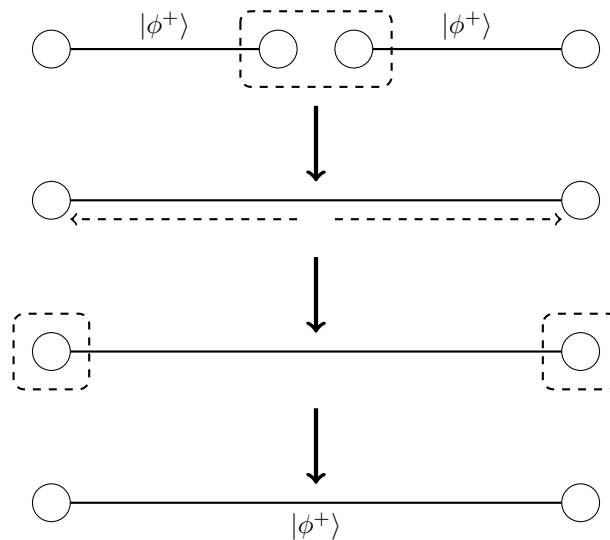


Codes correcteurs et répéteurs quantiques

Jean Rax

Encadrants : Romain Alléaume et Hugues Randriambololona

Stage L3 du 17 Juin au 26 Juillet 2013



*We cannot clone, perforce ; instead, we split
Coherence to protect it from that wrong
That would destroy our valued quantum bit
And make our computation take too long.*

*Correct a flip and phase - that will suffice.
If in our code another error's bred,
We simply measure it, then God plays dice,
Collapsing it to X or Y or Zed.*

*We start with noisy seven, nine, or five
And end with perfect one. To better spot
Those flaws we must avoid, we first must strive
To find which ones commute and which do not.*

*With group and eigenstate, we've learned to fix
Your quantum errors with our quantum tricks.*

Quantum Error Correction Sonnet, Daniel Gottesman

Table des matières

1	Théorie de l'information quantique	6
1.1	Matrice densité	6
1.1.1	Définition et propriétés	6
1.1.2	Transformations de ρ	7
1.1.3	Trace partielle	8
1.1.4	Décomposition de Schmidt et purification	8
1.2	Opérations quantiques	9
1.2.1	Représentation de Kraus	10
1.2.2	Opérations imparfaites	10
1.2.3	Canal et mémoire quantiques	11
1.3	Comparaison d'états	12
1.3.1	Indistinguabilité et théorème de non clonage	12
1.3.2	Fidélité et théorème de Uhlmann	12
1.4	Entropie	14
1.4.1	Entropie de Shannon	14
1.4.2	Entropie de von Neumann	15
2	Codes correcteurs d'erreur	16
2.1	Généralités sur les codes correcteurs quantique	16
2.1.1	Codes classiques	16
2.1.2	Particularités du cas quantique	17
2.1.3	Exemple : le code à 3 qubits et le code de Shor	18
2.1.4	Correction des effacements	19
2.2	Codes stabilisateurs	21
2.2.1	Formalisme général	21
2.2.2	Réalisation des codes stabilisateurs	23
2.2.3	Exemples	24
3	Répéteurs quantiques	25
3.1	Utilisation de l'intrication	25
3.1.1	Quantité d'intrication	25
3.1.2	Téléportation quantique	26
3.1.3	Permutation d'intrication	27
3.2	Protocoles de purification	29
3.2.1	Protocole IBM	29
3.2.2	Protocole d'Oxford	32
3.2.3	Hachage	34
3.3	Répéteurs quantiques	36
3.3.1	Idée générale	36
3.3.2	Protocole partiel et architecture générale	38
4	Comparaison des deux méthodes	39
4.1	Capacité théorique	39
4.1.1	Définition	39
4.1.2	Capacités du canal à effacement	39
4.2	Comparaison asymptotique	40
4.2.1	Cas des mémoires parfaites	40
4.2.2	Cas des mémoires imparfaites	42
4.3	Comparaison avec ressources finies	43
4.3.1	Ressources physiques	43
4.3.2	Résultats numériques	43
4.4	Équivalence entre purification et codes correcteurs	44

Introduction

Ce stage s'est déroulé à Télécom ParisTech du 17 Juin au 26 Juillet et a pour sujet les codes correcteurs d'erreurs quantiques ainsi que les répéteurs quantiques. Il a été précédé d'une partie bibliographique traitant des codes correcteurs d'erreur classique ([17]) ainsi qu'une introduction aux codes correcteurs d'erreur quantiques (notamment [8]). Le point de départ du stage à Télécom a été l'article [11] avant de s'orienter d'une part vers l'information quantique (à travers principalement [12]) et les codes correcteurs quantiques afin d'une part de mieux comprendre les bornes théoriques de la transmission d'information quantique et d'autre part les protocoles de répéteurs quantiques permettant ainsi de comparer ce système à celui des codes correcteurs.

Je tiens à remercier mes encadrants, Romain Alléaume et Hugues Randriambololona, l'équipe Information Quantique de Télécom ParisTech ainsi que toute l'équipe de SeQureNet pour leur accueil et leur disponibilité

Rappels de mécanique quantique

En mécanique quantique un système est décrit de manière générale non pas par un point dans un espace des phases mais par un vecteur de norme 1 d'un espace de Hilbert (à un scalaire multiplicatif $e^{i\theta}$ nommé phase globale près). On utilise la notation de Dirac désignant par $|\psi\rangle$ un vecteur et $\langle\psi|$ la forme linéaire associée du dual.

Les postulats de la mécanique quantique sont les suivants :

- L'état d'un système est décrit par un vecteur $|\psi\rangle$ d'un espace de Hilbert \mathcal{H} .
- À toute quantité observable est associée un opérateur autoadjoint A . Les résultats de la mesure de cette quantité ne peuvent être que les valeurs propres de A . De plus en notant P_m la projection sur le sev associé à la valeur propre λ_m la probabilité d'obtenir λ_m est $\|P_m|\psi\rangle\|^2$ et après la mesure l'état du système devient $\frac{P_m|\psi\rangle}{\|P_m|\psi\rangle}$.
- L'évolution d'un système quantique est décrite par l'équation de Schrödinger :

$$i\hbar \frac{d|\psi\rangle}{dt} = H(t)|\psi\rangle$$

Avec H le hamiltonien, un opérateur autoadjoint.

- L'espace de Hilbert associé à la réunion de deux systèmes A et B est $\mathcal{H}_A \otimes \mathcal{H}_B$, le produit tensoriel des espaces de Hilbert individuels.

Notion de qubit

On s'intéresse au plus simple des systèmes quantiques, le système à deux niveaux pouvant correspondre à de nombreuses réalisations physiques avec par exemple le spin $\frac{1}{2}$, deux niveaux atomiques, la polarisation de la lumière ou encore des modes spatiaux ou temporels de photons. On parlera désormais de qubit sans préciser le système physique.

On note une base de l'espace de Hilbert de dimension 2 associé ($|0\rangle, |1\rangle$) et par analogie avec le spin $\frac{1}{2}$ on notera les opérateurs de Pauli :

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

De plus plutôt que d'écrire l'équation de Schrödinger on écrira une évolution comme l'action d'un opérateur unitaire

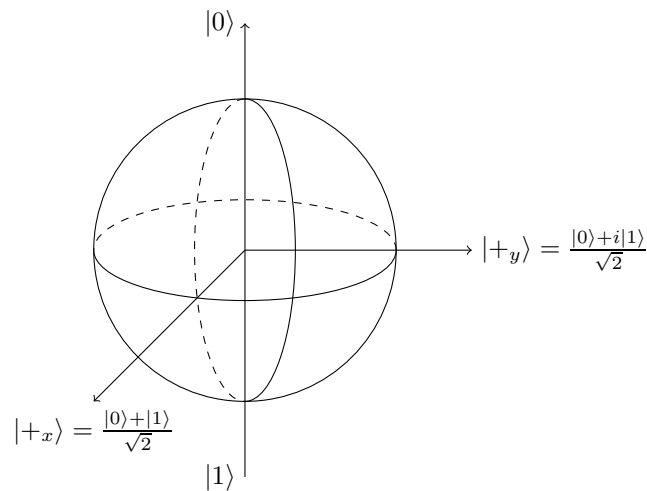
$$U = \exp\left(-\frac{i}{\hbar} \int_0^T H(t) dt\right)$$

Il existe de nombreuses différences entre un qubit et un bit classique :

- Tandis qu'un bit classique prend soit la valeur 0 soit la valeur 1 un qubit peut prendre toute les valeurs de la forme :

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

avec $|\alpha|^2 + |\beta|^2 = 1$, i.e n'importe quel vecteur de norme 1 de \mathbb{C}^2 . De plus la phase totale étant sans aucune importance, de $SO_3 \simeq SU_2/\{\pm 1\}$ on déduit que l'on peut représenter un qubit par un vecteur de la sphère de Bloch :



- L'effet de la mesure est aussi très différent : comme pour tout système quantique lorsqu'on effectue une mesure on projette l'état sur un des états propres et donc on perd de l'information.
- Dans le cas de plusieurs qubits il peut se produire un phénomène d'intrication, par exemple pour deux qubits on peut avoir les états dits de Bell :

$$\begin{cases} |\phi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\ |\phi^-\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) \\ |\psi^+\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) \\ |\psi^-\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) \end{cases}$$

Qui n'admettent pas d'équivalent classique, en particulier si on effectue une mesure sur un des deux qubits alors l'état du second est entièrement déterminé.

Ces particularités ainsi que la physique sous-jacente aux réalisations des qubits rendent ceux-ci très sensibles au bruit et erreurs dus à une interaction non contrôlée avec l'environnement, rendant nécessaire l'utilisation de schémas permettant de corriger ou réduire les erreurs.

Plan du rapport

L'objectif de ce travail est d'étudier la transmission de qubits en présence de bruit et les moyens de corriger ou du moins diminuer l'importance des erreurs.

- La première partie (s'appuyant principalement sur [12]) traite des bases de l'information quantique permettant, de même que dans le cas classique, d'introduire les outils nécessaires au traitement des erreurs ainsi que de mieux quantifier celles-ci.
- La seconde introduit les codes correcteurs d'erreurs quantiques à travers notamment le formalisme des stabilisateurs. Ces codes s'inspirant des codes classiques permettent de réduire les erreurs au prix d'une augmentation de la taille (dimension) du système.
- On considère ensuite les protocoles de répéteurs quantiques qui permettent de tirer partie de l'intrication pour transmettre des qubits à longue distance.
- La dernière partie compare les deux méthodes en fonction de paramètres physiques tels que les ressources physiques nécessaires ou encore la qualité des mémoires quantiques disponibles.

1 Théorie de l'information quantique

De même que dans le cas classique on peut définir les notions de canaux, entropie ou encore fidélité en mécanique quantique. Pour cela on introduit tout d'abord le formalisme très utile de la matrice densité (qui permet de traiter le cas d'une probabilité classique d'avoir certains états quantiques).

1.1 Matrice densité

1.1.1 Définition et propriétés

Lorsqu'un système est dans un état $|\psi\rangle$ (on parle d'état pur), étant donné une observable A sa valeur moyenne est :

$$\langle A \rangle = \langle \psi | A | \psi \rangle = \text{tr}(\langle \psi | A | \psi \rangle) = \text{tr}(|\psi\rangle \langle \psi | A)$$

De même si le système présente une probabilité p_i d'être dans l'état $|\psi_i\rangle$ alors on a :

$$\langle A \rangle = \sum_i p_i \langle \psi_i | A | \psi_i \rangle = \text{tr} \left(\sum_i p_i |\psi_i\rangle \langle \psi_i | A \right)$$

On définit donc la matrice densité par :

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i |$$

et de manière générale on obtient :

$$\langle A \rangle = \text{tr}(\rho A)$$

Remarques :

- Les probabilités de la matrice densité sont des probabilités classiques d'avoir des états quantiques qui ne sont pas de la même nature que les probabilités liées à la mesure quantique par exemple l'état $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ est différent d'avoir $|0\rangle$ avec probabilité $\frac{1}{2}$ et $|1\rangle$ avec probabilité $\frac{1}{2}$, même si une mesure selon l'axe z donnera les mêmes résultats avec les mêmes probabilités.
- Étant donné ρ il y a plusieurs possibilités physiques conduisant à cette même matrice densité, par exemple $I/2 = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2} \times \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}(\langle 0| + \langle 1|) + \frac{1}{2} \times \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \frac{1}{\sqrt{2}}(\langle 0| - \langle 1|)$. (cf A.1)

Pour toute matrice densité ρ on a $\text{tr}(\rho) = \text{tr}(\sum_i p_i |\psi_i\rangle \langle \psi_i |) = \text{tr}(\sum_i p_i \langle \psi_i | \psi_i \rangle)$, c'est-à-dire

$$\text{tr}(\rho) = 1$$

De plus $\rho^\dagger = \rho$ et $\langle \psi | \rho | \psi \rangle = \sum_i p_i \|\langle \psi | \psi_i \rangle\|^2 \geq 0$. On en déduit d'après le théorème spectral que ρ est diagonalisable dans une base orthonormée avec des valeurs propres positives et de somme 1, i.e on peut écrire $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i |$ avec les $|\psi_i\rangle$ formant une base orthonormée et $\sum_i p_i = 1$.

Réciproquement pour toute matrice autoadjointe positive de trace 1 correspond une matrice densité, en effet il suffit de la diagonaliser grâce au théorème spectral pour l'écrire $\sum_i p_i |\psi_i\rangle \langle \psi_i |$ avec les (p_i) positifs de somme 1.

Cette diagonalisation permet par exemple de montrer que $\rho^2 = \sum_i p_i^2 |\psi_i\rangle \langle \psi_i |$ et que donc $\text{tr}(\rho^2) \leq 1$ avec égalité ssi on a un état pur.

On remarque que dans le cas où on a une probabilité p_i d'avoir la matrice densité ρ_i on a au total d'après la définition une matrice densité de la forme $\rho = \sum_i p_i \rho_i$.

Ce formalisme possède de plus une interprétation supplémentaire pour les qubits, en effet dans ce cas particulier on peut représenter la matrice densité par un vecteur \vec{r} de la boule unité de \mathbb{R}^3 :

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}$$

avec $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$, les vecteurs de norme 1 de la sphère de Bloch étant ainsi le cas particulier des états purs.

Pour montrer ce résultat il suffit de le montrer pour les états purs (ce qui se fait par un simple calcul), puis en écrivant $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$ on obtient directement $\vec{r} = \sum_i p_i \vec{r}_i$.

1.1.2 Transformations de ρ

Si on applique une transformation unitaire U alors on obtient une probabilité p_i d'être dans l'état $U |\psi_i\rangle$. On en déduit que sous l'action de U , ρ se transforme selon :

$$\rho \rightarrow U \rho U^\dagger$$

Si on effectue une mesure ayant pour projecteur P_m alors la probabilité d'obtenir m est

$$p(m) = \sum_i p_i \times p(m|i) = \sum_i p_i \langle \psi_i | P_m^\dagger P_m | \psi_i \rangle$$

Et donc :

$$p(m) = \text{tr} (P_m^\dagger P_m \rho)$$

Comme après la mesure, si on a obtenu m on a $|\psi_i^m\rangle = \frac{P_m |\psi_i\rangle}{\sqrt{p(m|i)}}$ on obtient après la mesure :

$$\rho_m = \sum_i p(i|m) |\psi_i^m\rangle \langle \psi_i^m| = \sum_i p(i|m) \frac{P_m |\psi_i\rangle \langle \psi_i| P_m^\dagger}{p(m|i)}$$

De plus on sait que $p(i|m) \times p(m) = p(m, i) = p(m|i) \times p(i)$ qui conduit à $\frac{p(i|m)}{p(m|i)} = p(i)/p(m)$. Et donc :

$$\rho_m = \frac{P_m \rho P_m^\dagger}{\text{tr} (P_m^\dagger P_m \rho)}$$

Si de plus on ne connaît pas le résultat de la mesure on a :

$$\rho = \sum_m p(m) \rho_m = \sum_m P_m \rho P_m^\dagger$$

On peut ainsi reformuler les postulats de la mécanique quantique en termes de matrice densité :

- A chaque système isolé on associe un espace de Hilbert \mathcal{H} . L'état du système est alors décrit par un opérateur autoadjoint positif de trace 1 de \mathcal{H} noté ρ . Si le système a une probabilité p_i d'être en ρ_i alors $\rho = \sum_i p_i \rho_i$.
- Une mesure est décrite par un ensemble (P_m) de projecteurs tels que $\sum_m P_m^\dagger P_m = 1$. On a alors une probabilité $p(m) = \text{tr} (P_m^\dagger P_m \rho)$ d'obtenir le résultat m et dans ce cas après la mesure l'état devient $\rho = \frac{P_m \rho P_m^\dagger}{\text{tr} (P_m^\dagger P_m \rho)}$.

- L'évolution d'un système isolé entre deux instants est décrite par un opérateur unitaire U agissant sur ρ par :

$$\rho \rightarrow U\rho U^\dagger$$

- Si on a n systèmes en interaction alors l'espace de Hilbert total est $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_n$. De plus si chaque système est dans l'état ρ_i alors $\rho = \rho_1 \otimes \rho_2 \otimes \dots \otimes \rho_n$.

1.1.3 Trace partielle

On s'intéresse à deux systèmes A et B intriqués.

Pour $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$ on définit la trace partielle par rapport à A par :

$$\text{tr}_A(\rho) = \sum_i \langle i_A | \rho | i_A \rangle \in \mathcal{H}_B$$

avec $|i_A\rangle$ une base orthonormée de \mathcal{H}_A (et de même pour tr_B , trace partielle par rapport à B).

On a alors :

$$\text{tr}_A(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|) = \text{tr}(|a_1\rangle \langle a_2|) \cdot |b_1\rangle \langle b_2|$$

Ce qui est aussi une définition de tr_A .

Alors si $\{A, B\}$ a pour matrice densité ρ^{AB} le système A est décrit par la matrice densité :

$$\rho^A = \text{tr}_B(\rho^{AB})$$

En effet soit M un opérateur autoadjoint sur le système A et M' le même sur le système AB . Alors forcément $M' = M \otimes 1_B$ (en effet si $M = \sum p_m P_m$, alors $M' = \sum p_m P'_m$ où P'_m est la projection sur le sev de A associé i.e $P'_m = P_m \otimes 1_B$).

On souhaite avoir :

$$\langle M' \rangle_A = \text{tr}(M \rho^A) = \text{tr}((M \otimes 1_B) \rho^{AB}) = \langle M' \rangle_{A,B}$$

Donc :

$$\begin{aligned} \rho_{(i,j)}^A &= \langle i_A | \rho^A | j_A \rangle = \text{tr}(|j_A\rangle \langle i_A| \rho^A) = \text{tr}(|j_A\rangle \langle i_A| \otimes 1_B) \rho^{AB} \\ &= \sum_{k,l} \langle k_A l_B | (|j_A\rangle \langle i_A| \otimes 1_B) \rho^{AB} | k_A l_B \rangle \\ &= \sum_{k,l} \delta_{k,j} \langle i_A l_B | \rho^{AB} | k_A l_B \rangle \\ &= \sum_l \langle i_A l_B | \rho^{AB} | j_A l_B \rangle = \langle i_A | \sum_l \langle l_B | \rho^{AB} | l_B \rangle | j_A \rangle \end{aligned}$$

Et donc on obtient bien :

$$\rho_{(i,j)}^A = \text{tr}_B(\rho^{AB})_{(i,j)}$$

1.1.4 Décomposition de Schmidt et purification

Soit $|\psi\rangle$ un état pur du système AB . Alors, il existe des réels positifs λ_i appelés coefficients de Schmidt et des bases orthonormées $|i_A\rangle$ et $|j_B\rangle$ de \mathcal{H}_A et \mathcal{H}_B respectivement telles que :

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$$

tel que $\sum_i \lambda_i^2 = 1$.

Démonstration : De manière générale on peut écrire :

$$|\psi\rangle = \sum_{i,j} a_{i,j} |i_A\rangle |j_B\rangle$$

avec $a = (a_{i,j})$ une matrice quelconque. D'après le théorème des valeurs singulières on peut écrire :

$$a = ubv$$

avec u et v unitaires et b diagonale positive. On obtient donc, comme $b_{k,l} = b_{k,k} \delta_{k,l}$:

$$\begin{aligned} |\psi\rangle &= \sum_{i,k,j} u_{i,k} b_{k,k} v_{k,j} |i_A\rangle |j_B\rangle \\ &= \sum_k b_{k,k} \left(\sum_i u_{i,k} |i_A\rangle \right) \left(\sum_j v_{k,j} |j_B\rangle \right) \end{aligned}$$

Et comme $(\sum_i u_{i,k} |i_A\rangle)$ et $(\sum_j v_{k,j} |j_B\rangle)$ forment des bases orthogonales, on a bien le résultat.

On considère un système A dans l'état ρ . Alors, on peut voir cet état comme l'état d'un sous-système d'un système dans un état pur : formellement, il existe R et $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_R$ tel que :

$$\rho = \text{tr}_R (|\psi\rangle \langle\psi|)$$

Pour prouver ce résultat on s'inspire de la décomposition de Schmidt ; on diagonalise ρ :

$$\rho = \sum_i p_i |i_A\rangle \langle i_A|$$

puis on prend \mathcal{H}_R de même dimension (ou plus grande) que \mathcal{H}_A , pour pouvoir poser :

$$|\psi\rangle = \sum_i \sqrt{p_i} |i_A\rangle |i_R\rangle$$

avec $|i_R\rangle$ une base orthonormée de \mathcal{H}_R . Alors on a :

$$\text{tr}_R (|\psi\rangle \langle\psi|) = \text{tr}_R \left(\sum_{i,j} \sqrt{p_i p_j} |i_A\rangle \langle j_A| |i_R\rangle \langle j_R| \right) = \sum_i p_i |i_A\rangle \langle i_A| = \rho$$

Remarque : il ne faut pas confondre cette construction théorique avec le procédé de purification d'intrication décrit plus tard qui permet à partir de plusieurs paires faiblement intriquées d'obtenir une paire mieux intriquée.

1.2 Opérations quantiques

On se pose la question de savoir si il est possible d'exprimer de manière simple en termes de matrices densité ρ l'effet de l'environnement sur le système, c'est-à-dire que l'on cherche à écrire une relation de la forme :

$$\rho' = \mathcal{E}(\rho)$$

entre le système initial et celui après interaction avec l'environnement.

1.2.1 Représentation de Kraus

On suppose que le système est couplé à un environnement E et que le tout subit l'action d'un opérateur unitaire U de $\mathcal{H}_{sys} \otimes \mathcal{H}_E$ (et que initialement le système et l'environnement ne sont pas intriqués). On a alors :

$$\mathcal{E}(\rho) = \text{tr}_E (U(\rho \otimes \rho_E)U^\dagger)$$

Quitte à purifier l'environnement, on peut supposer que celui-ci commence dans un état pur $|e_0\rangle$ que l'on complète en une base orthonormale $(|e_k\rangle)$. On peut donc écrire :

$$\mathcal{E}(\rho) = \text{tr}_E (U(\rho \otimes |e_0\rangle \langle e_0|)U^\dagger) = \sum_k \langle e_k|U(\rho \otimes |e_0\rangle \langle e_0|)U^\dagger|e_k\rangle$$

Avec :

$$E_k = \langle e_k|U|e_0\rangle \in \mathcal{L}(\mathcal{H}_{sys})$$

On obtient donc la représentation de Kraus :

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$$

Dans le cas d'opérations unitaires on a \mathcal{E} qui préserve la trace c'est-à-dire :

$$\sum_k E_k E_k^\dagger = 1$$

On peut interpréter comme une évolution selon U suivie d'une mesure selon la base $(|e_k\rangle)$ dont le résultat n'est pas connu.

Dans le cas où on effectue une mesure par rapport à l'environnement et au système on obtient que le système total si la mesure donne m est :

$$\frac{P_m \rho \otimes |e_0\rangle \langle e_0| P_m}{\text{tr}(P_m \rho \otimes |e_0\rangle \langle e_0| P_m)}$$

Si on trace par rapport à l'environnement :

$$\rho' = \frac{\text{tr}_E(P_m \rho \otimes |e_0\rangle \langle e_0| P_m)}{\text{tr}(P_m \rho \otimes |e_0\rangle \langle e_0| P_m)}$$

Avec $E_k = \langle e_k|P_m|e_0\rangle$ en posant :

$$\mathcal{E}_m(\rho) = \sum_k E_k \rho E_k^\dagger$$

qui ne préserve pas la trace, on obtient, avec une probabilité $\text{tr}(\mathcal{E}_m(\rho))$:

$$\rho' = \frac{\mathcal{E}_m(\rho)}{\text{tr}(\mathcal{E}_m(\rho))}$$

1.2.2 Opérations imparfaites

On peut ainsi modéliser une opération effectuée sur un qubit de manière imparfaite. Ainsi une porte U opérant sur un sous-espace \mathcal{K} ayant une probabilité p de fonctionner peut être modélisée par :

$$U = pU^{ideal} + \frac{1-p}{\dim(\mathcal{K})} 1_{\mathcal{K}} \text{tr}_{\mathcal{K}}(\rho)$$

ce qui signifie que la porte effectue l'opération demandée avec une probabilité p et qu'avec une probabilité $1-p$ elle retourne un résultat au hasard (on peut aussi le modéliser par une opération parfaite suivie d'un canal à dépolarisation).

Et une mesure imparfaite peut être modélisée de la même façon par exemple sur la base $|0\rangle, |1\rangle$, si on a une probabilité η d'effectuer la bonne mesure on a les projecteurs qui deviennent :

$$\begin{cases} P_0 = \eta |0\rangle \langle 0| + (1-\eta) |1\rangle \langle 1| \\ P_1 = \eta |1\rangle \langle 1| + (1-\eta) |0\rangle \langle 0| \end{cases}$$

On utilisera ces deux modélisations dans la suite.

1.2.3 Canal et mémoire quantiques

On utilise la notion de canal quantique pour modéliser la transmission spatiale ou temporelle d'information quantique. Il s'agit d'un certain point de vue de l'opération 1 effectuée de manière imparfaite, que l'on note \mathcal{E} .

Il existe plusieurs modèles de canal bruité :

- Inversion de bit : on prend pour représentation de Kraus $E_0 = \sqrt{p}I$ et $E_1 = \sqrt{1-p}X$, c'est-à-dire :

$$\mathcal{E}(\rho) = p\rho + (1-p)X\rho X$$

Cela correspond à une probabilité p que le qubit soit inchangé et $1-p$ que X soit appliqué. De même pour des erreurs de phase avec Z et des erreurs de phase et d'inversion de qubit avec Y . (géométriquement cela correspond à la contraction de la sphère de Bloch de manière anisotrope).

- Canal à dépolarisation : il correspond à une probabilité p de garder le qubit inchangé et $1-p$ de perdre l'information, néanmoins sans le savoir (contrairement au canal à effacement standard). On a :

$$\mathcal{E}(\rho) = p\rho + (1-p)\frac{I}{2}$$

Comme $I = \frac{1}{2}(\rho + X\rho X + Y\rho Y + Z\rho Z)$ on peut aussi écrire :

$$\mathcal{E}(\rho) = \frac{1+3p}{4}\rho + (1-p)\frac{1}{4}(X\rho X + Y\rho Y + Z\rho Z)$$

C'est-à-dire une probabilité $\frac{1-p}{4}$ d'appliquer X, Y ou Z .

Géométriquement cela correspond à une contraction isotrope de la sphère de Bloch.

- Canal à effacement : correspond à une probabilité $1-p$ de perdre le qubit sur un état orthogonal $|2\rangle$ à $|0\rangle, |1\rangle$. On peut alors déterminer l'emplacement de l'erreur sans modifier l'état du qubit en mesurant selon $|2\rangle$. On a :

$$\mathcal{E}(\rho) = p\rho + (1-p)|2\rangle \langle 2|$$

Contrairement à la dépolarisation il est alors possible de vérifier si il y a eu une erreur sans modifier l'état.

De plus on a souvent la probabilité de transmettre correctement le message qui décroît de manière exponentielle avec la longueur (par exemple si les qubits sont des photons transmis à travers une fibre optique). On modélise donc le canal de longueur L par un canal à effacement

avec $p = e^{-\alpha L}$ où $1/\alpha$ est la longueur caractéristique de transmission (typiquement pour une fibre optique $1/\alpha = 25km$ [11]). De même pour les mémoires quantiques où le paramètre p dépend du temps.

En plus du canal quantique on s'autorisera l'envoi de messages classiques (et supposés non bruités) entre les deux extrémités de celui-ci (Alice et Bob), cette information mettant un temps $\frac{L}{c}$ proportionnel à la longueur du canal physique à être transmise. On distingue de plus les communications classiques dans les deux sens (de Alice vers Bob et Bob vers Alice) utilisées par exemple pour certains protocoles de purification et les communications classiques à sens unique, typiquement dans le cas des mémoires quantiques (car la longueur étant remplacée par le temps, il n'est possible d'envoyer de l'information que vers des instants ultérieurs).

1.3 Comparaison d'états

1.3.1 Indistinguabilité et théorème de non clonage

Étant donné deux états $|\phi\rangle$ et $|\psi\rangle$ du même système on peut se demander s'il est possible de les distinguer. S'ils sont orthogonaux alors il suffit d'effectuer une mesure selon la base adaptée, mais cela n'est plus possible avec certitude dès que les états ne sont plus orthogonaux.

Ce résultat est relié au théorème de non clonage quantique qui affirme qu'il est impossible de concevoir un processus prenant en entrée $|\psi\rangle$ et retournant $|\psi\rangle \otimes |\psi\rangle$ pour tout $|\psi\rangle$.

En effet si un tel processus existe alors quitte à purifier il peut se mettre sous la forme d'une opération unitaire prenant en entrée $|i\rangle \otimes |\psi\rangle$ et en sortie $|f_\psi\rangle \otimes |\psi\rangle |\psi\rangle$. Alors comme ce résultat est valable pour tout état on a :

$$\begin{cases} U |i\rangle |\psi\rangle = |f_\psi\rangle |\psi\rangle |\psi\rangle \\ U |i\rangle |\phi\rangle = |f_\phi\rangle |\phi\rangle |\phi\rangle \end{cases}$$

Et comme U est unitaire on obtient :

$$\langle i|i\rangle \langle \phi|\psi\rangle = \langle f_\phi|f_\psi\rangle \langle \phi|\psi\rangle^2$$

Ce qui n'est possible ssi $|\psi\rangle = |\phi\rangle$ (à une phase près) ou bien s'ils sont orthogonaux. Il est donc impossible de construire un tel dispositif fonctionnant pour tous les états (cela reste possible pour un nombre fini d'états mutuellement orthogonaux, par exemple CNOT).

Ce résultat est équivalent à l'impossibilité de distinguer complètement deux états non orthogonaux. En effet si on pouvait déterminer un état pour dupliquer il suffit de déterminer l'état puis de le construire en double et réciproquement s'il était possible de dupliquer un état en fabriquant à partir de $|\psi\rangle$ et $|\phi\rangle$ les états $|\psi\rangle^{\otimes n}$ et $|\phi\rangle^{\otimes n}$ on peut distinguer les deux états car pour n grand $\langle \phi|^{\otimes n} |\psi\rangle^{\otimes n}$ tend vers 0.

1.3.2 Fidélité et théorème de Uhlmann

De manière générale on définit la fidélité entre deux états ρ et σ par :

$$F(\rho, \sigma) = \text{tr} \left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} \right)$$

avec $\sqrt{\bullet}$ la racine carrée définie positive.

Si on a un des deux états qui est pur alors on a :

$$F(|\psi\rangle \langle \psi|, \rho) = \text{tr} \left(\sqrt{|\psi\rangle \langle \psi| \rho |\psi\rangle \langle \psi|} \right) = \text{tr}(\sqrt{\langle \psi|\rho|\psi\rangle |\psi\rangle \langle \psi|}) = \sqrt{\langle \psi|\rho|\psi\rangle}$$

Ce qui correspond bien pour deux états purs à "l'angle" entre ces deux états : $F(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = |\langle\psi|\phi\rangle|$.

De cette définition on tire par exemple facilement le fait que la fidélité est invariante par transformation unitaire c'est-à-dire que :

$$F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma)$$

De plus le théorème de Uhlmann apporte une caractérisation permettant de mieux comprendre la fidélité :

Si ρ et σ sont deux états d'un système A alors on a :

$$F(\rho, \sigma) = \max_{|\psi\rangle, |\phi\rangle} |\langle\psi|\phi\rangle|$$

où le maximum est pris sur l'ensemble des purifications $|\psi\rangle$ et $|\phi\rangle$ de ρ et σ .

En effet soient $|\psi\rangle$ et $|\phi\rangle$ deux telles purifications. On écrit la décomposition de Schmidt :

$$|\psi\rangle = \sum_i \sqrt{\lambda_i} |i_A\rangle |i_R\rangle$$

comme

$$\rho = \text{tr}_R(|\psi\rangle\langle\psi|) = \sum_i \lambda_i |i_A\rangle\langle i_A|$$

On obtient :

$$|\psi\rangle = (\sqrt{\rho} \otimes 1_R) \sum_i |i_A\rangle |i_R\rangle$$

Et de même on a :

$$|\phi\rangle = (\sqrt{\sigma} \otimes 1_R) \sum_i |i'_A\rangle |i'_R\rangle = (\sqrt{\sigma} U_A \otimes U_R) \sum_i |i_A\rangle |i_R\rangle$$

avec U_A et U_R des matrices unitaires.

On a donc :

$$\begin{aligned} \langle\phi|\psi\rangle &= \sum_{i,j} \langle i_A | \langle i_R | \left(U_A^\dagger \sqrt{\sigma} \sqrt{\rho} \otimes U_R^\dagger \right) | j_A \rangle | j_R \rangle = \sum_{i,j} \langle i_A | U_A^\dagger \sqrt{\sigma} \sqrt{\rho} | j_A \rangle \langle j_R | U_R | i_R \rangle^* \\ &= \text{tr}(U_A^\dagger \sqrt{\sigma} \sqrt{\rho} U_R) = \text{tr}(\sqrt{\sigma} \sqrt{\rho} (U_A U_R^\dagger)^\dagger) \end{aligned}$$

Et par Cauchy-Schwarz :

$$\begin{aligned} \left| \text{tr}(\sqrt{\sigma} \sqrt{\rho} (U_A U_R^\dagger)^\dagger) \right| &= \left| \text{tr} \left(\sqrt{\sqrt{\sigma} \sqrt{\rho}} \sqrt{\sqrt{\sigma} \sqrt{\rho}} (U_A U_R^\dagger)^\dagger \right) \right| \\ &\leq \sqrt{\text{tr} \left(\left(\sqrt{\sqrt{\sigma} \sqrt{\rho}} \right) \left(\sqrt{\sqrt{\sigma} \sqrt{\rho}} \right)^\dagger \right) \text{tr} \left(\left(\sqrt{\sqrt{\sigma} \sqrt{\rho}} (U_A U_R^\dagger)^\dagger \right) \left(\sqrt{\sqrt{\sigma} \sqrt{\rho}} (U_A U_R^\dagger)^\dagger \right)^\dagger \right)} \\ &= \text{tr} \left(\sqrt{\sqrt{\sigma} \sqrt{\rho} \sqrt{\sigma}} \right) \end{aligned}$$

ce qui donne bien le résultat recherché.

La fidélité mesure la proximité entre deux états quantiques et possède les propriétés suivantes :

- Du théorème de Uhlmann on déduit que $0 \leq F(\sigma, \rho) \leq 1$ avec égalité à gauche ssi les purifications sont toutes orthogonales c'est-à-dire ρ et σ sont à supports orthogonaux et égalité à droite ssi ils admettent une purification commune c'est-à-dire $\rho = \sigma$.
- La fidélité est augmentée par un canal quantique :

$$F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq F(\rho, \sigma)$$

- Elle est reliée à la distance $D(\rho, \sigma) = |\text{tr}(\rho - \sigma)|$ par :

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}$$

ce qui explique pourquoi on peut utiliser les deux pour mesurer la proximité des états.

- On peut montrer que la fidélité est fortement concave c'est-à-dire :

$$F\left(\sum_i p_i \rho_i, \sum_i q_i \sigma_i\right) \geq \sqrt{p_i q_i} F(\rho_i, \sigma_i)$$

si on définit alors la fidélité d'un canal comme :

$$\min_{\rho} F(\rho, \mathcal{E}(\rho))$$

comme $F(\sum \lambda_i |i\rangle \langle i|, \sum \lambda_i \mathcal{E}(|i\rangle \langle i|)) \geq \sum \lambda_i F(|i\rangle \langle i|, \mathcal{E}(|i\rangle \langle i|))$ on voit que le minimum peut être pris sur les états purs, ce que l'on fera désormais.

1.4 Entropie

1.4.1 Entropie de Shannon

Étant donnée une variable aléatoire X de distribution de probabilité p_1, \dots, p_n on définit son entropie de Shannon par :

$$H(X) = - \sum_i p_i \log(p_i)$$

En particulier si on a uniquement deux résultats possibles avec probabilités respectives p et $1 - p$ on notera :

$$H(p) = -p \log(p) - (1 - p) \log(1 - p)$$

L'entropie mesure le manque d'information sur le système ou d'un autre point de vue quantifie l'information gagnée sur l'état de celui-ci après une mesure, ainsi si l'état du système est certain $p = 1$ et l'entropie est nulle tandis qu'elle est maximale pour les p_i égaux.

Si X et Y ont pour distributions de probabilités (p_i) et (q_i) on définit ensuite l'entropie relative par :

$$H(X||Y) = \sum_i p_i \log(p_i) - \sum_i p_i \log(q_i)$$

On définit ensuite l'entropie jointe de X et Y suivant :

$$H(X, Y) = - \sum_{i,j} p_{i,j} \log(p_{i,j})$$

avec $p_{i,j}$ la probabilité d'avoir X dans l'état i et Y dans l'état j , puis l'entropie conditionnelle de X sachant Y comme

$$H(X|Y) = H(X, Y) - H(Y)$$

qui représente l'incertitude sur X sachant la valeur de Y ainsi que l'information mutuelle

$$H(X : Y) = H(X) + H(Y) - H(X, Y)$$

qui représente l'information que X et Y ont en commun.

On peut montrer les propriétés suivantes qui sont intuitives du point de vue de l'interprétation en terme d'incertitude :

- $H(Y|X) \geq 0$ d'où $H(X : Y) \leq H(Y)$ avec égalité ssi Y est une fonction de X ainsi que $H(X, Y) \geq H(X)$ (avec le même cas d'égalité).
- $H(X, Y) \leq H(X) + H(Y)$ et donc $H(Y|X) \leq H(Y)$ ainsi que $H(X : Y) \geq 0$ avec égalité ssi X et Y sont des variables indépendantes.

L'entropie joue un rôle important en théorie de l'information et du codage à travers par exemple le théorème de Shannon relatif aux codes correcteurs d'erreurs classique (cf 2.1.1).

1.4.2 Entropie de von Neumann

De même que pour une distribution d'états classiques on définit une entropie de Shannon associée, pour une distribution d'états quantiques représentée par la matrice densité ρ on définit l'entropie de von Neumann par :

$$S(\rho) = -\text{tr}(\rho \log(\rho))$$

Si on diagonalise $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$ avec les $|\psi_i\rangle$ orthogonaux, on obtient bien l'entropie de Shannon associée :

$$S\left(\sum_i p_i |\psi_i\rangle \langle \psi_i|\right) = H((p_i))$$

ce qui était prévisible car si les états sont mutuellement orthogonaux alors ils sont parfaitement distinguables et peuvent être traités comme des états classiques.

Mais si on a par exemple une probabilité p d'avoir $|0\rangle$ et $1-p$ d'avoir l'état $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ alors l'entropie associée n'est pas l'entropie binaire $H(p)$, en effet si on diagonalise on obtient comme valeurs propres $\frac{1}{2} \left(1 \pm \sqrt{2p^2 - 2p + 1}\right)$ d'où l'entropie est $H\left(\frac{1}{2} \left(1 + \sqrt{2p^2 - 2p + 1}\right)\right)$

De même que dans le cas classique on peut définir :

- L'entropie relative $S(\rho||\sigma) = \text{tr}(\rho \log(\rho)) - \text{tr}(\rho \log(\sigma))$.
- L'entropie jointe de deux systèmes : $S(A, B) = -\text{tr}(\rho^{AB} \log(\rho^{AB}))$.
- L'entropie conditionnelle $S(A|B) = S(A, B) - S(A)$.
- L'information mutuelle $S(A : B) = S(A) + S(B) - S(A, B)$.

On peut de même que dans le cas classique interpréter ces définitions et énoncer un certain nombre de propriétés ([12]). Mais certaines propriétés sont fausses, notamment si A et B sont intriqués, alors $S(A|B) < 0$, c'est-à-dire que la connaissance de l'état de B apporte de l'information supplémentaire sur l'état de A .

2 Codes correcteurs d'erreur

2.1 Généralités sur les codes correcteurs quantique

2.1.1 Codes classiques

Dans le cas classique on définit un code correcteur \mathcal{C} de M mots de longueur n sur le corps \mathbb{F}_q comme un sous-ensemble de \mathbb{F}_q^n . On munit \mathbb{F}_q^n de la distance de Hamming :

$$d(x, y) = |\{i \text{ tq } x_i \neq y_i\}|$$

La distance minimale d'un code est alors $\min_{x, y \in \mathcal{C}} d(x, y)$.

Le schéma de transmission de l'information codée est alors le suivant :

- L'émetteur transmet un message x^i , $i \in \{1, \dots, n\}$ avec une probabilité p_i .
- Au cours de la transmission une erreur peut se produire transformant x_i en y , par exemple chacun des n caractères composant x^i a une probabilité $1 - p$ d'être erroné de manière indépendante des autres.
- Le récepteur reçoit le message y et tente d'en déduire x^i . Pour cela une méthode est de chercher le mot de \mathcal{C} le plus proche de y c'est-à-dire le j minimisant $d(y, x^j)$.

Suivant cette procédure on en déduit donc que la distance minimale d'un code permet de quantifier le nombre d'erreurs pouvant être corrigées : un code ayant une distance minimale d peut corriger $\lfloor \frac{d-1}{2} \rfloor$ erreurs (et en détecter $\lfloor \frac{d}{2} \rfloor$) car les sphères de rayon $\lfloor \frac{d-1}{2} \rfloor$ et de centres les mots de \mathcal{C} sont deux à deux disjointes.

Un exemple typique est le code à répétition, qui consiste à prendre (sur $\mathbb{Z}/2\mathbb{Z}$ mais plus généralement sur tout \mathcal{F}_q) comme code $\{000, 111\}$ qui permet de coder un bit logique.

Si le récepteur reçoit 010 par exemple il en déduit alors que le message envoyé était 000 car $d(000, 010) = 1$ tandis que $d(111, 010) = 2$.

Cela permet bien d'augmenter la probabilité de recevoir correctement un bit logique : si la probabilité de transmettre correctement un caractère est p alors la probabilité que le mot déduit par le récepteur soit bien celui envoyé par l'émetteur est de $p^3 + 3p^2(1-p) < p$ pour $p < 1/2$.

Une question qui se pose alors est de savoir quelle est la longueur n nécessaire à un code de M éléments pour atteindre une certaine probabilité d'erreur.

On définit le taux d'un code par $R = \frac{1}{n} \log_q(|\mathcal{C}|)$.

D'après un théorème de Shannon ([17]) il est possible de faire tendre la probabilité d'erreur vers 0 dans la limite de n grand et ce à taux fixé, étant donné que celui-ci est inférieur à ce qu'on appelle la capacité du canal.

Dans le cas d'un canal où la probabilité d'erreur sur un bit est de $1 - p$ il s'énonce de la manière suivante :

Soit P_C la probabilité de décodage incorrect pour un code \mathcal{C} et $P^*(M, n) = \min P_C$ sur l'ensemble des codes de longueur n possédant M mots. Alors si :

$$R < 1 + p \log(p) + (1 - p) \log(1 - p)$$

on a $P^*(2^{\lfloor Rn \rfloor}, n) \rightarrow 0$ quand $n \rightarrow \infty$. (De manière plus générale le théorème de Shannon affirme que la capacité est $\max_X H(X : \mathcal{E}(X))$ avec $\mathcal{E}(X)$ la variable correspondant au passage de X par le canal).

Mais le théorème de Shannon ne donne qu'un résultat asymptotique sans expliciter les codes atteignant la borne. On peut donc s'intéresser à des réalisations particulières de codes correcteurs,

une d'entre elles étant les codes linéaires où \mathcal{C} est un sous espace vectoriel de \mathbb{F}_q . Si le sous espace est de dimension k on parle de $[n, k]$ -code linéaire.

On définit alors la matrice génératrice comme étant la matrice dont les lignes sont une base de \mathcal{C} . Les mots du code sont alors les aG avec a des vecteurs lignes.

On définit ensuite le code dual \mathcal{C}^\perp par :

$$\mathcal{C}^\perp = \{y \in \mathbb{F}_q^n \text{ tel que } \forall x \in \mathcal{C} \langle x, y \rangle = 0\}$$

Il s'agit d'un $[n, n - k]$ code linéaire, et en notant H sa matrice génératrice (appelé aussi matrice parité de \mathcal{C}) on a la caractérisation suivante :

$$x \in \mathcal{C} \leftrightarrow xH^t = 0$$

On définit alors le syndrome d'un mot reçu y par yH^t .

Un des avantages de ces codes est que le décodage se fait de manière beaucoup plus facile à travers la mesure d'un syndrome, en effet si on a $y = x + e$ avec e on a le syndrome de y est eH^t . Chaque syndrome définit donc un sous espace affine et il suffit ensuite de choisir un mot de poids minimal dans ce sous espace.

Il est possible de trouver des bornes sur M à n et d fixés ([17]), mais la plupart d'entre elles n'ont pas d'équivalent quantique direct.

2.1.2 Particularités du cas quantique

De même que dans le cas classique un code correcteur quantique utilise une procédure de codage/transmission imparfaite/décodage afin de réduire l'erreur par rapport à la même transmission sans codage au prix d'un accroissement de la taille (dans le cas quantique la dimension) des messages envoyés. On s'intéressera principalement à la transmission d'un seul qubit logique c'est-à-dire à des espaces de dimension 2.

Mais plusieurs particularités du cas quantique rendent impossible l'adaptation directe des stratégies classiques :

- Tout d'abord la structure du qubit est différente de celle du bit classique, alors que dans le cas classique il faut transmettre un 0 ou un 1 dans le cas quantique c'est un état de la forme $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ c'est-à-dire deux nombres complexes.
- De plus du fait du caractère unitaire certaines opérations classiques sont impossibles à réaliser de manière quantique, par exemple à cause du théorème de non clonage il est impossible d'implémenter un code à répétition qui transforme $|\psi\rangle$ en $|\psi\rangle|\psi\rangle|\psi\rangle$. À cela s'ajoute l'impossibilité de mesurer directement les états car toute mesure conduit à l'altération de cet état de manière irréversible.
- Enfin les erreurs quantiques possibles sont plus nombreuses que celles classiques. Tandis que classiquement une erreur sur un bit est une interversion $0 \leftrightarrow 1$, une erreur sur un qubit peut être n'importe quelle rotation de SU_2 .

Néanmoins il est tout de même possible de concevoir des codes correcteurs d'erreur quantique. Pour cela on utilise de même que dans les codes linéaires une méthode de mesure de syndrome qui permet de corriger n'importe quelle erreur du moment qu'un nombre fini d'erreurs peut être corrigé : l'effet d'un canal est de la forme $\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_k E_k |\psi\rangle\langle\psi| E_k^\dagger$, et si on suppose que les erreurs sur chaque qubit sont indépendantes alors l'effet de E_k sur le i -ième qubit est de la forme $a_1I + a_2X + a_3Z + a_4XZ$. D'où si on mesure le syndrome correspondant aux erreurs X et Z , on projette $E_k |\psi\rangle$ sur l'une de ces erreurs ce qui permet ensuite de corriger l'état, il s'agit de la discrétisation des erreurs quantiques qui explique pourquoi on s'intéressera désormais uniquement aux erreurs d'inversion X et de phase Z .

2.1.3 Exemple : le code à 3 qubits et le code de Shor

Le code classique le plus simple étant le code à répétition on peut s'intéresser à son équivalent quantique : même si par le théorème de non clonage il est impossible de répéter un même état on peut comme $|0\rangle$ et $|1\rangle$ sont orthogonaux considérer l'opération qui consiste à coder $|0\rangle$ par $|0\rangle^{\otimes 3}$ et $|1\rangle$ par $|1\rangle^{\otimes 3}$, d'où $\alpha|0\rangle + \beta|1\rangle$ donne $\alpha|000\rangle + \beta|111\rangle$ constituant ainsi un code à trois qubits (il ne s'agit pas d'un code quantique à proprement parler puisqu'il ne corrige pas les erreurs de phase Z mais permet de mettre en évidence les points évoqués précédemment).

Après la transmission on effectue la mesure de syndrome ce qui projette l'état sur l'un des sevs de dimension 2 correspondant respectivement à une erreur X sur le qubit 1, 2 ou 3 ou bien à aucune erreur, les projections commutant deux à deux correspondantes étant :

$$\begin{cases} P_1 = |100\rangle\langle 100| + |011\rangle\langle 011| \\ P_2 = |010\rangle\langle 010| + |101\rangle\langle 101| \\ P_3 = |001\rangle\langle 001| + |110\rangle\langle 110| \\ P_0 = |000\rangle\langle 000| + |111\rangle\langle 111| \end{cases}$$

Et on a donc bien via cette projection une discrétisation des erreurs.

On peut de plus calculer explicitement la fidélité résultant de l'utilisation de ce code étant donné un canal $\mathcal{E}(\rho) = p\rho + (1-p)X\rho X$ (dans ce cas ne se pose même pas le problème de la discrétisation).

Sans codage :

$$F = \sqrt{\langle \psi | (p|\psi\rangle\langle \psi| + (1-p)X|\psi\rangle\langle \psi|X) | \psi \rangle} \geq \sqrt{p}$$

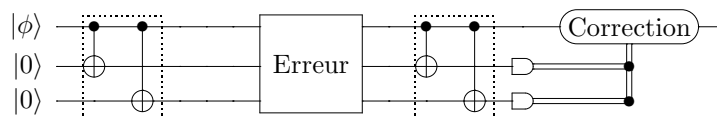
et avec codage comme une erreur est corrigée tandis que deux erreurs entraînent un syndrome indiquant une erreur sur le qubit restant, on a :

$$\mathcal{R} \circ \mathcal{E}(\rho) = (p^3 + 3p^2(1-p))\rho + (3p(1-p)^2 + (1-p)^3)X_1X_2X_3\rho X_1X_2X_3$$

et donc la fidélité est d'au moins :

$$F_{\text{codage}} = \sqrt{p^3 + 3p^2(1-p)} > \sqrt{p} \text{ dès que } p > 1/2$$

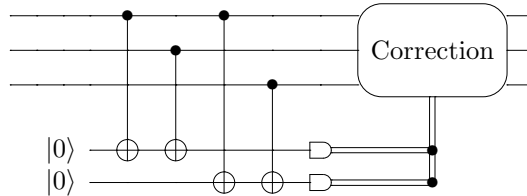
En termes de circuits quantiques il y a plusieurs moyens d'implémenter un tel code : la première méthode consiste à utiliser une transformation unitaire pour le codage puis son inverse pour le décodage (moins facilement généralisable mais utilisé dans 4.4) :



- On part d'un état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ à coder ainsi que deux états auxiliaires que l'on prend égaux à $|0\rangle$.
- Grâce à deux portes CNOT on transforme l'état en $\alpha|000\rangle + \beta|111\rangle$.
- On transmet cet état à travers un canal quantique où peut se produire une erreur. On suppose par exemple qu'il se produit une erreur sur le deuxième qubit (erreur avec une probabilité $(3p^2(1-p))$). L'état est donc $\alpha|010\rangle + \beta|101\rangle$.
- On applique la transformation unitaire inverse à travers deux portes CNOT ce qui donne $\alpha|010\rangle + \beta|110\rangle = |\psi\rangle|1\rangle|0\rangle$.

- On mesure selon la base canonique les deux qubits correspondants aux syndromes. On obtient 1 et 0 ce qui correspond bien à une erreur sur le deuxième qubit.
- On effectue donc une opération I sur le premier qubit et on obtient donc $|\psi\rangle$

Une autre méthode qui se généralise aisément aux codes stabilisateurs (dont le code à 3 qubits fait partie) consiste à mesurer les syndromes grâce à des qubits auxiliaires. À la différence du premier cas la correction ne se fait pas sur un qubit physique décodé mais directement sur le qubit logique :



- Le qubit est d'abord codé par une transformation unitaire similaire au cas précédent donnant $\alpha|000\rangle + \beta|111\rangle$.
- Il peut alors se produire des erreurs donnant par exemple une erreur sur le deuxième donnant $\alpha|010\rangle + \beta|101\rangle$.
- A l'aide de qubits auxiliaires on mesure les syndromes qui donnent 1 et 0.
- On applique donc l'opération X_2 qui donne bien finalement $\alpha|000\rangle + \beta|111\rangle$.

À partir de ce code on peut concevoir un véritable code quantique à 9 qubits, le code de Shor (qui est historiquement le premier véritable code correcteur d'erreur quantique proposé). En effet il suffit de remarquer que pour corriger une erreur Z on peut prendre la version du code à 3 qubits suivante :

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

qui consiste à remplacer simplement $|0\rangle$ et $|1\rangle$ par $\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$ qui sont intervertis par l'opération Z .

En combinant les deux codes c'est-à-dire remplaçant dans le code corrigeant Z $|0\rangle$ et $|1\rangle$ par $|0_L\rangle$ et $|1_L\rangle$ du code corrigeant X on obtient :

$$\begin{cases} |0\rangle \longrightarrow \frac{|000\rangle + |111\rangle}{\sqrt{2}} \frac{|000\rangle + |111\rangle}{\sqrt{2}} \frac{|000\rangle + |111\rangle}{\sqrt{2}} \\ |1\rangle \longrightarrow \frac{|000\rangle - |111\rangle}{\sqrt{2}} \frac{|000\rangle - |111\rangle}{\sqrt{2}} \frac{|000\rangle - |111\rangle}{\sqrt{2}} \end{cases}$$

qui corrige bien n'importe quelle erreur X ou Z et donc par discrétisation une erreur quelconque.

2.1.4 Correction des effacements

On a jusqu'ici considéré des erreurs qui envoient le qubit sur un autre état du système à deux niveaux. Mais de même que dans le cas classique il peut se produire des effacements, modélisés par la transformation envoyant sur un état $|2\rangle$ orthogonal à $|0\rangle$ et $|1\rangle$. En remplaçant cet état $|2\rangle$ par un état quelconque, par exemple $|0\rangle$ on voit que tous les protocoles de correction proposés précédemment fonctionnent aussi dans ce cas.

Mais on peut aussi concevoir des codes adaptés à ce type d'erreur qui présente l'avantage de pouvoir déterminer l'emplacement des erreurs (il suffit prendre comme projecteurs $|2\rangle\langle 2|$ et $|0\rangle\langle 0| + |1\rangle\langle 1|$).

Un exemple est notamment le code utilisé dans le protocole de [11], on remplace $\alpha|0\rangle + \beta|1\rangle$ par :

$$\alpha \left(\frac{|0\rangle^{\otimes m} + |1\rangle^{\otimes m}}{\sqrt{2}} \right)^{\otimes n} + \beta \left(\frac{|0\rangle^{\otimes m} - |1\rangle^{\otimes m}}{\sqrt{2}} \right)^{\otimes n}$$

Un effacement sur le qubit i s'écrit :

$$\mathcal{E}(\rho) = \text{tr}_i(\rho) |2_i\rangle\langle 2_i|$$

Qui donne :

$$\left\{ \begin{array}{l} \frac{|0\rangle^{\otimes m} \pm |1\rangle^{\otimes m}}{\sqrt{2}} \frac{\langle 0|^{\otimes m} \pm \langle 1|^{\otimes m}}{\sqrt{2}} \rightarrow \frac{|0\rangle^{\otimes(m-1)} \langle 0|^{\otimes(m-1)} + |1\rangle^{\otimes(m-1)} \langle 1|^{\otimes(m-1)}}{2} |2\rangle\langle 2| \\ \frac{|0\rangle^{\otimes m} \pm |1\rangle^{\otimes m}}{\sqrt{2}} \frac{\langle 0|^{\otimes m} \mp \langle 1|^{\otimes m}}{\sqrt{2}} \rightarrow \frac{|0\rangle^{\otimes(m-1)} \langle 0|^{\otimes(m-1)} - |1\rangle^{\otimes(m-1)} \langle 1|^{\otimes(m-1)}}{2} |2\rangle\langle 2| \end{array} \right.$$

En mesurant ensuite selon la base canonique les qubits restants on obtient donc soit 0 et dans ce cas :

$$\left\{ \begin{array}{l} \frac{|0\rangle^{\otimes m} \pm |1\rangle^{\otimes m}}{\sqrt{2}} \frac{\langle 0|^{\otimes m} \pm \langle 1|^{\otimes m}}{\sqrt{2}} \rightarrow |0\rangle^{\otimes(m-1)} \langle 0|^{\otimes(m-1)} |2\rangle\langle 2| \\ \frac{|0\rangle^{\otimes m} \pm |1\rangle^{\otimes m}}{\sqrt{2}} \frac{\langle 0|^{\otimes m} \mp \langle 1|^{\otimes m}}{\sqrt{2}} \rightarrow |0\rangle^{\otimes(m-1)} \langle 0|^{\otimes(m-1)} |2\rangle\langle 2| \end{array} \right.$$

Soit 1 et dans ce cas :

$$\left\{ \begin{array}{l} \frac{|0\rangle^{\otimes m} \pm |1\rangle^{\otimes m}}{\sqrt{2}} \frac{\langle 0|^{\otimes m} \pm \langle 1|^{\otimes m}}{\sqrt{2}} \rightarrow |1\rangle^{\otimes(m-1)} \langle 1|^{\otimes(m-1)} |2\rangle\langle 2| \\ \frac{|0\rangle^{\otimes m} \pm |1\rangle^{\otimes m}}{\sqrt{2}} \frac{\langle 0|^{\otimes m} \mp \langle 1|^{\otimes m}}{\sqrt{2}} \rightarrow -|1\rangle^{\otimes(m-1)} \langle 1|^{\otimes(m-1)} |2\rangle\langle 2| \end{array} \right.$$

De même tant qu'il y a moins de m effacements n mesurant les qubits restants selon la base canonique on obtient $|0\rangle^{\otimes(m-k)} \langle 0|^{\otimes(m-k)}$ et $\pm |1\rangle^{\otimes(m-k)} \langle 1|^{\otimes(m-k)}$.

Si on suppose que nN blocs parmi n n'ont aucun de leurs m qubits effacés alors le résultat final est :

$$\begin{aligned} |\alpha|^2 \left(\frac{|0\rangle^{\otimes m} + |1\rangle^{\otimes m}}{\sqrt{2}} \frac{\langle 0|^{\otimes m} + \langle 1|^{\otimes m}}{\sqrt{2}} \right)^{\otimes N} &+ |\beta|^2 \left(\frac{|0\rangle^{\otimes m} - |1\rangle^{\otimes m}}{\sqrt{2}} \frac{\langle 0|^{\otimes m} - \langle 1|^{\otimes m}}{\sqrt{2}} \right)^{\otimes N} \\ &+ (-1)^{k_1} \alpha \beta^* \left(\frac{|0\rangle^{\otimes m} + |1\rangle^{\otimes m}}{\sqrt{2}} \frac{\langle 0|^{\otimes m} - \langle 1|^{\otimes m}}{\sqrt{2}} \right)^{\otimes N} \\ &+ (-1)^{k_1} \alpha^* \beta \left(\frac{|0\rangle^{\otimes m} - |1\rangle^{\otimes m}}{\sqrt{2}} \frac{\langle 0|^{\otimes m} + \langle 1|^{\otimes m}}{\sqrt{2}} \right)^{\otimes N} \end{aligned}$$

avec k_1 le nombre de mesures ayant donné 1 comme résultat. En appliquant $X^{\otimes m}$ dans le cas où k_1 est impair on obtient finalement :

$$\left(\alpha \left(\frac{|0\rangle^{\otimes m} + |1\rangle^{\otimes m}}{\sqrt{2}} \right)^{\otimes N} + \beta \left(\frac{|0\rangle^{\otimes m} - |1\rangle^{\otimes m}}{\sqrt{2}} \right)^{\otimes N} \right) \left(\alpha^* \left(\frac{\langle 0|^{\otimes m} + \langle 1|^{\otimes m}}{\sqrt{2}} \right)^{\otimes N} + \beta^* \left(\frac{\langle 0|^{\otimes m} - \langle 1|^{\otimes m}}{\sqrt{2}} \right)^{\otimes N} \right)$$

Un tel code fonctionne ssi parmi les n blocs de m qubits aucun bloc n'est totalement effacé et au moins un bloc ne contient aucun effacement.

Si $1 - p$ est la probabilité d'un effacement la probabilité de succès est alors de :

$$f(p, m, n) = (1 - (1 - p)^m)^n - (1 - p^m - (1 - p)^m)^n$$

en effet il y a une probabilité $(1 - (1 - p)^m)^n$ qu'aucun bloc de m qubits ne soit effacé et $(1 - p^m - (1 - p)^m)$ que ce soit le cas mais qu'aucun bloc soit intact.

On peut montrer par le raisonnement suivant que ce protocole n'améliore pas la capacité du canal si $p \leq 1/2$ (en particulier on garde $p \leq 1/2$ ce qui est nécessaire d'après 4.1.2).

En effet pour chaque configuration entrainant un décodage possible on associe la configuration obtenue en remplaçant le premier bloc intact (aucun qubit effacé) par un bloc totalement effacé. On obtient alors des configurations deux à deux distinctes et conduisant toutes à l'échec du protocole. De plus comme en faisant ainsi on a multiplié la probabilité d'apparition de la configuration par $\left(\frac{1-p}{p}\right)^m$ on a :

$$1 - f(p, m, n) \geq \left(\frac{1-p}{p}\right)^m f(p, m, n)$$

Et donc comme pour $p < 1/2$ on a $\left(\frac{1-p}{p}\right)^m \leq \frac{1-p}{p}$ on a indépendamment de m et n :

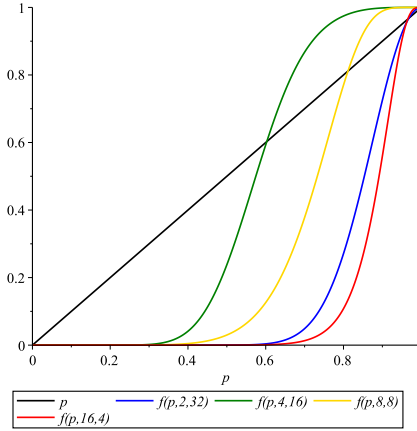
$$f(p, m, n) \leq \frac{1}{1 + \frac{1-p}{p}} = p$$

Il faut donc optimiser m et n à produit mn qui est la longueur du code fixée : si m est trop faible la probabilité d'avoir un bloc complètement effacé est élevée tandis que si m est trop élevée la probabilité d'avoir un bloc intact est faible.

En dérivant on obtient que le maximum à p fixé est obtenu le long de :

$$n = \frac{\ln\left(\frac{\ln(1-(1-p)^m)}{\ln(1-p^m-(1-p)^m)}\right)}{\ln(1-p^m-(1-p)^m) - \ln(1-(1-p)^m)}$$

De manière générale on peut calculer numériquement l'optimum à produit mn fixé, ainsi si on trace pour $mn = 64$ les différentes courbes :



2.2 Codes stabilisateurs

2.2.1 Formalisme général

L'idée générale du formalisme stabilisateur est le suivant : on définit un sous espace vectoriel \mathcal{C} de \mathcal{H} non plus par une base de ce sev mais par un ensemble d'opérateurs de Pauli qui commutent et stabilisant \mathcal{C} , c'est-à-dire on écrit :

$$\mathcal{C} = \bigcap_i \ker(A_i - 1)$$

L'ensemble \mathcal{G} des tels $A_i \in \mathcal{P}^n$ nommés stabilisateurs est un groupe (le groupe stabilisateur).

On voit réciproquement que tout groupe d'opérateurs de Pauli ne contenant pas -1 définit bien un tel sous espace. Un tel formalisme permet de simplifier l'étude des états : appliquer l'opérateur unitaire U revient à remplacer \mathcal{G} par UGU^\dagger ce qui redonne bien un groupe stabilisateur si U est dans le groupe de Clifford (ensemble des opérateurs unitaires laissant \mathcal{P}^n invariant). En effet on a $A_i |\psi\rangle = |\psi\rangle$ ssi $UA_iU^\dagger U|\psi\rangle = U|\psi\rangle$.

De même pour certaines mesures, dans le cas où le groupe stabilisateur définit un unique élément $|\psi\rangle$, si g est un opérateur de \mathcal{P}^n alors on a deux possibilités :

- g commute avec tous les éléments du groupe stabilisateur, dans ce cas $g|\psi\rangle = \pm|\psi\rangle$ et le résultat de la mesure est déterminé à l'avance.
- Sinon on peut se ramener au cas où g anticommute avec A_1 et commute avec les autres générateurs du groupe. On peut alors montrer ([12]) que la probabilité d'obtenir 1 ou -1 est de $1/2$ et que des générateurs de l'état obtenu après la mesure peut être obtenu en remplaçant A_1 par g .

Ainsi pour suivre l'évolution d'un état lors d'un calcul quantique il suffit d'actualiser à chaque étape son groupe stabilisateur ce qui requiert $O(n^2)$ si le groupe est de taille n , donnant ainsi le théorème de Gottesman-Knill selon lequel tout circuit quantique n'utilisant que des portes du groupe de Clifford est modélisable de manière classique en un temps polynomial.

Dans le cadre des codes correcteurs d'erreur on prend pour encoder un sous espace de dimension 2^k (dans la suite on s'intéresse à $k = 1$ correspondant à 1 qubit) avec n qubits physiques il faut donc $n - k$ générateurs indépendants.

Pour ces codes on définit donc A_1, A_2, \dots, A_{n-1} générateurs ainsi qu'un opérateur \tilde{Z} qui est indépendant et commute avec les générateurs (de manière générale pour un espace de dimension supérieure $A_1, \dots, A_{n-k}, \tilde{Z}_1, \dots, \tilde{Z}_k$), la base logique étant alors :

$$\begin{cases} |0_L\rangle \text{ stabilisé par } A_1, \dots, A_{n-1}, \tilde{Z} \\ |1_L\rangle \text{ stabilisé par } A_1, \dots, A_{n-1}, -\tilde{Z} \end{cases}$$

(et de manière plus générale $A_1, \dots, A_{n-k}, \pm\tilde{Z}_1, \dots, \pm\tilde{Z}_k$)

Il y a alors trois types d'erreurs possibles (on considère uniquement le cas où les erreurs sont dans \mathcal{P}^n car on s'y ramène par discrétisation).

- L'erreur est dans le groupe stabilisateur et donc ne modifie pas l'état.
- L'erreur anticommute avec un certain nombre de générateurs, alors par une mesure de syndromes on peut la détecter et la corriger.
- L'erreur commute avec le groupe stabilisateur mais n'y appartient pas c'est-à-dire appartient à $N(\mathcal{G}) \setminus \mathcal{G}$. Dans ce cas on ne peut pas corriger l'erreur.

On définit alors le poids d'une erreur comme le nombre de termes dans le produit tensoriel de n termes qui ne sont pas égaux à l'identité, la distance minimale étant donc le poids minimal des éléments de $N(\mathcal{G}) \setminus \mathcal{G}$ (et de même que dans le cas classique on peut alors corriger $\lfloor \frac{d}{2} \rfloor$ erreurs).

On peut aussi voir les codes stabilisateurs d'une autre manière (utile notamment pour la purification). On a $A_1, \dots, A_{n-1}, \tilde{Z}$ est un ensemble complet d'observables qui commutent et il s'agit alors de faire un changement de la base canonique vers la base associée, en particulier :

$$\begin{cases} |0_L\rangle = |0'\rangle \otimes |0' \dots 0'\rangle \\ |1_L\rangle = |1'\rangle \otimes |0' \dots 0'\rangle \end{cases}$$

les erreurs se transformant alors en erreurs X_i que l'on peut détecter et corriger (cf 4.4).

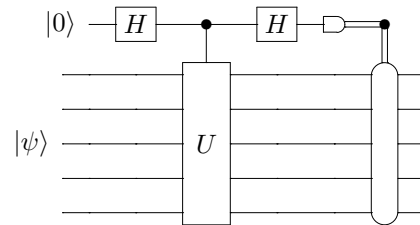
2.2.2 Réalisation des codes stabilisateurs

La construction se fait plus précisément de la manière suivante :

- Pour coder il suffit de projeter $|0/1\rangle \otimes |0 \dots 0\rangle$ sur $|0_L/1_L\rangle$.
- Pour une erreur E du groupe de Pauli on a pour tout A_i , $A_i E = (-1)^{k_i} E A_i$ d'où $A_i E |\psi_L\rangle = (-1)^{k_i} E |\psi_L\rangle$. En mesurant selon A_i on obtient donc la valeur de k_i qui est le syndrome recherché.
- Une fois les syndromes connus on effectue une l'opération de correction.

Si l'erreur appartient à $N(\mathcal{G}) \setminus \mathcal{G}$ ou bien que les syndromes donnent une mauvaise erreur (c'est-à-dire que l'erreur a un poids trop important) alors il se produit une erreur au niveau logique c'est-à-dire dans la base $|0_L\rangle, |1_L\rangle$.

Les seules opérations nécessaires sont les mesures selon les sous espaces propres des A_i qui peuvent se réaliser en pratique à l'aide de portes élémentaires, la projection sur un sous espace propre de U s'effectuant de la manière suivante :



- On utilise un qubit auxiliaire $|0\rangle$ que l'on fait passer par une porte de Hadamard, l'état est alors de $\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |\psi\rangle$
- On effectue une porte U contrôlée par le qubit auxiliaire conduisant à :

$$\frac{1}{\sqrt{2}} (|0\rangle |\psi\rangle + |1\rangle U |\psi\rangle)$$

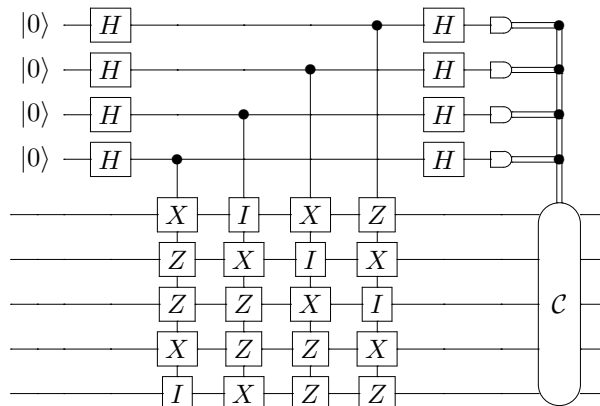
- On effectue de nouveau une porte de Hadamard sur le qubit auxiliaire ce qui donne :

$$\frac{1}{\sqrt{2}} \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} |\psi\rangle + \frac{|0\rangle-|1\rangle}{\sqrt{2}} U |\psi\rangle \right) = |0\rangle \frac{|\psi\rangle+U|\psi\rangle}{2} + |1\rangle \frac{|\psi\rangle-U|\psi\rangle}{2}$$

- On mesure ensuite le qubit auxiliaire.
 - Si on obtient 0 (avec probabilité $\left| \frac{|\psi\rangle+U|\psi\rangle}{2} \right|^2$) on ne fait rien.
 - Si on obtient 1 (avec probabilité $\left| \frac{|\psi\rangle-U|\psi\rangle}{2} \right|^2$) il suffit d'effectuer un opérateur anti-commutant avec U pour obtenir aussi $1+U$.

Comme $\frac{1+U}{2}$ est le projecteur sur le sev propre de valeur propre 1 de U on obtient bien le résultat désiré.

Ainsi par exemple le circuit permettant d'encoder et de corriger le code à 5-qubits (le plus petit code permettant de corriger une erreur quelconque) est :



2.2.3 Exemples

Le code à trois qubits est un code stabilisateur : il s'agit du code stabilisé par le groupe engendré par ZIZ et ZZI (ce qui explique les circuits de codage et décodage) et a pour opérateur logique $\tilde{Z} = ZII$.

On obtient bien que toute erreur Z_i commute avec les générateurs et donc n'est pas corrigible tandis qu'une erreur X_i anticommute avec l'un deux ou les deux ce qui permet de la corriger.

Par exemple on a $IXI \times ZIZ = ZIZ \times IXI$ tandis que $IXI \times ZZI = -ZZIIXI$. La mesure selon ZZI et ZIZ donne alors +1 et -1 ce qui correspond bien aux syndromes d'une erreur sur le deuxième qubit. Un autre exemple de codes stabilisateurs est le code à 5 qubits dont on peut montrer qu'il s'agit du plus petit code corrigeant une erreur quelconque. Ses stabilisateurs sont : $XZZXI, IXZZX, XIXZZ, ZXIXZ$.

Un autre exemple est la famille des codes CSS (Calderbank, Shor, Steane) qui utilisent les codes classiques : on considère C_1 et C_2 des $[n, k_1]$ et $[n, k_2]$ codes linéaires avec $C_2 \subset C_1$ et tels que C_1 et C_2^\perp corrigent chacun t erreurs. On peut alors construire un $[n, k_1 - k_2]$ code quantique corrigeant t erreurs.

Les mots du code sont les éléments de C_2/C_1 plus précisément pour $x \in C_2$ on note :

$$|\bar{x}\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$$

avec $|x + y\rangle = |x_1 \oplus y_1\rangle \otimes \dots \otimes |x_n \oplus y_n\rangle$.

Si les erreurs X sont décrites par un e_1 possédant n composantes et les erreurs Z par e_2 , l'état après l'erreur devient :

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_2} |x + y + e_1\rangle$$

On utilise alors des qubits auxiliaires pour obtenir avec H_1 la matrice parité de C_1 :

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_2} |x + y + e_1\rangle |H_1(x + y + e_1)\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_2} |x + y + e_1\rangle |H_1 e_1\rangle$$

ce qui permet ensuite de corriger l'erreur e_1 . On utilise un procédé similaire pour corriger e_2 après avoir appliqué des portes de Hadamard (cf [12]).

Une autre des particularités des codes stabilisateurs (mais non exclusive à ceux-ci) est la possibilité d'effectuer facilement certaines opérations quantiques directement sur l'état encodé sans avoir à le décoder. Ainsi si on veut effectuer une opération du groupe de Clifford, plutôt que d'encoder, décoder, effectuer l'opération, puis ré-encoder il suffit d'appliquer les opérateurs logiques correspondants ([8]) (par exemple à la place de Z on applique \tilde{Z}). Même si on ne peut appliquer ainsi que des opérateurs de Clifford (et donc tout calcul ainsi effectué peut être fait classiquement en temps polynomial), cela est très utile dans le cadre de la tolérance à l'erreur : on dit qu'un ensemble d'opérations est tolérant à l'erreur si une erreur à l'entrée se traduit par au plus une erreur à la sortie, ce qui requiert une architecture particulière (cf [12]) pour éviter la propagation des erreurs, alors si on utilise ces circuits tolérants à l'erreur afin de corriger de nouveaux tels circuits de manière récursive, on obtient le théorème du seuil : si la probabilité d'erreur d'une porte élémentaire est de p , en effectuant la même opération sur un qubit logique de manière tolérante à l'erreur, la probabilité d'erreur devient au premier ordre cp^2 . Si on recommence le même schéma en remplaçant les portes élémentaires par celles que l'on vient d'obtenir on obtient $c(cp^2)^2$. En continuant ainsi on obtient $\frac{1}{c}(cp^2)^k$. Si $p < p_c = \frac{1}{c}$ il est alors possible d'effectuer avec une erreur arbitrairement faible n'importe quelle opération quantique, il s'agit du théorème du seuil (et de plus la taille du circuit nécessaire pour obtenir une erreur de ε est polynomiale en $\frac{1}{\varepsilon}$).

3 Répéteurs quantiques

Une alternative afin de transporter un qubit est d'utiliser la téléportation quantique : si Alice et Bob partagent un état de Bell alors, par des opérations locales ainsi que des communications classiques il peuvent échanger un qubit. Le problème devient alors celui de la distribution d'intrication entre les deux parties. En combinant permutations d'intrication qui permettent d'étendre la distance sur laquelle les états sont partagés et purification d'intrication qui permet d'augmenter la fidélité de l'intrication au prix de ressources physiques, on aboutit alors aux protocoles des répéteurs quantiques qui se traduisent notamment par des coûts polynomiaux en ressources et possédant des seuils intéressants, mais nécessitant l'usage de mémoires quantiques.

3.1 Utilisation de l'intrication

3.1.1 Quantité d'intrication

Il est possible de quantifier l'intrication entre deux systèmes. Dans le cas d'un système AB ayant un état pur $|\psi\rangle$ on définit la quantité d'intrication comme :

$$E(|\psi\rangle) = S(\rho^A) = S(\rho^B)$$

avec $\rho^A = \text{tr}_B(|\psi\rangle\langle\psi|)$, l'égalité entre les deux se déduit par exemple de la décomposition de Schmidt. On peut montrer ([12]) à l'aide de cette décomposition de Schmidt et du théorème des suites typiques (3.2.3) et en écrivant :

$$|\psi\rangle^{\otimes m} \simeq \sum_{(i_k)_{\varepsilon\text{-typique}}} \lambda_{i_1} \lambda_{i_2} \dots \lambda_{i_m} |i_1^A \dots i_m^A\rangle |i_1^B \dots i_m^B\rangle$$

que si on possède m copies de $|\psi\rangle$, i.e l'état $|\psi\rangle^{\otimes m}$ il est possible d'obtenir à l'aide d'opérations locales et de communication classique dans la limite de $m \rightarrow \infty$ un nombre $mE(|\psi\rangle)$ de paires de Bell (possédant une quantité d'intrication 1) et que réciproquement on peut à partir de $mS(|\psi\rangle)$ états maximales intriqués obtenir $|\psi\rangle^{\otimes m}$, ces rendements étant de plus optimaux.

Dans le cas des états mixtes on définit ([18]) l'intrication de formation E_C comme la limite quand N tend vers l'infini du rapport M/N où M est le nombre de paires de Bell nécessaires pour obtenir $\rho^{\otimes n}$ par des opérations locales et communications classiques, et l'intrication purifiable comme $E_P = \lim_{n \rightarrow \infty} \frac{M}{N}$ avec M le nombre de paires de Bell que l'on peut obtenir à partir de $\rho^{\otimes n}$. Si pour les états purs ces deux quantités sont égales, ce n'est plus le cas pour des états mixtes, on a seulement $E_C > E_P$ traduisant l'irréversibilité. Par exemple pour un état de la forme $F |\psi^+\rangle \langle \phi^+| + (1-F) |\psi^-\rangle \langle \phi^-|$ on a ([18]) :

$$E_C = H \left(\frac{1 + \sqrt{F(1-F)}}{2} \right)$$

mais on peut aussi montrer que :

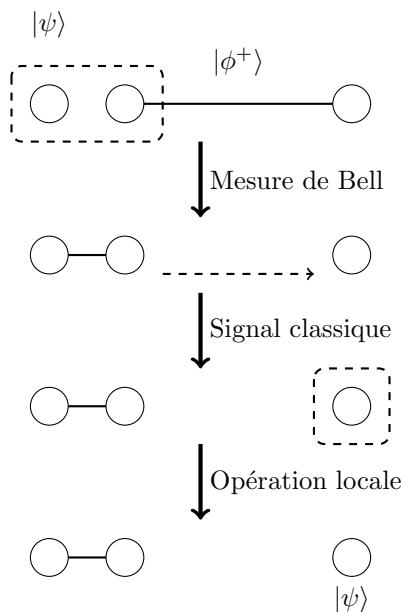
$$E_P = 1 - H(F)$$

ce qui correspond au rendement de la purification par hachage décrite au 3.2.3.

3.1.2 Téléportation quantique

La téléportation quantique (historiquement proposée par [2]) est au cœur des protocoles de purification : elle permet d'utiliser de l'intrication partagée pour transmettre de l'information quantique entre deux personnes quelle que soit la distance L qui les sépare, cela nécessite néanmoins une communication classique et donc un temps au moins $\frac{L}{c}$ (conformément à la relativité) et détruit l'état initialement envoyé (conformément au principe de non clonage).

On suppose que Alice et Bob partagent un état de Bell, plus précisément Alice a en sa possession un qubit 1 et Bob un qubit 2 l'ensemble des deux qubits étant dans l'état $|\phi_{1,2}^+\rangle = \frac{1}{\sqrt{2}} (|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2)$ (mais n'importe quel état de Bell convient, notamment dans le cas où on ne connaît pas l'état de Bell exact comme dans 3.3.2). Alors à l'aide de communication classique et d'opérations locales Alice peut transmettre un état $|\psi_0\rangle = \alpha |0\rangle + \beta |1\rangle$ quelconque à Bob.



- Initialement on a l'état :

$$|\varphi\rangle = (\alpha |0\rangle_0 + \beta |1\rangle_0) \otimes \frac{1}{\sqrt{2}} (|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2) = \frac{\alpha}{\sqrt{2}} |000\rangle + \frac{\alpha}{\sqrt{2}} |011\rangle + \frac{\beta}{\sqrt{2}} |100\rangle + \frac{\beta}{\sqrt{2}} |111\rangle$$

Avec les qubits 0 et 1 du côté d'Alice et le 2 du côté de Bob.

- Alice effectue une mesure de Bell sur les qubits 0 et 1. On obtient alors :

- La probabilité d'obtenir $|\phi^+\rangle$ est de $\frac{1}{4}$ et dans ce cas on obtient comme état final

$$2 \times \frac{|00\rangle_{0,1} + |11\rangle_{0,1}}{\sqrt{2}} \frac{\langle 00|_{0,1} + \langle 11|_{0,1}}{\sqrt{2}} \left(\frac{\alpha}{\sqrt{2}} |000\rangle + \frac{\alpha}{\sqrt{2}} |011\rangle + \frac{\beta}{\sqrt{2}} |100\rangle + \frac{\beta}{\sqrt{2}} |111\rangle \right) = |\phi_{0,1}^+\rangle \otimes |\psi_2\rangle$$

On a donc bien le qubit 2 qui est dans l'état $|\psi\rangle$.

- De même la probabilité d'avoir $|\phi^-\rangle$ est de $1/4$ et dans ce cas on obtient du côté de Bob $\alpha|0\rangle - \beta|1\rangle$ et celui-ci lorsqu'il reçoit le résultat de la mesure d'Alice doit effectuer une opération Z afin d'obtenir le bon qubit.
- Pour $|\psi^+\rangle$ la probabilité est de $1/4$ et Bob obtient $\beta|0\rangle + \alpha|1\rangle$. Il applique donc une opération X .
- Pour $|\psi^-\rangle$ la probabilité est de $1/4$ et Bob obtient $-\beta|0\rangle + \alpha|1\rangle$. Il applique donc une opération $ZX = -iY$.

Dans tous les cas après que Bob ait reçu le résultat de la mesure d'Alice et effectué la bonne opération il obtient le qubit 2 dans l'état $|\psi\rangle$. On remarque que de son côté Alice a bien perdu l'état $|\psi\rangle$ comme le théorème de non clonage le prédisait et que Bob doit attendre la communication classique d'Alice avant d'obtenir $|\psi\rangle$, il n'y a donc pas de transmission d'information plus rapidement que la lumière (avant la communication on a du côté de Bob $\rho_2 = \frac{1}{4}|\psi\rangle\langle\psi| + \frac{1}{4}X|\psi\rangle\langle\psi|X + \frac{1}{4}Z|\psi\rangle\langle\psi|Z + \frac{1}{4}Y|\psi\rangle\langle\psi|Y = \frac{1}{2}1_2$ et il n'y a donc aucune information).

En pratique si Alice et Bob partagent une paire intriquée mais celle-ci n'est pas dans un état de Bell alors la téléportation donne pour résultat un état proche de celui initial mais non identique.

Prenons par exemple le cas où la distribution de l'état de Bell s'est effectuée à travers un canal à dépolarisation de paramètre p .

Alors si on part de ρ on obtient :

$$p^2\rho + \frac{p(1-p)}{2}1_1 \text{tr}_1(\rho) + \frac{p(1-p)}{2}1_2 \text{tr}_2(\rho) + \frac{1-p}{4}1_{1,2}$$

Dans le cas où $\rho = |\phi^+\rangle\langle\phi^+|$, on a $\text{tr}_1(\rho) = 1_2$ (et de même pour l'inverse). D'où $\rho = p^2|\phi^+\rangle\langle\phi^+| + \frac{(1-p^2)}{4}1_{1,2}$ (on obtiendrait le même résultat si Alice envoie un photon vers Bob à travers un canal de paramètre p^2).

On a alors $p^2|\psi\rangle\langle\psi| \otimes |\phi^+\rangle\langle\phi^+| + (1-p^2)|\psi\rangle\langle\psi| \otimes \frac{1_{1,2}}{4}$ auquel on applique les opérations précédentes.

On obtient finalement du côté de Bob :

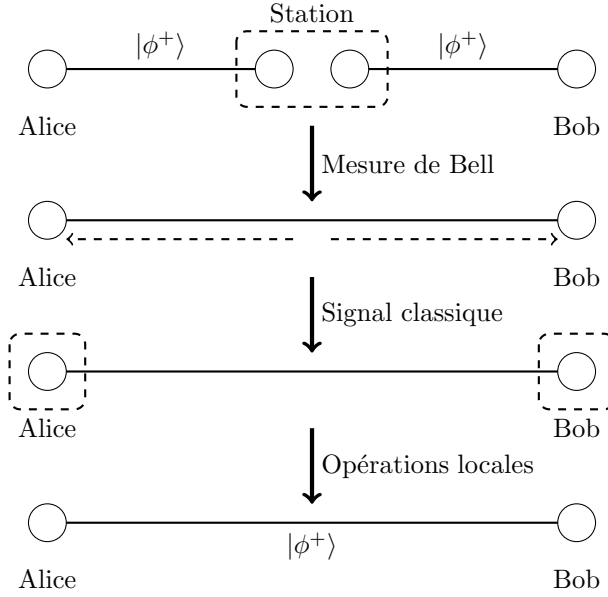
$$p^2|\psi\rangle\langle\psi| + \frac{1-p^2}{2}1$$

Ce qui revient au même que dans le cas où Alice envoie l'état $|\psi\rangle$ à Bob à travers le canal.

3.1.3 Permutation d'intrication

On cherche à augmenter la distance à laquelle l'intrication est partagée, plus précisément on suppose que Alice partage une paire de Bell $|\phi_{1,2}^+\rangle$ (mais n'importe quelle paire de Bell convient) avec une station intermédiaire S et que Bob partage aussi une paire de Bell $|\phi_{3,4}^+\rangle$ avec S.

Par des opérations locales et communications classiques on peut alors aboutir à une situation où Alice et Bob partagent une paire intriquée.



En effet le protocole est le suivant, en partant de $|\phi_{1,2}^+\rangle \otimes |\phi_{3,4}^+\rangle = \frac{1}{2} (|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)$.

- La station S effectue une mesure de Bell sur les deux qubits 2 et 3.
- La station envoie alors le résultat de la mesure à Alice et Bob qui en fonction de celui-ci effectuent une opération locale :

– Si le résultat est $|\phi^+\rangle$ ce qui arrive avec une probabilité 1/4 alors l'état devient :

$$2 \times \frac{\langle 0_2 0_3 |}{\sqrt{2}} \left(\frac{|0_1 0_2 0_3 0_4\rangle + |0_1 0_2 1_3 1_4\rangle + |1_1 1_2 0_3 0_4\rangle + |1_1 1_2 1_3 1_4\rangle}{2} \right) = \frac{|0_1 0_4\rangle + |1_1 1_4\rangle}{\sqrt{2}} = |\phi_{1,4}^+\rangle$$

- Si le résultat est $|\phi^-\rangle$ (probabilité 1/4) on obtient $|\phi_{1,4}^-\rangle$ que l'on retransforme en $|\phi_{1,4}^+\rangle$ en effectuant une porte Z du côté d'Alice (ou Bob).
- Si le résultat est $|\psi^+\rangle$ (probabilité 1/4) on obtient $|\psi_{1,4}^+\rangle$ que l'on retransforme en $|\phi_{1,4}^+\rangle$ en effectuant une porte X du côté d'Alice (ou Bob).
- Si le résultat est $|\psi^-\rangle$ (probabilité 1/4) on obtient $|\psi_{1,4}^-\rangle$ que l'on retransforme en $|\phi_{1,4}^+\rangle$ en effectuant une porte Y du côté d'Alice (ou Bob).

Remarque : il s'agit en fait d'une téléportation de l'état du photon 3 vers le photon 1.

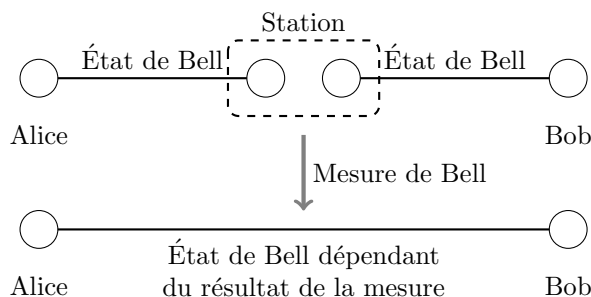
Si les deux paires de Bell sont imparfaites on obtient alors de même que pour la téléportation une paire imparfaite à l'arrivée, typiquement si on a des deux côtés $\rho = p|\phi^+\rangle\langle\phi^+| + \frac{1-p}{4}1$ on obtient finalement $p^2|\phi^+\rangle\langle\phi^+| + \frac{1-p^2}{4}1$. Une autre erreur possible est l'erreur de mesure, idéalement afin d'effectuer une mesure de Bell on applique une porte CNOT et on mesure le qubit cible sur z et la source sur x . En termes de fidélité, la fidélité après une telle permutation est donc de :

$$F' = \frac{1}{4}(1 + p^2(4\eta^2 - 1) \left(\frac{4F - 1}{3}\right)^2)$$

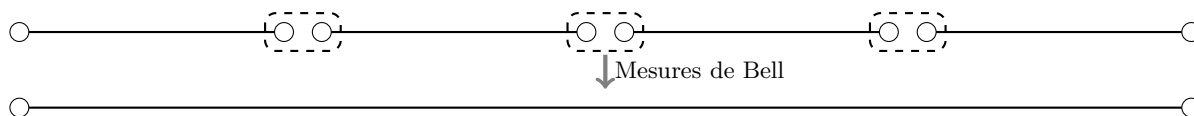
avec p la probabilité qu'une porte soit effectuée correctement.

On remarque que cette permutation nécessite néanmoins un temps proportionnel à la distance : c'est le temps nécessaire au message classique contenant les résultats de la mesure ainsi que la confirmation du succès des mesures envoyée par la station intermédiaire pour atteindre Alice et Bob.

Dans le cas où les mémoires quantiques sont imparfaites ce temps conduit à une dégradation exponentielle en la longueur de l'intrication. Une variante consiste alors à effectuer des permutations dites "aveugles". Pour cela on remarque que si Alice et la station partagent un état de Bell quelconque de même que la station et Bob, après une mesure de Bell le résultat sera une paire de Bell quelconque entre Alice et Bob, et même si on ne connaît pas l'état exact de cette paire on peut tout de même l'utiliser afin d'effectuer par exemple une téléportation ou bien d'autres permutations d'intrications (voir le protocole de permutations imbriquées partiel 3.3.2). Schématiquement cela correspond à :



Cela permet de plus d'effectuer plusieurs permutations à la fois sans attendre les résultats intermédiaires :



La fidélité (après application des opérations locales) est pour k permutations de :

$$F^{(k)} = \frac{1}{4} \left(1 + 3 \left(p^2 \frac{4\eta^2 - 1}{3} \right)^{k-1} \times \left(\frac{4F - 1}{3} \right)^k \right)$$

3.2 Protocoles de purification

On suppose que Alice et Bob possèdent un nombre n de paires mal intriquées c'est-à-dire d'états mixtes ρ de fidélité $F = \langle \phi^+ | \rho | \phi^+ \rangle < 1$ et souhaitent obtenir un nombre $m < n$ de paires de plus grande fidélité $F' > F$ via des opérations locales et des communications classiques (on peut ensuite utiliser ces paires pour effectuer une téléportation et transporter de l'information quantique). Il existe alors plusieurs protocoles explicites permettant d'arriver à un tel résultat.

3.2.1 Protocole IBM

Ce protocole proposé par [3] même si moins efficace que d'autres protocoles ultérieurs présente l'avantage de pouvoir être traité analytiquement afin de mettre en évidence certaines propriétés partagées par tous les protocoles de purification fonctionnant sur le même principe (protocoles itératifs avec communications dans les deux sens).

Un point essentiel de ce protocole est qu'en effectuant de manière bilatérale des rotations aléatoires sur une paire intriquée de fidélité F on peut se ramener à un état de Werner de fidélité F , de matrice densité diagonale dans la base de Bell :

$$\rho_F = F |\phi^+\rangle \langle \phi^+| + \frac{1-F}{3} |\phi^-\rangle \langle \phi^-| + \frac{1-F}{3} |\psi^-\rangle \langle \psi^-| + \frac{1-F}{3} |\psi^+\rangle \langle \psi^+|$$

- On commence avec deux paires de fidélité F :

$$\left(F |\phi^+\rangle \langle \phi^+| + \frac{1-F}{3} |\phi^-\rangle \langle \phi^-| + \frac{1-F}{3} |\psi^-\rangle \langle \psi^-| + \frac{1-F}{3} |\psi^+\rangle \langle \psi^+| \right)^{\otimes 2}$$

- On effectue un BXOR sur ces deux paires. On obtient alors :

$$\begin{aligned} F^2 |\phi^+\phi^+\rangle \langle \phi^+\phi^+| + F \left(\frac{1-F}{3} \right) (|\phi^-\phi^-\rangle \langle \phi^-\phi^-| + |\phi^-\phi^+\rangle \langle \phi^-\phi^+|) \\ + \left(\frac{1-F}{3} \right)^2 (|\psi^+\phi^+\rangle \langle \psi^+\phi^+| + |\psi^-\phi^+\rangle \langle \psi^-\phi^+| + |\psi^+\phi^-\rangle \langle \psi^+\phi^-| + |\psi^-\phi^-\rangle \langle \psi^-\phi^-|) \\ + \dots \end{aligned}$$

On n'explicite pas les termes avec ψ^\pm pour la deuxième paire.

- Alice et Bob effectuent chacun de leur côté une mesure selon z de la seconde paire (paire cible de BXOR) et ne gardent la paire source que si les résultats sont parallèles (i.e on est dans ϕ^\pm). On a la probabilité d'un tel résultat :

$$p(F) = F^2 + \frac{2F(1-F)}{3} + \frac{5(1-F)^2}{9}$$

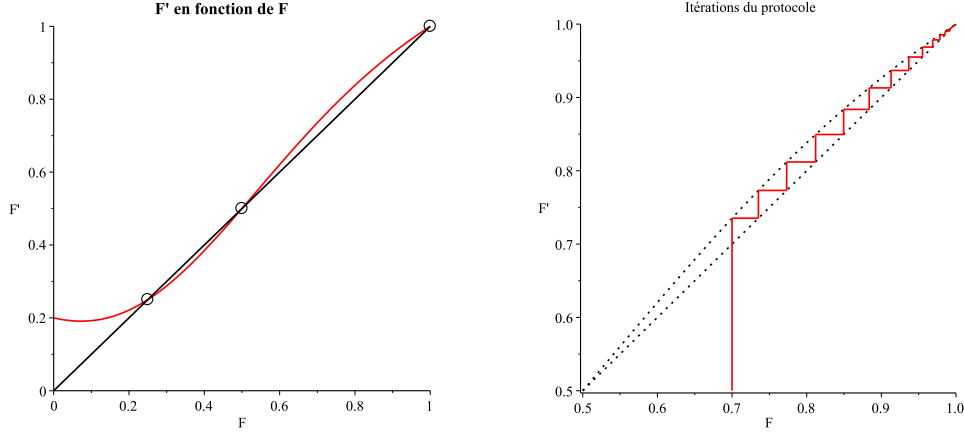
et on obtient alors pour la première paire :

$$\begin{aligned} \frac{1}{p(F)} \left(F^2 |\phi^+\rangle \langle \phi^+| + F \left(\frac{1-F}{3} \right) (|\phi^-\rangle \langle \phi^-| + |\phi^+\rangle \langle \phi^+|) \right. \\ \left. + \left(\frac{1-F}{3} \right)^2 (|\psi^+\rangle \langle \psi^+| + |\psi^-\rangle \langle \psi^-| + |\psi^+\rangle \langle \psi^+| + |\psi^-\rangle \langle \psi^-|) \right) \end{aligned}$$

- On effectue de nouveau des rotations aléatoires pour obtenir $\rho_{F'}$ avec :

$$F' = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2}$$

On réitère ensuite le protocole avec les nouvelles paires de fidélité F' . Comme les seuls points fixes de $F \mapsto F'$ sont 1 et $\frac{1}{4}$ comme points fixes attractifs $\frac{1}{2}$ (et 0) comme points fixes répulsifs, si la fidélité initiale est supérieure à $1/2$, on peut s'approcher d'une fidélité de 1 en théorie. Mais à chaque étape on doit sacrifier en moyenne $1/2 + 1/2 \times \left(1 - \left(F^2 + \frac{2F(1-F)}{3} + \frac{5(1-F)^2}{9} \right) \right)$ des paires ce qui rend le protocole coûteux en ressources physiques (et si $F < 1/2$ on tend vers une fidélité de $1/4$ c'est-à-dire vers l'identité, on perd toute information).

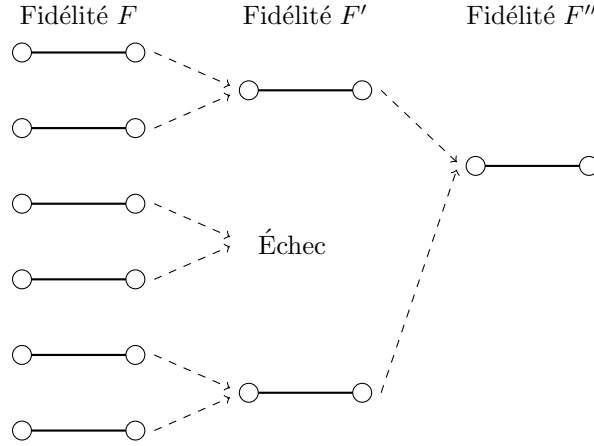


On peut raffiner le modèle([9]) en prenant en compte des erreurs de mesure (probabilité η d'effectuer la bonne mesure) et de portes (probabilité p d'effectuer la bonne porte).

On obtient alors :

$$F' = \frac{(F^2 + \frac{1}{9}(1-F)^2) \times (\eta^2 + (1-\eta)^2) + (\frac{1}{3}F(1-F) + \frac{1}{9}(1-F)^2) \times 2\eta(1-\eta) + \frac{1-P^2}{8P^2}}{(F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2) \times (\eta^2 + (1-\eta)^2) + (\frac{1}{3}F(1-F) + \frac{1}{9}(1-F)^2) \times 8\eta(1-\eta) + \frac{1-P^2}{2P^2}}$$

Du fait de ces erreurs les points fixes deviennent $1/4$ et $F_{max} < 1$ comme point fixe attractif ainsi que $F_{min} > 1/2$ comme point fixe répulsif. Ainsi en itérant le protocole, on a une amélioration de la fidélité ssi la fidélité initiale est plus grande que F_{min} et même au bout d'un grand nombre d'itérations la plus grande fidélité atteignable est de $F_{max} < 1$.



De plus si les erreurs sont trop importantes ces points fixes disparaissent, c'est-à-dire que le protocole n'améliore pas la fidélité. On peut par exemple calculer ce seuil dans le cas où il n'y a pas d'erreur de mesure ($\eta = 1$). Dans ce cas $F' = \frac{(F^2 + \frac{1}{9}(1-F)^2) + \frac{1-P^2}{8P^2}}{(F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2) + \frac{1-P^2}{2P^2}}$ et on obtient :

$$\begin{cases} F_{min} = \frac{3}{4} - \frac{\sqrt{10P^2-9}}{P} \\ F_{max} = \frac{3}{4} + \frac{\sqrt{10P^2-9}}{P} \end{cases}$$

On obtient donc que pour $P < \sqrt{\frac{9}{10}} \approx 0.95$ il n'y a plus de purification possible.

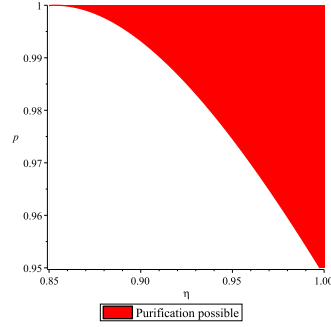
De même pour $P = 1$ on a $F' = \frac{(F^2 + \frac{1}{9}(1-F)^2) \times (\eta^2 + (1-\eta)^2) + (\frac{1}{3}F(1-F) + \frac{1}{9}(1-F)^2) \times 2\eta(1-\eta)}{(F^2 + \frac{2}{3}F(1-F) + \frac{8}{9}(1-F)^2) \times (\eta^2 + (1-\eta)^2) + (\frac{1}{3}F(1-F) + \frac{1}{9}(1-F)^2) \times 8\eta(1-\eta)}$
et on obtient :

$$\begin{cases} F_{min} = \frac{1}{2(4\eta^2 - 4\eta + 1)} \\ F_{max} = 1 \end{cases}$$

et donc si on peut toujours atteindre une fidélité de 1 il est encore une fois impossible d'effectuer une purification pour $\eta < \frac{1}{2} + \frac{\sqrt{2}}{4} \approx 0.85$.

Et de manière générale on peut calculer les points fixes. On obtient que la purification devient impossible dès que $64\eta^4 p^2 - 128\eta^3 p^2 + 116\eta^2 p^2 - 52\eta p^2 - 36\eta^2 + 10p^2 + 36\eta - 9 < 0$ ce qui définit la zone suivante en (η, p) :

On remarque que comparé aux seuils nécessaires pour le passage à l'échelle de circuits quantiques tolérants à l'erreur un tel protocole résiste assez bien aux erreurs de porte rendant possible une réalisation physique.



Il faut cependant noter que même si on se situe dans la zone où une purification est possible le changement de F_{min} et F_{max} rend plus difficile l'insertion de la purification dans un schéma de répéteurs quantiques.

3.2.2 Protocole d'Oxford

Le protocole proposé par [7] suit le même principe qualitatif que le précédent considère des états quelconques (et pas forcément diagonaux dans la base de Bell).

Avec les mêmes hypothèses et notations et en notant A, B, C, D les coefficients diagonaux de ρ dans la base $|\phi^+\rangle, |\psi^-\rangle, |\psi^+\rangle, |\phi^-\rangle$ (on ne s'intéresse pas aux termes non diagonaux) :

- Des opérations locales afin de "mélanger" les états de Bell :

Du côté d'Alice une rotation de $\frac{\pi}{2}$ autour de l'axe x de la sphère de Bloch i.e : Du côté de Bob une rotation de $-\frac{\pi}{2}$ autour de l'axe x de la sphère de Bloch i.e :

$$\begin{cases} |0\rangle \longrightarrow \frac{|0\rangle - i|1\rangle}{\sqrt{2}} \\ |1\rangle \longrightarrow \frac{|1\rangle - i|0\rangle}{\sqrt{2}} \end{cases} \qquad \begin{cases} |0\rangle \longrightarrow \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \\ |1\rangle \longrightarrow \frac{|1\rangle + i|0\rangle}{\sqrt{2}} \end{cases}$$

On obtient alors dans la base de Bell :

$$\begin{cases} |\phi^+\rangle \longrightarrow |\phi^+\rangle \\ |\phi^-\rangle \longrightarrow |\psi^-\rangle \\ |\psi^+\rangle \longrightarrow |\psi^+\rangle \\ |\psi^-\rangle \longrightarrow |\phi^-\rangle \end{cases}$$

- On effectue alors de même que précédemment une porte BXOR, l'évolution des termes diagonaux est :

$$\begin{pmatrix} A' \\ B' \\ C' \\ D' \end{pmatrix} = \begin{pmatrix} \frac{A^2+B^2}{(A+B)^2+(C+D)^2} \\ \frac{2CD}{(A+B)^2+(C+D)^2} \\ \frac{C^2+D^2}{(A+B)^2+(C+D)^2} \\ \frac{2AB}{(A+B)^2+(C+D)^2} \end{pmatrix}$$

En effet on a par exemple le résultat de BXOR est $|\phi^+\rangle\langle\phi^+| \otimes |\phi^\pm\rangle\langle\phi^\pm|$ uniquement pour les états $|\phi^+\rangle\langle\phi^+| \otimes |\phi^+\rangle\langle\phi^+|$ ou bien $|\phi^-\rangle\langle\phi^-| \otimes |\phi^-\rangle\langle\phi^-|$, c'est-à-dire $A^2 + B^2$ le facteur de normalisation $(A+B)^2 + (C+D)^2$ correspondant à la probabilité d'avoir le qubit cible dans $|\phi^\pm\rangle$.

On peut alors montrer que dans le cas où la fidélité (A ici) initiale est de $1/2 + \varepsilon > \frac{1}{2}$ on arrive bien à $A = 1, B = C = D = 0$, même si la fidélité n'est pas toujours monotone.

Pour cela on remarque d'abord que grâce à $A + B + C + D = 1$ on obtient $1 - 2A' = \frac{(2A-1)(2B-1)}{(A+B)^2+(C+D)^2}$ et donc que la fidélité reste supérieure à $1/2$ tout au long du protocole.

Comme de plus $1 - 2B' = \frac{(A+B)^2+(C-D)^2}{(A+B)^2+(C+D)^2}$ on obtient :

$$(2A' - 1)(1 - 2B') = (2A - 1)(1 - 2B) \times \left(\frac{(A+B)^2 + (C-D)^2}{((A+B)^2 + (C+D)^2)^2} \right)$$

Or on a :

$$\frac{(A+B)^2 + (C-D)^2}{((A+B)^2 + (C+D)^2)^2} = \frac{(1 - (C+D))^2 + (C-D)^2}{((1 - (C+D))^2 + (C+D)^2)^2}$$

qui après une étude de polynôme est plus grand que 1 dans $\{C, D \in [0, \frac{1}{2} - \varepsilon], C + D \leq \frac{1}{2} - \varepsilon\}$ avec égalité uniquement pour $C = D = 0$.

Donc $(2A-1)(1-2B)$ croissante et majorée converge et donc $\frac{(1-(C+D))^2+(C-D)^2}{((1-(C+D))^2+(C+D)^2)^2}$ converge vers 1. La seule possibilité est alors que $C + D \rightarrow 0$ comme C et D positifs on a $CD \rightarrow 0$ d'où $B \rightarrow 0$ et donc on a bien $A \rightarrow 1$.

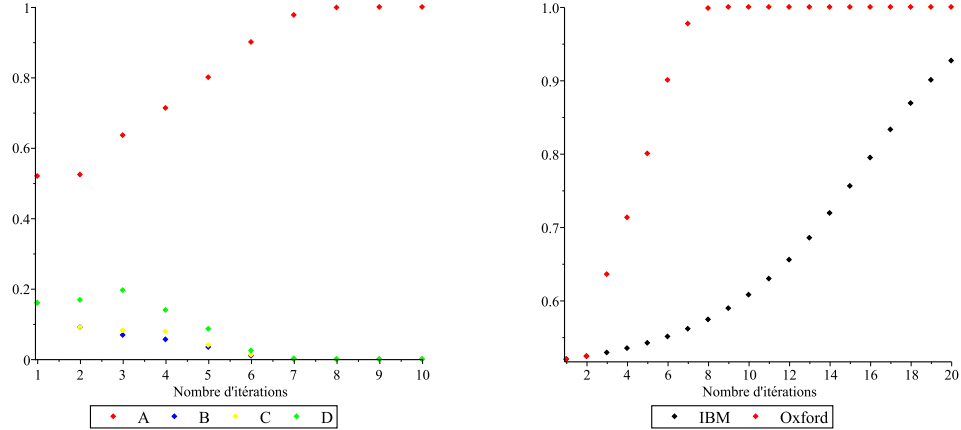
De plus comme on doit avoir ρ matrice autoadjointe positive (et de trace 1), on obtient que les coefficients non diagonaux doivent forcément être nuls si la diagonale est $1, 0, 0, 0$.

On obtient donc bien un état $|\phi^+\rangle$ purifié.

On peut aussi s'intéresser à ce qui se passe dans les autres cas :

- Dans le cas où $B > 1/2$, on a $1 - 2A' = \frac{(2A-1)(2B-1)}{(A+B)^2+(C+D)^2} < 0$ donc au bout d'une itération on se ramène au cas $A > 1/2$.
- Comme on (A, B) et (C, D) jouent le même rôle, si $C > 1/2$ ou $D > 1/2$ la matrice densité tend vers $|\psi^+\rangle\langle\psi^+|$.
- Si initialement aucun des termes diagonaux n'est plus grand que $1/2$ alors comme $1 - 2A' = \frac{(2A-1)(2B-1)}{(A+B)^2+(C+D)^2} > 0$ et $1 - 2B' = \frac{(A+B)^2+(C-D)^2}{(A+B)^2+(C+D)^2} > 0$ (et idem pour C et D), à l'itération suivante tous les termes sont encore $< 1/2$ et donc aucune purification n'est possible.

On observe numériquement que ce protocole est bien plus rapide que le précédent, on peut tracer à gauche l'évolution de A, B, C, D pour des conditions initiales $A=0.52, B = C = D = 0.16$ et le comparer au protocole d'Oxford avec les mêmes conditions initiales (à droite) :



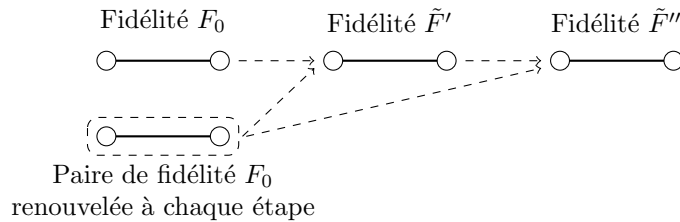
Mais de même que précédemment chaque itération consomme une fraction de $1/2 + 1/2 \times (1 - (A + B)^2 + (C + D)^2)$ des paires.

Une variante consiste alors à utiliser le protocole avec deux paires de fidélité différentes. Plus précisément on utilise le protocole avec une paire ρ que l'on souhaite purifier récursivement et une autre ρ_0 de fidélité constante tout au long des itérations et que l'on recrée à chaque étape.

On obtient alors à chaque nouvelle itération si A_0, B_0, C_0 et D_0 sont les coefficients diagonaux (constants) de ρ_0 :

$$\begin{pmatrix} A' \\ B' \\ C' \\ D' \end{pmatrix} = \begin{pmatrix} \frac{AA_0 + BB_0}{(A+B)(A_0+B_0) + (C+D)(C_0+D_0)} \\ \frac{CD_0 + C_0D}{(A+B)(A_0+B_0) + (C+D)(C_0+D_0)} \\ \frac{CC_0 + DD_0}{(A+B)(A_0+B_0) + (C+D)(C_0+D_0)} \\ \frac{AB_0 + A_0B}{(A+B)(A_0+B_0) + (C+D)(C_0+D_0)} \end{pmatrix}$$

L'avantage de cette variante est que les ressources physiques nécessaires (i.e le nombre de paires initiales) nécessaires sont bien plus faibles que dans le cas précédent ; mais en contrepartie non seulement le nombre d'itérations nécessaires est plus important mais surtout en cas d'échec d'une étape il faut recommencer tout le protocole depuis le début, ce qui conduit donc à un temps nécessaire pour la purification bien plus important.



3.2.3 Hachage

Il s'agit d'un exemple de purification avec communication à sens unique proposé par [3, 5] qui s'apparente aux méthodes de hachage classiques. Même si le rendement est plus élevé cette méthode ne fonctionne que pour F assez grand (et pour un nombre de paires asymptotiquement grand).

De même que dans le protocole IBM on se ramène tout d'abord à un état de Werner W_F de fidélité F (en fait il suffit d'avoir un état diagonal dans la base de Bell), c'est-à-dire n paires de Bell chacune ayant une probabilité F d'être dans l'état ϕ^+ et $\frac{1-F}{3}$ d'être dans ϕ^-, ψ^+, ψ^- .

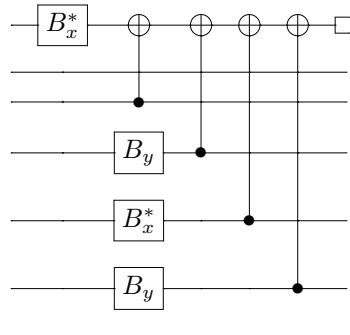
Par commodité on notera $\phi^+, \phi^-, \psi^+, \psi^-$ par deux bits classiques respectivement 00, 10, 01, 11. On obtient donc une suite x de taille $2n$ avec une distribution X de probabilité issue de la fidélité.

Étant donné une telle suite x de longueur $2n$ et une autre suite s on définit la parité de x par rapport à s par $s.x = \sum_{i=1}^{2n} x_i \oplus s_i$, alors pour deux suites quelconques la probabilité d'avoir la même parité par rapport à une suite s est de $1/2$ par distributivité : $(s.x) \oplus (s.y) = s.(x \oplus y)$ qui vaut $1/2$ en moyenne.

On extrait $s.x$ de la manière suivante :

- On choisit une occurrence 11 dans s (on a n assez grand). Pour simplifier on suppose qu'il s'agit de la première paire i.e $s = 11 \dots$. L'information sur $s.x$ sera alors enregistrée dans la première paire (ψ^\pm correspondant à 1 et ϕ^\pm à 0).
- Pour chaque paire selon la valeur de s on effectue les opérations :
 - Si on a 00 on ne fait rien.
 - Pour les paires 01 on effectue une porte $BXOR$ ayant comme contrôle la paire en question et comme cible la paire stockant la parité.
 - Pour les paires 10 on effectue d'abord une rotation de $\pi/2$ autour de y sur les deux qubits (noté B_y) de la paire échangeant ϕ^- et ψ^+ et laissant ϕ^+ et ψ^- invariants. Puis on effectue une porte $BXOR$.
 - Pour les paires 11 on effectue une rotation de $\pi/2$ autour de x pour un qubit et de $-\pi/2$ autour de x pour l'autre (noté B_x^*) échangeant ϕ^- et ψ^- et laissant ϕ^+ et ψ^+ invariants. Puis on effectue une porte $BXOR$.
- On mesure ensuite les deux qubits de la première paire pour déterminer la parité selon s .

Par exemple si on a $s = 11, 00, 01, 10, 11, 10, 00$ cela correspond à (avec chaque ligne correspondant non pas à un qubit mais à une paire, en notant les portes $BXOR$ comme les portes $CNOT$) :



Par exemple si on a une paire $\psi^+ = 01$ et que les bits de s correspondants sont 10 on obtient comme opération sur le qubit cible un $BXOR$ ayant pour contrôle ψ^- ce qui ne change pas l'état entre ϕ et ψ et on vérifie que de même dans les autres cas les opérations décrites calculent bien la parité par rapport à s . On peut donc en sacrifiant un qubit mesurer $s.x$ sans mesurer les autres qubits. On utilise ensuite le théorème des suites typiques :

On dit qu'une suite est ε -typique si :

$$\left| -\frac{1}{n} \log(p(x_i)) - H(X) \right| \leq \varepsilon$$

D'après le théorème des suites typiques ([16]) on a :

- Pour ε fixé la probabilité qu'une suite soit ε -typique tend vers 1 quand n tend vers l'infini (et plus précisément est de l'ordre de $1 - O(e^{-\varepsilon^2 n})$)
- Pour ε et δ fixés pour n assez grand le nombre de suites est compris entre $(1 - \delta)2^{n(H(X) - \varepsilon)}$ et $2^{n(H(X) + \varepsilon)}$.

On effectue donc la procédure m fois et pour tout k entre 0 et m on note x_k la suite de taille $2(n - k)$ obtenue à l'étape k .

Alors étant donné deux telles suites (x_k) et (y_k) on a la probabilité que $x_m \neq y_m$ et que $\forall k, x_k \cdot s_k = y_k \cdot s_k$ est au plus de 2^{-m} car à chaque itération si ils sont distincts la probabilité qu'ils aient la même parité par rapport à s est de $1/2$.

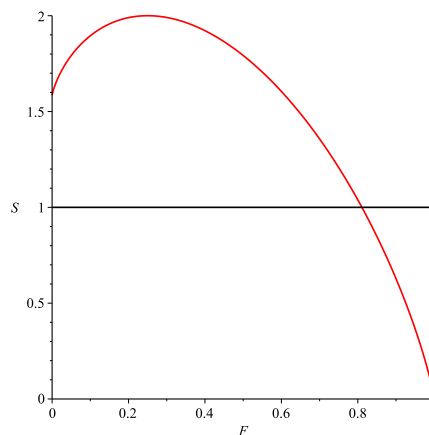
Si on connaît les m résultats de mesure de parité, la probabilité d'en déduire incorrectement x_m est alors au plus de (comme $H(X) = S(W_F)$) :

$$2^{n(S(W_F) + \varepsilon) - m} + O(e^{-\varepsilon^2 n})$$

En prenant $m = n(1 - S(W_F)) + 2\varepsilon$ et $\varepsilon = n^{-1/4}$ puis en faisant tendre n vers l'infini on obtient alors une probabilité d'échec qui tend vers 0 pour un rendement de $1 - S(W_F)$ (si $S(W_F) < 1$). Il suffit ensuite d'appliquer les opérations appropriées pour obtenir des $|\phi^+\rangle$

Et on a donc une purification possible dès que $F > 0.81\dots$ car :

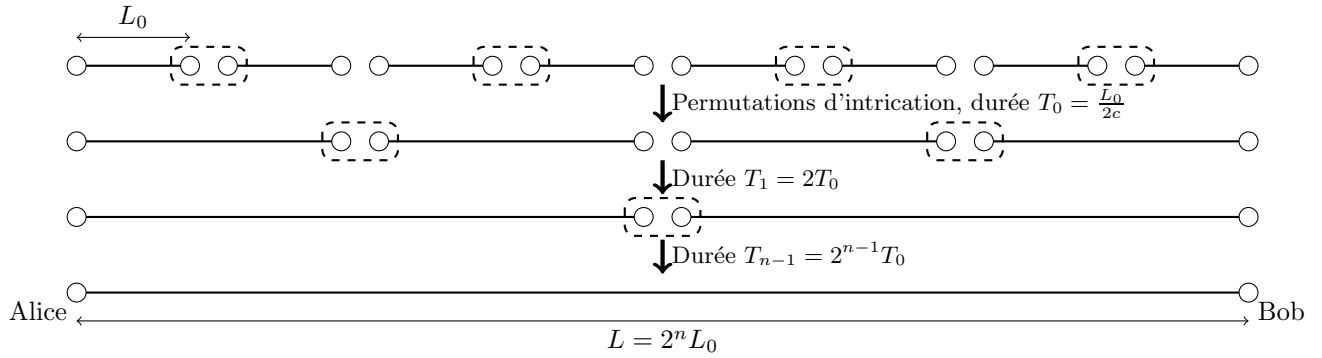
$$S(W_F) = -F \log(F) - (1 - F) \log\left(\frac{1 - F}{3}\right)$$



3.3 Répéteurs quantiques

3.3.1 Idée générale

Ce protocole a été proposé par [6, 9] afin de transmettre de l'intrication entre Alice et Bob (qui peut être ensuite utilisée pour transmettre de l'information quantique via téléportation). Même si il peut paraître plus efficace qu'une structure de code correcteur du fait de la croissance logarithmique des ressources il est en fait très sensible à la qualité des mémoires. On s'intéresse d'abord au protocole idéal avec des mémoires parfaites.



Le principe est le suivant : on subdivise la longueur totale L en $2^n - 1$ stations intermédiaires $S_1, S_2, \dots, S_{2^n-1}$ on note Alice S_0 et Bob S_{2^n} .

On commence par distribuer l'intrication entre les stations S_{2i} et S_{2i+1} à distance $L_0 = \frac{L}{2^n}$, puis pour tout k jusqu'à $n - 1$ on effectue des permutations d'intrication aux stations $2^k(2i + 1)$ pour i allant de 0 à $2^{n-1-k} - 1$.

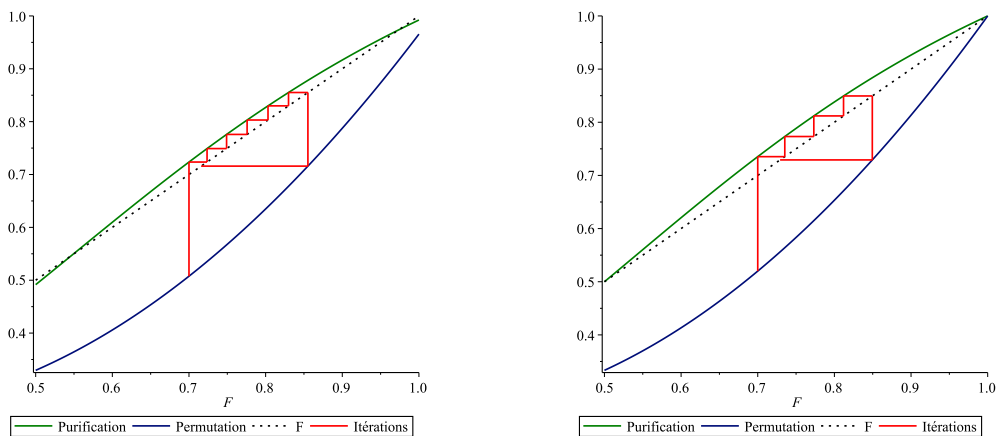
À chaque étape on augmente ainsi la distance de l'intrication, au prix d'une perte de fidélité.

Cette perte de fidélité peut être corrigée par des purifications d'intrication successives si besoin donnant ainsi le protocole suivant :

- On distribue initialement l'intrication entre les stations.
- On effectue des permutations d'intrication, ce qui a pour effet de diminuer la fidélité.
- On effectue des purifications d'intrication pour augmenter la fidélité.
- On recommence.

Comme les permutations d'intrication diminuent la fidélité il faut effectuer un certain nombre de purifications pour obtenir une fidélité suffisamment élevée pour faire de nouveau une permutation.

On obtient ainsi des "boucles" entre permutation et purification avec un nombre de purifications plus important quand les erreurs sont élevées (à droite sans aucune erreur et à gauche pour $p = 0.99$ et $\eta = 0.99$) :

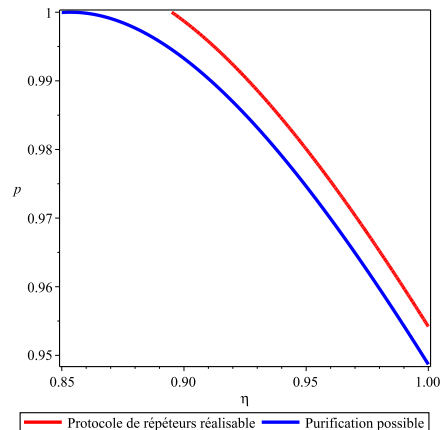


De plus il faut qu'après purification la fidélité soit telle que la permutation rende possible une nouvelle purification. Dans le cas sans erreur il faut donc qu'après purification la fidélité soit d'au moins $\frac{1+\sqrt{3}}{4}$.

Mais cela n'est pas forcément possible s'il y a des erreurs car on doit avoir :

$$F_{min} < \frac{1}{4}(1 + p^2(4\eta^2 - 1)) \left(\frac{4F_{max} - 1}{3} \right)^2$$

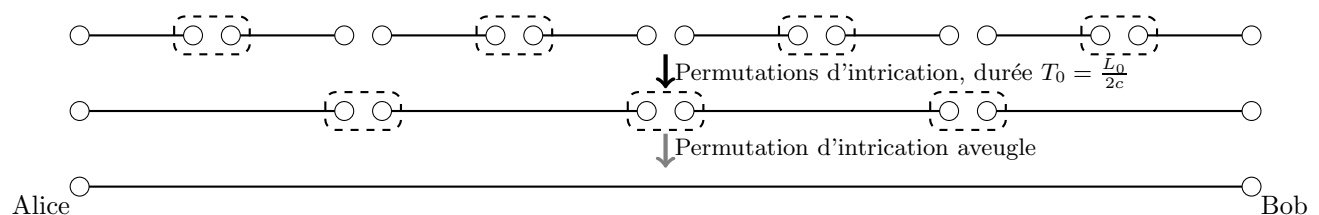
avec F_{min} et F_{max} les fidélités minimales et maximales de la purification (que l'on peut expliciter dans le cas du protocole IBM). Cela définit donc un seuil pour le taux d'erreur en dessous duquel il n'est plus possible d'effectuer un tel protocole. Ainsi si on représente sur le même schéma la zone où la purification est possible et celle où un protocole de répéteur est possible pour une telle purification on obtient :



3.3.2 Protocole partiel et architecture générale

L'inconvénient du protocole précédent est que les permutations d'intrication et certaines purifications d'intrication nécessitent l'acheminement de signaux classiques et donc prennent un temps proportionnel à la distance entre les stations. Si les mémoires sont imparfaites, durant ce temps la fidélité va décroître, enlevant tout intérêt à un tel protocole.

L'idée est alors d'effectuer un protocole partiel [14] : lorsque la distance entre deux stations est importante on termine le protocole en effectuant des permutations d'intrication sans attendre la transmission des résultats des mesures de Bell, ce qui n'empêche pas d'utiliser les états obtenus : ainsi si on effectue une téléportation sans connaître l'état de Bell précis on obtient l'état voulu à une transformation unitaire près (X, Y ou Z) que l'on peut ensuite déterminer lorsque les signaux classiques atteignent Bob. Plus précisément si on possède 2^n stations au lieu de faire n étapes de purification et permutations successives on s'arrête à l'étape m pour effectuer ensuite une permutation aveugle sur l'ensemble des paires intriquées à l'étape $m - 1$



Il faut alors choisir judicieusement m : si m est trop élevé les pertes dues aux mémoires sont importantes mais si il est trop faible la permutation aveugle se fait sur de nombreuses paires diminuant ainsi la fidélité finale.

On peut raffiner cette méthode [10] afin de tirer parti des différents modes de purification :

- Aux faibles niveaux on utilise des protocoles de permutation standard et pour la purification on utilise la version modifiée du protocole d'Oxford en recréant à chaque fois de nouvelles paires, permettant d'économiser les ressources physiques.

- Aux niveaux intermédiaires on utilise une permutation standard et on utilise les états déjà créés afin d'effectuer la purification, en effet le temps nécessaire pour recréer de nouveaux états est suffisamment important pour rendre la purification utilisée précédemment inefficace.
- Au dernier niveau on effectue une permutation aveugle et pour la purification on utilise par exemple un protocole de purification nécessitant uniquement une communication à sens unique (par exemple le hachage).

4 Comparaison des deux méthodes

4.1 Capacité théorique

4.1.1 Définition

De même que dans le cas classique on peut définir la capacité d'un canal quantique bruité comme le rendement asymptotique maximum conduisant à des erreurs arbitrairement proches de 0. Mais si la capacité d'un canal quantique utilisé afin de transporter de l'information classique est connue (il s'agit du théorème de Holevo-Schumacher-Westmoreland [12] montrant de manière similaire au théorème de Shannon qu'elle vaut : $C_c(\mathcal{E}) = \sup_{(\rho_j)} S(\mathcal{E}(\sum p_j \rho_j)) - \sum p_j S(\mathcal{E}(\rho_j))$) il n'y a pas de tel équivalent général pour la transmission d'information quantique par un canal quantique. De plus il faut distinguer les cas selon la possibilité ou non d'utiliser des messages classiques supplémentaires et dans quels sens (un seul ou dans les deux sens). On définit alors fidélité C_1 (resp. C_2) comme le plus grand réel vérifiant $\forall R < C_1$ et $\forall \varepsilon > 0$ il existe un code codant m qubits logiques en n qubits physiques avec $\frac{m}{n} > r$ et tel que la fidélité entre le message envoyé et le message reçu après décodage (resp. en autorisant les communications classiques dans les deux sens) soit au moins de $1 - \varepsilon$. Un premier résultat de [5] montre que quelque soit le canal, sa capacité n'est pas accrue par l'utilisation de communication classique dans un seul sens. On note alors C_1 la capacité classique avec communication dans un seul sens (ou sans communication) et C_2 avec communication classique dans les deux sens. Des définitions on tire $C_1 \leq C_2$ et $C_1 \leq C$ car on peut tout simplement transporter de l'information classique avec des états mutuellement orthogonaux.

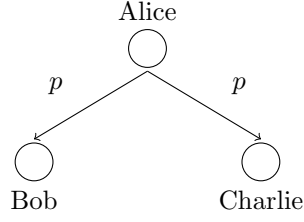
4.1.2 Capacités du canal à effacement

On peut calculer de manière explicite (cf [4]) la capacité d'un canal quantique à effacement de probabilité $1 - p$ d'effacer un qubit :

$$C_2 = C_c = p$$

$$C_1 = \max(0, 2p - 1)$$

Le fait que la capacité quantique soit nulle pour $p < 1/2$ peut s'interpréter à l'aide du théorème de non clonage : pour $p < 1/2$ on suppose que Alice possède un état $|\psi\rangle$ et communique avec Bob et Charlie. Pour chaque qubit elle l'envoie à Bob avec une probabilité p tandis que Charlie reçoit $|2\rangle$ un effacement et avec probabilité p elle fait l'inverse (et avec probabilité $1 - 2p$ elle le détruit). Du point de vue de Bob ou Charlie il s'agit d'un canal à effacement de paramètre p . Si la capacité d'un tel canal était non nulle il pourraient alors à l'aide d'un codage approprié en déduire tous les deux l'état $|\psi\rangle$, ce qui contredit le théorème de non clonage.



Il est aussi possible d'obtenir des résultats sur d'autres canaux (par exemple pour le canal à dépolarisation si $1/3 < p < 2/3$ $C_1 = 0$ et $C_2 > 0$ tandis que $p < 1/3$ conduit à $C_1 = C_2 = 0$ mais $C > 0$), mais de manière générale on s'intéressera pas directement à la capacité (sauf pour les limites théoriques notamment lorsque la capacité est nulle) mais plutôt au rendement c'est-à-dire au nombre de qubits étant transmis correctement par unité de temps.

4.2 Comparaison asymptotique

4.2.1 Cas des mémoires parfaites

On s'intéresse d'abord au cas des mémoires parfaites et plutôt que de calculer la fidélité à travers des erreurs de dépolarisation on prend comme modèle d'erreur des canaux à effacements par commodité (ce qui équivaut qualitativement à des purifications par détection du type IBM ou Oxford, ces dernières étant néanmoins plus coûteuses en ressources physiques) .

Si on considère un protocole de répéteurs partiel on peut alors calculer le taux de transmission : avec N le nombre de mémoires à chaque station, n le nombre de niveaux du répéteur et m l'étape à laquelle on effectue les permutations aveugles. On note $P_S = e^{-\alpha L_0}$ la probabilité d'une distribution correcte entre les stations voisines et P_M la probabilité de succès des opérations de permutation. On procède alors de la manière suivante :

- Pour chaque qubit de stations non intriquées on tente de l'intriquer avec une station voisine avec une probabilité de succès P_S , en régime permanent cela donne :

$$NP_S \frac{1 - P_M}{(1 - P_M) + P_S(1 - P_M^m)}$$

paires intriquées (en effet on a à chaque étape $\frac{N}{1 + P_S + P_S P_M + P_S P_M^2 + \dots + P_S P_M^{m-1}}$ paires non intriquées).

- A l'étape k on a alors $\frac{1 - P_M}{(1 - P_M) + P_S(1 - P_M^m)} NP_S P_M^k$ paires intriquées sur une distance $L_0 2^k$.
- Au moment d'effectuer la permutation aveugle on a donc $N \frac{1 - P_M}{(1 - P_M) + P_S(1 - P_M^m)} P_S P_M^{m-1}$ paires intriquées subissant cette permutation, ayant un taux de $P_M^{2^{n-m+1}-1}$ car il y a $2^{n-m+1} - 1$ permutations effectuées. On obtient donc finalement :

$$N \frac{1 - P_M}{(1 - P_M) + P_S(1 - P_M^m)} P_S P_M^{2^{n-m+1} + m - 2}$$

paires partagées entre Alice et Bob et comme chaque étape élémentaire de temps $T_0 = L_0/c = L/(2^n c)$ et donc le rendement est :

$$Q_m^{(n)} = \frac{(1 - P_M) P_S P_M^{2^{n-m+1} + m - 2}}{((1 - P_M) + P_S(1 - P_M^m)) T_0} \simeq \frac{P_S P_M^{2^{n-m+1} + m - 2}}{m T_0}$$

En dérivant on observe que dès que :

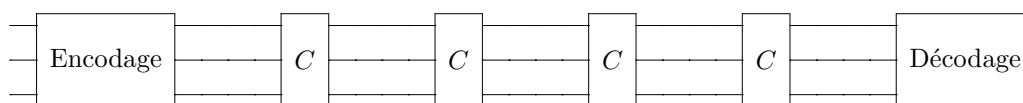
$$P_M < e^{\frac{1}{n(1-2\ln(2))}}$$

le protocole standard sans permutation aveugle est le plus efficace (et dans le cas contraire la dernière étape permet de faire gagner du temps ce qui explique ce résultat).

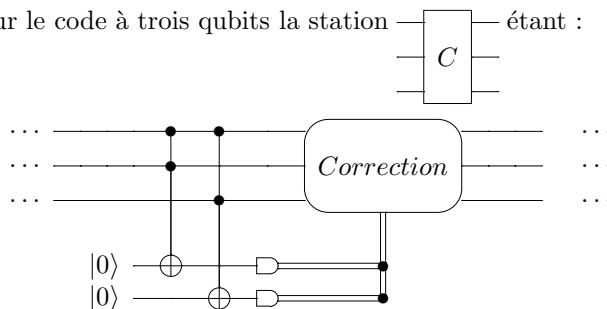
On considère un système similaire dans le cas des codes correcteurs d'erreur : plutôt que d'encoder le message et de le transmettre directement sur une longueur L on utilise des stations intermédiaires séparées d'une distance L_0 corrigeant les erreurs avant de renvoyer les messages. Avec $\tilde{p}(L_0) > p(L_0)$ la probabilité d'une transmission correcte, le rendement est alors dans le cas d'un canal à effacement de :

$$(\tilde{p}(L_0))^{2^n}$$

où 2^n est le nombre de stations,



avec par exemple pour le code à trois qubits la station C étant :



(de même que précédemment un canal à inversion et le code à 3 qubit agit de manière similaire à l'effacement, dans ce cas les coefficients en $|\psi_L\rangle$ et $\tilde{X}|\psi_L\rangle$ sont multipliés par

$$\begin{pmatrix} p^3 + 3p^2(1-p) & 3p(1-p)^2 + (1-p)^3 \\ 3p(1-p)^2 + (1-p)^3 & p^3 + 3p^2(1-p) \end{pmatrix} = \begin{pmatrix} \tilde{p} & 1-\tilde{p} \\ 1-\tilde{p} & \tilde{p} \end{pmatrix}$$

Et donc à la n -ième itération l'état est donc de :

$$\left(\frac{1}{2} + \frac{1}{2}(1-2\tilde{p})^n\right) |\psi_L\rangle \langle\psi_L| + \left(\frac{1}{2} - \frac{1}{2}(1-2\tilde{p})^n\right) \tilde{X} |\psi_L\rangle \langle\psi_L| \tilde{X}$$

Et de même pour un canal de dépolarisation, on a une décroissance exponentielle vers la matrice identité.)

Si on compare les deux protocoles pour L asymptotiquement grand

- Pour les codes correcteurs la probabilité d'erreur est de la forme

$$\left(\tilde{p}(L_0)^{\frac{1}{L_0}}\right)^L$$

qui une fois optimisée en L_0 (car du fait des erreurs de portes possibles on a $\tilde{p}(0) < 1$), indépendamment de L , décroît exponentiellement (pour vraiment comparer il faudrait de plus diviser par la taille du code qui est une constante).

- Pour les répéteurs, à P_M fixé pour n assez grand l'optimum est atteint en $m = n$. On a alors :

$$\frac{(1 - P_M)P_S P_M^n}{((1 - P_M) + P_S(1 - P_M^n))T_0} \propto P_S P_M^n = \exp(-\alpha L_0 + \ln(P_M) \ln(L/L_0) / \ln(2))$$

Alors le L_0 optimum est $\frac{-\log(P_M)}{\alpha}$ et correspond à une décroissance polynomiale en L , plus précisément dès que L_0 est indépendant de L on a un rendement proportionnel à :

$$\propto L^{\log(P_M)}$$

La méthode des répéteurs semble dans ce cas bien plus efficace, mais on a ici supposé que les mémoires utilisées sont parfaites. Si ce n'est pas un problème majeur pour les systèmes de codes correcteurs d'erreur, pour les répéteurs comme la durée d'attente de la communication classique augmente exponentiellement avec n , cela diminue le rendement.

4.2.2 Cas des mémoires imparfaites

On s'intéresse donc ensuite au cas où les mémoires sont imparfaites. Dans le cas des codes correcteurs cela n'influe pas sur le comportement qualitatif du circuit. On prend le modèle de mémoires suivant : on pose $p(t) = \frac{1+e^{-t/\tau}}{2}$ et on prend comme mémoire un canal avec erreur de phase :

$$\mathcal{E}_i(\rho) = p(t/2)\rho + p(t/2)Z\rho Z$$

On montre alors ([14]) que un état de Bell dont les deux qubits sont soumis à une telle erreur possède une fidélité de $p(t)$ et que une permutation d'intrication avec deux tels états donne une fidélité $p(2t)$. Pour calculer le rendement on suppose que l'on possède $NQ_m^{(n)}$ paires de fidélité $p(t_m)$ où t_m est le temps nécessaire pour effectuer la m -ième et dernière permutation standard. En effet on peut supposer qu'à chaque étape avant la m -ième on effectue autant de purifications que nécessaire (ce qui n'est pas forcément possible pour $m+1$) et de plus les erreurs de mémoires commutent avec les effacements et les purifications (car envoient un état de Bell sur un autre état de Bell). On multiplie ensuite le nombre de paires imparfaites obtenues par $E_P(\rho(p(t_m)))$ le nombre asymptotique de paires maximales intriquées pouvant être obtenu à partir de ρ avec communication classique dans un seul sens. Dans le cas présent on a ([18])

$$E_P(\rho(t)) = 1 - H(p(t))$$

ce qui correspond au rendement du protocole de Hachage. On a donc un rendement de :

$$Q_m^{(n)} E_P(t_m) = Q_m^{(n)} E_P(t_m) \simeq \frac{e^{-\alpha L_0} P_M^{2^{n-m+1}+m-2}}{mT_0} \left(1 - H\left(\frac{1 + e^{-L_0 2^{m-1}/c\tau}}{2}\right)\right)$$

Si n reste fini quand L augmente, du fait du terme en P_S , on a une décroissance exponentielle et si $n - m$ est fini comme $L_0 2^{m-1} = L/2^{n-m+1}$ on a aussi une décroissance exponentielle en L . On suppose donc que n ainsi que $n - m$ tendent vers $+\infty$ avec L . Dans ce cas si on ne s'intéresse qu'au comportement exponentiel on a en négligeant les termes polynomiaux :

$$Q_m^{(n)} E_P(t_m) \propto \exp\left(-\alpha L_0 + \frac{L \ln(P_M)}{2^{m-1} L_0}\right) \left(1 - H\left(\frac{1 + e^{-L_0 2^{m-1}/c\tau}}{2}\right)\right)$$

De plus même si $n - m \rightarrow \infty$ il faut que $2^m L_0 = L/2^{n-m}$ tende vers l'infini sinon on a encore une fois une décroissance exponentielle due au terme en P_M . Sous ces conditions, comme $H\left(\frac{1+x}{2}\right) =$

$1 - \frac{1}{2\ln(2)}x^2 + O(x^4)$ on a finalement :

$$Q_m^{(n)} \propto \exp\left(-\alpha L_0 + \frac{L \ln(P_M)}{2^{m-1}L_0} - \frac{2^m L_0}{c\tau}\right)$$

En optimisant on obtient en L_0 et m on obtient :

$$Q_m^{(n)} \propto e^{-2\sqrt{\frac{\ln(1/P_M)}{c\tau}}\sqrt{L}}$$

ce qui est le cas pour une longueur L_0 constante et 2^m en \sqrt{L} , plus précisément :

$$\begin{cases} L_0 \simeq 2 \ln\left(\frac{1}{P_M}\right)/\alpha \\ 2^m \simeq \alpha \sqrt{\frac{2c\tau}{\ln\left(\frac{1}{P_M}\right)}}\sqrt{L} \end{cases}$$

4.3 Comparaison avec ressources finies

4.3.1 Ressources physiques

Les résultats précédents supposent pour la purification que le nombre de mémoires est asymptotiquement grand non seulement pour faciliter l'analyse mais aussi pour permettre l'utilisation du protocole de hachage, tandis que pour les codes correcteurs on se fixe une taille finie du code, ce qui est justifié faisant tendre cette taille vers ∞ on peut pour $L_0 < \ln(2)/\alpha$ obtenir une fidélité arbitraire mais au prix de l'augmentation du nombre de qubits physiques pour un qubit logique, ce qui n'est pas le cas pour les répéteurs quantiques.

Si on s'impose de plus des ressources finies on remarque que comme les codes optimisés on une longueur L_0 fixe il suffit de s'intéresser aux ressources par station.

- Pour un code stabilisateur chaque station est identique et ne nécessite un nombre de portes logiques qui n'est que fonction de la taille du code utilisé.
- Pour un répéteur quantique le nombre de mémoires nécessaires varie entre les stations (selon le nombre d'étapes dans lesquelles elles sont impliquées) et croît avec m c'est-à-dire avec la longueur totale. De plus l'utilisation de protocoles de purification de type IBM augmente le nombre de mémoires nécessaires, en effet effectuer k étapes de purification multiplie le nombre de mémoires par :

$$\prod_{i \leq k} \frac{2}{p_i}$$

où p_i est la probabilité d'échec à l'étape i .

Pour diminuer le nombre de ressources physiques nécessaires on utilise donc aux faibles niveaux un protocole recréant à chaque étape les paires nécessaires à la purification, ce qui augmente en contrepartie le temps. On peut alors calculer le temps ainsi que les ressources physiques nécessaires pour obtenir une fidélité fixée, ce qui est effectué par exemple dans [6] et [10], dont les résultats montrent bien qu'il est possible d'éviter une explosion exponentielle des ressources physiques au prix d'une augmentation du temps nécessaire.

4.3.2 Résultats numériques

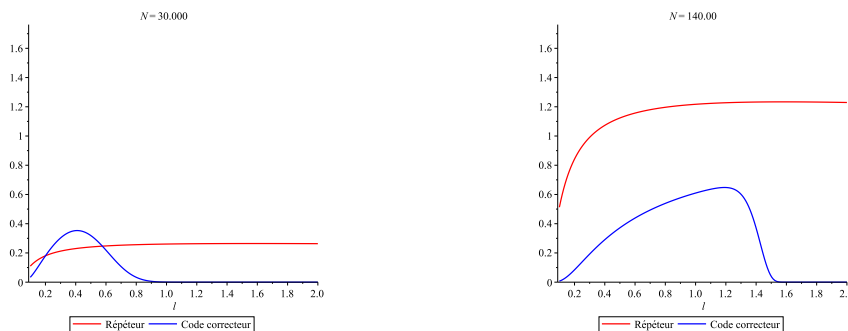
On peut aussi s'intéresser aux performances de différents protocoles explicites à ressources fixées. De même que pour l'analyse asymptotique des mémoires imparfaites on considère tout d'abord

à des mémoires parfaites, en rajoutant ensuite un facteur de purification d'intrication pour les répéteurs. On a pris comme canal un canal à effacement avec $1/\alpha = 25km$ une probabilité d'erreur de porte de 0.01 et une longueur totale de $100km$.

Si on fixe le nombre N de qubits pouvant être traités par station on observe alors :

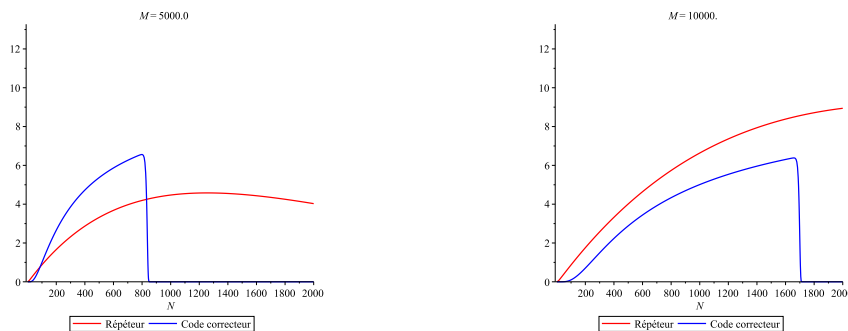
- Que pour N assez faible, le protocole de code correcteur même si la distance L_0 est plus faible possède un meilleur rendement.
- Pour N élevé c'est les répéteurs qui possèdent le meilleur rendement, en effet accroître trop la taille du code n'est plus rentable tandis qu'ajouter des mémoires permet par le traitement en parallèle entre deux stations d'augmenter sensiblement la qualité de transmission.

On représente pour différents N la fidélité atteinte multipliée par le nombre de tels qubits ayant cette fidélité (ce qui explique que les valeurs puissent être > 1)



Un autre critère est non plus de fixer les ressources physiques par station mais plutôt les ressources physiques totales le long de la longueur L . On observe alors un comportement similaire : du fait du parallélisme le protocole de répéteur est bien meilleur. Mais si on implémente de plus dans le protocole de code correcteur plusieurs codes correcteurs et qu'on comptabilise tous les qubits transmis on obtient alors :

- Pour le nombre total M faible le protocole des répéteurs est plus efficace.
- Lorsque ce nombre total augmente, les répéteurs deviennent plus efficaces.



4.4 Équivalence entre purification et codes correcteurs

On peut montrer que si on néglige en premier lieu le problème des mémoires quantiques que les protocoles de purification et les codes correcteurs d'erreur sont équivalents, c'est-à-dire qu'il est

possible d'utiliser un code correcteur (resp. purification) afin d'effectuer une purification (resp. correction d'erreur).

Pour cela il faut distinguer deux types de codes correspondant aux deux types de purification :

- Les codes pouvant détecter les erreurs sans les corriger, dans ce cas Bob doit demander à Alice de renvoyer le message si une erreur est détectée. Ils nécessitent une communication classique dans les deux sens et correspondent aux protocoles de purification avec une communication classique dans les deux sens.
- Les codes pouvant corriger les erreurs (ne nécessitant pas forcément de communication classique), qui correspondent aux protocoles de purification avec communication classique dans les deux sens.

Tout d'abord on peut passer de l'un à l'autre en utilisant la téléportation quantique (5), l'idée étant que celle-ci permet de transformer l'intrication en canal quantique. Ainsi pour passer d'un code correcteur (ou détecteur) à une purification avec communication dans un sens (ou les deux) on utilise le schéma suivant :

- Alice et Bob partagent n paires mal intriquées $\rho^{\otimes n}$. Alice génère m paires de Bell et $n - m$ états auxiliaires $|0\rangle$.
- Alice encode alors un qubit de chacune des m paires de Bell ainsi que les états auxiliaires en un état codé de taille n .
- Elle utilise alors une téléportation quantique à l'aide de $\rho^{\otimes n}$ pour téléporter ces états codés à Bob. Celui-ci applique alors le décodage, les erreurs dues à l'imperfection de l'intrication étant répercutées sur le code en corrigeant les erreurs il obtient ainsi m paires mieux intriquées (ou bien s'il s'agit d'une détection d'erreur il doit de plus communiquer avec Alice pour savoir si la purification est un échec ou non de même que dans le protocole IBM ou Oxford).

Réciproquement il est possible de transformer une purification en code correcteur :

- Alice crée n paires de Bell et elle en envoie la moitié à Bob à travers le canal bruité.
- Alice et Bob effectuent alors un protocole de purification, qui du côté de l'un d'entre eux correspond à un code correcteur d'erreur assisté de signaux classiques.
- Ils utilisent alors les paires restantes par téléportation pour transmettre un état quelconque, modélisant ainsi un canal quantique de meilleure fidélité que l'initial.

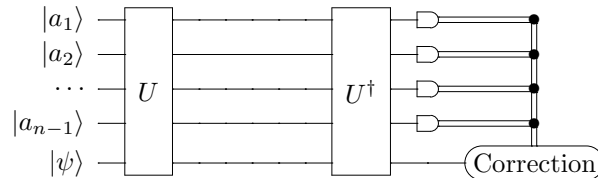
De plus non seulement il existe des schémas permettant de passer de l'un à l'autre, mais il est aussi possible de construire à partir de codes correcteurs une purification et réciproquement (sans utiliser de téléportation quantique). On utilise pour cela la formulation unitaire des codes correcteurs d'erreurs : un code peut être représenté comme une opération unitaire sur les qubits à coder et ceux auxiliaires, transformant la base canonique $|0/1\rangle \otimes |0/1 \dots 0/1\rangle$ en une nouvelle base telle que l'effet d'une erreur (qui s'exprime dans la base canonique) affecte, après retour dans la base canonique les qubits auxiliaires de syndrome permettant de retrouver l'erreur.

Par exemple le code à 3 qubits a pour opération unitaire :

$$U = \begin{array}{c} \text{---} \\ \oplus \\ \text{---} \\ \oplus \\ \text{---} \end{array} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

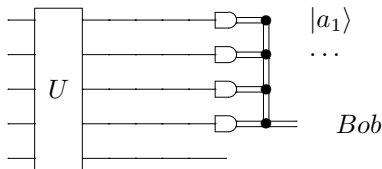
Alors on a $UX_1U^\dagger = X_1X_2X_3$ ce qui permet en mesurant les syndromes de retrouver l'erreur.

Un code quantique peut alors se représenter de manière générale de la manière suivante : Alice prépare les états auxiliaires $|a_i\rangle$ dans $|0\rangle$ ou $|1\rangle$, puis effectue l'encodage unitaire. Bob à la réception effectue U^\dagger . Du fait de la structure de la base induite par U pour chaque erreur des erreurs X_i apparaissent que l'on peut déterminer si Alice envoie de plus à Bob la liste des $|a_i\rangle$:

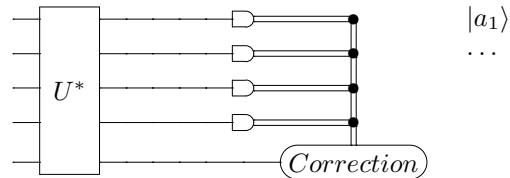


On peut représenter de même les protocoles de purification ([1]) : si Bob et Alice partagent des paires mal intriquées (par exemple issue de $|\phi^+\rangle$), Alice effectue une opération unitaire sur ses qubits puis en mesure un certain nombre d'entre eux avant de communiquer les résultats à Bob. Celui-ci effectue alors U^* sur ses propres paires et mesure les qubits qu'Alice avait précédemment mesuré.

Du côté d'Alice on effectue :



Et de celui de Bob :



Les deux sont bien équivalents car on a $U_A |\phi^+\rangle^{\otimes n} = U_B^t |\phi^+\rangle^{\otimes n}$ c'est-à-dire que l'opération d'Alice revient à encoder les qubits, la différence étant que la mesure des syndromes se fait des deux côtés.

De même que précédemment on obtient une équivalence entre code correcteur et purification avec communication classique dans un seul sens et entre codes détecteurs et purification avec communication classique dans les deux sens.

Cette équivalence sans construction supplémentaire permet par exemple de déduire du protocole de hachage l'existence d'un code de distance minimale d à n qubits corrigeant $nS(W_{1-\frac{d-1}{2n}})$ erreurs ([1]).

Malgré cette équivalence théorique on peut expliquer la différence entre les protocoles avec codes correcteurs et ceux avec répéteurs :

- Dans le cas des codes correcteurs les opérations s'effectuent en série, les unes après les autres ce qui explique la faible dépendance vis à vis des mémoires (à chaque nouvelle étape on oublie celles précédentes) mais aussi les plus faibles fidélités.

- Dans le cadre des répéteurs les purifications sont effectuées en parallèle, en effet la transmission de l'information n'est effectuée qu'à la fin du protocole à l'aide de la téléportation quantique. Cela présente l'avantage d'augmenter la fidélité mais rend aussi plus sensible aux erreurs de mémoires.

Conclusion

La problématique de la transmission fidèle de l'information quantique permet de mettre en avant les particularités de la théorie de l'information quantique : si elle s'approche de la théorie de l'information classique le caractère unitaire des transformations ainsi que la notion d'intrication font apparaître des limites théoriques strictes (théorème de non clonage) mais aussi de nouvelles possibilités telles que la téléportation quantique.

Ainsi une fois le formalisme associé à la matrice densité et aux interactions avec l'environnement introduit, on observe qu'il est possible de définir de même que dans le cas classique des codes correcteurs d'erreur quantique, les difficultés émergeant du caractère non classique des qubits et des transformations étant résolues par des propriétés propres au monde quantique. De plus la gestion de l'intrication permet d'utiliser des protocoles de répéteurs quantiques utilisant la téléportation quantique (analogue en terme d'intrication au canal dans le cas des codes correcteurs) ainsi que des procédures de purification (analogues aux codes correcteurs). La différence entre ces deux méthodes qui partagent des éléments théoriquement équivalents est issue de l'architecture particulière de chacune d'entre elles rendant les répéteurs plus efficaces asymptotiquement mais aussi plus dépendant des mémoires.

Afin d'implémenter de manière efficace des transmissions de qubits à longue distance, il est donc nécessaire d'optimiser cette architecture non seulement en équilibrant le temps et les ressources nécessaires avec des protocoles partiels mais aussi en augmentant la qualité des opérations et des mémoires que ce soit au niveau physique ou bien en utilisant des codes correcteurs au niveau de celles-ci et à l'intérieur des répéteurs. Il existe notamment des réalisations expérimentales de codes correcteurs et de répéteurs quantique ([15]) implémentant des stratégies physiques supplémentaires pour augmenter l'efficacité. Du point de vue théorique une question qui se pose est la quantification précise de l'intrication, question proche de celle de la capacité des canaux quantiques.

D'un point de vue personnel ce stage ayant initialement pour problématique les seuls codes correcteurs d'erreur avant d'aborder des sujets connexes et complémentaires comme la théorie de l'information quantique et les répéteurs quantiques m'a permis d'acquérir une première expérience de recherche dans ce domaine à la croisée des mathématiques et de la physique.

A Propriétés de la matrice densité

A.1 Liberté d'écriture de la matrice densité

On peut caractériser les états donnant naissance à la même matrice densité ; plus précisément on a $\sum_i p_i |\psi_i\rangle \langle \psi_i| = \sum_i q_i |\phi_i\rangle \langle \phi_i|$ ssi :

$$\sqrt{p_i} |\psi_i\rangle = \sum_j u_{i,j} \sqrt{q_j} |\phi_j\rangle$$

avec $(u_{i,j})$ une matrice unitaire (quitte à rajouter des $q_i = 0$ on peut supposer qu'il y a autant de $|\psi\rangle$ que de $|\phi\rangle$).

En effet si $\sqrt{p_i} |\psi_i\rangle = \sum_j u_{i,j} \sqrt{q_j} |\phi_j\rangle$ alors on a :

$$\begin{aligned} \sum_i p_i |\psi_i\rangle \langle \psi_i| &= \sum_i \left(\sum_j u_{i,j} \sqrt{q_j} |\phi_j\rangle \right) \left(\sum_k u_{i,k}^* \sqrt{q_k} \langle \phi_k| \right) \\ &= \sum_{j,k} \sum_i u_{i,j} u_{i,k}^* \sqrt{q_j q_k} |\phi_j\rangle \langle \phi_k| \\ &= \sum_{j,k} \delta_{j,k} \sqrt{q_j q_k} |\phi_j\rangle \langle \phi_k| \\ &= \sum_i q_i |\phi_i\rangle \langle \phi_i| \end{aligned}$$

Réciproquement si $\sum_i p_i |\psi_i\rangle \langle \psi_i| = \sum_i q_i |\phi_i\rangle \langle \phi_i|$ alors comme le produit de deux matrices unitaires est unitaire et que ρ est diagonalisable en base orthonormée on peut supposer que $(|\phi_i\rangle)$ est orthonormée et donc $\sum_i q_i = 1$. On peut alors écrire :

$$|\psi_i\rangle = \sum_j c_{i,j} |\phi_j\rangle$$

On obtient :

$$\begin{aligned} \sum_i p_i |\psi_i\rangle \langle \psi_i| &= \sum_i p_i \left(\sum_j c_{i,j} |\phi_j\rangle \right) \left(\sum_k c_{i,k}^* \langle \phi_k| \right) \\ &= \sum_{j,k} \sum_i p_i c_{i,j} c_{i,k}^* |\phi_j\rangle \langle \phi_k| \\ &= \sum_l q_l |\phi_l\rangle \langle \phi_l| \end{aligned}$$

Donc par indépendance des $|\phi_j\rangle \langle \phi_k|$ on obtient :

$$\sum_i (\sqrt{p_i} c_{i,j}) (\sqrt{p_i} c_{i,k})^* = q_j \delta_{j,k}$$

Donc $u_{i,j} = c_{i,j} \sqrt{\frac{p_i}{q_j}}$ est unitaire et on a :

$$\sqrt{p_i} |\psi_i\rangle = \sum_j u_{i,j} \sqrt{q_j} |\phi_j\rangle$$

A.2 Écriture d'une opération quantique comme une somme d'opérateurs

On se donne un système Q et $\mathcal{E} : \mathcal{H}_Q \mapsto \mathcal{H}_Q$ (on peut toujours se ramener avec le même espace au départ et à l'arrivée) tel que :

- Pour toute matrice densité ρ on a :

$$0 \leq \text{tr}(\mathcal{E}(\rho)) \leq 1$$

(Physiquement, cela veut dire que on s'autorise aussi des mesures).

- Pour p_i des coefficients positifs de somme 1 et ρ_i des matrices densités :

$$\mathcal{E} \left(\sum_i p_i \rho_i \right) = \sum_i p_i \mathcal{E}(\rho_i)$$

- Pour tout \mathcal{H}_R et $\sigma \in \mathcal{L}(\mathcal{H}_Q \otimes \mathcal{H}_R)$ on a :

$$(1_R \otimes \mathcal{E}) \sigma \text{ est un opérateur autoadjoint positif}$$

En particulier pour $R = \emptyset$, on obtient le fait que \mathcal{E} envoie une matrice densité sur une matrice densité (à une renormalisation correspondant à la mesure près).

Remarque : La dernière condition est importante, elle signifie que non seulement \mathcal{E} est une transformation valide pour le système isolé mais aussi pour le système couplé avec un environnement.

Par exemple $\mathcal{E}(\rho) = \rho^T$ n'est pas une transformation valide : même si elle vérifie bien toutes les conditions pour un système isolé, on a :

$$\begin{aligned} (1 \otimes \rho) \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \frac{\langle 00| + \langle 11|}{\sqrt{2}} \right) &= \frac{1}{2} (|00\rangle \langle 00| + |11\rangle \langle 11| + |01\rangle \langle 10| + |10\rangle \langle 01|) \\ &= \frac{1}{2} \left(|00\rangle \langle 00| + |11\rangle \langle 11| + \left(\frac{|01\rangle + |10\rangle}{\sqrt{2}} \right) \left(\frac{\langle 01| + \langle 10|}{\sqrt{2}} \right) - \left(\frac{|01\rangle - |10\rangle}{\sqrt{2}} \right) \left(\frac{\langle 01| - \langle 10|}{\sqrt{2}} \right) \right) \end{aligned}$$

Qui n'est donc pas un état physique.

Alors on peut écrire \mathcal{E} sous la forme :

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$$

On voit facilement que tout $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$ vérifie ces conditions.

De plus toute telle opération quantique peut s'écrire comme somme d'opérateurs, i.e il existe des E_k linéaires tels que $\sum_k E_k E_k^\dagger \leq 1$ et :

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$$

Pour cela on prend Q^* un espace de Hilbert de même dimension que Q . Soient $(|i_Q\rangle)$ et $(|i_{Q^*}\rangle)$ des bases orthonormées respectives.

On pose :

$$\begin{aligned} \sigma &= (1_{Q^*} \otimes \mathcal{E}) \left(\sum_i |i_Q\rangle \langle i_{Q^*}| \right) \left(\sum_j \langle j_Q| \langle j_{Q^*}| \right) \\ &= \sum_{i,j} |i_{Q^*}\rangle \langle j_{Q^*}| \mathcal{E}(|i_Q\rangle \langle j_Q|) \end{aligned}$$

qui représente l'effet du canal sur un état intriqué de manière maximale. On diagonalise σ dans une base orthonormale de $\mathcal{H}_Q \otimes \mathcal{H}_{Q^*}$ (pas forcément normée) :

$$\sigma = \sum_k |s_k\rangle \langle s_k|$$

On pose alors :

$$E_k = \sum_i \langle i_{Q^*} | s_k \rangle \langle i_Q | \in \mathcal{L}(\mathcal{H}_Q)$$

On obtient :

$$\begin{aligned} \sum_k E_k |\psi\rangle \langle \psi| E_k^\dagger &= \sum_k \sum_{i,j} \langle i_{Q^*} | s_k \rangle \langle i_Q | \psi \rangle \langle \psi | j_Q \rangle \langle s_k | j_{Q^*} \rangle \\ &= \sum_{i,j} \langle i_Q | \psi \rangle \langle \psi | j_Q \rangle \sum_k \langle i_{Q^*} | s_k \rangle \langle s_k | j_{Q^*} \rangle \\ &= \sum_{i,j} \langle i_Q | \psi \rangle \langle \psi | j_Q \rangle \langle i_{Q^*} | \sigma | j_{Q^*} \rangle \\ &= \sum_{i,j} \langle i_Q | \psi \rangle \langle \psi | j_Q \rangle \mathcal{E}(|i_Q\rangle \langle j_Q|) \\ &= \mathcal{E} \left(\sum_{i,j} \langle i_Q | \psi \rangle |i_Q\rangle \langle j_Q| \langle \psi | j_Q \rangle \right) \\ &= \mathcal{E}(|\psi\rangle \langle \psi|) \end{aligned}$$

Et comme $\mathcal{E}(\sum_i p_i \rho_i) = \sum_i p_i \mathcal{E}(\rho_i)$ on a bien le résultat souhaité (la condition sur $\sum_k E_k E_k^\dagger$ découle de celle sur la trace).

De plus comme $\dim(\mathcal{H}_Q \otimes \mathcal{H}_R) = d^2$, on en déduit que on peut toujours prendre l'environnement qui a une dimension au plus d^2 .

B Portes logiques

Comme dans le cas classique on peut définir des portes quantiques opérant sur les qubits. Physiquement il s'agit de l'application d'un hamiltonien spécifique \mathcal{H} sur le système durant un temps t qui se traduit par une transformation unitaire $U = e^{-i\frac{\mathcal{H}t}{\hbar}}$. En particulier comme la transformation est unitaire les portes logiques sont réversibles.

B.1 Portes à 1 qubit

Les opérations à un qubit correspondent sont les matrices unitaires (à un facteur de phase près) de dimension deux. On note en particulier les opérateurs de Pauli :

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Notée respectivement :

$$\text{---} \boxed{Z} \text{---} \quad \text{---} \boxed{X} \text{---} \quad \text{---} \boxed{Y} \text{---}$$


Alors on a toute opération unitaire peut s'écrire sous la forme (à une phase près) :

$$U = \exp(-i\theta \vec{n} \cdot \vec{\sigma} / 2) = \exp\left(-\frac{i\theta}{2}(n_x X + n_y Y + n_z Z)\right)$$

Cette écriture peut s'interpréter sur la sphère de Bloch : il s'agit d'un certain point de vue en fait d'une rotation d'angle θ autour du vecteur \vec{n} .

Ainsi appliquer X revient à effectuer une rotation de π autour de l'axe x ce qui échange bien $|0\rangle$ et $|1\rangle$ (mais transforme $|-x\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ en $-|-x\rangle$ tout en laissant invariant $|+x\rangle$).

En plus des portes de Pauli d'autres sont beaucoup utilisées dont notamment la porte de Hadamard :

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$


échangeant $|0\rangle, |1\rangle$ avec $\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ et correspondant aussi à une rotation de π autour de $(1/\sqrt{2}, 0, 1/\sqrt{2})$, ainsi que :

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

Toutes ces portes à l'exception de T appartiennent au groupe de Clifford c'est-à-dire stabilisent \mathcal{P} le groupe de Pauli.

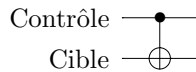
B.2 Porte CNOT

De même que pour un seul qubit on peut définir des portes ayant un nombre quelconque k de qubits en entrée (et autant en sortie du fait de la réversibilité) comme des opérateurs unitaires de dimension 2^k .

Une porte très utile est la porte CNOT (Controlled-NOT) prenant en entrée un qubit de contrôle et qubit cible et appliquant une porte X à ce dernier ssi le premier est dans l'état $|1\rangle$, autrement dit appliquant $|0\rangle\langle 0| \otimes 1 + |1\rangle\langle 1| \otimes X$:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

que l'on représente :



Que l'on peut généraliser en des portes appliquant U de manière contrôlée i.e $|0\rangle\langle 0| \otimes 1 + |1\rangle\langle 1| \otimes U$:



On peut montrer que de manière générale n'importe quelle porte à n qubits (opérateur unitaire de dimension n) peut se décomposer en un circuit composé de portes à un qubit et de portes CNOT ([12]).

B.3 Opérateur BXOR

Alice et Bob partagent deux paires, plus précisément Alice possède les qubits 1 et 3 et Bob ceux 2 et 4, les qubits 1 et 2 étant intriqués ainsi que ceux 3 et 4.

Alice effectue une porte CNOT avec 1 comme qubit de contrôle et 3 comme cible et Bob fait de même avec 2 comme contrôle et 4 comme cible.

On obtient alors avec la notation :

BXOR	Contrôle
Cible	Contrôle/Cible

la décomposition dans la base de Bell de cette opération donne :

BXOR	ϕ^+	ϕ^-	ψ^+	ψ^-
ϕ^+	ϕ^+/ϕ^+	ϕ^-/ϕ^+	ψ^+/ψ^+	ψ^-/ψ^+
ϕ^-	ϕ^-/ϕ^-	ϕ^+/ϕ^-	ψ^-/ψ^-	ψ^+/ψ^-
ψ^+	ϕ^+/ψ^+	ϕ^-/ψ^+	ψ^+/ϕ^+	ψ^-/ϕ^+
ψ^-	ϕ^-/ψ^-	ϕ^+/ψ^-	ψ^-/ϕ^-	ψ^+/ϕ^-

C États de Bell

Les états de Bell sont des états d'un système à deux qubits :

$$\begin{cases} |\phi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\ |\phi^-\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) \\ |\psi^+\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) \\ |\psi^-\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) \end{cases}$$

C.1 Propriétés des états de Bell

Les états de Bell vérifient de nombreuses propriétés. La première est la raison historique pour laquelle ils ont été introduits : on peut montrer que ceux-ci violent les inégalités dites de Bell prouvant ainsi la pertinence de la mécanique quantique (et excluant tout modèle de variables cachées).

D'après leur définition si on mesure un des deux qubits d'un état de Bell alors l'état du second est entièrement déterminé : par exemple si on mesure le premier qubit de $|\phi^\pm\rangle$ selon la base canonique $|0\rangle, |1\rangle$, alors l'état du second après la mesure est identique à l'état du premier.

Les états de Bell sont des états maximalelement intriqués et forment une base pour un système à deux qubits et sont donc particulièrement adaptés à l'étude de l'intrication.

C.2 Construction des états de Werner

Une autre propriété est l'invariance selon des rotations de SU_2 appliquées localement au deux qubits. Plus précisément soit U une transformation unitaire, alors :

$$(U \otimes U^*) |\phi^+\rangle = |\phi^+\rangle$$

En effet on a :

$$\begin{aligned} \langle \phi^+ | U \otimes U^* | \phi^+ \rangle &= \frac{1}{2} (\langle 00 | U \otimes U^* | 00 \rangle + \langle 00 | U \otimes U^* | 11 \rangle + \langle 11 | U \otimes U^* | 00 \rangle + \langle 11 | U \otimes U^* | 11 \rangle) \\ &= \frac{1}{2} (|\langle 0 | U | 0 \rangle|^2 + |\langle 0 | U | 1 \rangle|^2 + |\langle 1 | U | 0 \rangle|^2 + |\langle 1 | U | 1 \rangle|^2) = 1 \end{aligned}$$

On a donc $U \otimes U^*$ qui laisse invariant $|\phi^+\rangle$ et agit comme une rotation de SU_3 sur dans l'espace vectoriel engendré par $|\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle$.

Pour une matrice ρ qui s'écrit dans la base de Bell sous la forme :

$$\rho = \begin{pmatrix} F & \alpha_1^* & \alpha_2^* & \alpha_3^* \\ \alpha_1 & a_{1,1} & a_{1,2} & a_{1,3} \\ \alpha_2 & a_{2,1} & a_{2,2} & a_{2,3} \\ \alpha_3 & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

On a alors si on applique $U \otimes U^*$:

- Le terme F reste constant.
- Le vecteur $\vec{\alpha}$ se transforme comme sous l'action d'une rotation $R \in SU_3$.
- La matrice $A = (a_{i,j})$ subi aussi une rotation et devient RAR^\dagger .

Si on applique de manière successive de telles opérations de manière aléatoire (on peut même se restreindre à un nombre fini de rotations [5]) alors ρ devient :

$$\frac{1}{N} \sum_i (U_i \otimes U_i^*) \rho (U_i \otimes U_i^*)^\dagger$$

c'est-à-dire :

- F reste constant.
- On a $\vec{\alpha}$ devient $\frac{1}{N} \sum_i R_i \vec{\alpha}$ qui tend vers 0 si les U_i aléatoires.
- Et A devient $\frac{1}{N} \sum_i R_i A R_i^\dagger$ qui tend vers $\frac{1}{3} \text{tr}(A) \mathbf{1}_3 = \frac{1-F}{3} \mathbf{1}_3$.

Et donc finalement on a bien un état de Werner :

$$\rho_F = \begin{pmatrix} F & 0 & 0 & 0 \\ 0 & \frac{1-F}{3} & 0 & 0 \\ 0 & 0 & \frac{1-F}{3} & 0 \\ 0 & 0 & 0 & \frac{1-F}{3} \end{pmatrix}$$

Références

- [1] Hans Aschauer. *Quantum communication in noisy environments*. PhD thesis, lmu, 2005.
- [2] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, 70(13) :1895, 1993.
- [3] Charles H Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A Smolin, and William K Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical Review Letters*, 76(5) :722, 1996.
- [4] Charles H Bennett, David P DiVincenzo, and John A Smolin. Capacities of quantum erasure channels. *Physical Review Letters*, 78(16) :3217, 1997.
- [5] Charles H Bennett, David P DiVincenzo, John A Smolin, and William K Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5) :3824, 1996.
- [6] H-J Briegel, W Dür, Juan I Cirac, and Peter Zoller. Quantum repeaters : The role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26) :5932, 1998.
- [7] David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, and Anna Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Physical Review Letters*, 77(13) :2818, 1996.
- [8] Simon J Devitt, William J Munro, and Kae Nemoto. Quantum error correction for beginners. *Reports on Progress in Physics*, 76(7) :076001, 2013.
- [9] W Dür, H-J Briegel, JI Cirac, and P Zoller. Quantum repeaters based on entanglement purification. *Physical Review A*, 59(1) :169, 1999.
- [10] L Hartmann, B Kraus, H-J Briegel, and W Dür. Role of memory errors in quantum repeaters. *Physical Review A*, 75(3) :032310, 2007.
- [11] WJ Munro, AM Stephens, SJ Devitt, KA Harrison, and Kae Nemoto. Quantum communication without the necessity of quantum memories. *Nature Photonics*, 2012.
- [12] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.
- [13] Jean-Michel Raimond. Introduction à la mécanique quantique. Cours de L3, 2012-2013.
- [14] M Razavi, M Piani, and N Lütkenhaus. Quantum repeaters with imperfect memories : cost and scalability. *Physical Review A*, 80(3) :032301, 2009.
- [15] Nicolas Sangouard, Christoph Simon, Hugues De Riedmatten, and Nicolas Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, 83(1) :33, 2011.
- [16] Benjamin Schumacher. Quantum coding. *Physical Review A*, 51(4) :2738, 1995.
- [17] J.H van Lint. *Introduction to coding theory*. Springer, 1982.
- [18] G Vidal, W Dür, and JI Cirac. Entanglement cost of mixed states. *arXiv preprint quant-ph/0112131*, 2001.