rangle$$

$$|1_L\rangle = |111\rangle$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow |\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle$$



CNot

X

$$|0\rangle \mapsto |1\rangle$$

$$|1\rangle \mapsto |0\rangle$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$$

$$|00\rangle \mapsto |00\rangle$$

$$|01\rangle \mapsto |01\rangle$$

$$|10\rangle \mapsto |11\rangle$$

$$|11\rangle \mapsto |10\rangle$$

Corriger des bit flips

$$|0_L\rangle = |0\rangle_{q_1} \otimes |0\rangle_{q_2} \otimes |0\rangle_{q_3} = |000\rangle$$

$$|1_L\rangle = |111\rangle$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow |\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle$$

X

$$|0\rangle \mapsto |1\rangle$$

$$|1\rangle \mapsto |0\rangle$$

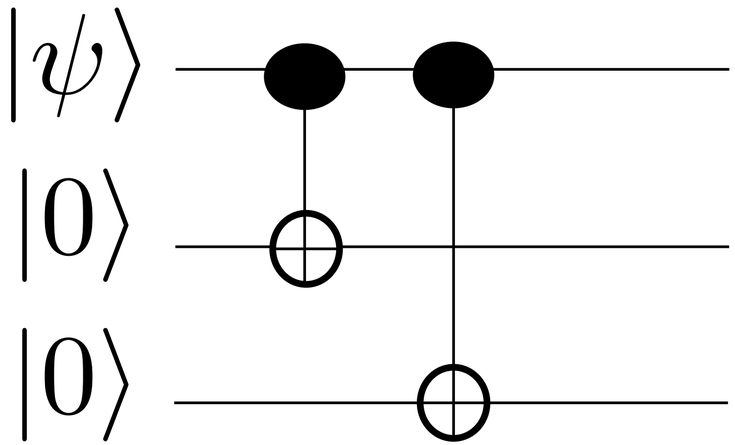
$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$$

Corriger des bit flips

$$|0_L\rangle = |0\rangle_{q_1} \otimes |0\rangle_{q_2} \otimes |0\rangle_{q_3} = |000\rangle$$

$$|1_L\rangle = |111\rangle$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow |\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle$$



X

$$|0\rangle \mapsto |1\rangle$$

$$|1\rangle \mapsto |0\rangle$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$$

Corriger des bit flips

$$|0_L\rangle = |0\rangle_{q_1} \otimes |0\rangle_{q_2} \otimes |0\rangle_{q_3} = |000\rangle$$

$$|1_L\rangle = |111\rangle$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow |\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle$$

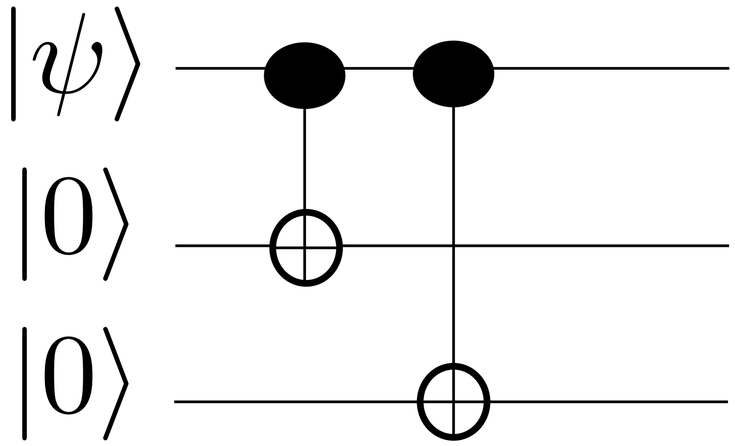
X

$$|0\rangle \mapsto |1\rangle$$

$$|1\rangle \mapsto |0\rangle$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$$

$$|\psi_0\rangle = |\psi\rangle|0\rangle|0\rangle = \alpha_0|0\rangle|0\rangle|0\rangle + \alpha_1|1\rangle|0\rangle|0\rangle$$



Corriger des bit flips

$$|0_L\rangle = |0\rangle_{q_1} \otimes |0\rangle_{q_2} \otimes |0\rangle_{q_3} = |000\rangle$$

$$|1_L\rangle = |111\rangle$$

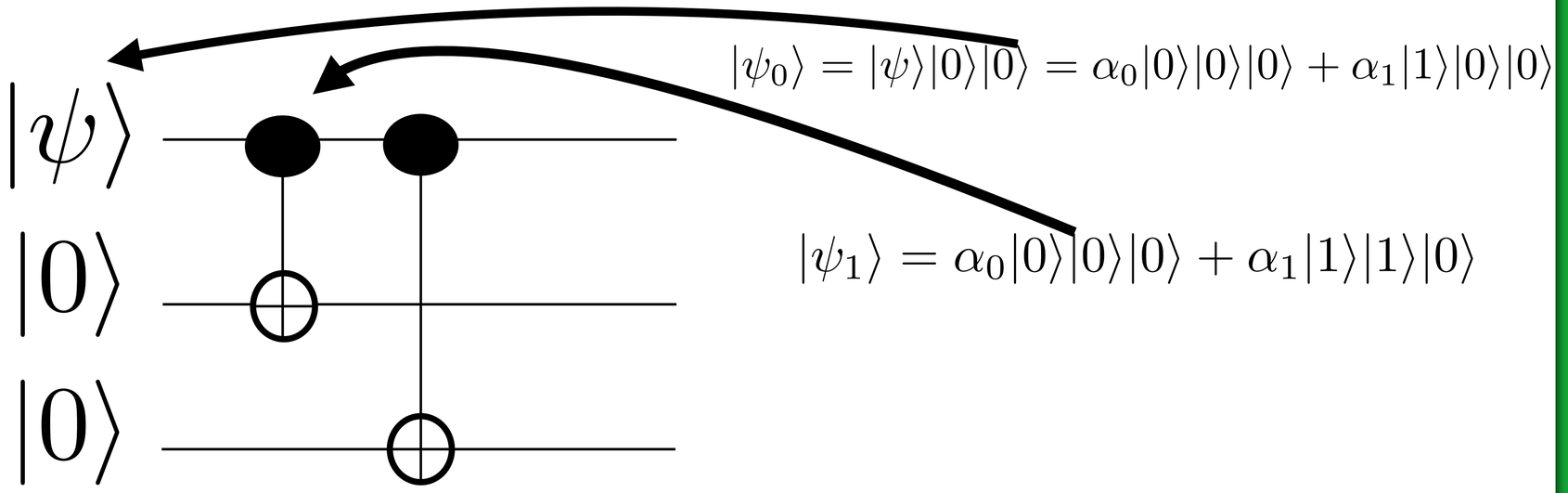
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow |\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle$$

X

$$|0\rangle \mapsto |1\rangle$$

$$|1\rangle \mapsto |0\rangle$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$$



Corriger des bit flips

$$|0_L\rangle = |0\rangle_{q_1} \otimes |0\rangle_{q_2} \otimes |0\rangle_{q_3} = |000\rangle$$

$$|1_L\rangle = |111\rangle$$

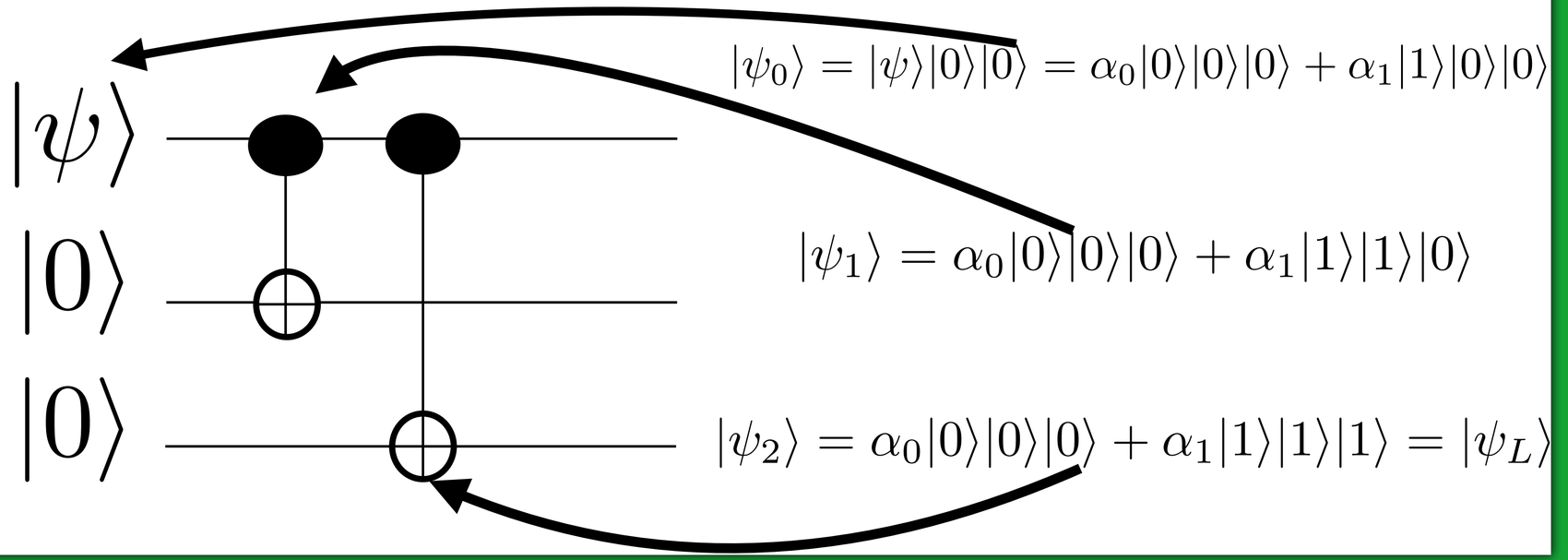
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow |\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle$$

X

$$|0\rangle \mapsto |1\rangle$$

$$|1\rangle \mapsto |0\rangle$$

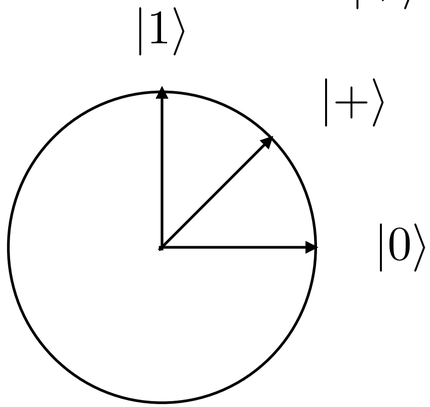
$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$$



Rappel : Mesure Quantique

- De nature probabiliste
- Change l'état du système : elle le **projette** sur les états qu'on peut observer
- Donne un bit classique

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



$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

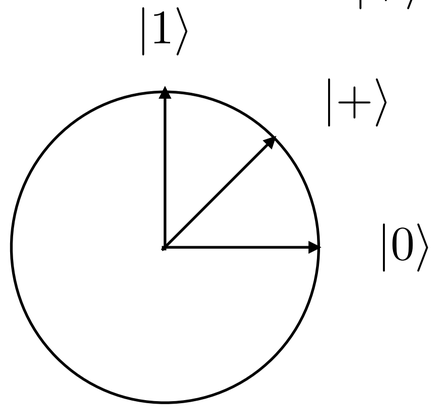
avec probabilité $|\alpha|^2$ le résultat classique est 0
l'état devient $|0\rangle$

avec probabilité $|\beta|^2$ le résultat classique est 1
l'état devient $|1\rangle$

Rappel : Mesure Quantique

- De nature probabiliste
- Change l'état du système : elle le **projette** sur les états qu'on peut observer
- Donne un bit classique

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



$$\{P_0 = |0\rangle\langle 0|,\ P_1 = |1\rangle\langle 1|\}$$

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

avec probabilité $|\alpha|^2$ le résultat classique est 0
l'état devient $|0\rangle$

avec probabilité $|\beta|^2$ le résultat classique est 1
l'état devient $|1\rangle$

Mesures Projectives

Matrices dans un espace de Hilbert (complexe)

$\{P_0, \ldots P_m\}$ Projecteurs Orthogonaux $P_i P_j = \delta_{i,j} P_i$

Couvrent l'espace $\sum P_i = Id$

Résultat classique $c \in \{0, \ldots m\}$ avec probabilité $p(c = i) = ||P_i|\psi\rangle||$

L'état du système après la mesure le résultat classique est i $\frac{P_i|\psi\rangle}{||P_i|\psi\rangle||}$

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$|\phi\rangle = \sum_{i,j,k\in\{0,1\}} \alpha_{ijk}|ijk\rangle$$

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$|\phi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk} |ijk\rangle$$

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$|\phi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk} |ijk\rangle$$

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$|\phi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk} |ijk\rangle$$

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$|\phi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk} |ijk\rangle$$

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

$$P_0 + P_1 + P_2 + P_3 = Id$$

Mesure projective

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

Quand on mesure

$$|\phi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk} |ijk\rangle$$

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

$$P_0 + P_1 + P_2 + P_3 = Id$$

Mesure projective

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

Quand on mesure

$$|\phi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk} |ijk\rangle$$

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

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

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

$$P_0 + P_1 + P_2 + P_3 = Id$$

Mesure projective

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

Quand on mesure

$$|\phi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk} |ijk\rangle$$

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$|\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle \qquad p(c=0) = 1$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

$$P_0 + P_1 + P_2 + P_3 = Id$$

Mesure projective

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

Quand on mesure

$$|\phi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk} |ijk\rangle$$

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$|\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle \qquad p(c=0) = 1$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$|\tilde{\psi}\rangle = \alpha|010\rangle + \beta|101\rangle$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

$$P_0 + P_1 + P_2 + P_3 = Id$$

Mesure projective

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$|\phi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk} |ijk\rangle$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

$$P_0 + P_1 + P_2 + P_3 = Id$$

Mesure projective

Quand on mesure

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

$$|\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle \qquad p(c=0) = 1$$

$$|\tilde{\psi}\rangle = \alpha|010\rangle + \beta|101\rangle \qquad p(c=2) = 1$$

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$|\phi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk} |ijk\rangle$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

$$P_0 + P_1 + P_2 + P_3 = Id$$

Mesure projective

Quand on mesure

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

$$|\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle \qquad p(c=0) = 1$$

$$|\tilde{\psi}\rangle = \alpha|010\rangle + \beta|101\rangle \qquad p(c=2) = 1$$

L'état du système ne change pas après la mesure !!!!!!!

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$|\phi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk}|ijk\rangle$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

$$P_0 + P_1 + P_2 + P_3 = Id$$

Mesure projective

Quand on mesure

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

$$|\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle \qquad p(c=0) = 1$$

$$|\tilde{\psi}\rangle = \alpha|010\rangle + \beta|101\rangle \qquad p(c=2) = 1$$

L'état du système ne change pas après la mesure !!!!!!!

La correction est possible avec *X* sur le deuxième qubit

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$|\phi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk}|ijk\rangle$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

$$P_0 + P_1 + P_2 + P_3 = Id$$

Mesure projective

Quand on mesure

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

$$|\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle \qquad p(c=0) = 1$$

$$|\tilde{\psi}\rangle = \alpha|010\rangle + \beta|101\rangle \qquad p(c=2) = 1$$

L'état du système ne change pas après la mesure !!!!!!!

La correction est possible avec *X* sur le deuxième qubit

$$X_2|\tilde{\psi}\rangle = I \otimes X \otimes I|\tilde{\psi}\rangle = |\psi_L\rangle$$

Bit flip : X

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$|\phi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk}|ijk\rangle$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

$$P_0 + P_1 + P_2 + P_3 = Id$$

Mesure projective

Quand on mesure

$$P_0|\phi\rangle = \alpha_{000}|000\rangle + \alpha_{111}|111\rangle$$

Le qubit 2 est différent des autres

$$|\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle \qquad p(c=0) = 1$$

$$|\tilde{\psi}\rangle = \alpha|010\rangle + \beta|101\rangle \qquad p(c=2) = 1$$

L'état du système ne change pas après la mesure !!!!!!!

La correction est possible avec *X* sur le deuxième qubit

$$X_2|\tilde{\psi}\rangle = I \otimes X \otimes I|\tilde{\psi}\rangle = |\psi_L\rangle$$

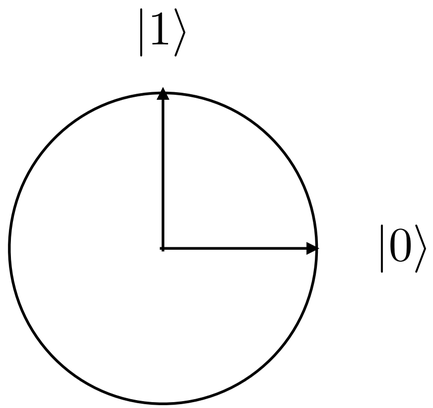
Phase flip: Z

Z

$$|0\rangle \mapsto |0\rangle$$

$$|1\rangle \mapsto -|1\rangle$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_0|0\rangle - \alpha_1|1\rangle$$



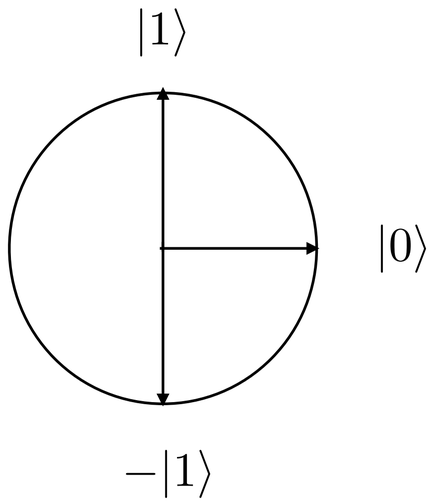
Phase flip: Z

Z

$$|0\rangle \mapsto |0\rangle$$

$$|1\rangle \mapsto -|1\rangle$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_0|0\rangle - \alpha_1|1\rangle$$



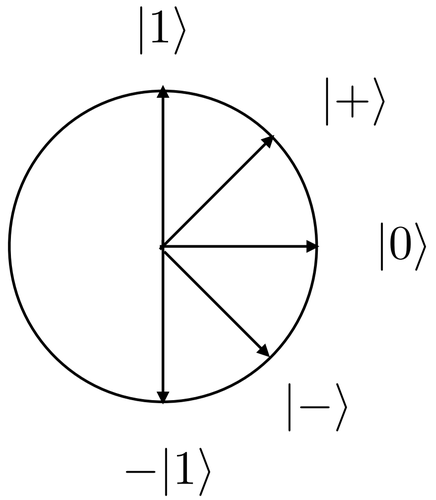
Phase flip: Z

Z

$$|0\rangle \mapsto |0\rangle$$

$$|1\rangle \mapsto -|1\rangle$$

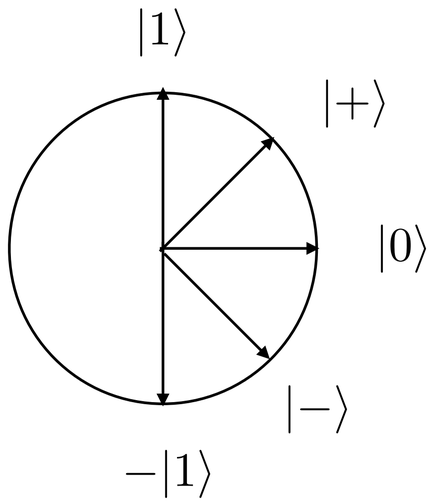
$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_0|0\rangle - \alpha_1|1\rangle$$



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

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Phase flip: Z



Z

$$|0\rangle \mapsto |0\rangle$$

$$|1\rangle \mapsto -|1\rangle$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_0|0\rangle - \alpha_1|1\rangle$$

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

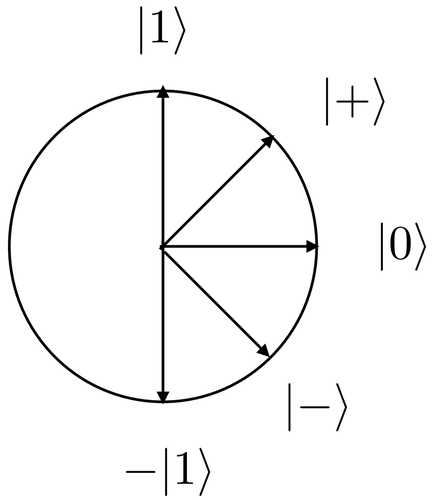
$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$Z|+\rangle = |-\rangle$$

$$Z|-\rangle = |+\rangle$$

Phase flip: Z

Changement de base



Z

$$|0\rangle \mapsto |0\rangle$$

$$|1\rangle \mapsto -|1\rangle$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_0|0\rangle - \alpha_1|1\rangle$$

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

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$Z|+\rangle = |-\rangle$$

$$Z|-\rangle = |+\rangle$$

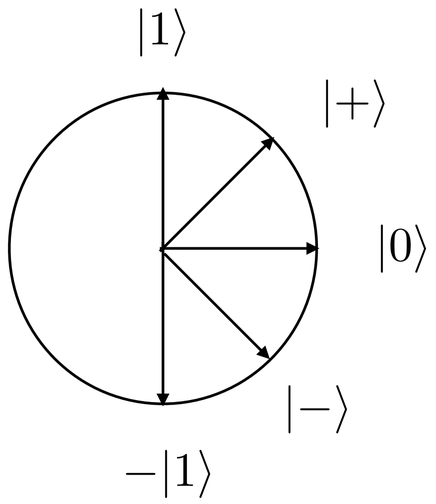
Phase flip: Z

Changement de base

Hadamard

$$H|0\rangle = |+\rangle$$

$$H|1\rangle = |-\rangle$$



Z

$$|0\rangle \mapsto |0\rangle$$

$$|1\rangle \mapsto -|1\rangle$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_0|0\rangle - \alpha_1|1\rangle$$

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

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$Z|+\rangle = |-\rangle$$

$$Z|-\rangle = |+\rangle$$

Corriger les flips de phase

$$|0_L\rangle = |+++\rangle$$

$$|1_L\rangle = |---\rangle$$

$$P'_0 = |+++\rangle\langle+++| + |---\rangle\langle---|$$

$$P'_1 = |-++\rangle\langle-++| + |+--\rangle\langle+--|$$

$$P'_2 = |+-+\rangle\langle+-+| + |-+-\rangle\langle-+-|$$

$$P'_3 = |++-\rangle\langle++-| + |--+\rangle\langle--+|$$

Corriger les flips de phase

$$|0_L\rangle = |+++\rangle$$

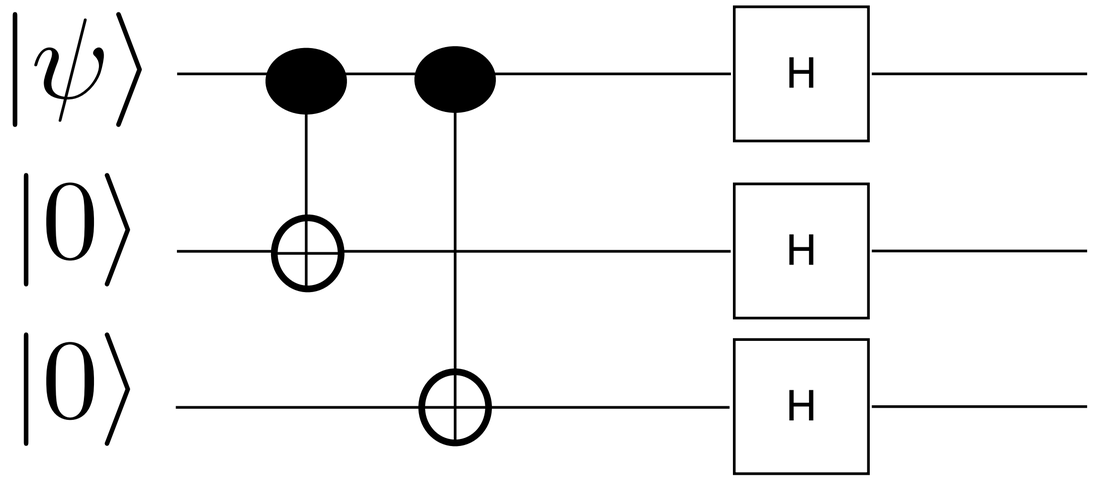
$$|1_L\rangle = |---\rangle$$

$$P'_0 = |+++\rangle\langle+++| + |---\rangle\langle---|$$

$$P'_1 = |-++\rangle\langle-++| + |+--\rangle\langle+--|$$

$$P'_2 = |+-+\rangle\langle+-+| + |-+-\rangle\langle-+-|$$

$$P'_3 = |++-\rangle\langle++-| + |--+\rangle\langle--+|$$

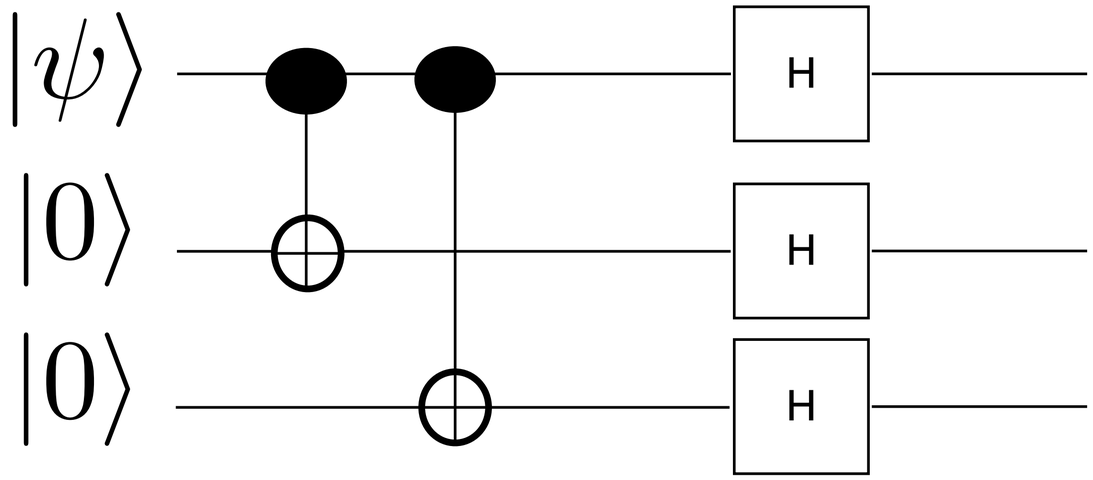


Corriger les flips de phase

$$|0_L\rangle = |+++\rangle$$

$$|1_L\rangle = |---\rangle$$

$$P'_0 = |+++\rangle\langle+++| + |---\rangle\langle---|$$
$$P'_1 = |-++\rangle\langle-++| + |+--\rangle\langle+--|$$
$$P'_2 = |+-+\rangle\langle+-+| + |-+-\rangle\langle-+-|$$
$$P'_3 = |++-\rangle\langle++-| + |--+\rangle\langle--+|$$



La correction est possible avec
Z sur le qubit correspondant

Mesures sur 2 qubits

$$|\phi\rangle = \sum_{i,j,k\in\{0,1\}} \alpha_{ijk}|ijk\rangle$$

$P_0 = |00\rangle\langle 00| + |11\rangle\langle 11|$

Les qubits 1 and 2 sont les mêmes dans la base standard

$P_1 = |01\rangle\langle 01| + |10\rangle\langle 10|$

Les qubits 1 and 2 sont différents dans la base standard

$$\alpha_{00}|00\rangle|\phi_0\rangle + \alpha_{01}|01\rangle|\phi_1\rangle + \alpha_{10}|10\rangle|\phi_2\rangle + \alpha_{11}|11\rangle|\phi_3\rangle$$

$$\frac{1}{|\alpha_{00}|^2 + |\alpha_{11}|^2}\left(\alpha_{00}|00\rangle|\phi_0\rangle + \alpha_{11}|11\rangle|\phi_3\rangle\right)$$

Avec probabilité $|\alpha_{00}|^2 + |\alpha_{11}|^2$

$$\frac{1}{|\alpha_{01}|^2 + |\alpha_{10}|^2}\left(\alpha_{01}|01\rangle|\phi_1\rangle + \alpha_{10}|10\rangle|\phi_2\rangle\right)$$

Avec probabilité $|\alpha_{01}|^2 + |\alpha_{10}|^2$

Mesures sur 2 qubits

$$|\phi\rangle = \sum_{i,j,k\in\{0,1\}} \alpha_{ijk}|ijk\rangle$$

$P_0 = |00\rangle\langle 00| + |11\rangle\langle 11|$

Les qubits 1 and 2 sont les mêmes dans la base standard

$P_1 = |01\rangle\langle 01| + |10\rangle\langle 10|$

Les qubits 1 and 2 sont différents dans la base standard

$\alpha_{00}|00\rangle|\phi_0\rangle + \alpha_{01}|01\rangle|\phi_1\rangle + \alpha_{10}|10\rangle|\phi_2\rangle + \alpha_{11}|11\rangle|\phi_3\rangle$

$$\frac{1}{|\alpha_{00}|^2 + |\alpha_{11}|^2}\left(\alpha_{00}|00\rangle|\phi_0\rangle + \alpha_{11}|11\rangle|\phi_3\rangle\right)$$

Avec probabilité $|\alpha_{00}|^2 + |\alpha_{11}|^2$

$$\frac{1}{|\alpha_{01}|^2 + |\alpha_{10}|^2}\left(\alpha_{01}|01\rangle|\phi_1\rangle + \alpha_{10}|10\rangle|\phi_2\rangle\right)$$

Avec probabilité $|\alpha_{01}|^2 + |\alpha_{10}|^2$

Si $|\alpha_{00}|^2 + |\alpha_{11}|^2 \in \{0, 1\}$ la mesure ne change pas l'état

Erreurs générales

- Les matrices de **Pauli:** $\{I, X, Y = iXZ, Z\}$ forment une base pour les matrices 2x2

$$E = e_0 I + e_1 X + e_2 Z + e_3 XZ$$

- Si la mesure de détection projette un état sur

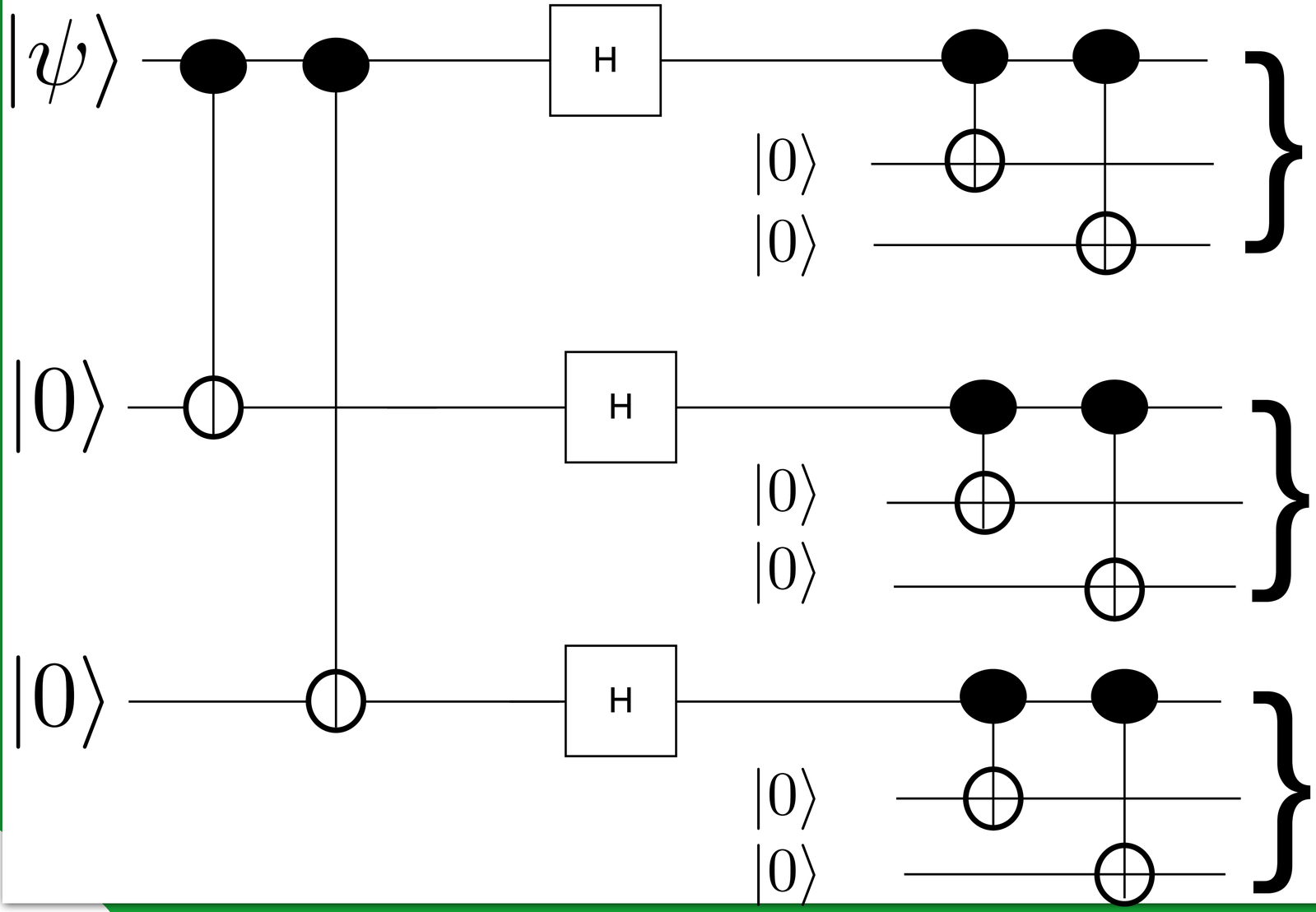
$$|\psi\rangle \text{ ou } X|\psi\rangle \text{ ou } Z|\psi\rangle \quad \text{ou} \quad XZ|\psi\rangle$$

- On a seulement besoin de corriger ces erreurs

Shor code

Encodage pour les phases

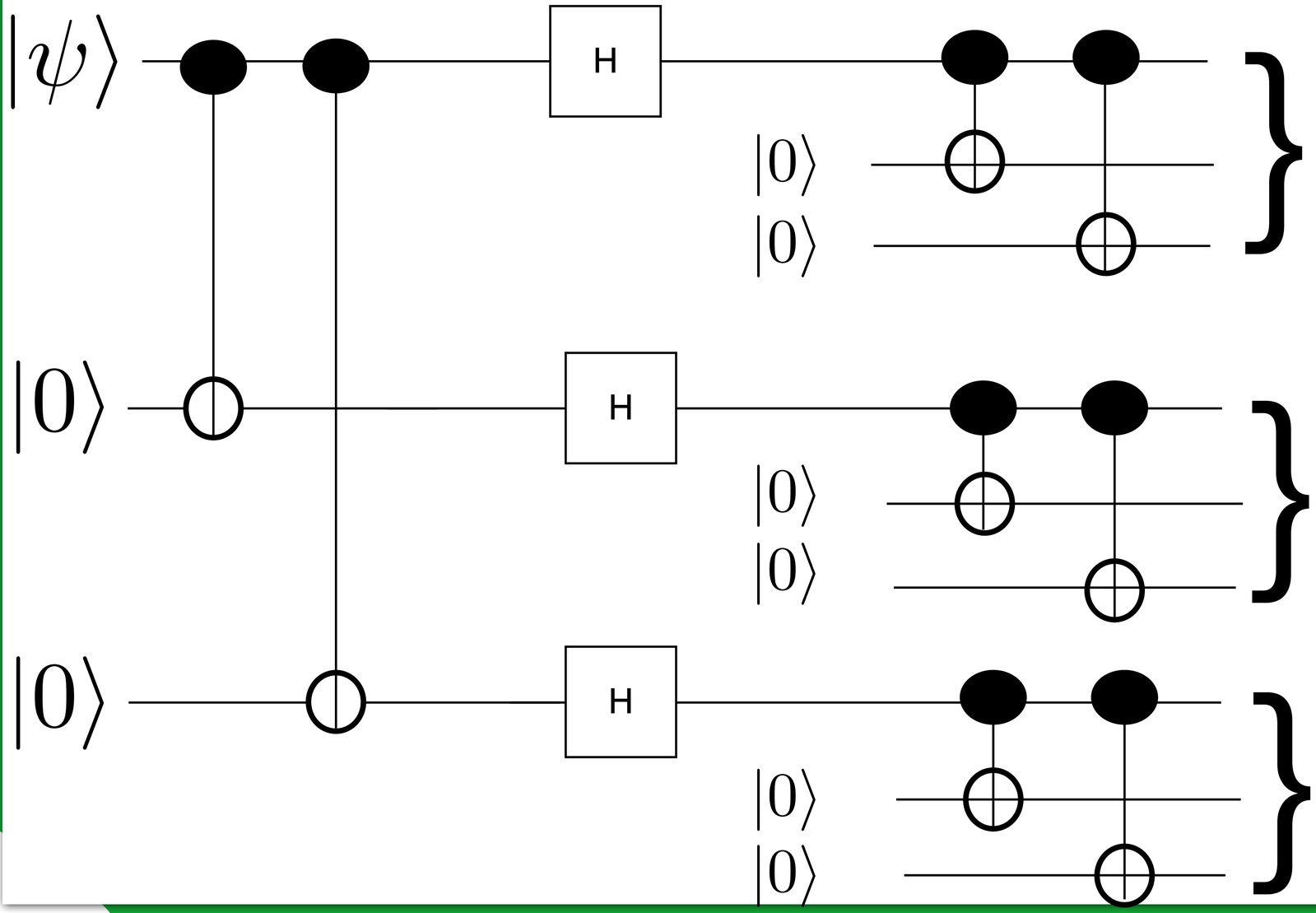
Encodage pour les amplitudes



Shor code

Encodage pour les phases

Encodage pour les amplitudes



$$|e_+\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

$$|e_-\rangle = \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

$$|0_L\rangle = \frac{|e_+\rangle|e_+\rangle|e_+\rangle + |e_-\rangle|e_-\rangle|e_-\rangle}{\sqrt{2}}$$

$$|1_L\rangle = \frac{|e_+\rangle|e_+\rangle|e_+\rangle - |e_-\rangle|e_-\rangle|e_-\rangle}{\sqrt{2}}$$

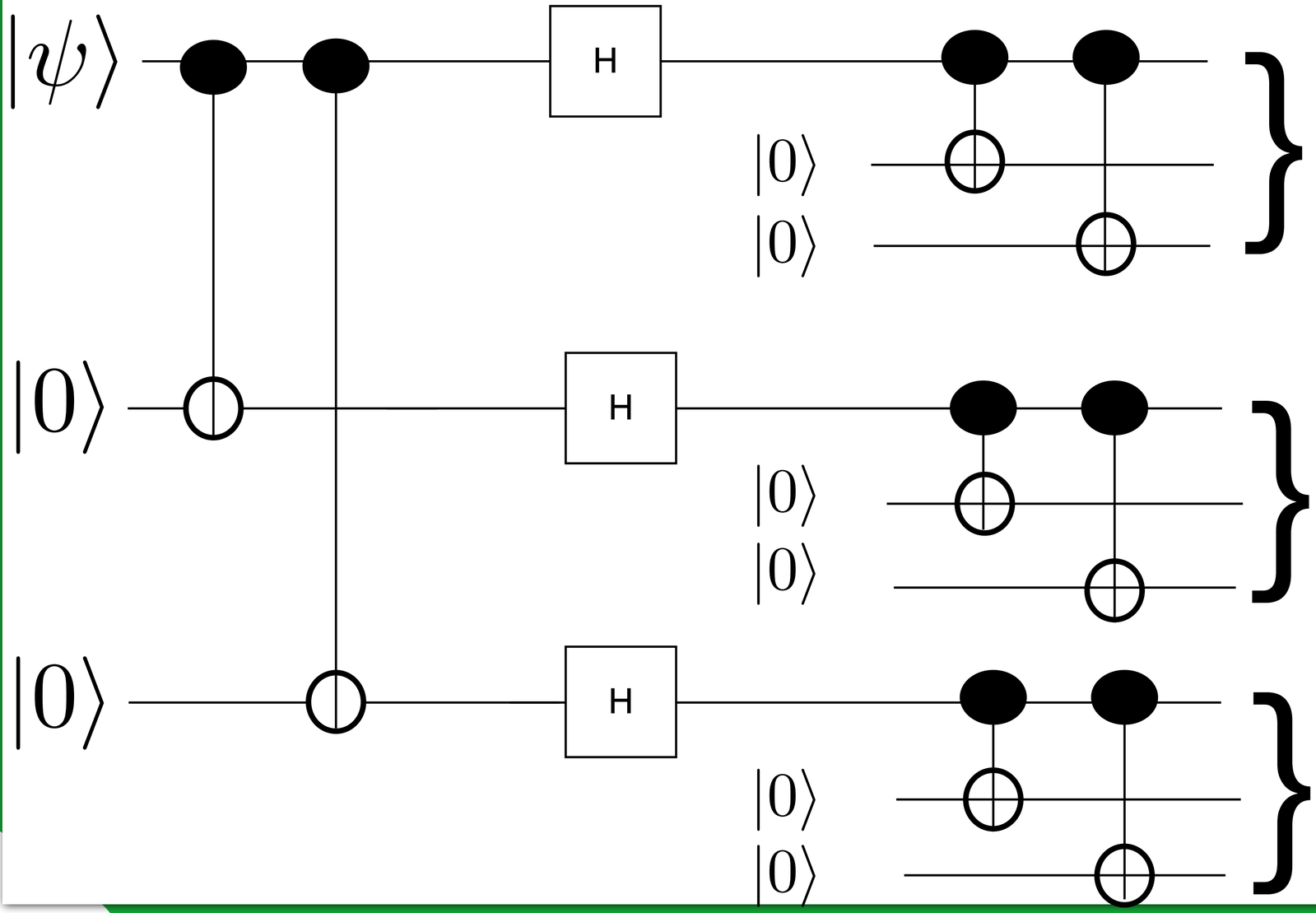
$$X_2|e_+\rangle = \frac{|010\rangle + |101\rangle}{\sqrt{2}}$$

Les bit flips peuvent être détectés dans chaque bloc

Shor code

Encodage pour les phases

Encodage pour les amplitudes



$$|e_+\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

$$|e_-\rangle = \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

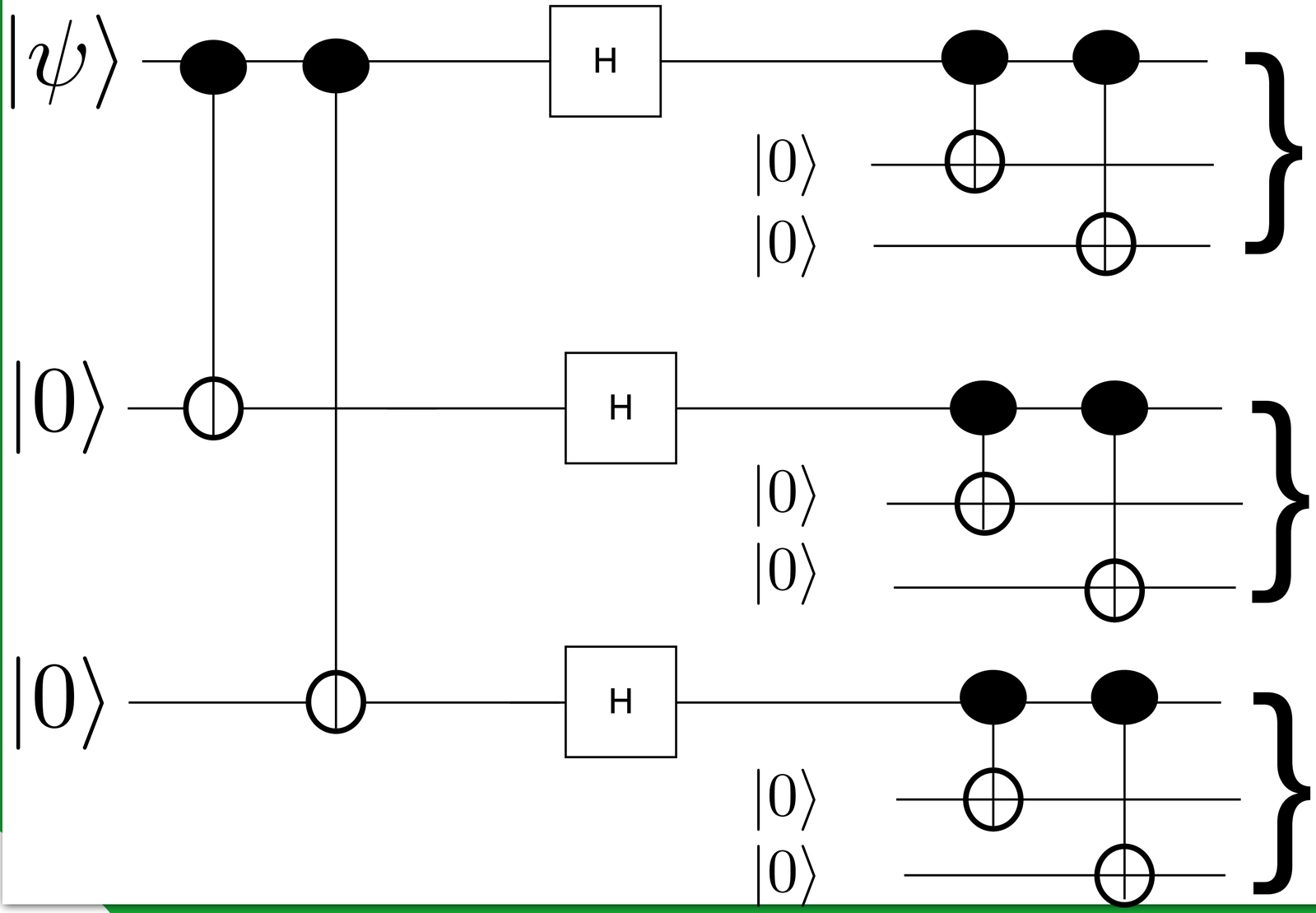
$$|0_L\rangle = \frac{|e_+\rangle|e_+\rangle|e_+\rangle + |e_-\rangle|e_-\rangle|e_-\rangle}{\sqrt{2}}$$

$$|1_L\rangle = \frac{|e_+\rangle|e_+\rangle|e_+\rangle - |e_-\rangle|e_-\rangle|e_-\rangle}{\sqrt{2}}$$

Shor code

Encodage pour les phases

Encodage pour les amplitudes



$$|e_+\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

$$|e_-\rangle = \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

$$|0_L\rangle = \frac{|e_+\rangle|e_+\rangle|e_+\rangle + |e_-\rangle|e_-\rangle|e_-\rangle}{\sqrt{2}}$$

$$|1_L\rangle = \frac{|e_+\rangle|e_+\rangle|e_+\rangle - |e_-\rangle|e_-\rangle|e_-\rangle}{\sqrt{2}}$$

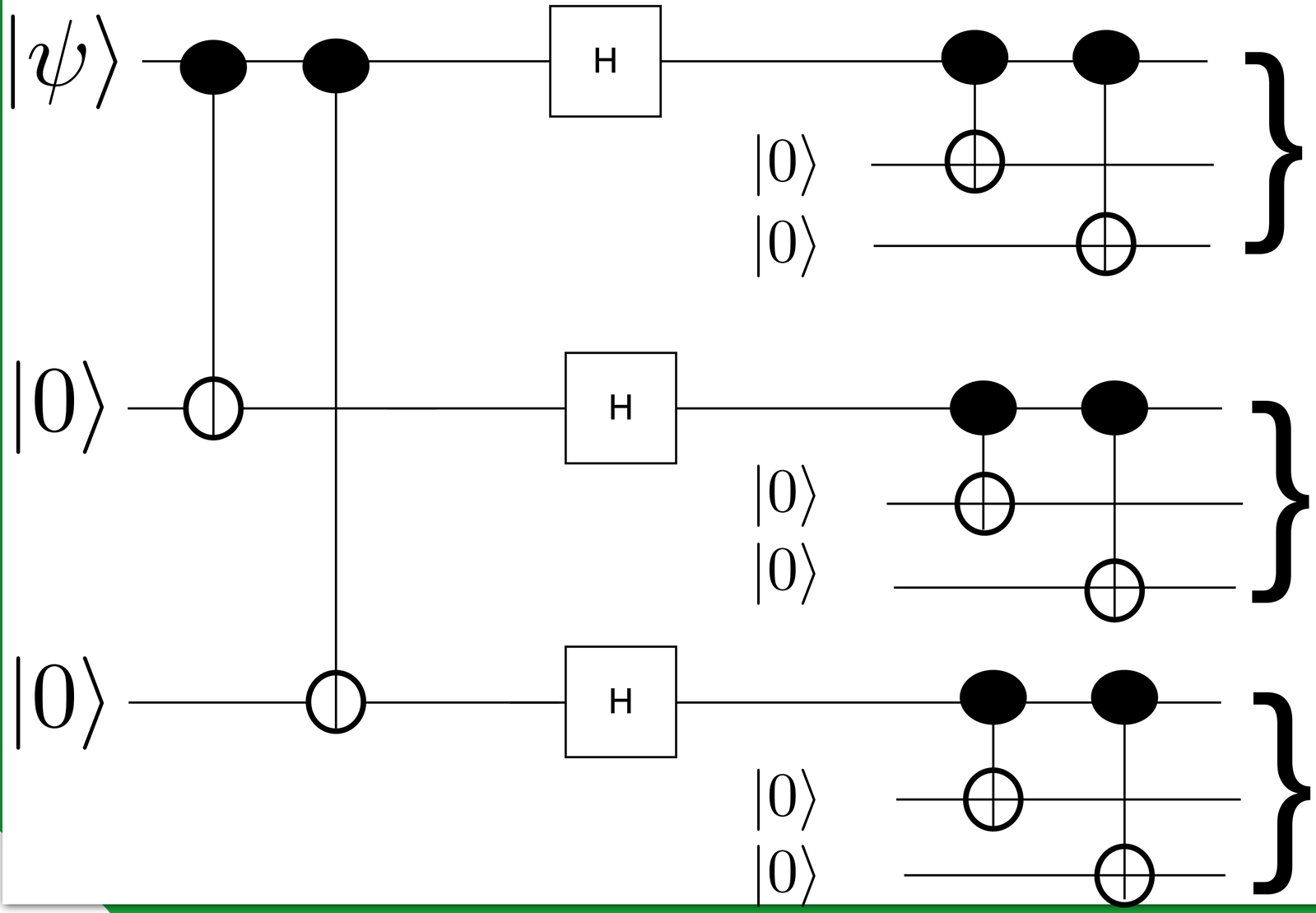
$$Z_i|e_+\rangle = |e_-\rangle$$

Les phase flip peuvent être détectés en comparant les blocs et corrigés en agissant sur un des qubits

Shor code

Encodage pour les phases

Encodage pour les amplitudes



$$|e_+\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

$$|e_-\rangle = \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

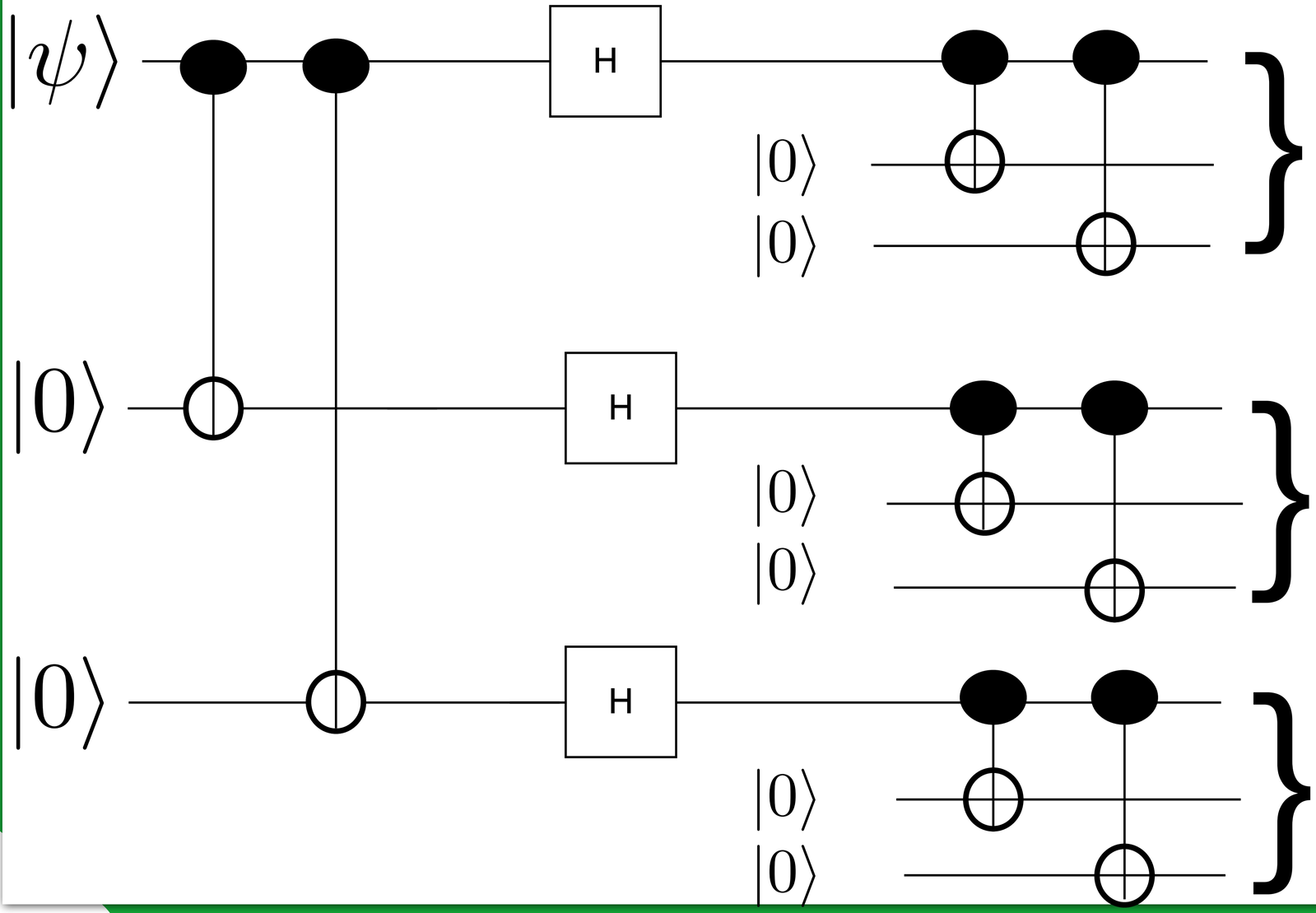
$$|0_L\rangle = \frac{|e_+\rangle|e_+\rangle|e_+\rangle + |e_-\rangle|e_-\rangle|e_-\rangle}{\sqrt{2}}$$

$$|1_L\rangle = \frac{|e_+\rangle|e_+\rangle|e_+\rangle - |e_-\rangle|e_-\rangle|e_-\rangle}{\sqrt{2}}$$

Shor code

Encodage pour les phases

Encodage pour les amplitudes



$$|e_+\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

$$|e_-\rangle = \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

$$|0_L\rangle = \frac{|e_+\rangle|e_+\rangle|e_+\rangle + |e_-\rangle|e_-\rangle|e_-\rangle}{\sqrt{2}}$$

$$|1_L\rangle = \frac{|e_+\rangle|e_+\rangle|e_+\rangle - |e_-\rangle|e_-\rangle|e_-\rangle}{\sqrt{2}}$$

$$X_2 Z_2 |e_+\rangle = \frac{|010\rangle - |101\rangle}{\sqrt{2}}$$

Les bits flips peuvent être corrigés en agissant sur le qubit correspondant Indépendemment de la possible erreur de phase

Codes Linéaires

- Mots du code :
  - Lignes d'une matrice **generatrice** $x_L = x.G$
  - Zéros d'une matrice de **parité (check)** $x \in \mathcal{C} \text{ iff } Hx = 0$

- **Syndrome** $Hx = s$

- **[*n*,*k*]** encode *k* bits dans des mots de *n* bits

Codes Linéaires

- Mots du code :
  - Lignes d'une matrice **generatrice**
  - Zéros d'une matrice de **parité (check)**

$$x_L = x.G$$

$$x \in \mathcal{C} \text{ iff } Hx = 0$$

G

$$(111) = (1).(111)$$

$$(000) = (0).(111)$$

- **Syndrome** $Hx = s$

- **[*n*,*k*]** encode *k* bits dans des mots de *n* bits

Codes Linéaires

- Mots du code :
  - Lignes d'une matrice **generatrice** $x_L = x.G$
  - Zéros d'une matrice de **parité (check)** $x \in \mathcal{C} \text{ iff } Hx = 0$

$$G$$

$$(111) = (1).(111)$$
$$(000) = (0).(111)$$

- **Syndrome** $Hx = s$

- **[*n*,*k*]** encode *k* bits dans des mots de *n* bits

$$H$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{pmatrix}$$

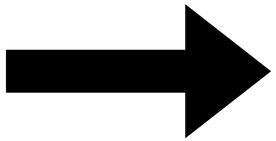
Quantum CSS codes

- Etant donné deux codes classiques $C_1[n, k_1]$ et $C_2[n, k_2]$ avec $C_2 \subset C_1$ et C_1 et $C_2^{\perp}$ corrigent t erreurs on peut construire un code quantique qui corrige au moins t erreurs en considérant les cosets de C_1/C_2 :
  avec les états logiques

$$|x + C_2\rangle = \frac{1}{\sqrt{C_2}} \sum_{y \in C_2} |x + y\rangle \qquad \text{pour} \qquad x \in C_1$$

Stabiliseurs

$$|\psi\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$



$$X|\psi\rangle = |\psi\rangle$$

Stabiliseurs

$$|\psi\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$X|\psi\rangle = |\psi\rangle$$

Stabiliseurs

$$|\psi\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \Longleftrightarrow \quad X|\psi\rangle = |\psi\rangle$$

Stabiliseurs

$$|\psi\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \Longleftrightarrow \quad X|\psi\rangle = |\psi\rangle$$

$$|\psi\rangle = |0\rangle \quad \Longleftrightarrow \quad Z|\psi\rangle = |\psi\rangle$$

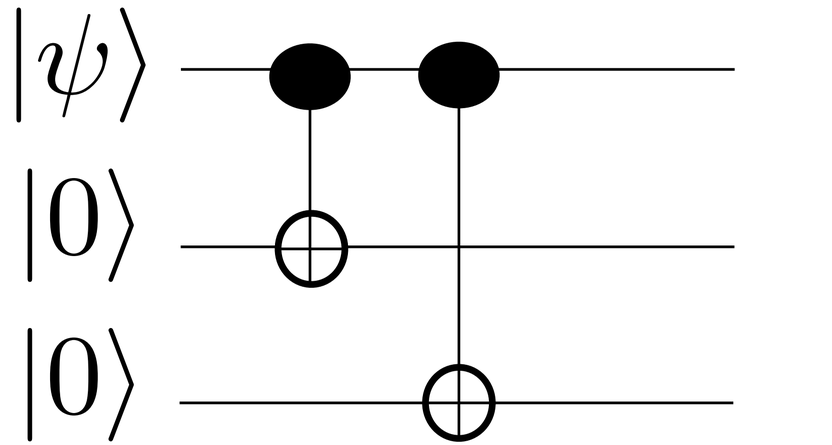
Stabiliseurs

$$|\psi\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \iff X|\psi\rangle = |\psi\rangle$$

$$|\psi\rangle = |0\rangle \iff Z|\psi\rangle = |\psi\rangle$$

Un ensemble d'opérateurs de Pauli sur plusieurs qubits qui commutent deux à deux forme un groupe qui permet de décrire un état ou un sous-espace

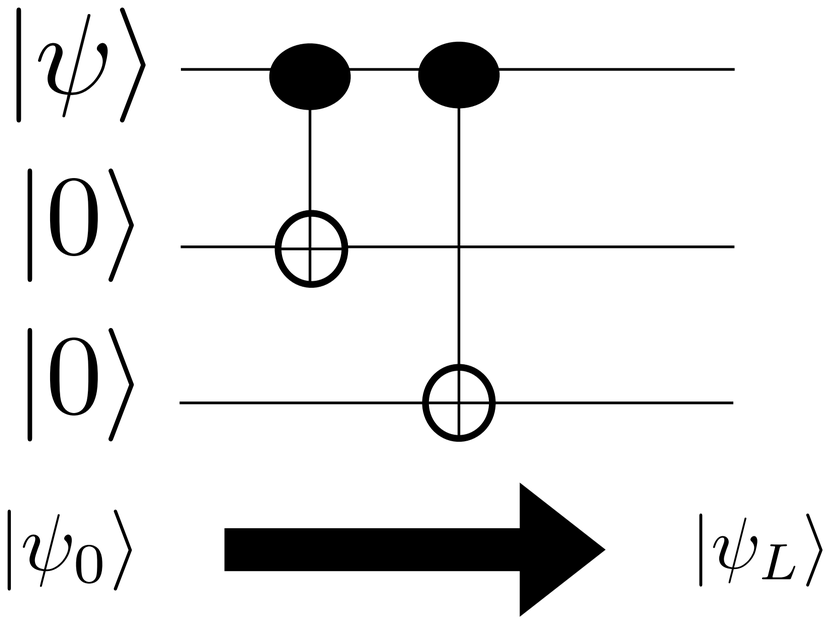
Stabiliseurs



$|\psi_0\rangle$ → $|\psi_L\rangle$

$$|\psi_0\rangle = |\psi\rangle|0\rangle|0\rangle$$

Stabiliseurs

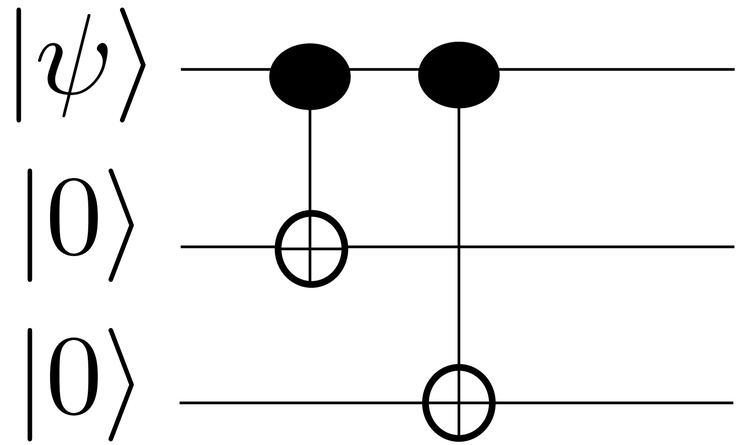


$$|\psi_0\rangle = |\psi\rangle|0\rangle|0\rangle$$

$$Z_2|\psi_0\rangle = |\psi_0\rangle$$

$$Z_3|\psi_0\rangle = |\psi_0\rangle$$

Stabiliseurs



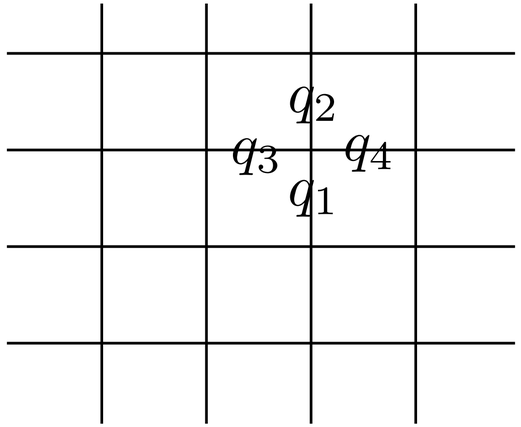
$|\psi_0\rangle$ → $|\psi_L\rangle$

$$|\psi_0\rangle = |\psi\rangle|0\rangle|0\rangle$$

$$Z_2|\psi_0\rangle = |\psi_0\rangle \qquad Z_1Z_2|\psi_L\rangle = |\psi_L\rangle$$

$$Z_3|\psi_0\rangle = |\psi_0\rangle \qquad Z_1Z_3|\psi_L\rangle = |\psi_L\rangle$$

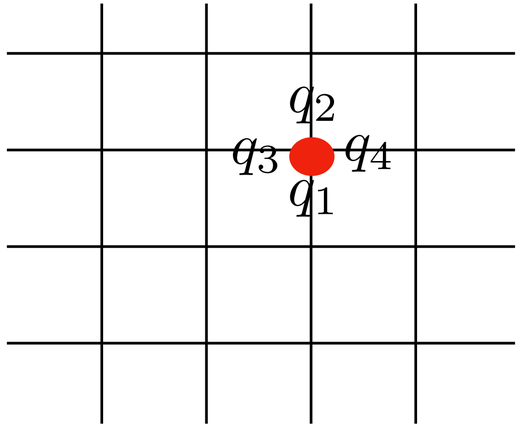
Codes Topologiques



Surface code

Codes Topologiques

$X_1X_2X_3X_4$

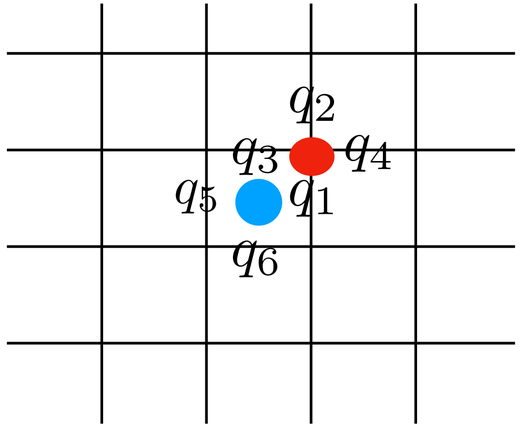


Surface code

Codes Topologiques

$X_1X_2X_3X_4$

$Z_1Z_2Z_5Z_6$

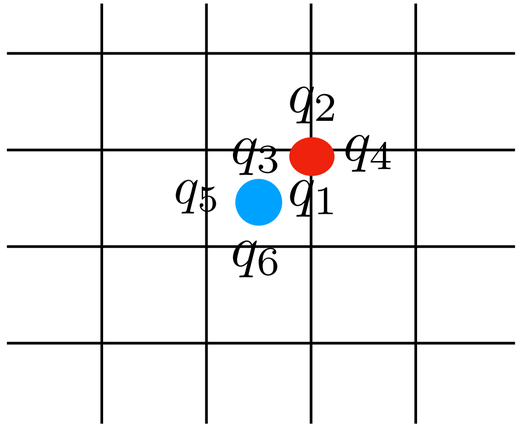


Surface code

Codes Topologiques

$X_1X_2X_3X_4$

$Z_1Z_2Z_5Z_6$



Surface code

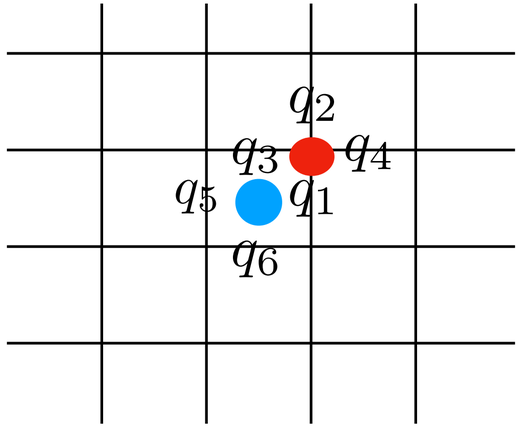
$$F \xrightarrow{H_Z} E \xrightarrow{H_X^*} V$$

Complexe de chaine

Codes Topologiques

$X_1X_2X_3X_4$

$Z_1Z_2Z_5Z_6$



Surface code

2 matrices binaires → stabiliseur

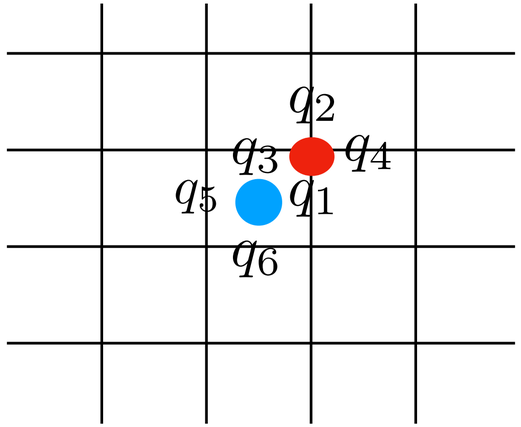
$$F \xrightarrow{H_Z} E \xrightarrow{H_X^*} V$$

Complexe de chaine

Codes Topologiques

$X_1X_2X_3X_4$

$Z_1Z_2Z_5Z_6$



Surface code

2 matrices binaires → stabiliseur

$$F \xrightarrow{H_Z} E \xrightarrow{H_X^*} V$$

Complexe de chaine

Quantum LDPC codes

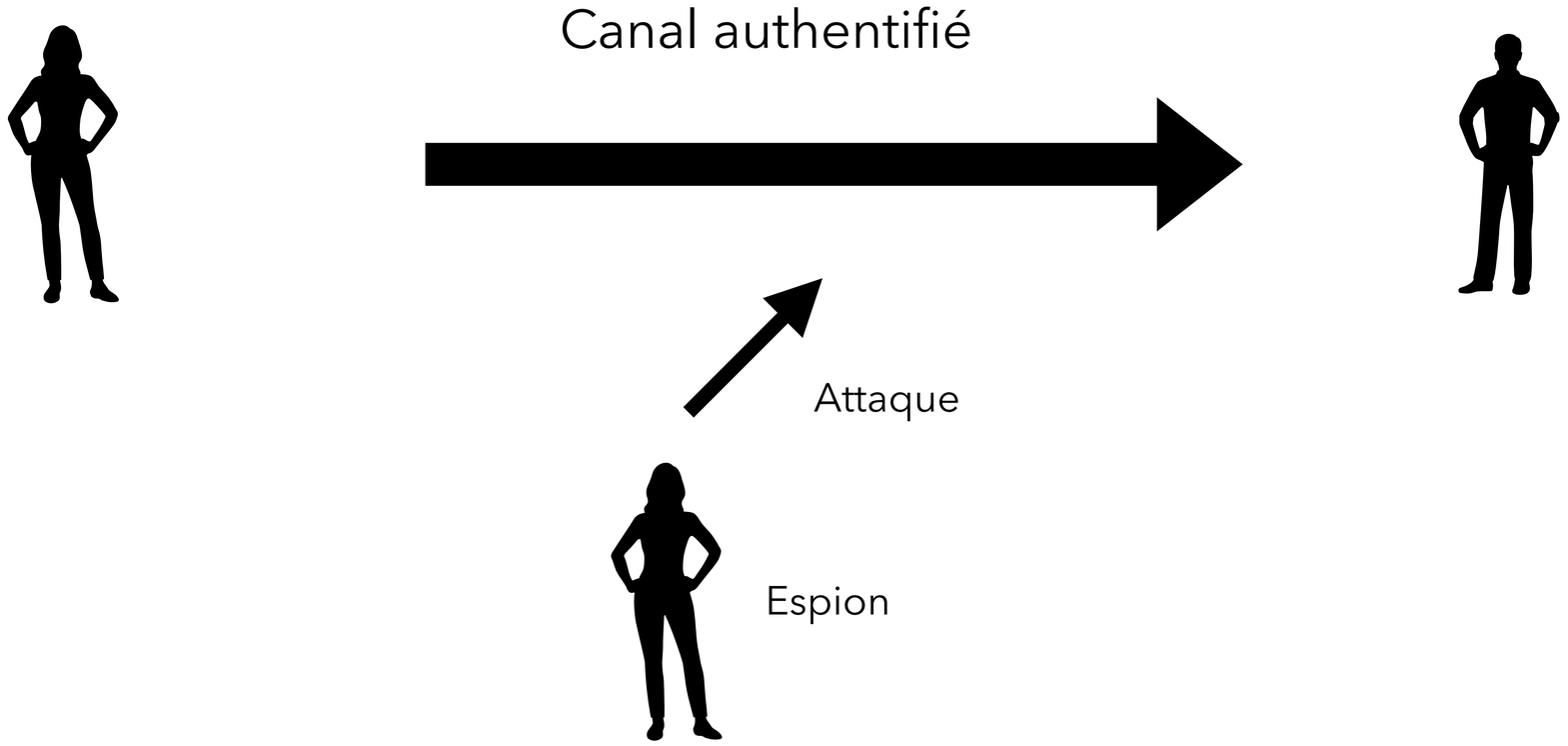
Codes correcteurs quantiques

- On peut protéger l'information quantique des erreurs
- Codes théoriques très bon asymptotiquement
- Codes surfaces sont implémentés
- Problèmes ouverts : de bon codes pratiques

Cryptographie quantique

BB84 : un protocole d ’échange de clé théoriquement sécurisé

Canal authentifié


Canal authentifié
Attaque
Espion

Un protocole classique parfaitement sécurisé :One time pad

- *x* mot sur n bits 000111
- *c* mot aléatoire uniforme 110101
- c⊕x 110010 est un mot aléatoire uniforme

Un protocole classique parfaitement sécurisé :One time pad

- *x* mot sur n bits 000111
- *c* mot aléatoire uniforme 110101
- c⊕x 110010 est un mot aléatoire uniforme

c⊕*x* pas d' information sur *x*

Un protocole classique parfaitement sécurisé :One time pad

- *x* mot sur n bits 000111
- *c* mot aléatoire uniforme 110101
- c⊕x 110010 est un mot aléatoire uniforme

$c \oplus x$ pas d' information sur x

$c \oplus x = x \oplus c \oplus c = x$ avec c on retrouve x

Un protocole classique parfaitement sécurisé :One time pad

- x mot sur n bits 000111
- c mot aléatoire uniforme 110101
- $c \oplus x$ 110010 est un mot aléatoire uniforme

$c \oplus x$ pas d' information sur x

$c \oplus x = x \oplus c \oplus c = x$ avec c on retrouve x

Problème : Comment créer des mots secrets aléatoires à distance ?

BB84

- Alice prepare *n'=n(4+a)* bits aléatoires (données) $d_1 \ldots d_{n'}$
- Alice prepare *n' =n(4+a)* bits aléatoires (bases) $b_1 \ldots b_{n'}$

BB84

- Alice prepare *n'=n(4+a)* bits aléatoires (données) $d_1 \dots d_{n'}$
- Alice prepare *n' =n(4+a)* bits aléatoires (bases) $b_1 \dots b_{n'}$
- Elle envoie *n'* qubits à Bob , l'état du qubit *i* est: $|\psi_i\rangle = H^{b_i}|d_i\rangle$
  - *Si* $b_i = 0$
    - *Si* $d_i = 0$ $|0\rangle$
    - *Si* $d_i = 1$ $|1\rangle$
  - *Si* $b_i = 1$
    - *Si* $d_i = 0$ $|+\rangle$
    - *Si* $d_i = 1$ $|-\rangle$

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

BB84

- Alice prepare *n'=n(4+a)* bits aléatoires (données) $d_1 \dots d_{n'}$
- Alice prepare *n' =n(4+a)* bits aléatoires (bases) $b_1 \dots b_{n'}$
- Elle envoie *n'* qubits à Bob , l'état du qubit *i* est: $|\psi_i\rangle = H^{b_i}|d_i\rangle$
  - *Si* $b_i = 0$
    - *Si* $d_i = 0$ $|0\rangle$
    - *Si* $d_i = 1$ $|1\rangle$
  - *Si* $b_i = 1$
    - *Si* $d_i = 0$ $|+\rangle$
    - *Si* $d_i = 1$ $|-\rangle$

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

Exemple n=2 , a=1/2

i	1	2	3	4	5	6	7	8	9
d	1	1	1	0	1	1	0	0	0
b	0	0	1	1	0	0	1	0	1
$\|\psi_i\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$

- Bob mesure aléatoirement avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ ou $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ et obtient *n'* bits *d'*

- Bob mesure aléatoirement avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ ou $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ et obtient *n'* bits *d'*

i	1	2	3	4	5	6	7	8	9
d	1	1	1	0	1	1	0	0	0
b	0	0	1	1	0	0	1	0	1
$\|\psi_i\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$
b'	0	1	0	1	1	0	1	1	0
d'	1	0	1	0	0	1	0	1	0

- Bob mesure aléatoirement avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ ou $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ et obtient *n'* bits *d'*

i	1	2	3	4	5	6	7	8	9
d	1	1	1	0	1	1	0	0	0
b	0	0	1	1	0	0	1	0	1
$\|\psi_i\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$
b'	0	1	0	1	1	0	1	1	0
d'	1	0	1	0	0	1	0	1	0

Résultats aléatoires

- Bob mesure aléatoirement avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ ou $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ et obtient *n'* bits *d'*
- Alice annonce sa base pour chaque qubit
- Bob jette les résultats obtenus en mesurant dans la mauvaise base. Avec très grande probabilité il reste plus de *2n* valeurs.

i	1	2	3	4	5	6	7	8	9
d	1	1	1	0	1	1	0	0	0
b	0	0	1	1	0	0	1	0	1
$\|\psi_i\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$
b'	0	1	0	1	1	0	1	1	0
d'	1	0	1	0	0	1	0	1	0

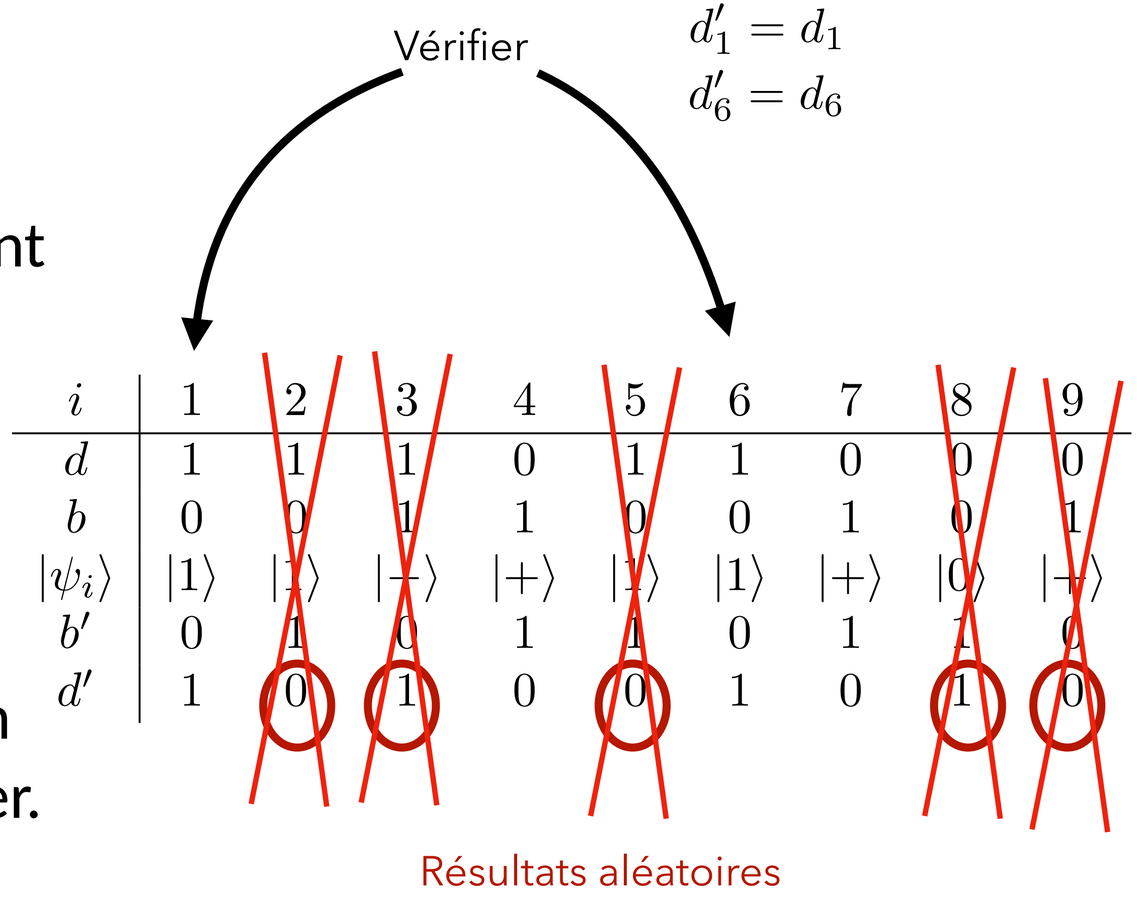
Résultats aléatoires

- Bob mesure aléatoirement avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ ou $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ et obtient *n'* bits *d'*
- Alice annonce sa base pour chaque qubit
- Bob jette les résultats obtenus en mesurant dans la mauvaise base. Avec très grande probabilité il reste plus de 2*n* valeurs.

i	1	2	3	4	5	6	7	8	9
d	1	1	1	0	1	1	0	0	0
b	0	0	1	1	0	0	1	0	1
$\|\psi_i\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$
b'	0	1	0	1	1	0	1	1	0
d'	1	0	1	0	0	1	0	1	0

Résultats aléatoires

- Bob mesure aléatoirement avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ ou $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ et obtient *n'* bits *d'*
- Alice annonce sa base pour chaque qubit
- Bob jette les résultats obtenus en mesurant dans la mauvaise base. Avec très grande probabilité il reste plus de 2*n* valeurs.
- Alice choisit 2*n* indices mesurés dans la même base et dévoile n valeurs pour vérifier que les résultats obtenus sont bien les mêmes. Si trop peut coïncident, annuler.



i	1	2	3	4	5	6	7	8	9
d	1	1	1	0	1	1	0	0	0
b	0	0	1	1	0	0	1	0	1
$\|\psi_i\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$
b'	0	1	0	1	1	0	1	1	0
d'	1	0	1	0	0	1	0	1	0

- Bob mesure aléatoirement avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ ou $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ et obtient *n'* bits *d'*
- Alice annonce sa base pour chaque qubit
- Bob jette les résultats obtenus en mesurant dans la mauvaise base. Avec très grande probabilité il reste plus de 2*n* valeurs.
- Alice choisit 2*n* indices mesurés dans la même base et dévoile n valeurs pour vérifier que les résultats obtenus sont bien les mêmes. Si trop peut coïncident, annuler.

Vérifier

$d'_1 = d_1$
$d'_6 = d_6$

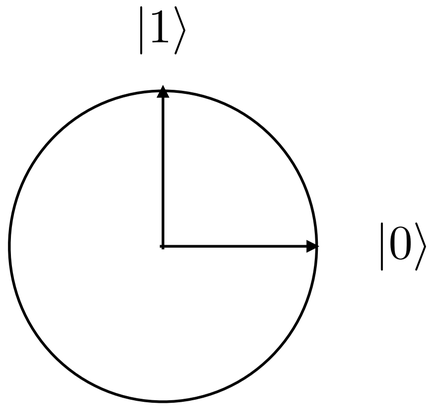
i	1	2	3	4	5	6	7	8	9
d	1	1	1	0	1	1	0	0	0
b	0	0	1	1	0	0	1	0	1
$\|\psi_i\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$
b'	0	1	0	1	1	0	1	1	0
d'	1	0	1	0	0	1	0	1	0

Résultats aléatoires

$$v = d_4 d_7$$

Attaque sur un qubit

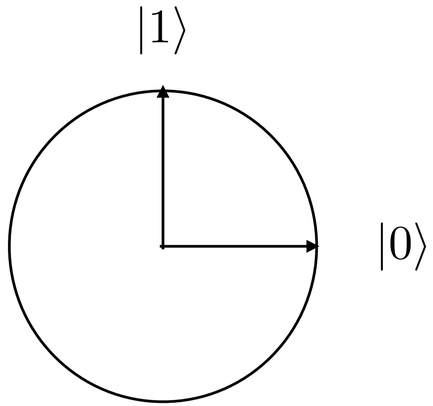
Mesure standard $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$



Attaque sur un qubit

Mesure standard $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$

$p = 1/2$ $\{|+\rangle, |-\rangle\}$



Attaque sur un qubit

Mesure standard $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$

$p = 1/2$ $\{|+\rangle, |-\rangle\}$

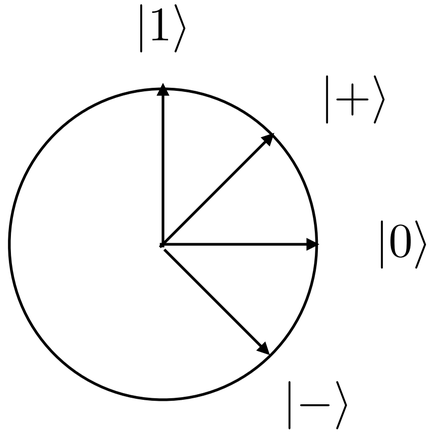
Si on mesure $|+\rangle$ $d = 0, b = 1$

$p = 1/2$ $c = 0$

Et l'état devient $|0\rangle$

$p = 1/2$ $c = 1$

Et l'état devient $|1\rangle$



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

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Attaque sur un qubit

Mesure standard $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$

$p = 1/2$ $\{|+\rangle, |-\rangle\}$

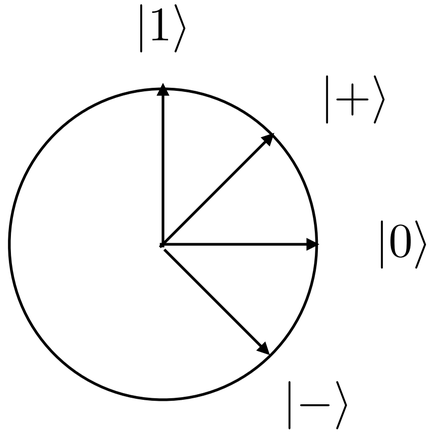
Si on mesure $|+\rangle$ $d = 0, b = 1$

$p = 1/2$ $c = 0$

Et l'état devient $|0\rangle$

$p = 1/2$ $c = 1$

Et l'état devient $|1\rangle$



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

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Dans les deux cas, avec $p = 1/2$ ce qubit est choisi dans la partie vérification

Bob le mesure avec $\{|+\rangle\langle +|, |-\rangle\langle -|\}$

Attaque sur un qubit

Mesure standard $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$

$p = 1/2$ $\{|+\rangle, |-\rangle\}$

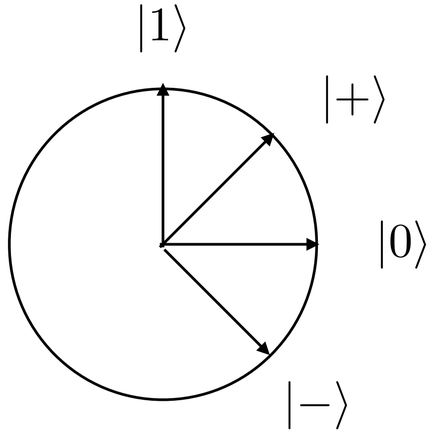
Si on mesure $|+\rangle$ $d = 0, b = 1$

$p = 1/2$ $c = 0$

Et l'état devient $|0\rangle$

$p = 1/2$ $c = 1$

Et l'état devient $|1\rangle$



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

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

Dans les deux cas, avec $p = 1/2$ ce qubit est choisi dans la partie vérification

Bob le mesure avec $\{|+\rangle\langle +|, |-\rangle\langle -|\}$

Attaque sur un qubit

Mesure standard $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$

$p = 1/2$ $\{|+\rangle, |-\rangle\}$

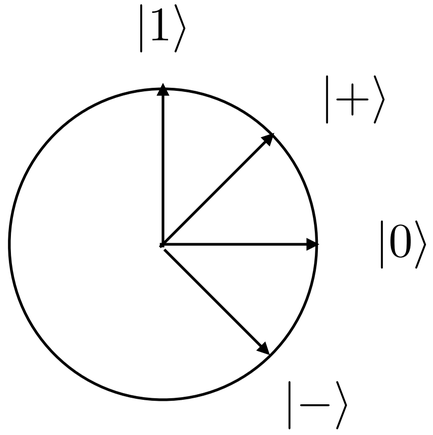
Si on mesure $|+\rangle$ $d = 0, b = 1$

$p = 1/2$ $c = 0$

Et l'état devient $|0\rangle$

$p = 1/2$ $c = 1$

Et l'état devient $|1\rangle$



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

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

Dans les deux cas, avec $p = 1/2$ ce qubit est choisi dans la partie vérification

Bob le mesure avec $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ $p = 1/2, d' \neq d$

Attaque sur un qubit

Mesure standard $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$

$p = 1/2$ $\{|+\rangle, |-\rangle\}$

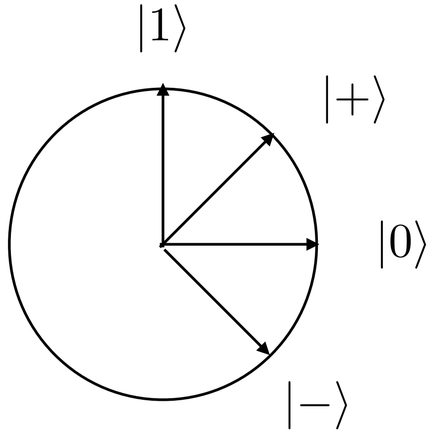
Si on mesure $|+\rangle$ $d = 0, b = 1$

$p = 1/2$ $c = 0$

Et l'état devient $|0\rangle$

$p = 1/2$ $c = 1$

Et l'état devient $|1\rangle$



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

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

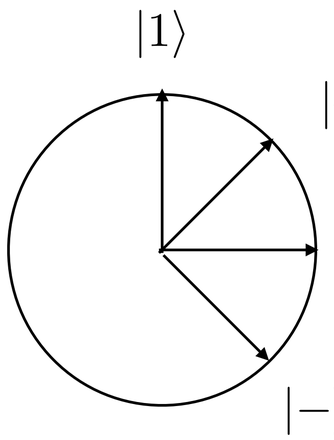
Dans les deux cas, avec $p = 1/2$ ce qubit est choisi dans la partie vérification

Bob le mesure avec $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ $p = 1/2,\ d' \neq d$

La mesure de l'espion donne le bon résultat avec probabilité 1/2 et il se fait détecter avec probabilité 1/4

Si l'espion mesure n qubits la probabilité de ne pas se faire détecter est $(3/4)^n \to 0$

Une attaque astucieuse

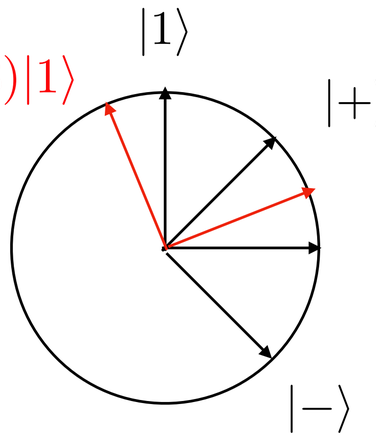


$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Une attaque astucieuse

$\{|\phi_0\rangle\langle\phi_0|, |\phi_1\rangle\langle\phi_1|\}$ $\quad |\phi_1\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$



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

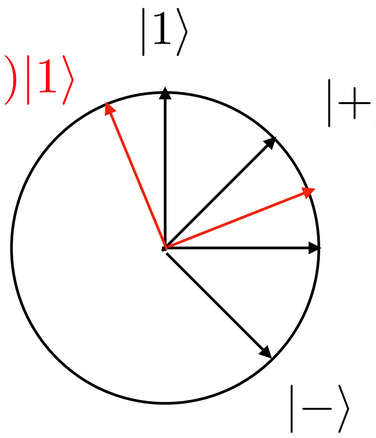
$$|\phi_0\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Une attaque astucieuse

$\{|\phi_0\rangle\langle\phi_0|, |\phi_1\rangle\langle\phi_1|\}$ $\quad |\phi_1\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$

Si on mesure $|0\rangle$ $\quad d = 0, b = 0$



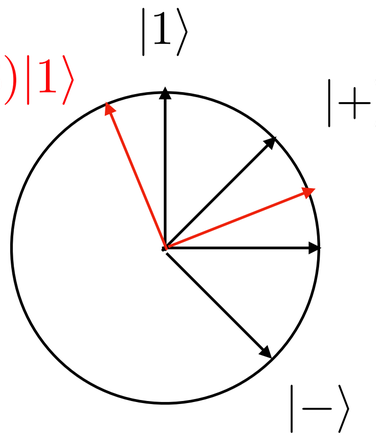
$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|\phi_0\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Une attaque astucieuse

$\{|\phi_0\rangle\langle\phi_0|, |\phi_1\rangle\langle\phi_1|\}$ $\quad |\phi_1\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$



$|+\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$

$|\phi_0\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$

$|-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

Si on mesure $|0\rangle$ $\quad d = 0,\ b = 0$

$p = \cos^2(\pi/8) \approx 0,85 \quad c = 0$

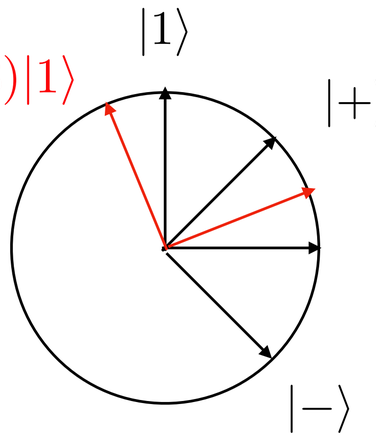
et l'état devient $|\phi_0\rangle$

$p = \sin^2(\pi/8) \approx 0,15 \quad c = 1$

et l'état devient $|\phi_1\rangle$

Une attaque astucieuse

$\{|\phi_0\rangle\langle\phi_0|, |\phi_1\rangle\langle\phi_1|\}$ $\quad |\phi_1\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$



$|+\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$

$|\phi_0\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$

$|-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

Si on mesure $|0\rangle$ $\quad d = 0,\ b = 0$

$p = \cos^2(\pi/8) \approx 0,85 \quad c = 0$

et l'état devient $|\phi_0\rangle$

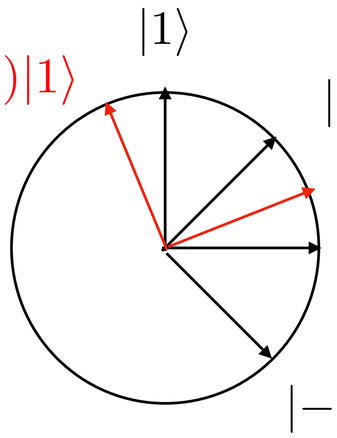
$p = \sin^2(\pi/8) \approx 0,15 \quad c = 1$

et l'état devient $|\phi_1\rangle$

Dans les deux cas, avec $p = 1/2$ ce qubit est choisi dans la partie vérification

Une attaque astucieuse

$\{|\phi_0\rangle\langle\phi_0|, |\phi_1\rangle\langle\phi_1|\}$ $|\phi_1\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$



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

$|\phi_0\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$

$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

Si on mesure $|0\rangle$ $d = 0, b = 0$

$p = \cos^2(\pi/8) \approx 0,85$ $c = 0$

et l'état devient $|\phi_0\rangle$

$p = \sin^2(\pi/8) \approx 0,15$ $c = 1$

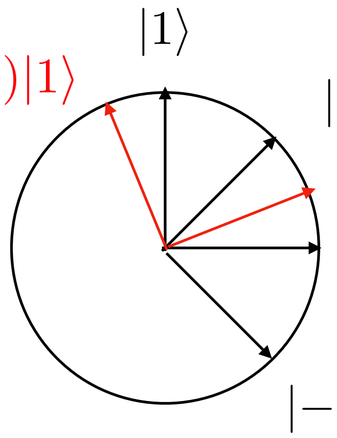
et l'état devient $|\phi_1\rangle$

Dans les deux cas, avec $p = 1/2$ ce qubit est choisi dans la partie vérification

Si Bob mesure $|\phi_0\rangle$ avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ $p = \sin^2(\pi/8) \approx 0,15$ $d' \neq d$

Une attaque astucieuse

$\{|\phi_0\rangle\langle\phi_0|, |\phi_1\rangle\langle\phi_1|\}$ $\quad |\phi_1\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$



$|+\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$

$|\phi_0\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$

$|-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

Si on mesure $|0\rangle$ $\quad d = 0,\ b = 0$

$p = \cos^2(\pi/8) \approx 0,85 \quad c = 0$

et l'état devient $|\phi_0\rangle$

$p = \sin^2(\pi/8) \approx 0,15 \quad c = 1$

et l'état devient $|\phi_1\rangle$

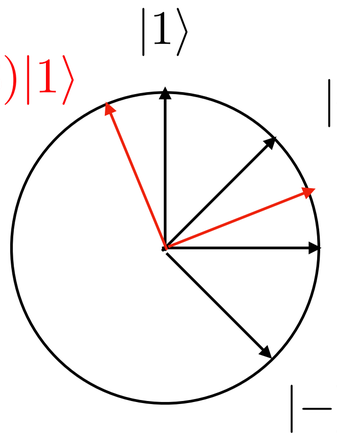
Dans les deux cas, avec $p = 1/2$ ce qubit est choisi dans la partie vérification

Si Bob mesure $|\phi_0\rangle$ avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ $\quad p = \sin^2(\pi/8) \approx 0,15 \quad d' \neq d$

Si Bob mesure $|\phi_1\rangle$ avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ $\quad p = \cos^2(\pi/8) \approx 0,85 \quad d' \neq d$

Une attaque astucieuse

$\{|\phi_0\rangle\langle\phi_0|, |\phi_1\rangle\langle\phi_1|\}$ $\quad |\phi_1\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$



$|+\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$

$|\phi_0\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$

$|-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

Si on mesure $|0\rangle$ $\quad d = 0,\ b = 0$

$p = \cos^2(\pi/8) \approx 0,85 \quad c = 0$

et l'état devient $|\phi_0\rangle$

$p = \sin^2(\pi/8) \approx 0,15 \quad c = 1$

et l'état devient $|\phi_1\rangle$

Dans les deux cas, avec $p = 1/2$ ce qubit est choisi dans la partie vérification

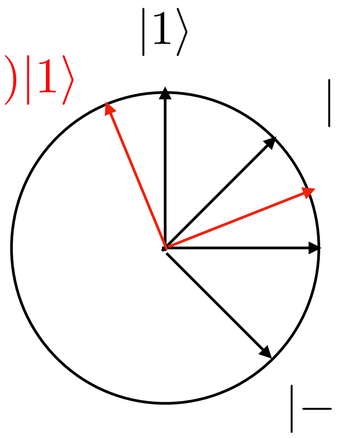
Si Bob mesure $|\phi_0\rangle$ avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ $\quad p = \sin^2(\pi/8) \approx 0,15 \quad d' \neq d$

Si Bob mesure $|\phi_1\rangle$ avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ $\quad p = \cos^2(\pi/8) \approx 0,85 \quad d' \neq d$

La mesure de l'espion donne le bon résultat avec probabilité 0,85 et il se fait détecter avec probabilité au moins 0,15

Une attaque astucieuse

$\{|\phi_0\rangle\langle\phi_0|, |\phi_1\rangle\langle\phi_1|\}$ $\quad |\phi_1\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$



$|+\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$

$|\phi_0\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$

$|-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

Si on mesure $|0\rangle$ $\quad d = 0,\ b = 0$

$p = \cos^2(\pi/8) \approx 0,85 \quad c = 0$

et l'état devient $|\phi_0\rangle$

$p = \sin^2(\pi/8) \approx 0,15 \quad c = 1$

et l'état devient $|\phi_1\rangle$

Dans les deux cas, avec $p = 1/2$ ce qubit est choisi dans la partie vérification

Si Bob mesure $|\phi_0\rangle$ avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ $\quad p = \sin^2(\pi/8) \approx 0,15 \quad d' \neq d$

Si Bob mesure $|\phi_1\rangle$ avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ $\quad p = \cos^2(\pi/8) \approx 0,85 \quad d' \neq d$

La mesure de l'espion donne le bon résultat avec probabilité 0,85 et il se fait détecter avec probabilité au moins 0,15

Si l'espion mesure n qubits la probabilité de ne pas se faire détecter tend vers 0

Résistance au bruit

Alice annonce $u \oplus v$ avec u mot aléatoire d'un code CSS quantique $u \in C_1$

Résistance au bruit

Alice annonce $u \oplus v$ avec u mot aléatoire d'un code CSS quantique $u \in C_1$

Bob ajoute $u \oplus v$ à ces qubits non utilisés pour la vérification $v \oplus \epsilon$

et obtient $u \oplus \epsilon$ qu'il corrige pour obtenir $u \in C_1$

Résistance au bruit

Alice annonce $u \oplus v$ avec u mot aléatoire d'un code CSS quantique $u \in C_1$

Bob ajoute $u \oplus v$ à ces qubits non utilisés pour la vérification $v \oplus \epsilon$

et obtient $u \oplus \epsilon$ qu'il corrige pour obtenir $u \in C_1$

Bob et Alice utilisent le coset de u dans C_1/C_2 comme clé secrète

Cryptographie quantique

- La théorie de l'information quantique peut casser des protocoles existants mais elle peut aussi proposer de nouveaux protocoles
- Sécurité théorique pour le partage de clé
- Sécuriser contre des adversaires quantiques

Corrélations quantiques

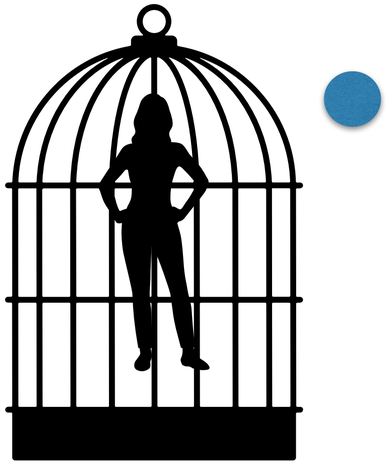
Pseudotélépathie: quand l’impossible devient possible

Jeu de pseudo-télépathie

- On place trois personnes dans des salles différentes, on leur présente à chacun une boule rouge ou bleue et ils doivent décider chacun de la prendre ou ne pas la prendre (chaque joueur a une vision partielle et un capacité d'action partielle)
- Ils gagnent ensemble s' il rendent un nombre impair de boules au total si et seulement si il n'y avait que des boules rouges

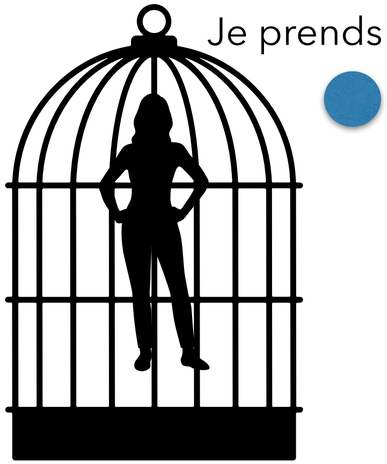
Jeu de pseudo-télépathie

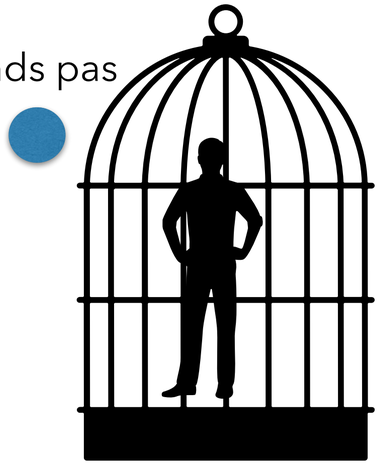
- On place trois personnes dans des salles différentes, on leur présente à chacun une boule rouge ou bleue et ils doivent décider chacun de la prendre ou ne pas la prendre (chaque joueur a une vision partielle et un capacité d'action partielle)
- Ils gagnent ensemble s' il rendent un nombre impair de boules au total si et seulement si il n'y avait que des boules rouges



Jeu de pseudo-télépathie

- On place trois personnes dans des salles différentes, on leur présente à chacun une boule rouge ou bleue et ils doivent décider chacun de la prendre ou ne pas la prendre (chaque joueur a une vision partielle et un capacité d'action partielle)
- Ils gagnent ensemble s' il rendent un nombre impair de boules au total si et seulement si il n'y avait que des boules rouges



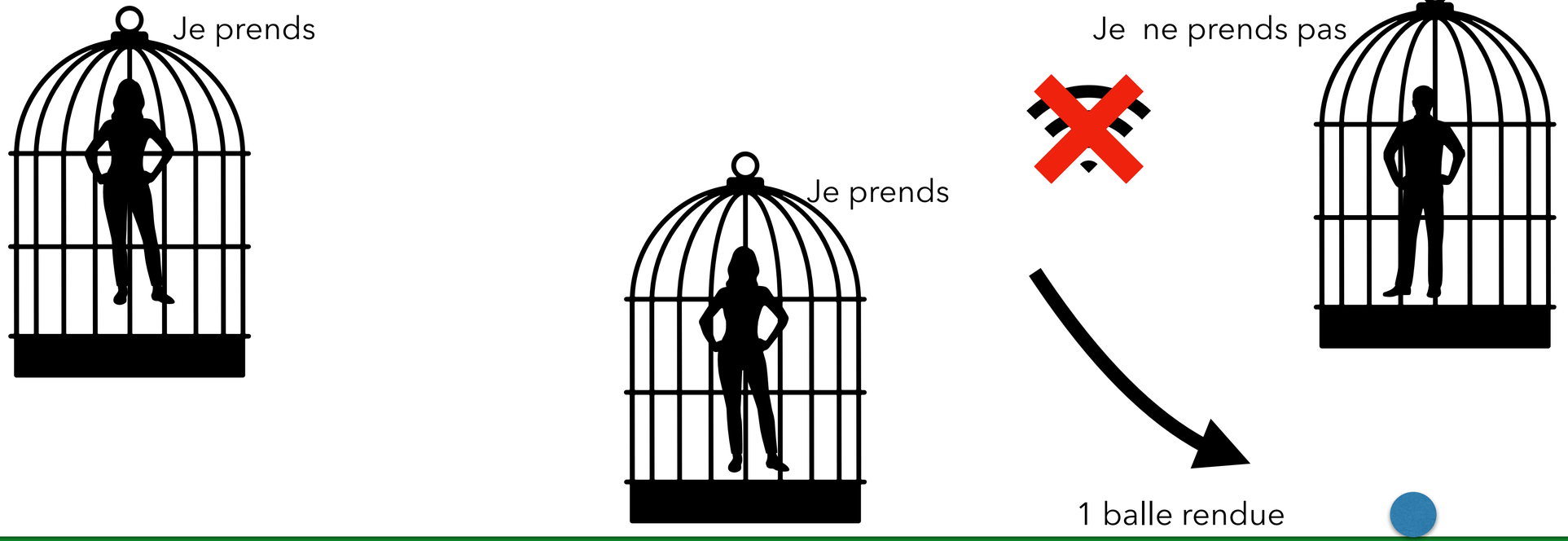


Jeu de pseudo-télépathie

- On place trois personnes dans des salles différentes, on leur présente à chacun une boule rouge ou bleue et ils doivent décider chacun de la prendre ou ne pas la prendre (chaque joueur a une vision partielle et un capacité d'action partielle)
- Ils gagnent ensemble s' il rendent un nombre impair de boules au total si et seulement si il n'y avait que des boules rouges

Jeu de pseudo-télépathie

- On place trois personnes dans des salles différentes, on leur présente à chacun une boule rouge ou bleue et ils doivent décider chacun de la prendre ou ne pas la prendre (chaque joueur a une vision partielle et un capacité d'action partielle)
- Ils gagnent ensemble s' il rendent un nombre impair de boules au total si et seulement si il n'y avait que des boules rouges



Jeu de pseudo-télépathie

- On place trois personnes dans des salles différentes, on leur présente à chacun une boule rouge ou bleue et ils doivent décider chacun de la prendre ou ne pas la prendre (chaque joueur a une vision partielle et un capacité d'action partielle)
- Ils gagnent ensemble s' il rendent un nombre impair de boules au total si et seulement si il n'y avait que des boules rouges

Jeu de pseudo-télépathie

- On place trois personnes dans des salles différentes, on leur présente à chacun une boule rouge ou bleue et ils doivent décider chacun de la prendre ou ne pas la prendre (chaque joueur a une vision partielle et un capacité d'action partielle)
- Ils gagnent ensemble s' il rendent un nombre impair de boules au total si et seulement si il n'y avait que des boules rouges

Jeu de pseudo-télépathie

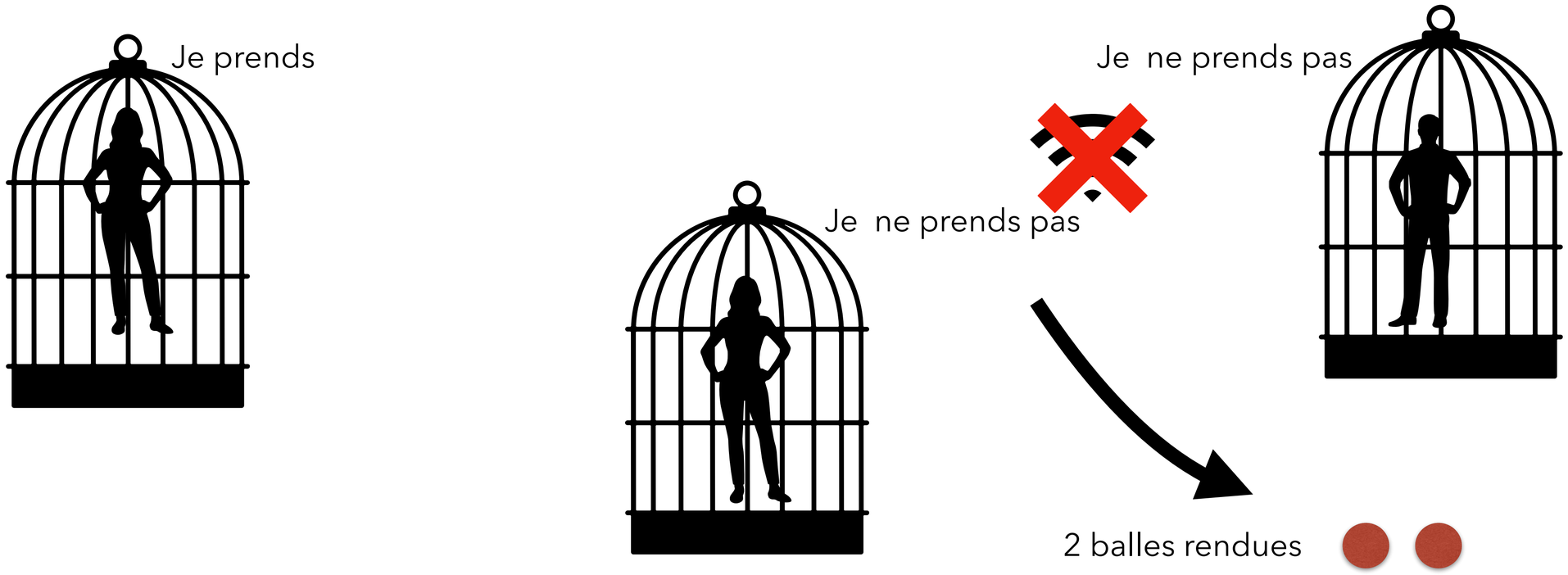
- On place trois personnes dans des salles différentes, on leur présente à chacun une boule rouge ou bleue et ils doivent décider chacun de la prendre ou ne pas la prendre (chaque joueur a une vision partielle et un capacité d'action partielle)
- Ils gagnent ensemble s' il rendent un nombre impair de boules au total si et seulement si il n'y avait que des boules rouges

Jeu de pseudo-télépathie

- On place trois personnes dans des salles différentes, on leur présente à chacun une boule rouge ou bleue et ils doivent décider chacun de la prendre ou ne pas la prendre (chaque joueur a une vision partielle et un capacité d'action partielle)
- Ils gagnent ensemble s' il rendent un nombre impair de boules au total si et seulement si il n'y avait que des boules rouges

Jeu de pseudo-télépathie

- On place trois personnes dans des salles différentes, on leur présente à chacun une boule rouge ou bleue et ils doivent décider chacun de la prendre ou ne pas la prendre (chaque joueur a une vision partielle et un capacité d'action partielle)
- Ils gagnent ensemble s' il rendent un nombre impair de boules au total si et seulement si il n'y avait que des boules rouges



Jeu de pseudo-télépathie

Ils perdent si :

On leur a présenté une seule boule rouge au total : 

et ils ont rendu 1 ou 3 boules :  ou  ou 

On leur a présenté 3 boules rouges : 

et ils ont rendu 0 ou 2 boules:  ou rien

Jeu de pseudo-télépathie

Ils perdent si :

On leur a présenté une seule boule rouge au total : 

et ils ont rendu 1 ou 3 boules :  ou  ou 

On leur a présenté 3 boules rouges : 

et ils ont rendu 0 ou 2 boules:  ou rien

Contrainte: La parité du nombre total de boules rendues doit être différente dans les scénario ou il n'ya qu'une boule rouge de celui ou il y a trois boules rouge

Impossibilité classique

- Si la réponse a_1 du joueur 1 est

0 s'il ne rend pas la boule

1 s'il rend la boule

- a_i : nombre de balles rendues par le joueur *i* en fonction de la couleur observée

Impossibilité classique

- Si la réponse a_1 du joueur 1 est

0 s'il ne rend pas la boule

1 s'il rend la boule

- a_i : nombre de balles rendues par le joueur *i* en fonction de la couleur observée

- On somme la réponse des joueurs sur les trois configurations: chaque joueur fera:
  - deux fois ce qu'il fait quand il voit du bleu
  - une fois ce qu'il fait quand il voit du rouge

Impossibilité classique

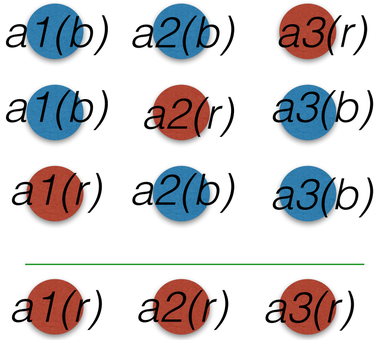
- Si la réponse a_1 du joueur 1 est

0 s'il ne rend pas la boule

1 s'il rend la boule

- a_i : nombre de balles rendues par le joueur *i* en fonction de la couleur observée

- On somme la réponse des joueurs sur les trois configurations: chaque joueur fera:
  - deux fois ce qu'il fait quand il voit du bleu
  - une fois ce qu'il fait quand il voit du rouge



Impossibilité classique

- Si la réponse a_1 du joueur 1 est

0 s'il ne rend pas la boule

1 s'il rend la boule

- a_i : nombre de balles rendues par le joueur *i* en fonction de la couleur observée

- On somme la réponse des joueurs sur les trois configurations: chaque joueur fera:

  - deux fois ce qu'il fait quand il voit du bleu
  - une fois ce qu'il fait quand il voit du rouge

a1(b) a2(b) a3(r)
a1(b) a2(r) a3(b)
a1(r) a2(b) a3(b)

---

a1(r) a2(r) a3(r)

Même parité totale que quand ils ont tous du rouge !
Donc impossible de gagner classiquement a 100% et pourtant on y arrive !!!!

Une stratégie parfaite

$$
\begin{aligned}
X \otimes Z \otimes Z|\psi> &= |\psi> \\
Z \otimes X \otimes Z|\psi> &= |\psi> \\
Z \otimes Z \otimes X|\psi> &= |\psi> \\
X \otimes X \otimes X|\psi> &= -|\psi>
\end{aligned}
$$

Stabiliseur

Chaque joueur mesure son qubit avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ si on lui présente une boule bleue et $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ si on lui présente une boule rouge
et décide de la rendre la balle si son résultat classique est 1

Une stratégie parfaite

$$
\begin{aligned}
X \otimes Z \otimes Z|\psi> &= |\psi> \\
Z \otimes X \otimes Z|\psi> &= |\psi> \\
Z \otimes Z \otimes X|\psi> &= |\psi> \\
X \otimes X \otimes X|\psi> &= -|\psi>
\end{aligned}
$$

Stabiliseur

Chaque joueur mesure son qubit avec $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ si on lui présente une boule bleue et $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ si on lui présente une boule rouge
et décide de la rendre la balle si son résultat classique est 1

Un phénomène plus général : **Contextualité**

Corrélations quantiques

- Carré de Mermin: un comportement impossible classiquement
- 2 joueurs qui ne communiquent pas, Claire et Louis
  - une question pour Claire : valeurs dans une colonne
  - une question pour Louis: valeurs dans une ligne
  - On veut satisfaire:
    - somme des lignes impaires
    - somme des colonnes paires
    - leur case commune a la même valeur pour les deux

0	0	1
0	1	0
0	1	1

Corrélations quantiques

- Carré de Mermin: un comportement impossible classiquement
- 2 joueurs qui ne communiquent pas, Claire et Louis
  - une question pour Claire : valeurs dans une colonne
  - une question pour Louis: valeurs dans une ligne
  - On veut satisfaire:
    - somme des lignes impaires
    - somme des colonnes paires
    - leur case commune a la même valeur pour les deux

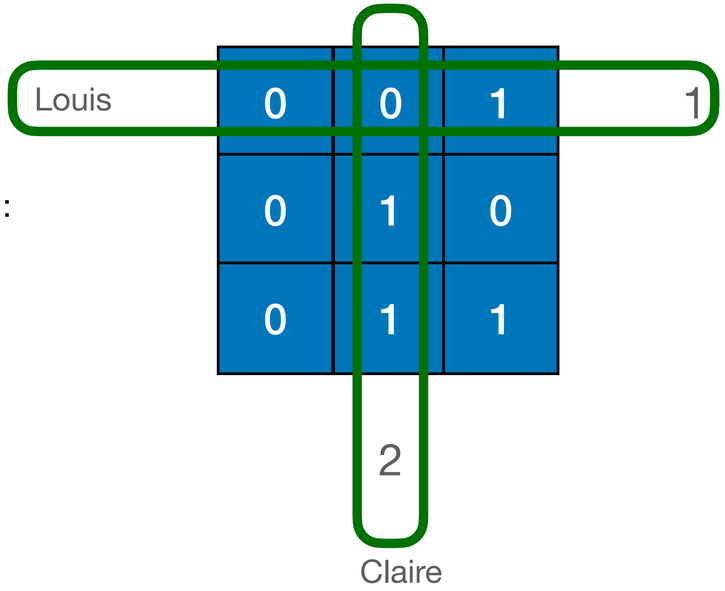
Exemple de question :
ligne 1 colonne 2

Louis	0	0	1	1
	0	1	0	
	0	1	1	

Corrélations quantiques

- Carré de Mermin: un comportement impossible classiquement
- 2 joueurs qui ne communiquent pas, Claire et Louis
  - une question pour Claire : valeurs dans une colonne
  - une question pour Louis: valeurs dans une ligne
  - On veut satisfaire:
    - somme des lignes impaires
    - somme des colonnes paires
    - leur case commune a la même valeur pour les deux

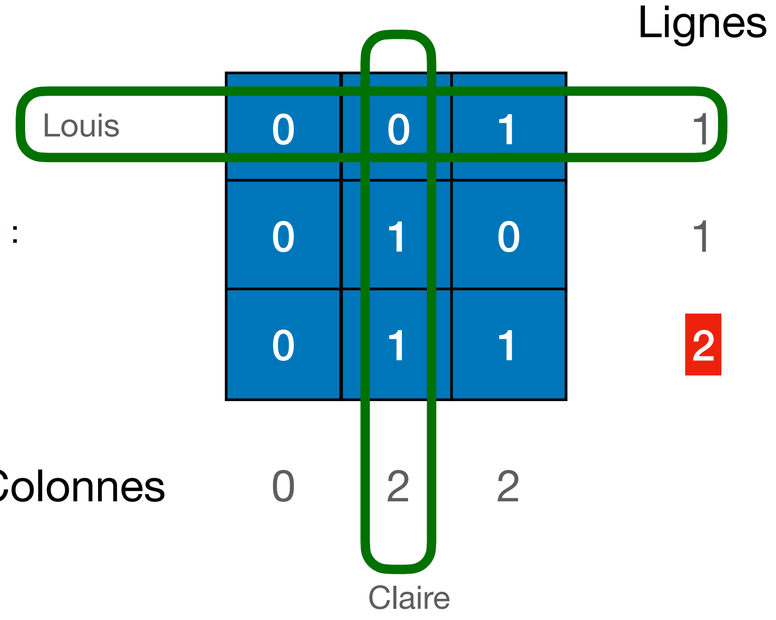
Exemple de question :
ligne 1 colonne 2



Corrélations quantiques

- Carré de Mermin: un comportement impossible classiquement
- 2 joueurs qui ne communiquent pas, Claire et Louis
  - une question pour Claire : valeurs dans une colonne
  - une question pour Louis: valeurs dans une ligne
  - On veut satisfaire:
    - somme des lignes impaires
    - somme des colonnes paires
    - leur case commune a la même valeur pour les deux

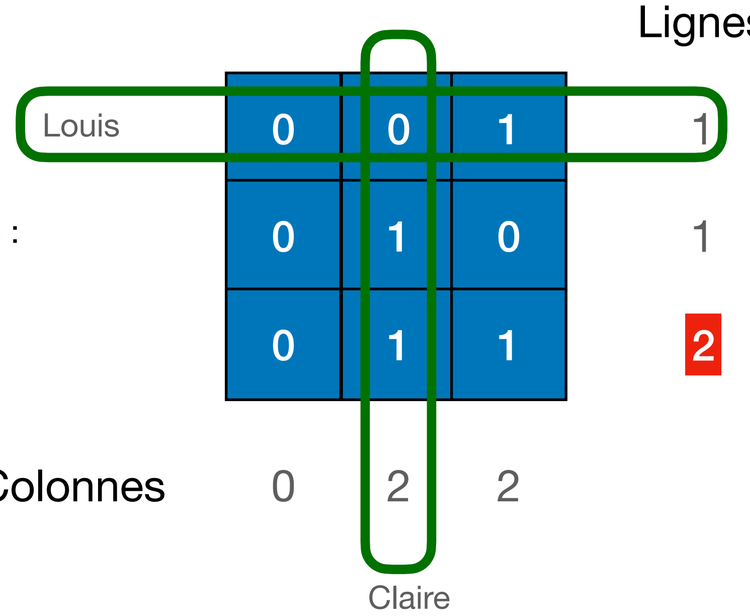
Exemple de question :
ligne 1 colonne 2



Corrélations quantiques

- Carré de Mermin: un comportement impossible classiquement
- 2 joueurs qui ne communiquent pas, Claire et Louis
  - une question pour Claire : valeurs dans une colonne
  - une question pour Louis: valeurs dans une ligne
  - On veut satisfaire:
    - somme des lignes impaires
    - somme des colonnes paires
    - leur case commune a la même valeur pour les deux

Exemple de question :
ligne 1 colonne 2



Somme des lignes =Somme des colonnes=Somme des cases

Corrélations quantiques

- Elargit le champ des possibles par rapport au monde classique et permet de nouvelles possibilités
- Gros avantages en complexité de communication

- Nouvelles notions à revisiter comme la causalité

- Nouvelle manière de voir le monde

Pour en savoir plus

- En Français:
  - Livre en gratuit en ligne d'Olivier Ezratty
    - https://www.oezratty.net/wordpress/2020/comprendre-informatique-quantique-edition-2020/
  - En ludique : BD "les mystères du monde quantique"
- En Anglais:
- Livre référence pour la théorie de l'information quantique:
  - "Quantum Computation and Quantum information" de Nielsen et Chuang
- Blog de Scott Aaronson
  - https://scottaaronson.blog/
- Notes de cours de Ronald de Wolf
  - https://homepages.cwi.nl/~rdewolf/qcnotes.pdf