République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

المدرسة الوطنية العليا المتعددة التقنيات
Ecole Nationale Supérieure Polytechnique

Ecole Nationale Polytechnique
Département Electronique

Thèse de Doctorat en Electronique

Présentée par

Aziz Mouzali

Magister en physique à l'USDB

Intitulée

Codes Convolutifs Quantiques

Soutenue publiquement le 16 /04 /2014 devant le jury composé de :

Pr M.S .Boucherit	*ENP*	*Président de jury*
Pr F.Merazka	*USTHB*	*Directrice de thèse*
Pr L.Hamami	*ENP*	*Examinatrice*
Pr A.Guessoum	*USDB*	*Examinateur*
Pr S.Bouroubi	*USTHB*	*Examinateur*

ENP 2014

Remerciements

Je remercie Dieu de m'avoir donné le courage et l'énergie nécessaires à l'accomplissement de ce travail difficile mais passionnant. Je remercie ma directrice de thèse pour sa patience et ses orientations utiles tout au long de cette thèse. Je remercie les membres de jury d'avoir accepté d'évaluer ce travail à travers leurs critiques constructives qui ont aidé à améliorer son contenu. Je remercie ma famille pour sa patience et son soutien durant les moments de fatigue et de nervosité. Je remercie monsieur Damian Markham pour son apport très utile à ce travail, lors de mon séjour au laboratoire de traitement et communication de l'information (LTCI) à Paris. Enfin, je remercie mes collègues pour leur soutien moral et leurs encouragements qui m'ont aidé à aller jusqu'au bout de cette tâche.

Table des matières

Chapitre II : Les codes correcteurs d'erreur quantiques

Chapitre III : Simulation du code convolutif à cinq qubits

Chapitre IV : Le partage de secret quantique

ملخص

الاعلام الكمي هو تركيب بين نظرية الاعلام و ميكانيكا الكم و يوفر فرص غير موجودة في الحالة الكلاسيكية بفضل خصائص معينة لحوامل المعلومات (qubits) التي تحكمها ميكانيكا الكم. من بين هذه ألخصائص تراكب و تشابك الحالات الكمية التى تمكن الحساب المتوازي وبعض البروتوكولات مثل «téléportation». واحدة من صعوبات الاعلام الكمي هي حساسية حوامل المعلومات الى البيئة الخارجية التي تعطل حالاتهم من خلال إدخال أخطاء في المعلومات المقدمة. لمواجهة هذه الظاهرة التى تسمى «decoherence» وضعت الرموز الكمية المصححة للخطأ. سننظر في هذا العمل الرموز الكمية الإلتوائية «convolutifs» المنجزة لحماية التدفقات المستمرة للمعلومات المنقولة عبر مسافات طويلة. وسيخصص جزء ثاني لبروتوكول خاص هو تقاسم سر كمى باستخدام خمسة qubits التي تنتقل عن طريق قنوات صاخبة وحمايتها من قبل ثلاثة رموز تصحيح الخطأ.

الكلمات الرئيسية : الكوبية , تشابك , تراكب , الرموز الإلتوائية , تقاسم سر كمى

Résumé

L'information quantique est une synthèse entre la théorie de l'information et la mécanique quantique. Elle offre des opportunités inexistantes dans le cas classique grâce à certaines propriétés des porteurs d'information (qubits) qui sont gouvernés par la mécanique quantique. Parmi ces propriétés, la superposition d'état et l'intrication qui permettent le calcul parallèle et certains protocoles quantiques tels que la téléportation. L'une des difficultés de l'information quantique est l'extrême sensibilité des qubits à l'environnement extérieur qui perturbe leur état en introduisant des erreurs dans l'information transmise. Afin de contrer ce phénomène appelé décohérence, des codes correcteurs d'erreur quantique ont été élaborés. Nous allons nous pencher dans ce travail sur les codes convolutifs quantiques destinés à la protection de flux continus d'information transmis à de longues distances. Une deuxième partie sera consacrée à un protocole de communication quantique particulier qui est le partage de secret à l'aide de cinq qubits transmis par des canaux bruités et protégés par trois codes correcteurs d'erreur.

Mots clés: Qubit, intrication, superposition, code convolutif , partage de secret quantique.

Summary

Quantum information is a synthesis between information theory and quantum mechanics. It offers opportunities not existing in the classical case thanks to properties of information holders (qubits) which are governed by quantum mechanics. Among these properties, the superposition and entanglement state enabling parallel computing and some protocols such as quantum teleportation. One of the difficulties of quantum information is the qubit extreme sensitivity to the external environment that disrupts their state by introducing errors in the provided information. To counteract this phenomenon called decoherence a quantum error correcting codes have been developed. We will consider in this work the quantum convolutional codes for the protection of continuous information flows transmitted over long distances. A second part will be devoted to a particular quantum communication protocol which is secret sharing using five qubits transmitted through noisy channels and protected by three error correcting codes.

Keywords : Qubit, entanglement, superposition, convolutional code, Quantum secret sharing.

Liste des figures

Liste des tableaux

Annexes : Simulations sur Maple

Introduction Générale

Introduction générale

Le traitement classique de l'information est effectué à l'aide de supports physiques dont les propriétés sont gouvernées par la physique classique. En effet, les bits d'information classiques sont par exemple représentés par des condensateurs chargés d'électrons (bit de valeur 1) ou bien complètement déchargés (bit de valeur 0). Le traitement quantique de l'information repose sur l'utilisation de supports physiques obéissant à la mécanique quantique. Un électron unique peut à lui seul être un support physique d'information : selon que son spin est haut ou bas il porte le bit 0 ou 1. Cependant, l'électron (contrairement au condensateur qui est exclusivement chargé ou vide) peut être dans un état superposé de spin haut et de spin bas. Dans ces conditions, l'unité élémentaire d'information quantique (appelé qubit) peut être 0, 1 ou bien une superposition linéaire quelconque des deux valeurs. Cette différence fondamentale avec l'information classique donne en théorie une supériorité énorme à l'information quantique. Cependant, si l'ordinateur classique est aujourd'hui une réalité partout présente, sa version quantique, elle, reste un idéal lointain à cause de très grandes difficultés expérimentales qui sont loin d'être résolues. Parmi elles, le phénomène de décohérence qui est la perturbation de l'état des qubits portant l'information par leur interaction avec le monde extérieur. Pour résoudre ce problème, des codes correcteurs d'erreurs quantiques ont été élaborés, parmi eux les codes convolutifs utilisés dans les communications à grande distance de flux d'information par des canaux bruités. On note toutefois que les ordinateurs classiques vont atteindre leur limite de performance lorsque les circuits électroniques auront des tailles tellement petites que les lois de la mécanique quantique remettront en cause leur bon fonctionnement. Depuis une vingtaine d'année des tentatives se font pour construire un ordinateur quantique sans grand succès. Néanmoins, la théorie de l'information quantique s'est beaucoup développée et un grand nombre d'algorithmes quantiques a été élaboré et simulé sur des ordinateurs classiques en attendant de l'être sur un ordinateur quantique [1]. Sur le plan pratique, des protocoles de communication quantique ont été réalisés avec un nombre restreint de qubits.

Ce travail de thèse se divise globalement en quatre parties. D'abord, une vue d'ensemble de l'information quantique sera donnée au chapitre I avec en premier quelques rappels utiles de mécanique quantique. On introduira au chapitre II les codes correcteurs d'erreurs quantiques et on décrira au chapitre III le code convolutif à cinq qubits et son implantation sur un ordinateur classique. Enfin, on va étudier au chapitre IV un protocole de communication quantique particulier qui est le partage de secret par un état de graphe à cinq qubits transmis par cinq canaux dépolarisants et protégés séparément par trois codes correcteurs quantiques.

Problématique

Problématique

L'un des problèmes majeurs du traitement quantique de l'information est la perturbation de l'état des porteurs d'information (décohérence), malgré toutes les tentatives de leur isolement du monde extérieur. Les codes correcteurs d'erreur quantiques ont pour finalité de protéger les qubits et corriger les erreurs sur l'information transmise. Ces codes corrigent parfaitement les erreurs sur un qubit, mais si plusieurs qubits sont infectés la correction peut réussir ou aboutir à l'échec. L'objet de ce travail consiste à investiguer le comportement de certains de ces codes lorsque des erreurs de canal se produisent sur deux qubits lors de la transmission et à comparer leur efficacité dans la protection des qubits.

La seconde partie de cette thèse a pour but l'étude d'un protocole de communication quantique appelé partage de secret dont l'originalité est l'utilisation de canaux bruités pour transmettre les qubits portant le secret. L'objet du travail est d'intégrer des codes correcteurs quantiques à ce protocole afin de protéger les qubits transmis et corriger les erreurs entachant le secret partagé. En réalité, l'objectif global futur est d'élaborer un formalisme général qui unifie le partage de secret, les codes correcteurs, le calcul quantique basé sur la mesure et la téléportation au moyen des états intriqués des qubits appelés les états de graphes.

Chapitre I :

Fondements de l’Information Quantique

I.1 Introduction

L'information quantique bien traitée dans la référence **[1]** est une synthèse entre la théorie de l'information classique et la mécanique quantique. Le tableau 1 résume les différences fondamentales entre les systèmes physiques classiques et les systèmes physiques quantiques qui font aussi la différence entre l'information classique et l'information quantique. L'outil de base de l'information quantique est le qubit (quantum bit) qui est une unité d'information portée par un système physique quantique pouvant avoir deux niveaux d'énergie représentés par deux états propres $|0\rangle$ et $|1\rangle$ de son hamiltonien. L'intérêt du qubit est qu'il peut être dans une superposition de ces deux états $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ qui permet de réaliser certaines performances impossibles avec des bits classiques. Nous présentons dans ce chapitre les fondements essentiels de l'information quantique en donnant d'abord des rappels de mécanique quantique.

Physique Classique	Physique Quantique
Un système physique se trouve à un instant donné en un seul état à la fois parmi ses états possibles.	Un système physique peut se trouver à un instant donné dans une superposition de ses états.
Les transformations d'états d'un système physique sont en général irréversibles.	Sans mesure les transformations d'états d'un système isolé sont réversibles et déterministes.
La mesure d'un système physique n'altère pas son état et donne le même résultat si elle est répétée dans les mêmes conditions. Elle donne le meme résultat pour un système identique.	La mesure de l'état d'un système physique modifie cet état de manière irréversible et donne des résultats différents si elle est répétée dans les mêmes conditions.
Il est possible de copier l'état d'un système sur un autre.	Il est impossible de copier l'état d'un système sur un autre.
L'état global d'un système composé de plusieurs sous système est toujours un produit des états des sous systèmes.	L'état global d'un système composé de sous système n'est pas toujours un produit des états de ces sous systèmes.

Tableau 1 : Les différences fondamentales entre les systèmes physiques classiques et les systèmes physiques quantiques.

I.2 Rappels de mécanique quantique

La mécanique quantique est une théorie qui décrit les propriétés et interactions des systèmes matériels microscopiques. Nous allons présenter dans ce chapitre les éléments de cette théorie utiles à l'information quantique et qui sont traités en détail dans la référence [2]. La référence [3] introduit en détail le calcul quantique pour des non-physiciens.

I.2.1 Espace de Hilbert

L'espace de Hilbert H est un espace vectoriel abstrait qui sert à représenter mathématiquement les états physiques des objets quantiques. Chaque état physique correspond à un vecteur de cet espace de dimension allant de 1 à l'infini. Tout vecteur peut être multiplié par un scalaire réel ou complexe pour obtenir un vecteur qui représente un autre état physique de l'objet quantique. On peut construire le produit scalaire de deux vecteurs pour représenter l'état physique d'un système de deux objets quantiques. Le résultat du produit scalaire dépend de l'ordre : $u.v=(v.u)^*$ avec l'asterisk pour désigner le complexe conjugué. En particulier, $u.u=(u.u)^*$ car le produit d'un vecteur avec lui-même (sa norme) est un nombre réel positif. En réalité, il est plus convenable d'utiliser une base orthonormée de vecteurs $\{u_i\}$ appartenant à H tel que $u_i.u_j=\delta_{ij}$ où δ_{ij} est le symbole de Kronecker égal à 1 pour i=j et 0 pour i≠j. On écrit un vecteur v de H comme une combinaison linéaire de vecteurs u_i, $v=\sum\alpha_i u_i$. Un cœfficient α_j est obtenu par produit scalaire : $u_j.v=\sum\alpha_i u_j u_i=\sum\alpha_i\delta_{ij} = \alpha_j$ ou $v.u_j= \alpha_j^*$. Le produit $\alpha_i\ \alpha_i^* = |\alpha_i|^2$ représente la probabilité pour que l'objet se trouve dans l'état u_i donnant alors $\sum|\alpha_i|^2=1$ [3].

I.2.2 Notation de Dirac

Dans la notation de Dirac le vecteur représentant l'état physique d'un système quantique est noté $|\psi\rangle$ (ket) et son conjugué $\langle\psi|$ (bras). La décomposition sur une base $|i\rangle$ s'écrit $|\psi\rangle=\sum_i \alpha_i|i\rangle$ avec $\langle i|j\rangle=\delta_{ij}$, $\langle i|\psi\rangle=\alpha_i$ et $\langle\psi|i\rangle=\alpha_i^*$**.** Le produit scalaire avec un vecteur $\phi=\sum_i \beta_i|i\rangle$ est $\langle\phi|\psi\rangle=\langle\psi|\phi\rangle^*=\sum_i \beta_i^*\alpha_i$.

I.2.3 Opérateurs

C'est un élément mathématique A qu'on peut écrire sous forme de matrice qui transforme un ket en un autre $A|\Psi\rangle=|\Psi'\rangle$ ou bien $\langle\phi|A=\langle\phi'|$. Nous obtenons $\langle\phi|\psi'\rangle=\langle\phi'|\psi\rangle=\langle\phi|A|\psi\rangle$ qui représente la variation de la valeur de A lorsque le système transite d'un état physique $|\psi\rangle$ vers un autre $|\phi\rangle$. L'opérateur est donc la représentation mathématique d'une action physique sur le système quantique.

Les opérateurs sont linéaires, $A(|\psi\rangle+|\phi\rangle)=A|\psi\rangle+A|\phi\rangle$ et $(A+B)|\psi\rangle=A|\psi\rangle+B|\psi\rangle$. Si le système subit deux actions physiques successives représentées par les opérateurs A et B nous écrirons $AB|\psi\rangle=A(B|\psi\rangle)$ où B représente la première action dans le temps. L'opérateur A possède un transposé ou adjoint qui est défini par : $A|\Psi\rangle=|\Psi'\rangle$ d'où $\langle\psi|A^t=\langle\psi'|$ ou bien $\langle\phi|A|\psi\rangle=\langle\psi|A^t|\phi\rangle^*$. On peut écrire un ket quelconque $|\psi\rangle=\sum_i\langle i|\psi\rangle|i\rangle$ où $\langle i|\psi\rangle=\alpha_i$ est un nombre qu'on peut permuter avec $|i\rangle$ pour obtenir $|\psi\rangle=\sum_i|i\rangle\langle i|\psi\rangle$. On utilise l'opérateur $P_i=|i\rangle\langle i|$ qui projette $|\psi\rangle$ sur le ket unitaire $|i\rangle$ de la base $|i\rangle$: $P_i|\psi\rangle=|i\rangle\langle i|\psi\rangle=\alpha_i|i\rangle$. Le ket s'écrit $|\psi\rangle=\sum_i P_i|\psi\rangle$ ou $\langle\psi|=\sum_i\langle\psi|P_i$. Le produit scalaire est : $\langle\psi|\psi\rangle=\sum_i\langle\psi|P_i|\psi\rangle=\langle\psi|\sum_i P_i|\psi\rangle=1$. Ce résultat étant valable pour tout ket $|\psi\rangle$, on déduit $\sum_i|i\rangle\langle i|=1=\sum_i P_i$ appelée relation de fermeture où 1 est l'opérateur identité qui laisse les kets et les opérateurs inchangés. Les opérateurs sont groupés en classes parmi lesquelles les opérateurs hermitiens ($A=A^t$) et unitaires ($A^t=A^{-1}$). Ces deux classes servent à décrire les phénomènes quantiques.

I.2.4 Vecteurs et matrices

Un ket peut être écrit sur une base à deux dimension par exemple sous forme d'un vecteur colonne $|\psi\rangle=\begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix}$ et un bras sous forme d'un vecteur ligne $\langle\psi|=(\alpha_1^*,\alpha_2^*)$. Le produit direct donne alors $|\psi\rangle\langle\psi|=\begin{pmatrix}\alpha_1\alpha_1^*,\alpha_1\alpha_2^*\\ \alpha_2\alpha_1^*,\alpha_2\alpha_2^*\end{pmatrix}$ qui est la matrice densité. Les opérateurs aussi peuvent être écrits sous forme matricielle. En utilisant la relation de fermeture avec deux indices i et j on aura :

$$A|\psi\rangle=\sum_{i,j}|i\rangle\langle i|A|j\rangle\langle j|\psi\rangle$$

Avec $A_{ij}=\langle i|A|j\rangle$, $\langle j|\psi\rangle=\alpha_j$, $\beta_i=\sum_j A_{ij}\alpha_j$

où A_{ij} sont les éléments de la matrice A. On obtient alors la décomposition du nouvel état sur la base $|i\rangle$:

$$A|\psi\rangle=\sum_i\beta_i|i\rangle$$

Nous pouvons aussi exprimer le produit de deux opérateurs comme un produit matriciel :

$$\langle i|BA|j\rangle=\sum_k\langle i|B|k\rangle\langle k|A|j\rangle=(BA)_{ij}=\sum_k B_{ik}A_{kj}$$

La matrice de l'opérateur adjoint est définie par ses éléments: $\langle i|A^t|j\rangle=\langle j|A|i\rangle^*$ donc : $A_{ij}^t=A_{ji}^*$ et on déduit alors $(AB)^t=B^tA^t$.

I.2.5 Valeurs et vecteurs propres

Soit un opérateur A et un ket $|\psi\rangle$ tels que $A|\psi\rangle = \lambda|\psi\rangle$ où λ est un nombre quelconque. Dans ce cas $|\psi\rangle$ est appelé vecteur propre de A avec la valeur propre λ. Nous interprétons λ comme le résultat de la mesure de la grandeur physique représentée par A lorsque le système quantique se trouve dans l'état $|\psi\rangle$. Les valeurs propres peuvent être déterminées en utilisant le formalisme matriciel :

$$A|\psi\rangle = \lambda|\psi\rangle \text{ donc } \sum_i \beta_i |i\rangle = \lambda \sum_i \alpha_i |i\rangle \text{ avec } \beta_i = \sum_j A_{ij}\alpha_j \text{ d'où :}$$

$$\sum_j (A_{ij} - \lambda\delta_{ij})\alpha_j = 0$$

La résolution se fait en annulant le déterminant :

$$\begin{vmatrix} A_{11}-\lambda & \cdots & A_{1n} \\ \cdot & A_{22}-\lambda & \cdots & A_{2n} \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ A_{n1} & \cdots & A_{nn}-\lambda \end{vmatrix} = 0$$

Nous obtenons un polynôme d'ordre n dont les racines sont les n valeurs propres de la matrice A qui sont indépendantes de la base choisie. Pour obtenir les vecteurs propres (leurs composantes dépendent de la base choisie) il suffit de résoudre les équations $\sum_j (A_{ij} - \lambda\delta_{ij})\alpha_j = 0$ pour chaque valeur propre λ déterminée. Notons que tout vecteur propre multiplié par $e^{i\phi}$ reste un vecteur propre avec la même valeur propre. Il arrive aussi qu'une seule valeur propre corresponde à deux vecteurs propres différents (dégénérescence). Dans ce dernier cas la combinaison linéaire des deux vecteurs propres est aussi vecteur propre. La matrice A peut donc s'écrire $A = S\Lambda S^{-1}$ avec Λ une matrice diagonale contenant sur sa diagonale les valeurs propres de A et S une matrice formée des vecteurs propres de A.

I.2.6 Trace d'un opérateur

On peut la définir par l'écriture matricielle tr(A)= $\sum_i \langle i|A|i\rangle = \sum_i A_{ii}$. On peut donc écrire tr(A)=tr $(S\Lambda S^{-1})$ =tr($\Lambda S^{-1}S$) = tr (Λ) car la trace est invariante par permutation cyclique. La trace d'un opérateur est donc la somme de ses valeurs propres et elle est par conséquent indépendante de la base choisie.

I.2.7 Opérateurs hermitiens

Un opérateur A hermitien a toujours des valeurs propres réelles : $A|a\rangle = a|a\rangle$ donc $\langle a|A|a\rangle = a\langle a|a\rangle$ de même $\langle a|A^t|a\rangle = a^*\langle a|a\rangle$. Puisque A=A^t nous avons a=a* donc a est un nombre réel. Nous montrons aussi que les vecteurs propres d'un opérateur hermitien sont orthogonaux :

$A|a_1\rangle = a_1|a_1\rangle$ et $A|a_2\rangle = a_2|a_2\rangle$ ou bien $\langle a_1|A = \langle a_1|a_1$ et $\langle a_2|A = \langle a_2|a_2$. Le produit donne alors $\langle a_2|A|a_1\rangle = a_1\langle a_2|a_1\rangle = a_2\langle a_2|a_1\rangle$ et par conséquent $\langle a_2|a_1\rangle = 0$. Les vecteurs propres d'un opérateur hermitien peuvent donc constituer une base pour cet opérateur.

I.2.8 Commutateurs

Nous avons en général $BA|\psi\rangle \neq AB|\psi\rangle$ et nous disons alors que les opérateurs A et B ne sont pas commutatifs. Dans certains cas deux opérateurs commutent (AB$|\psi\rangle$=BA$|\psi\rangle$ $\forall$ ψ) donc [A,B]=AB-BA=0 où [A,B] est appelé commutateur. Parmi les propriétés d'un commutateur nous avons la nullité de sa trace tr([A,B])=tr(AB-BA)=tr(AB)-tr(BA)=0.

I.2.9 Opérateurs unitaires

Un opérateur unitaire (U^t=U^{-1}) conserve la norme des kets sur lesquels il s'applique : $U|\psi\rangle = |\psi'\rangle \; et \; \langle\psi|U^t = \langle\psi'|$ ou $\langle\psi'|\psi'\rangle = \langle\psi|U^tU|\psi\rangle = \langle\psi|\psi\rangle$ car U^{t}U=U^{-1}U=1. De la même façon on montre que le produit entre deux kets quelconques est conservé si on leur applique un opérateur unitaire : $U|\psi\rangle = |\psi'\rangle \; et \; \langle\phi|U^t = \langle\phi'|$ ou $\langle\phi'|\psi'\rangle = \langle\phi|U^tU|\psi\rangle = \langle\phi|\psi\rangle$. Le produit de deux opérateurs unitaires est un opérateur unitaire : (UV)^t(UV)=(V^{t}U^{t}UV)=V^{t}V=1 car U^t=U^{-1} et V^t=V^{-1}. Nous montrons aussi que les vecteurs propres d'un opérateur unitaire sont orthogonaux et ses valeurs propres égales à l'unité :

$U|\psi_1\rangle = \lambda_1|\psi_1\rangle \; et \; U|\psi_2\rangle = \lambda_2|\psi_2\rangle \quad donc \quad \langle\psi_1|U^tU|\psi_2\rangle = \lambda_1^*\lambda_2\langle\psi_1|\psi_2\rangle = \langle\psi_1|\psi_2\rangle$ Pour un seul ket quelconque $|\psi\rangle = |\psi_1\rangle = |\psi_2\rangle$ nous obtenons $\lambda_1^*\lambda = |\lambda|^2 = 1 \; donc \; \lambda = 1$. Pour deux kets et deux valeurs propres différentes nous aurons $(\lambda_1^*\lambda_2 - 1)\langle\psi_1|\psi_2\rangle = 0 \; d'où : \langle\psi_1|\psi_2\rangle = 0$. Tout opérateur unitaire U peut être associé à un opérateur hermitien A tel que U=exp(-iA). En effet, une valeur propre λ_j de U étant de module égal à un on peut l'écrire λ_j=exp(-iα_j) avec α_j un nombre réel tel que

$A|\psi_j\rangle = \alpha_j|\psi_j\rangle$ et $U|\psi_j\rangle = \lambda_j|\psi_j\rangle$ ($|\psi_j\rangle$ ket propre commun aux opérateurs A et U). L'exponentiel d'une matrice diagonale est défini par $\exp\left[\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right] = \begin{pmatrix} \exp(a) & 0 \\ 0 & \exp(b) \end{pmatrix}$. Pour une matrice quelconque A on procède d'abord à sa diagonalisation : $\exp(A)=\exp(S\Lambda S^{-1})=S\exp(\Lambda)S^{-1}$.

I.2.10 Systèmes physiques

Les propriétés d'un système quantique et son évolution sont décrites en utilisant la notation de Dirac. L'une de ces propriétés est son énergie qui sera représentée par un opérateur hermitien H appelé l'hamiltonien du système. Soit une base propre orthonormée { $|j\rangle$ } de H telle que $H|j\rangle = \hbar\omega_j|j\rangle$ avec $\lambda_j = \hbar\omega_j$ la valeur propre correspondant à l'état $|j\rangle$. Le système peut être dans une combinaison linéaire des états de base $|\psi\rangle = \sum_j \alpha_j|j\rangle$. Lorsque le système évolue dans le temps nous décrivons son évolution par l'équation de Schrödinger dépendante du temps $\frac{\partial}{\partial t}|\psi\rangle = -i\frac{H}{\hbar}|\psi\rangle$ dont la solution est $|\psi\rangle = U(t)|\psi(0)\rangle$ avec U(t)=exp(-iHt/ħ) l'opérateur unitaire associé à l'hamiltonien H et appelé propagateur. Dans certaines situations le système peut avoir des interactions complexes avec le monde extérieur tel que l'hamiltonien peut varier avec le temps. Souvent, on peut le considérer comme constant sur un petit intervalle de temps et on peut écrire par exemple $|\psi(t)\rangle = U_1....U_n|\psi(0)\rangle$ avec $U_i=\exp(-iH_it/\hbar)$. Notons qu'on applique sur $|\psi(t)\rangle$ en premier U_1 puis U_2 et ainsi de suite jusqu'à U_n.

I.3 La sphère de Bloch

C'est un outil mathématique représenté sur la figure 1 qui permet de décrire efficacement un qubit. En effet, sachant que $|\alpha|^2 + |\beta|^2 = 1$ on peut écrire : $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$ avec $0 \le \theta \le \pi$ et $0 \le \Phi \le 2\pi$ les angles sphériques. Le qubit peut donc être représenté par un point d'une sphère de rayon égal à l'unité localisé par les angles θ et Φ reliés aux cœfficients α et β . On peut aussi considérer l'état $|\psi\rangle$ comme un vecteur d'origine le centre de la sphère et d'extrémité un point de cette sphère. Les états de base $|0\rangle$ (θ=0) et $|1\rangle$ (θ=π) correspondent respectivement au pole nord et au pole sud de la sphère. Parmi les qubits intéressants en information quantique les points qui se trouvent sur l'équateur de la sphère de Bloch et correspondant à une superposition équiprobable $|\alpha| = |\beta| = 1/\sqrt{2}$.

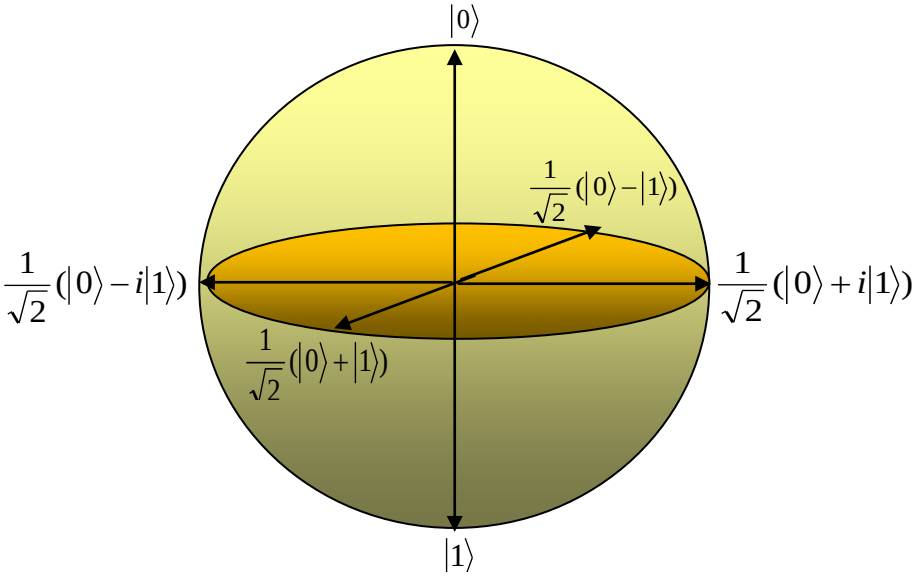

Figure 1 : La sphère de Bloch

I.4 Matrice densité

L'état d'un qubit peut être décrit par un ket $|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ ou un bra $\langle\psi| = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}$ et les états de base sont donc donnés par $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ et $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. On construit deux produits différents qui sont respectivement la norme et la matrice densité de l'état:

$$\langle\psi|\psi\rangle = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha^*\alpha + \beta^*\beta = 1 \quad \text{et} \quad |\psi\rangle\langle\psi| = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}\begin{pmatrix}\alpha^* & \beta^*\end{pmatrix} = \begin{pmatrix}\alpha\alpha^* & \alpha\beta^*\\ \beta\alpha^* & \beta\beta^*\end{pmatrix}.$$

Nous constatons que la matrice densité est de trace égale à l'unité et peut représenter un opérateur hermitien. Le qubit peut être aussi dans un mélange d'états décrit par la matrice densité :

$$\rho = \sum_n P_n |\psi_n\rangle\langle\psi_n| = \sum_n P_n \rho_n$$

avec $|\psi_n\rangle = \alpha_n|0\rangle + \beta_n|1\rangle$ des états dits pures et $P_n \geq 0$ la probabilité ou poids de chacun d'eux. Puisque chaque matrice ρ_n est hermitienne alors la matrice ρ l'est aussi. De plus, $tr(\rho_n) = 1$ et $\sum P_n = 1$ entraîne que $tr(\rho) = 1$. Chaque état mélangé est illustré par un point donné de la sphère de Bloch. La matrice densité décrit l'évolution du qubit dans le temps :

Nous avons : $|\psi(t)\rangle = U(t)|\psi(0)\rangle$ et l'expression conjuguée $\langle\psi(t)| = \langle\psi(0)|U^t(t)$ donc :

$|\psi(t)\rangle\langle\psi(t)| = U(t)|\psi(0)\rangle\langle\psi(0)|U^t(t)$ d'où : $\rho(t) = U(t)\rho(0)U^t(t)$.

I.5 Matrices de Pauli

Ce sont quatre matrices 2X2 unitaire et hermitiennes définies par $\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$; $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. La matrice densité peut alors s'écrire comme une combinaison linéaire des matrices de Pauli : $|\psi\rangle\langle\psi| = (1/2)(\sigma_0 + s_x\sigma_x + s_y\sigma_y + s_z\sigma_z)$ avec s_x, s_y et s_z des coefficients réels tel que $s_x^2 + s_y^2 + s_z^2 = 1$. De même, tout hamiltonien qui s'applique sur un qubit peut s'écrire comme une combinaison linéaire des matrices de Pauli qui sont alors un bon outil mathématique pour décrire les états et les interactions du qubit.

I.6 Propagateurs

Les propagateurs associés aux hamiltoniens H du qubit donnés par U(t)=exp(-iHt/ħ) décrivent l'évolution dans le temps de l'état du qubit $|\psi(t)\rangle = U(t)|\psi(0)\rangle$. Etant unitaires ils possèdent un inverse et s'ensuit que toute évolution dans le temps du qubit est réversible en absence de mesure, contrairement à celle d'un système classique qui est irréversible. Par ailleurs, les propagateurs réalisent une transformation unitaire qui conserve la norme des kets sur lesquels ils s'appliquent. Nous notons que puisque les matrices de Pauli sont unitaires elles peuvent être des propagateurs et correspondre à des portes logiques quantiques lesquelles sont une combinaison appropriée de propagateurs.

I.7 Portes logiques quantiques

Le traitement quantique de l'information consiste à stoker l'information dans un qubit puis à la manipuler par des portes logiques quantiques. Comme son homologue classique, la porte quantique transforme le qubit d'un état vers un autre. Pour cela il suffit d'ajouter à l'hamiltonien du système une perturbation contrôlée qui le fait évoluer selon une transformation unitaire réversible. Avec un bit classique unique il existe deux portes réversibles, NOT qui change le bit 0 en 1 et vis versa et IDENTITÉ qui le laisse inchangé. Il existe aussi deux portes irréversibles, SET qui impose au bit la valeur 1 et CLEAR qui le transforme en 0 quelque soit sa valeur initiale.
Ces deux dernières portes ne peuvent être réalisées par des transformations unitaires. Les matrices de Pauli σ_0 et σ_x peuvent être des portes logiques IDENTITÉ et NOT respectivement

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad ; \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad ; \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad ; \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

La matrice σ_x joue le rôle d'un propagateur qui peut être relié à un hamiltonien. En effet, Puisque $\exp(-i\theta\sigma_j)=\cos(\theta)\sigma_0 - i\sin(\theta)\sigma_j$ on obtient pour j=x et $\theta=\pi/2$ $\exp(-i\pi\sigma_x/2)=-i\sigma_x$ ou bien exp(-iH)=U (on ignore le facteur -i car c'est juste une phase globale).

La porte quantique NOT appliquée à un état général agit comme son équivalente classique, $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}\beta\\ \alpha\end{pmatrix}$. En écrivant le ket en coordonnées polaires on obtient :

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\cos(\theta/2)\\ e^{i\phi}\sin(\theta/2)\end{pmatrix}=\begin{pmatrix}e^{i\phi}\sin(\theta/2)\\ \cos(\theta/2)\end{pmatrix}=e^{i\phi}\begin{pmatrix}\cos((\pi-\theta)/2)\\ e^{-i\phi}\sin((\pi-\theta)/2)\end{pmatrix}$$

En négligeant le terme de phase global $e^{i\phi}$, on constate que NOT fait tourner le vecteur Ket de 180° autour de l'axe ox dans la sphère de Bloch. La porte NOT appliquée deux fois fait tourner le ket de 360° qui revient donc logiquement à l'état initial. De manière générale un propagateur $U=\exp(-i\theta\sigma_j/2)$ correspondant à l'application sur le qubit d'un hamiltonien $H=\theta\sigma_j/2$ fait tourner le ket d'un angle θ autour de j=x,y ou z dans la sphère de Bloch. L'angle de rotation dépend de l'intensité et de la durée d'application de l'hamiltonien. La rotation d'un angle 90° autour de l'axe ox correspond au propagateur $\exp(-i(\pi/2)\sigma_x/2)=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -i\\ -i & 1\end{pmatrix}$ qui transforme un état de base en superposition, $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -i\\ -i & 1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -i\end{pmatrix}$ et $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -i\\ -i & 1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}-i\\ 1\end{pmatrix}$.

L'application deux fois donne la porte NOT, $\frac{1}{2}\begin{pmatrix}1 & -i\\ -i & 1\end{pmatrix}\begin{pmatrix}1\\ -i\end{pmatrix}=-i\begin{pmatrix}0\\ 1\end{pmatrix}$ et $\frac{1}{2}\begin{pmatrix}1 & -i\\ -i & 1\end{pmatrix}\begin{pmatrix}-i\\ 1\end{pmatrix}=-i\begin{pmatrix}1\\ 0\end{pmatrix}$. Pour cette raison on appelle cette porte purement quantique (pas d'équivalent classique) la racine carrée de NOT. En réalité, tout propagateur qui fait tourner un ket d'un angle quelconque autour d'un des trois axes est une porte logique quantique réalisée par un hamiltonien adéquat appliqué pendant un temps convenable. Parmi les portes quantiques les plus importantes celle d'Hadamard $H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ et la porte de phase $S=\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$. La première transforme un état de base en superposition:

$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix}=|+\rangle$ et $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix}=|-\rangle$.

L'application deux fois fait retourner le qubit à l'état initial :

$$\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix}=\begin{pmatrix}1\\ 0\end{pmatrix} \text{ et } \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ -1\end{pmatrix}=\begin{pmatrix}0\\ 1\end{pmatrix}.$$

La porte d'Hadamard correspond à une rotation de 180° autour d'un axe décalé de 45° par rapport à l'axe des x et en direction de l'axe z. La porte S fait tourner le Ket $|1\rangle$ de 90° autour de oz et laisse le Ket $|0\rangle$ inchangé :

$\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=\begin{pmatrix}1\\ 0\end{pmatrix}$ et $\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}=i\begin{pmatrix}0\\ 1\end{pmatrix}=\begin{pmatrix}\cos(\theta/2)\\ e^{i\phi}\sin(\theta/2)\end{pmatrix}$ avec θ=π et Φ=π/2.

La porte S est considérée comme la racine carrée de la porte σ_z car l'application deux fois sur le Ket $\begin{pmatrix}0\\ 1\end{pmatrix}$ donne $\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\begin{pmatrix}0\\ i\end{pmatrix}=\begin{pmatrix}0\\ -1\end{pmatrix}$ ce qui correspond à θ=π et une rotation Φ=π autour de l'axe z. La porte σ_z donne aussi $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}=\begin{pmatrix}0\\ -1\end{pmatrix}$ et $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=\begin{pmatrix}1\\ 0\end{pmatrix}$.

I.8 Réseaux quantiques

Un réseau quantique est un assemblage adéquat de n portes quantiques appliquées sur un ou plusieurs qubits et destiné à réaliser un traitement donné de l'information. On prend comme exemple le réseau HSSH :

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

Ce réseau est donc équivalent à NOT puisque $HSSH=H\sigma_zH=\sigma_x$.

I.9 Système de deux qubits

La supériorité théorique de l'information apparaît lorsqu'on utilise plusieurs qubits. Prenons l'exemple de deux qubits qu'on identifie par a et b et qui peuvent être dans un des quatre états de base $|ab\rangle=|00\rangle,\ |01\rangle,\ |10\rangle,\ et\ |11\rangle$. Le système peut aussi être dans une superposition des états de base $|ab\rangle=\alpha|00\rangle+\beta|01\rangle+\gamma|10\rangle+\chi|11\rangle$ qui appartient à un espace de Hilbert à quatre dimensions. Les états d'un système à n qubits appartiennent à un espace de Hilbert à 2^n dimensions ce qui présage de la puissance d'un ordinateur quantique s'il existera un jour. Les portes quantiques agissant sur un tel système sont un produit de n portes agissant chacune sur un qubit. Par exemple on applique IH sur $|00\rangle$: $IH|00\rangle=|0\rangle(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)=\frac{1}{\sqrt{2}}(|00\rangle+|01\rangle))$ où $I=\sigma_0$ s'applique sur le premier qubit et H sur le second.

On peut représenter un système de deux qubit respectivement dans l'état $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ et $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$ par une matrice colonne de la façon suivante :

$$|\psi_1\psi_2\rangle = \begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix}\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} = \begin{pmatrix}\alpha_1\alpha_2\\ \alpha_1\beta_2\\ \beta_1\alpha_2\\ \beta_1\beta_2\end{pmatrix}$$

Par exemple :

$$|00\rangle = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad ; \quad |01\rangle = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|10\rangle = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad ; \quad |11\rangle = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Il est possible de représenter l'application d'une porte quantique sur un système de plusieurs qubit par une matrice. Reprenons le cas précédent de deux qubit :

$$IH|00\rangle = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\\0\\0\end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$$

Parmi les portes quantiques à deux qubits les plus intéressantes la porte

controlled-Not:
$$CN = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} = \begin{pmatrix}I & 0\\ 0 & \sigma_x\end{pmatrix}$$

Appliquons cette porte sur les quatre états de base :

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=CN|00\rangle=|00\rangle,\quad \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}0\\1\\0\\0\end{pmatrix}=\begin{pmatrix}0\\1\\0\\0\end{pmatrix}=CN|01\rangle=|01\rangle,$$

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=CN|10\rangle=|11\rangle,\quad \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}0\\0\\1\\0\end{pmatrix}=CN|11\rangle=|10\rangle$$

Nous constatons donc que cette porte change la valeur du second qubit seulement lorsque le premier a la valeur 1. Nous qualifions le premier qubit de qubit contrôleur et le second de qubit cible. On montre qu'une combinaison de CN et de portes à un qubit constitue un réseau capable de réaliser toutes les opérations du calcul quantique. On peut écrire CN à l'aide de matrices densités :

$$CN=|0\rangle\langle 0|I+|1\rangle\langle 1|\sigma_x=\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix}+\begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

D'où :

$$CN=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}+\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

La porte CN est utile dans la théorie de l'information quantique mais lors des implémentations expérimentales on utilise la porte controlled-Z qui lui est proche :

$$CZ=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix}$$

Cette dernière réalise la transformation $CZ=|11\rangle=-|11\rangle$ et laisse les trois autres kets de la base inchangés. On peut passer de CZ à CN en utilisant la porte d'Hadamard, (IHCZIH)=CN ou bien :

$$CN = \frac{1}{2}\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\end{pmatrix}\begin{pmatrix}1 & 1 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{pmatrix}\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\end{pmatrix} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$$

I.10 Circuits quantiques

Les réseaux à deux qubits sont plus simples à décrire en les illustrant par des circuits. Dessinons le circuit de la porte (IH)(CZ)(IH) = CN :

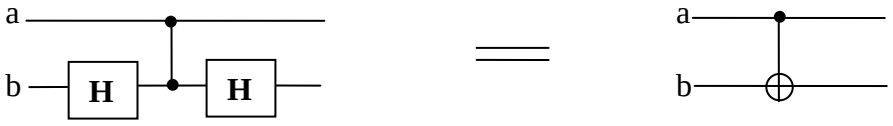

Figure 2 : Porte Controlled-not.

Les deux traits horizontaux correspondent chacun à un qubit alors que le trait vertical représente la porte CZ. Les deux carrés expriment la double action de H sur le qubit b intercalée par l'action de CZ. Notons donc que le temps s'écoule de gauche à droite. Le petit cercle noir sur le trait horizontal indique que le qubit associé à ce trait contrôle la valeur de l'autre. Remarquons la différence entre les dessins de gauche et de droite, à gauche nous avons un contrôle mutuel alors qu'à droite seul le premier contrôle le second qui est sa cible. Le dessin de droite illustre la porte CN ou le symbole $\oplus$ sur le trait du bas indique l'action sur le second qubit b, $0 \oplus b = b$ et $1 \oplus b = \text{NOT}(b)$ veut dire que ce qubit change de valeur seulement lorsque le premier vaut 1. Nous allons dessiner un circuit intéressant appelé SWAP formé d'une triple application de CN sur deux qubits a et b :

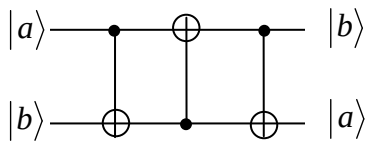

Figure 3 : Porte SWAP.

La porte SWAP permute les états des deux qubits sur lesquels elle s'applique. La seconde action NOT est obtenue par la matrice suivante :

$$I|0\rangle\langle 0| + \sigma_x|1\rangle\langle 1| = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{pmatrix} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\end{pmatrix}$$

Prenons l'exemple des Kets $|01\rangle$ et $|10\rangle$:

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

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

Nous avons donc : $SW|01\rangle = |10\rangle$ et $SW|10\rangle = |01\rangle$.

I.11 Les états intriqués

L'état d'un système à plusieurs qubits est intriqué s'il n'est pas égal à un produit d'états individuels de ces qubits. Ainsi, chaque qubit n'a plus d'état intrinsèque mais dépend du reste du système dont toute évolution agit sur lui. Un moyen simple pour générer un état intriqué à partir d'un état basique à deux qubits $|ab\rangle$ est la porte CNH = $(CN)_{ab}H_aI_b$:

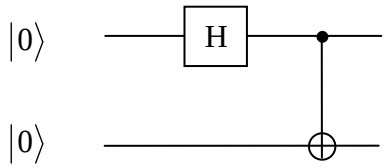

Figure 4 : Porte CNH.

$$H_a I_b = \left(\frac{1}{\sqrt{2}}\right)\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix} = \left(\frac{1}{\sqrt{2}}\right)\begin{pmatrix}1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{pmatrix}$$

$$CNH|00\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1\\0\\1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$$

$$CNH|10\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1\\0\\-1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}$$

Nous avons donc :

$$CNH|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad ; \qquad CNH|10\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$CNH\ |00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\ ;\ CNH\ |10\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

On peut écrire le calcul autrement : $H_a I_b|00\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

$CN\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(CN|00\rangle + CN|10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (CN étant une transformation unitaire elle est donc linéaire). La particularité d'un état intriqué apparaît lorsqu'on mesure l'un des deux qubits. Par exemple si on mesure le qubit a de l'état $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ on trouve 0 avec une probabilité 1/2 et on sait dans l'immédiat que b à la même valeur 0. La mesure sur a peut aussi donner la valeur 1 avec la probabilité 1/2 et l'on sait par conséquent que b à la valeur 1. Nous constatons que l'état de b n'est pas mesuré mais indirectement déduit de la mesure de a avec qui il est intriqué.

Il existe une infinité d'états intriqués parmi lesquels les quatre états de Bell qui sont :

$$\phi^{\pm} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \quad et \quad \psi^{\pm} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$

Les états de Bell sont dits maximalement intriqués car ils sont les plus éloignés des états dits séparables lesquels sont égaux à un produit direct d'états indépendants des deux qubits. Ils constituent une base orthonormée à quatre dimensions pour les états maximalement intriqués. L'intrication qui n'a pas d'équivalent classique joue un rôle fondamental en information quantique.

I.12 Mesure et décohérence

Parmi les portes qui ne sont pas unitaires READOUT qui permet de lire le résultat d'une mesure. Nous allons décrire mathématiquement l'effet d'une mesure sur un état quantique. La matrice densité initiale est $|\psi\rangle\langle\psi| = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}\begin{pmatrix}\alpha^* & \beta^*\end{pmatrix} = \begin{pmatrix}\alpha\alpha^* & \alpha\beta^*\\ \beta\alpha^* & \beta\beta^*\end{pmatrix}$ alors que la matrice

densité après mesure $\rho = \sum_n P_n |\psi_n\rangle\langle\psi_n| = \sum_n P_n \rho_n$ est un mélange des états pures avec n=0,1 donc $\rho = \alpha\alpha^* |0\rangle\langle 0| + \beta\beta^* |1\rangle\langle 1| = \alpha\alpha^* \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \beta\beta^* \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha\alpha^* & 0 \\ 0 & \beta\beta^* \end{pmatrix}$.

La mesure annule donc les éléments non diagonaux de la matrice densité de l'état initial. Nous parlons de décohérence car les termes non diagonaux correspondent à un état de superposition cohérent du système. Considérons de plus prés le problème de la mesure sur un qubit unique se trouvant dans l'état inconnu $\psi = \alpha|0\rangle + \beta|1\rangle$.

La mesure consiste à déterminer les valeurs de α et β, ce qui nécessite d'effectuer plusieurs fois l'opération. Or, la première mesure transforme la superposition initiale Ψ en un état de base $|0\rangle$ ou $|1\rangle$. Les mesures suivantes donneront le même résultat $|0\rangle$ (ou $|1\rangle$) car le phénomène de décohérence ne concerne pas les états de base mais les superpositions d'états. En fait, la décohérence se produit lorsque le système quantique interagit avec l'environnement extérieur. Ce phénomène est l'ennemi essentiel de l'information quantique et rend impératif d l'isolement des qubits du monde extérieur. Notons que la décohérence ne peut être contournée en disposant de plusieurs copies semblables de l'état inconnu $\psi = \alpha|0\rangle + \beta|1\rangle$ car cela est impossible à cause du théorème de non clonage.

I.13 Théorème de non clonage

Ce théorème qui n'a pas d'équivalent classique exprime l'impossibilité de copier l'état inconnu $\psi = \alpha|0\rangle + \beta|1\rangle$ d'un qubit dans un autre qubit. Remarquons d'abord qu'il est possible de copier l'état de base $|a\rangle$ d'un qubit a sur un qubit b ayant la valeur initiale $|0\rangle$ en utilisant la porte à deux qubit CN, $|ab\rangle = |00\rangle \to |00\rangle$; $|ab\rangle = |10\rangle \to |11\rangle$. Nous avons donc un transfert de l'état de a vers b. Soit l'état $\psi = \alpha|0\rangle + \beta|1\rangle$ qu'on voudrait reproduire sur un autre qubit se trouvant dans l'état $|0\rangle$. L'application de CN sur le système donne : $CN\,|\psi\rangle|0\rangle = CN\,(\alpha|00\rangle + \beta|10\rangle) = \alpha|00\rangle + \beta|11\rangle$. Comparons le résultat obtenu avec l'état final du système constitué de deux copies semblables :
$|\psi\psi\rangle = (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) = \alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle$ Ces deux expressions ne sont égales que dans deux cas $(\alpha = 1, \beta = 0)$ ou $(\alpha = 0, \beta = 1)$ c'est-à-dire les états de base $|0\rangle$ ou $|1\rangle$. Le non clonage est d'une part problématique pour le calcul quantique mais d'autre part utile en cryptographie. Dans le premier cas le problème qui se pose est l'impossibilité d'utiliser le résultat d'une étape de calcul dans la suite car sa lecture équivaut à le copier sur un autre support quantique ce qui est interdit. Dans le second cas le non clonage empêche d'espionner une communication censée être confidentielle.

I.14 Fidélité

La manipulation des qubits ne peut se faire sans commettre des erreurs. On se pose alors la question de savoir dans quelle mesure les résultats des mesures sont proches de la vérité. Pour cela, on introduit la notion de fidélité définie par :

$F(|\phi\rangle,|\psi\rangle) = |\langle\phi|\psi\rangle|^2 = \langle\psi|\phi\rangle\langle\phi|\psi\rangle$ où $|\phi\rangle$ est l'état mesuré et $|\psi\rangle$ l'état réel.

On peut aussi comparer l'état pur d'un qubit $\psi = \alpha|0\rangle + \beta|1\rangle$ à son état mélangé décrit par sa matrice densité $\rho = \sum_n P_n |\psi_n\rangle\langle\psi_n| = \sum_n P_n \rho_n$. On défini dans ce cas la fidélité par $F(\rho,|\psi\rangle) = \langle\psi|\rho|\psi\rangle$. Vérifions pour le cas $\rho = |\psi\rangle\langle\psi|$, on a $F = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}\alpha\alpha^* & \alpha\beta^* \\ \beta\alpha^* & \beta\beta^*\end{pmatrix}\begin{pmatrix}\alpha \\ \beta\end{pmatrix} = (|\alpha|^2 + |\beta|^2)^2 = 1$ ce qui est logique. Considérons aussi l'état d'un qubit après mesure et son état pur initial, $F = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}\alpha\alpha^* & 0 \\ 0 & \beta\beta^*\end{pmatrix}\begin{pmatrix}\alpha \\ \beta\end{pmatrix} = |\alpha|^4 + |\beta|^4 = 1 - 2|\alpha|^2|\beta|^2$ avec F=1 pour α=0 ou β=0 (la mesure ne modifie que les états superposés). La mesure a le maximum d'effet pour $|\alpha| = |\beta| = \frac{1}{\sqrt{2}}$ qui donne F=1/2. On montre que F vaut en moyenne 2/3 pour un cas général. Cette modification de l'état quantique après mesure permet de déduire qu'il y a eu espionnage lors d'une communication confidentielle.

I.15 Calcul quantique

Le calcul quantique [3] consiste à manipuler l'état d'un circuit quantique. La procédure générale c'est de disposer d'un système de n qubits qu'il faut isoler de l'environnement extérieur. On commence par initialiser le système en mettant par exemple tous les qubits à l'état $|0\rangle$ ce qui nous fournit un registre d'entrée représenté par le ket $|00.....0\rangle$. Nous procédons alors à la transformation graduelle de l'état global en appliquant à chaque étape des portes quantiques à un ou plusieurs qubits. Physiquement, on fait évoluer les qubits par des actions adéquates telles que l'interaction avec des lasers. Enfin, on peut aussi utiliser des lasers afin de lire les résultats en mesurer l'état des qubits. La figure 5 illustre le calcul quantique où t_0 et t sont l'instant initial et l'instant de mesure et $U(t, t_0)$ un opérateur unitaire d'évolution du système dans le temps :

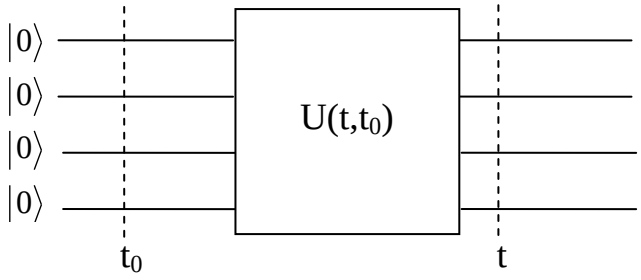

Figure 5 : Schéma général du calcul quantique.

L'intérêt de la transformation unitaire est qu'elle est réversible car on peut remonter à l'état initial à partir de l'état mesuré en utilisant l'opérateur inverse $U^{-1}(t,t_0)=U(t_0,t)$. Souvent, le défi du calcul quantique est de transposer les algorithmes classiques au domaine quantique. Le problème qui se pose est que la plupart des portes logiques classiques sont irréversibles ce qui ne permet pas de remonter à l'état initial. Par exemple, la porte NAND $x \uparrow y = 1 \oplus xy$ où $\oplus$ désigne l'addition modulo 2 et qui donne les transformations $(00) \longrightarrow 1$; $(01) \longrightarrow 1$; $(10) \longrightarrow 1$; $(11) \longrightarrow 0$. Cette porte réalise le passage 2 bits $\longrightarrow$ 1 bit qui empêche de retrouver l'état initial. Il est connu que les porte NAND et COPY sont suffisantes pour construire tous les circuits logiques. Il est donc nécessaire de remplacer NAND par une opération réversible et réaliser une porte quantique qui joue le rôle de COPY tout en étant conforme au théorème de non clonage. Pour cela on utilise les portes CNOT et TOFFOLI qui est illustrée par le dessin suivant :

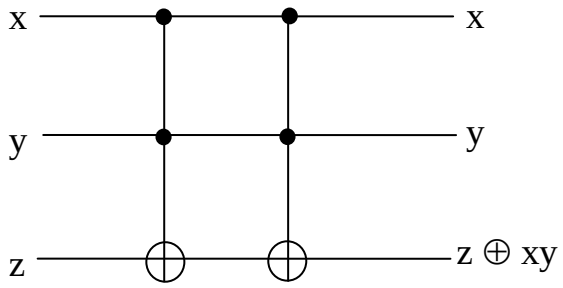

Figure 6 : Porte TOFFOLI

La nécessité de la porte TOFFOLI vient du fait qu'avec CNOT et une des portes à un bit $x \to 1 \oplus x \ ou \ x \to \neg x$ on ne construit que des fonctions linéaires. Dans le cas d'un système à n bits il existe un théorème qui énonce que toute transformation unitaire sur le système peut se décomposer en un produit de portes à un qubit et de portes CNOT. L'annexe A présente un exemple de calcul quantique qui est l'algorithme de Deusch.

I.16 Communications quantiques

Les communications quantiques ont lieu lorsque plusieurs qubit sont manipulés par plusieurs opérateurs séparés par des distances plus ou moins grandes. Historiquement, on considère un système à deux qubits manipulés par deux personnes appelées Alice et Bob. Notons que chacun d'eux ne manipule qu'un seul qubit en le mesurant ou en lui appliquant une porte logique ou toute autre opération possible. Nous disons qu'Alice et Bob ont accès à un ensemble complet d'opérations locales. Ils peuvent aussi communiquer par des canaux classiques et reporter les résultats des mesures sur des qubits qui sont à leur disposition. En particulier, chacun d'eux peut interroger l'autre sur les portes qu'il a utilisées lors de la manipulation de son qubit.
Toutes ces possibilités offertes aux opérateurs sont résumées par l'expression « opérations locales et communications classiques » ou LOCC.

En réalité, les communications quantiques ne sont intéressantes qu'avec un système de qubit intriqués. En effet, dans ce cas chacun des deux opérateurs peut agir sur l'état total du

système rien qu'en manipulant un seul qubit. Cependant, la théorie de l'information quantique prédit qu'il est impossible pour un des deux opérateurs de produire un état intriqué à partir d'un état séparable. De plus, on ne peut élever le degré d'intrication d'un système quantique avec la procédure LOCC. En fait, il y'a deux moyens pour disposer d'un état intriqué, soit que les deux opérateurs procèdent à une interaction directe adéquate de leur qubit ou bien qu'ils reçoivent l'état intriqué préparé par une tierce personne.

I.17 La téléportation

Ce processus purement quantique décrit dans [20] consiste à transmettre l'état inconnu $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ d'un système physique sur une très grande distance qui ne permet pas une transmission classique. Soient deux personnes appelées Alice et Bob qui disposent de deux qubits initialement séparés et à l'état $|0\rangle$ puis intriqués. Chacun d'eux prend un qubit et ils s'éloignent l'un de l'autre d'une très grande distance. Un jour Alice veut communiquer à Bob l'état d'un troisième qubit qu'elle dispose en utilisant la paire intriquée commune. La procédure de téléportation schématisée sur la figure 7 est simulée dans l'annexe B.

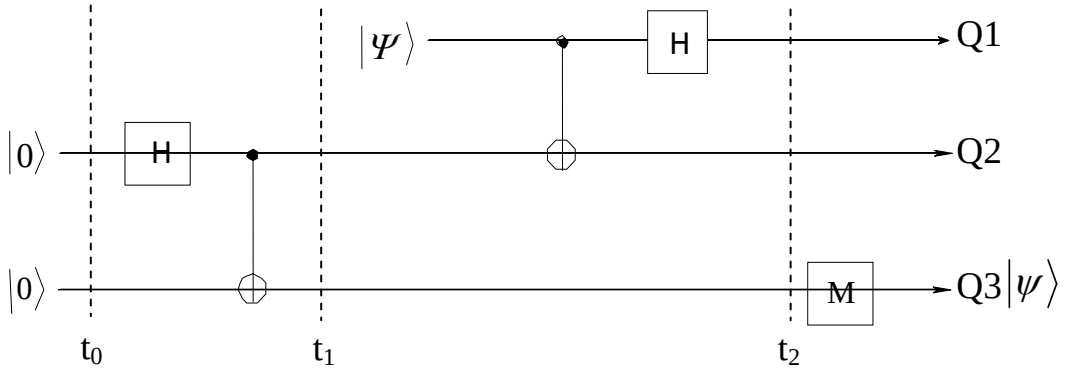

Figure 7 : Circuit de la téléportation. Alice possède les qubits (Q1,Q2) aux états initiaux |0> et |Ψ> puis finaux |0> ou |1> et Bob le qubit Q3 sur lequel il applique la porte M pour accéder à l'état |Ψ>.

Décrivons ici-bas le protocole quantique (figure 7) qui permet à Alice de transmettre à Bob l'état superposé de qubit 1.

Etape 1 ($t_0 \leq t \leq t_1$) : Intrication des qubits 2 et 3 initialement à l'état $\phi_O = |00\rangle$ par application de H sur qubit 2 :

$$HI|00\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

Application de CNOT avec le qubit 2 contrôleur et qubit 3 cible :

$$|\psi_0^{'}\rangle = \frac{1}{\sqrt{2}} CNOT(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Etape 2 ($t_1 \leq t \leq t_2$) : Rajout de qubit 1 dans l'état superposé :

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

Etat initial séparé : $|\psi_0\rangle = |\psi\rangle \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle)$

Application par Alice de CNOT sur ses deux qubits où le second est la cible :

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(\alpha(|000\rangle + |011\rangle) + \beta(|110\rangle + |101\rangle)$$

Alice applique H sur son premier qubit :

$$|\psi_1\rangle = \frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle))$$

$$|\psi_1\rangle = \frac{1}{2}(\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle))$$

$$|\psi_1\rangle = \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)$$

$$|\psi_1\rangle = \frac{1}{2}(|00\rangle|\psi\rangle + |01\rangle X|\psi\rangle + |10\rangle Z|\psi\rangle + |11\rangle XZ|\psi\rangle)$$

Nous avons donc obtenu un système à trois qubits intriqués. Alice effectue alors une mesure sur ses deux qubits (1 et 2) qui va se répercuter instantanément sur l'état de qubit 3 à la possession de Bob. Cette mesure donne quatre résultats possibles $|00\rangle, |01\rangle, |10\rangle$ *ou* $|11\rangle$ qui transformeront le qubit de Bob dans les états respectifs $|\psi\rangle, X|\psi\rangle, Z|\psi\rangle$ *et* $XZ|\psi\rangle$. Finalement, Alice communique à Bob le résultat de sa mesure et ce dernier applique en fonction du résultat un des opérateurs X, Z ou XZ sur l'état de son qubit afin d'obtenir $|\psi\rangle$.

I.18 Conclusion

L'information quantique présente une supériorité évidente sur l'information classique grâce à l'intrication et superposition des états de qubits. Cependant, le phénomène de décohérence causé par l'extrême sensibilité des qubits aux agressions extérieures induit des erreurs dans l'information qu'ils portent, aussi bien lors d'un calcul que dans une communication quantique. D'où la nécessité de protection des qubits par des codes correcteurs quantiques qui seront abordés dans le chapitre II.

Chapitre II :

Codes Correcteurs d’Erreurs Quantiques

II.1 Introduction

Ce chapitre est consacré aux codes correcteurs d'erreurs quantiques [4][29] qui sont nécessaires au calcul et aux communications quantiques à cause de la décohérence produite par l'interférence des qubits avec le monde extérieur. Le calcul et communications quantiques ne peuvent exister sans des codes correcteurs d'erreur efficaces. En effet, si la probabilité d'erreur est négligeable sur un ordinateur classique elle est par contre très élevée sur un ordinateur quantique. La différence provient de la nature du support physique : un condensateur rempli d'électrons est un bit qui vaut 1 même si le nombre d'électrons varie alors qu'un électron unique qui change de spin est un qubit qui change de valeur. La source d'erreur dans le calcul quantique est la décohérence causée par l'interaction du système avec son environnement. Cette interaction peut être indésirable ou bien une opération de mesure destinée à connaître des résultats de calcul. La décohérence est une modification irréversible de l'état quantique qui empêche définitivement de connaître l'état précédent, ce qui est problématique pour le calcul quantique. Les codes correcteurs d'erreur ont été élaborés par analogie avec les codes classiques mais possèdent néanmoins des particularités. Un code classique est basé sur la redondance où on réalise plusieurs copies du même bit pour qu'au moins une des copies reste indemne d'altération. Dans le cas quantique le théorème de non clonage est une barrière à la réalisation de copies semblables. Parmi les erreurs que l'environnement introduit sur les systèmes quantiques le basculement de la valeur du qubit (0 en 1 ou 1 en 0), un changement de phase ($|+\rangle$ devient $|-\rangle$ et inversement) et la disparition de certains termes dans une superposition d'état à la suite d'une mesure.
Nous allons voir dans ce qui suit quelques méthodes simples de correction d'erreur qui sont traitées dans la référence [28].

II.2 Erreurs sur qubits

Soit un qubit qui voit son état initial $\alpha|0\rangle+\beta|1\rangle$ basculer vers l'état $\alpha|1\rangle+\beta|0\rangle$. Pour corriger cette erreur on peut utiliser un code répétitif en codant $|0\rangle$ comme $|000\rangle$ et $|1\rangle$ comme $|111\rangle$. L'état initial est donc codé $\alpha|000\rangle+\beta|111\rangle$ et devient après erreur sur, par exemple, le second qubit $\alpha|010\rangle+\beta|101\rangle$. On a supposé que le basculement du qubit s'effectue sur tous les termes de la superposition d'états. Afin d'identifier le qubit altéré nous rajoutons un registre initialisé à $|0\rangle$ qui va localiser et enregistrer sa position. L'état global devient alors $(\alpha|010\rangle+\beta|101\rangle)|0\rangle$ [28]. Après avoir déterminé par calcul la position de l'erreur nous obtenons l'état $\alpha|010\rangle|2\rangle+\beta|101\rangle|2\rangle$ où le nombre 2 indique que le second qubit est perturbé. Nous procédons alors à la correction du qubit désigné par le registre rajouté ce qui donne $\alpha|000\rangle|2\rangle+\beta|111\rangle|2\rangle$. En supprimant la redondance on retourne à l'état initial $\alpha|0\rangle+\beta|1\rangle$.

La procédure précédente reste valable lorsque l'erreur se produit en superposition. Soit une altération du système qui aboutit à l'état suivant : $\frac{1}{\sqrt{2}}(\alpha|100\rangle+\beta|010\rangle+\alpha|010\rangle+\beta|101\rangle)$. Après avoir rajouté le registre d'erreur et localisé les qubits altérés l'état global du système prend l'une des deux formes [28] :

$$\frac{1}{\sqrt{2}}(\alpha|100\rangle|1\rangle+\beta|011\rangle|1\rangle+\alpha|010\rangle|2\rangle+\beta|101\rangle|2\rangle)$$

$$\frac{1}{\sqrt{2}}((\alpha|100\rangle+\beta|011\rangle)|1\rangle+(\alpha|010\rangle+\beta|101\rangle)|2\rangle)$$

La mesure effectuée sur le registre d'erreur peut donner deux résultats possibles : $(\alpha|100\rangle+\beta|011\rangle)|1\rangle$ *ou* $(\alpha|010\rangle+\beta|101\rangle)|2\rangle$. Enfin on bascule les valeurs des qubits désignés par le registre d'erreur pour revenir à l'état $\alpha|000\rangle+\beta|111\rangle$ puis en enlevant les répétitions on revient à l'état original $\alpha|0\rangle+\beta|1\rangle$ [28].

II.3 Erreurs sur phase

Soit un qubit dans un état initial $\alpha|0\rangle+\beta|1\rangle$ qu'on voudrait protéger d'une erreur de phase. Pour cela on code cet état comme $\alpha|+++\rangle+\beta|---\rangle$ où les états $|+\rangle$ et $|-\rangle$ sont donnée par [28]:

$H|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle=|+\rangle \quad et \quad H|1\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle=|-\rangle$ Une erreur de phase sur le second qubit donne l'état $\alpha|+-+\rangle+\beta|-++-\rangle$.

La correction se fait d'abord par une triple transformation $H^{\otimes 3}$ qui nous ramène aux états de base $H^{\otimes 3}(\alpha|+-+\rangle+\beta|-++-\rangle)=\alpha|010\rangle+\beta|101\rangle)$.

On procède alors à la correction de la valeur du qubit altéré pour restaurer l'état $\alpha|000\rangle+\beta|111\rangle$. Enfin, on applique de nouveau $H^{\otimes 3}$ pour revenir à notre état codé $\alpha|+++\rangle+\beta|---\rangle$. L'astuce consiste donc à transformer une erreur de phase qu'on ne peut directement corriger en erreur sur qubit qui est corrigeable [28].

II.4 Erreurs de mesure

Considérons par exemple un système à trois qubits dans l'état $\frac{1}{\sqrt{3}}(|001\rangle+|010\rangle+|101\rangle)$ qui subit une mesure de son second qubit. L'état obtenu est soit

$\frac{1}{\sqrt{2}}(|001\rangle + |101\rangle)$ ou bien $|010\rangle$ ce qui correspond à la perte irréversible respectivement d'un terme et de deux termes de la superposition d'état. Dans ce cas le code répétitif ne peut corriger l'erreur car on ne peut copier un état superposé sans le déformer [28].

II.5 Erreurs combinées sur qubit et sur phase

Prenons l'exemple du code de Shor qui utilise neuf qubits pour corriger une erreur combinée sur qubit et sur phase. Soit l'état initial $\alpha|0\rangle + \beta|1\rangle$ codé $\alpha|+++\rangle + \beta|---\rangle = \alpha(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle))^{\otimes 3} + \beta(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))^{\otimes 3}$ afin de le protéger contre les erreurs de phase.

La protection contre les erreurs sur qubit se fait en codant chaque $|0\rangle$ comme $|000\rangle$ et chaque $|1\rangle$ comme $|111\rangle$ pour obtenir $\alpha(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle))^{\otimes 3} + \beta(\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle))^{\otimes 3}$. L'algorithme de Shor commence par corriger les erreurs de qubits (en ignorant les erreurs de phase) puis corrige les erreurs de phase [28].

II.6 Schéma général des erreurs quantiques

Considérons un système quantique de n qubits en couplage avec l'environnement. Nous représentons l'erreur comme une transformation unitaire U sur l'état de l'ensemble « n-qubits+environnement ». Cette erreur peut être un basculement des valeurs de certains qubits, un changement de phase ou bien une combinaison de ces deux déformations. Dans le cas d'une erreur sur un seul qubit nous donnons les différentes représentations matricielles de cette erreur [30]:

Absence d'erreur : $I\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\beta\\ \alpha\end{pmatrix}$

Basculement de qubit (erreur X) : $X\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\beta\\ \alpha\end{pmatrix}$

Changement de phase (erreur Z) : $Z\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\alpha\\ -\beta\end{pmatrix}$

Basculement de qubit+ Changement de phase :

$$XZ\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}\beta\\ -\alpha\end{pmatrix}$$

Erreur Y : $Y\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=i\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=i\begin{pmatrix}-\beta\\ \alpha\end{pmatrix}$=-iXZ$\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$

Les annexes C, D et E décrivent les codes correcteurs à deux, trois et neufs qubits avec leurs simulations faites sur Maple.

II.7 Théorie générale de la correction d'erreur

Un code correcteur d'erreur est un sous espace S de l'espace de Hilbert H_c constitué de l'ensemble des kets $\{|c_j\rangle\}$ et de toutes leurs combinaisons linéaires, avec $1 \le j \le K$ qui servent au codage de l'information à protéger. On définit alors le projecteur $S=\sum_j |c_j\rangle\langle c_j|$ qui projette les kets sur le sous espace S. L'entier $K=2^k$ où k est le nombre de qubits à protéger désigne la dimension de S égal à 2 dans les exemples précédents. L'information à protéger est un ket $|\psi\rangle$ d'un espace de Hilbert H_a de dimension K. Le codage nécessite des qubits auxiliaires dont les états appartiennent à un espace de Hilbert H_b et qui interagissent avec les qubits à protéger de manière réversible. Le codage consiste donc en une transformation unitaire C : $H_a \otimes H_b \rightarrow H_c$ et nous pouvons écrire $C(|a_p\rangle \otimes |b_0\rangle) = |c_p\rangle$.

L'erreur due à une interaction entre les qubits et l'environnement peut être représentée par un groupe d'opérateurs $\{K_i\}$ qui satisfont la condition de normalisation $\sum_i K_i^t K = I$ et transforme un état de H_c en un autre état de H_c. Le décodage qui réalise la correction d'erreur est réalisé par un opérateur D qui transforme l'état altéré qui est intriqué dans H_c en un état séparable dans $H_a \otimes H_f$ ($D : H_c \rightarrow H_a \otimes H_f$) où H_f est l'espace des états finaux des qubits auxiliaires. Nous écrivons la procédure de correction d'erreur sous la forme suivante : $DK_iC|\psi\rangle = |\psi\rangle \otimes |s_i\rangle \quad \forall\ |\psi\rangle \ et\ K_i$ où les kets $|s_i\rangle$ appelés syndromes appartiennent à H_f et dépendent seulement de K_i mais pas de $|\psi\rangle$. On remarque que les syndromes ne sont généralement ni orthogonaux ni normalisés. Notons que pour une même opération de codage C il peut exister plusieurs opérations de décodage D. Tout opérateur d'erreur E sur un qubit peut être écrit comme une combinaison linéaire des quatre opérateurs de Pauli I, X, Y et Z : $\{E\}=\{I,X,Y,Z\}^{\otimes n}$. En conséquence, si un décodage donné D corrige des erreurs de type X, Y et Z sur un qubit alors il corrige toutes les erreurs sur ce qubit. Un ensemble $\varepsilon_c=\{E_j\}$ d'opérateurs est considéré comme correcteur d'erreur si l'on vérifie la condition $\langle C_p | E_j^t E_k | C_q \rangle = \alpha_{jk}\delta_{pq} \quad \forall(j,k,p,q)$ avec $\alpha_{jk} = \alpha(E_j, E_k)$ une matrice de nombres complexes hermitienne de valeurs propres positives.

II.8 Codes convolutifs classiques

II.8.1 Introduction

Les communications à grandes distances (sondes spatiales) sont inévitablement parasitées par diverses sources comme les perturbations électromagnétiques, ce qui pose le problème de la fiabilité des messages transmis. Il est alors impératif de sécuriser les informations transmises en les protégeant par des codes correcteurs d'erreurs. En fait, des informations supplémentaires sont rajoutées au message afin de le reconstituer à la réception,

II.8.2 Codes en blocs linéaires

Lors d'un traitement informatique (automatisé) de l'information, le signal à transmettre (image, son,..) est numérisé en le ramenant à une séquence de bits. Afin de contrer les parasites, la séquence est codée en répétant chaque bit un certain nombre de fois. Le récepteur comparera les copies et saura alors si elles sont différentes qu'il y'a eu erreur lors de la transmission. Il pourra donc considérer que les copies majoritaires représentent le bit correct. Dans le cas ou le canal est faiblement bruité, on réduit la redondance au minimum requis et on utilise le bit de parité qui permet de détecter l'erreur. En effet, le message est divisé en blocs contenant chacun un nombre égal de k bits en plus d'un bit rajouté tel que le nombre de bits 1 est pair dans chaque bloc. Les blocs sont traités séparément par le codeur. Un code est un ensemble de 2^k n-uplets de bits (n > k) dont les éléments sont appelés mots. Les blocs sont traduits en éléments du code tel que chacun des 2^k messages différents possibles correspond de manière unique à un des mots du code.

On définit la distance de Hamming entre deux mots du code le nombre de leurs composantes qui les différencient. La plus petite distance entre deux mots quelques est appelée la distance d du code lequel sera alors défini par les trois paramètres [n,k,d] ou n et k sont respectivement sa taille et sa dimension. Considérons en exemple le code (5,2,3) suivant :

Message	Mot
(0,0)	(0,0,1,1,0)
(0,1)	(0,1,0,1,1)
(1,0)	(1,0,1,0,1)
(1,1)	(1,1,0,0,0)

On montre qu'un code peut corriger e = E((d-1)/2) erreurs. Le rapport d/n lorsqu'il est élevé traduit une bonne fiabilité du code. Le rapport R = k/n appelé taux du code est proche du 0 si la redondance et par suite le temps de transmission sont importants. Un code est construit de manière à trouver le bon compromis entre le taux et la fiabilité.

II.8.3 Théorème de Shannon

Un canal de transmission est defini comme un système physique qui transmet une information entre deux points distants. On définit le taux d'erreurs binaire (TEB) comme le rapport du nombre de bits erronés par le nombre de bits du message.

Le théorème de Shannon qui est fondamental à la théorie de l'information (1948) s'énonce comme suit [23] :

Tout canal de transmission admet un paramètre C, appelé capacité du canal, tel que pour tout e > 0 et pour tout R < C, il existe un code de taux R permettant la transmission du message avec un taux d'erreurs binaire de e.

Ce théorème nous informe, sans indiquer comment, qu'il est possible d'améliorer la fiabilité de la transmission avec des codes de taux plus bas que la capacité du canal utilisé. On construit donc des codes de taux le plus élève possible (limité par le temps et le coût) et donnant la meilleure fiabilité. Le codage simple décrit précédemment ayant des performances limitées on a développé d'autres systèmes de codage permettant d'approcher la capacité du canal tels que les codes convolutifs.

II.8.4 Codes convolutifs

Les codes convolutifs, inventés par Peter Elias en 1954 ne découpent pas le message en blocs finis, mais le considèrent comme une séquence semi-infinie de symboles qui passe à travers une succession de registres à décalage, dont le nombre est appelé *mémoire du code* [24]. Le décodage se fait à l'aide d'algorithme approprié dont le plus connu est celui construit par Viterbi [31] qui permet de trouver l'erreur de canal la plus vraisemblable. Les codes convolutifs utilisent la technique d'entrelacement qui consiste à permuter une séquence de bits de manière à ce que deux symboles proches à l'origine soient le plus éloignés possibles l'un de l'autre. Cela permet en particulier de transformer une erreur portant sur des bits regroupés en une erreur répartie sur l'ensemble de la séquence. Il existe deux categories courantes de codes convolutifs :

- Les codes non systématiques ou NSC : Un code convolutif est dit *systématique* si l'un des bits de sortie est identique au bit d'entrée. Les codes NSC fournissent plus d'information que les codes systématiques : tout bit sortant du codeur renseigne sur plusieurs bits du message codé. Le décodeur dispose donc de plus d'éléments dans un code NSC, et permet donc de corriger plus d'erreurs. L'expérience montre que la capacité d'un code à corriger les erreurs augmente plus ou moins linéairement avec sa mémoire ν. On a donc construit des codes en essayant d'élever la valeur de ν ce qui induit en contrepartie une élévation de sa complexité qui est en 2^{ν}.

- Les codes systématiques récursifs ou RSC : Un code convolutif est dit *récursif* si la séquence passant dans les registres à décalages est « alimentée » par le contenu de ces registres. Certains travaux expérimentaux laisse présager que seuls les codes RSC sont susceptibles d'atteindre la limite de Shannon.

II.8.5 Turbocodes

Les turbo-codes inventés en 1991, sont aujourd'hui adoptés par toutes les agences spatiales mondiales, et utilisés dans la transmission des données du nouveau standard de téléphonie mobile qui va succéder au GSM. Les turbo-codes utilisent conjointement deux codeurs convolutifs récursifs qui ne sont pas en série mais en parallèles.

L'entrelacement permet ainsi de coder avec le même codeur deux séquences d'autant plus différentes que l'entrelacement sera chaotique, ce qui rapproche les turbocodes des limites théoriques de Shanon [25][26][27].

II.9 Codes convolutifs quantiques

II.9.1 Introduction

Nous décrivons dans ce chapitre un type particulier de codes correcteurs d'erreur qui sont les codes convolutifs quantiques [5][6] [7][8] utilisées lors de la transmission de flux continus d'informations portées par des qubits à travers des canaux bruités. Il existe deux classes de codes qui sont les codes en blocs et les codes convolutifs utilisés respectivement pour les erreurs en éclatement comme dans les mémoires secondaires et dans la transmission continue de flux d'information à grande distance (tableau 2). Dans les codes en blocs il faut attendre que tous les qubits atteignent l'encodeur pour les diviser en un nombre fini de blocs égaux. Ces blocs sont alors encodés séparément tel que chacun d'eux est indépendant de tous les autres durant toute la procédure d'encodage. En conséquence, le receveur attend l'arrivée de tous les qubits pour commencer à effectuer séparément sur chaque bloc un nombre fini d'opération d'extraction de syndromes et de recouvrement d'erreurs. Les codes convolutifs sont destinés à la protection des flux informations portés par des qubits et transmis sur de longues distances à travers des canaux bruités. Ils possèdent une structure assez similaire à leurs homologues utilisés dans les communications classiques. Ces codes convertissent les flux d'information en un mot de code unique quelque soit sa longueur par l'encodage en ligne de groupes successifs inégaux de qubits. L'encodage de chaque groupe sera lié à celui des groupes précédents et suivants. A l'inverse des codes en blocs, l'encodage démarre dés l'arrivée à l'encodeur des premiers qubits à transmettre sans attendre le reste du flux. Le récepteur procède à l'extraction des syndromes et au recouvrement d'erreur sur chaque groupe de qubits dés qu'ils atteignent le décodeur. Cet encodage et décodage en ligne permet de réduire le temps de traitement des qubits transmettant alors rapidement l'information au récepteur, évitant ainsi de subir le phénomène de décohérence mieux que les codes en blocs. La plus importante propriété des codes convolutifs est leur algorithme d'estimation d'erreur au maximum de vraisemblance (canaux sans mémoire) ayant une complexité croissant linéairement avec le nombre de qubits encodé (exponentiellement pour les codes en blocs).

Code	Code en blocs	Code convolutifs
Application	Rafales d'erreurs de canal (mémoires secondaires,...)	Transmission à longue distance par canal bruité.
Codage	Codage séparé de blocs égaux après l'arrivée de tous les bits à l'encodeur.	Codage en ligne de groupes inégaux de qubits en un seul mot de code.
Détection d'erreur	Algorithme d'estimation d'erreur à complexité exponentielle et démarrant après l'arrivée de tous les bits au receveur.	Algorithme d'estimation d'erreur en ligne à complexité linéaire et démarrant à l'arrivée du premier groupe de qubits
Décodage	Les blocs sont séparément décodés après l'arrivée de tous les bits au décodeur.	Décodage en ligne de chaque groupe de qubits dés sa correction.

Tableau 2 : Comparaison entre les codes en blocs et les codes convolutifs.

II.9.2 Code stabilisateur

Les codes convolutifs quantiques peuvent être décrits par le code stabilisateur. Nous encodons les k qubits à protéger dans un groupe de n qubits contenant (n-k) qubits protecteurs appelés ancillas (nous disons que le code à un taux =k/n). En général, nous définissons pour un code à (n,k) qubits un groupe stabilisateur G_k contenant (n-k) générateurs M_i qui sont des produits tensoriels des opérateurs de Pauli (I, X,Y,Z) et que nous pouvons résumer par l'expression : $G_k = \{M_i, i = 1 \ldots..(n-k)\}$ avec $M_i = \{\pm 1, \pm i\} \times \{I, X, Y, Z\}^n$

Nous définissons le poids d'un générateur comme étant le nombre d'opérateurs de Pauli X, Y ou Z qu'il contient. Le sous espace code C associé au groupe stabilisateur (n,k) est l'ensemble des vecteurs propres $\{|\Psi\rangle\}$ des générateurs M_t avec la valeur propre +1 :

$$M_i |\Psi\rangle = |\Psi\rangle, \forall\ M_i \in G_k \qquad |\Psi\rangle \in C$$

Si une erreur E affecte l'état $|\psi\rangle$, qui devient alors $|\psi'\rangle = E|\psi\rangle$, on applique les générateurs sur $|\psi'\rangle$ afin de mesurer leurs valeurs propres : $M_i|\psi'\rangle = M_iE|\psi\rangle = \pm EM_i|\psi\rangle = \pm|\psi'\rangle$ (M_i commute ou anticommute avec E). L'ensemble des valeurs propres des (n-k) générateurs M_t correspondant à une erreur donnée E est appelé le syndrome d'erreur. Comme on peut connaitre tous les syndromes d'erreur possibles, on déduit une liste d'erreur probable correspondant aux syndromes mesurés. Enfin, on choisit dans la liste l'erreur la plus vraisemblable et on procède au recouvrement de l'état codé initial. Le groupe stabilisateur des codes convolutifs quantiques possède une structure convolutive qui lui donne deux propriétés spécifiques. D'abord, ils possèdent pour tous les canaux sans mémoire un algorithme d'estimation d'erreur au maximum de vraisemblance ayant une complexité croissant linéairement avec le nombre de qubits encodé (exponentiellement pour les codes en blocs). Ensuite, un encodage en ligne des qubits où l'état codé est transmis à travers le canal de communication sans attendre l'arrivée à l'encodeur des autres qubits [4]. L a procédure générale d'un code convolutif est décrite dans la référence [5]. L'émetteur réalise le circuit d'encodage en appliquant successivement sur tous les groupes de qubits le même ensemble U de portes unitaires. Une particularité du codage convolutif est que deux groupes de portes successifs U_i et U_{i+1} agissent sur un certain nombre de différents qubits dont un nombre m sont en commun. Un groupe de qubits « i » est envoyé à travers le canal dés que l'action sur lui du groupe de portes U_i est achevée et sans attendre le traitement des autres qubits. Le circuit d'encodage est alors considéré en ligne car il agit à la fois sur un groupe contenant un petit nombre de qubits. Ce traitement rapide est nécessaire à cause du phénomène de décohérence. Comme le canal bruité va probablement perturber les qubits, le récepteur effectue les mesures de syndromes pour détecter les erreurs. Ces mesures exigent que les générateurs utilisés doivent avoir un poids fini car les groupes de qubits envoyé sont composés d'un nombre fini de qubits. De plus, les générateurs doivent être divisés en des groupes identiques agissant sur des groupes égaux de qubits afin d'assurer une mesure en ligne des syndromes. Les syndromes mesurés sont traités par un algorithme d'estimation d'erreur (tel que l'algorithme de Viterbi) qui permet d'identifier l'erreur la plus probable dans un groupe de qubits donné. Les portes adéquates sont appliquées pour recouvrir l'état codé initial envoyé. Finalement, les qubits reçus sont décodés en ligne car le décodage d'un groupe de qubits démarre juste après l'achèvement de sa correction. Chaque étape de la procédure peut commencer même si l'étape précédente n'est pas encore terminée. Les qubits sont traités par groupes pour obtenir les données quantiques correctes prêtes pour le calcul quantique.

En conclusion, toutes les opérations de codage, mesure, correction et décodage sont en ligne dans un code convolutif, tel que l'émetteur et le récepteur ne sont pas obligés de procéder séquentiellement [6]. La figure 8 schématise les codes convolutifs.

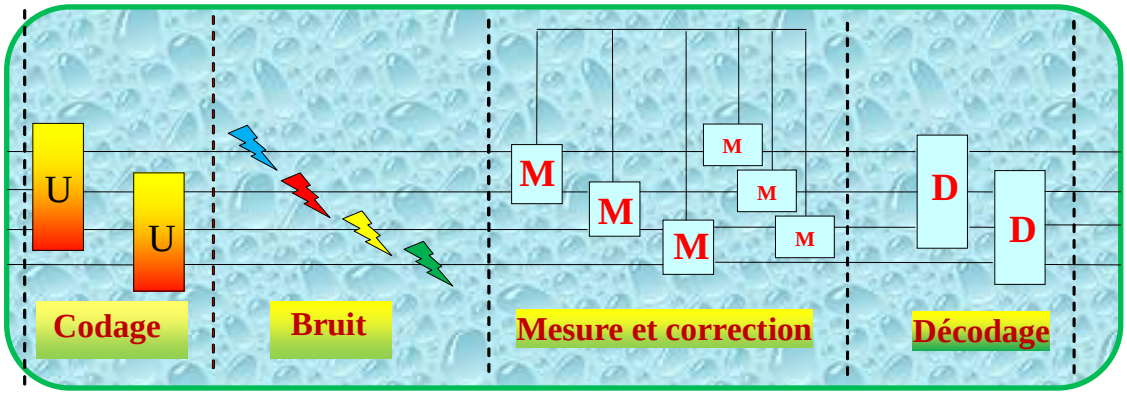

Figure 8 : Procédure générale d'un code convolutif quantique [5].

II.9.3 Code convolutif à cinq qubits

Nous utilisons ici cinq qubits pour protéger l'information portée par l'un d'eux (taux =1/5). Ce code est mieux décrit en utilisant le formalisme stabilisateur car il permet d'une part de comprendre facilement les opérations de codage et de décodage et d'autre part d'identifier sans difficultés les syndromes d'erreur. Ce qui simplifie considérablement la description de l'algorithme d'estimation d'erreur.

II.9.4 Générateurs

Dans le cas d'un code à n qubits on définit un groupe stabilisateur $G_k=\{S_i, i=1.....k\}$ avec k<n le nombre de qubits à protéger (taux=k/n). Ce groupe est constitué de (n-k) générateurs S_i qui sont des produits tensoriels des opérateurs de Pauli I, X, Y et Z. Le sous-espace code C associé au groupe stabilisateur (n,k) est l'ensemble des vecteurs propres $\{|\psi\rangle\}$ de ces générateurs avec la valeur propre +1 tel que pour tout $S_i \in G_k$ [7] : $S_i|\psi\rangle=|\psi\rangle \quad \forall\ |\psi\rangle \in C$

Considérons les générateurs particuliers au cas (n=5, k=1) suivants : S_0=XZIIIII….., S_1=ZXXZIIII…., S_2=IZXXZIII…., S_3=IIZXXZII…., S_4=IIIZXXZI…., $S_{4i+j}=I^{\otimes 5i}\otimes Sj$, avec $i > 0$ et $1 \leq j \leq 4$, S_∞=...IIIIZX. On constate donc que dans ce code convolutif la position de chaque opérateur de Pauli dans un générateur S_k ($k \geq 1$) sera cinq fois décalée vers la droite dans S_{k+4}. On montre aussi que ces générateurs commutent entre eux et sont donc indépendants. Ce qui diffère les codes convolutifs des codes en blocs est la structure particulière des générateurs stabilisateurs. En effet, à l'exception de S_0 et S_∞ , les générateurs peuvent être regroupés en sous-groupes de taille fixe (même nombre d'opérateurs de Pauli) agissant sur un certain nombre de qubits consécutifs. De plus, il existe un nombre constant de qubits en commun (recouvrement) entre un sous-groupe et ses voisins immédiats. Ces propriétés donnent aux codes convolutifs la possibilité d'un encodage en ligne et l'existence d'un algorithme efficace d'estimation d'erreur [8].

II.9.5 Circuit d'encodage

L'encodage d'un flux de qubits portant l'information utile portée par les qubits Q_i consiste en premier lieu à rajouter des qubits protecteurs (ancillas) tous dans l'état $|0\rangle$ de manière à ce que chaque qubit Q_i occupera la position 5i+1. L'état initial $|Q_1,Q_2,....,Q_i,...\rangle$ devient alors $|o,o,o,o,o,Q_1,o,o,o,o,Q_2....,o,o,o,o,Q_i...\rangle$ avec $Q_i \in \{0,1\}$. On implémente alors les portes quantiques sur le sous espace code C qui réalisera les transformations unitaires sur tout l'espace de Hilbert [8] :

$$P|o,o,o,o,o,Q_1,o,o,o,o,Q_2....,o,o,o,o,Q_i...\rangle = |Q_1,Q_2,....,Q_i...\rangle$$

Le circuit d'encodage obtenu est représenté sur la figure 9 suivante :

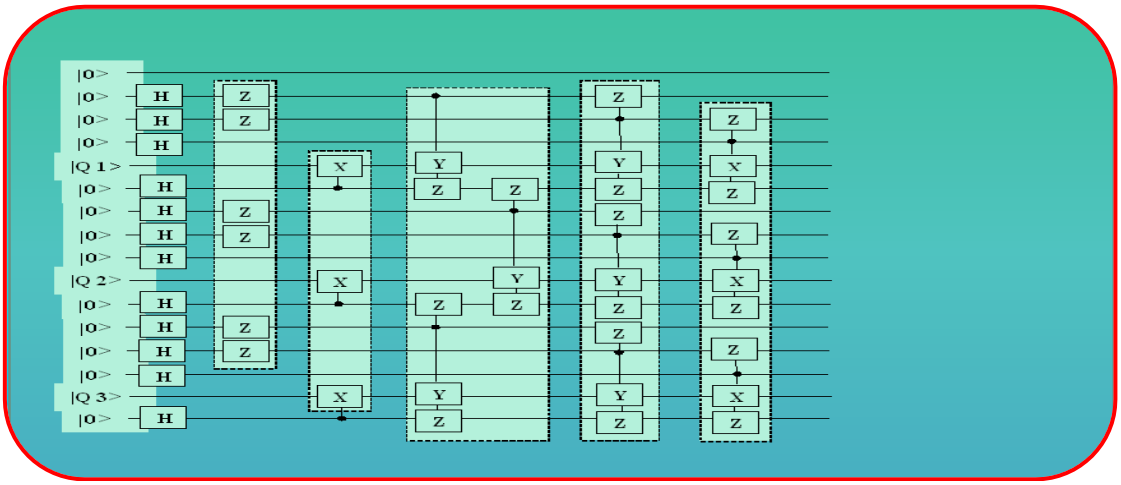

Figure 9 : Circuit de codage d'un code convolutif à cinq qubits **[8].**

II.9.6 Propagation de l'erreur et décodage en ligne

La structure d'un code convolutif entraîne un transfert de l'information contenu dans un qubit donné vers ses successeurs (voir figure précédente). Ceci pose problème lors du décodage car une erreur affectant un petit nombre de qubits dans le canal de transmission peut se propager vers un nombre beaucoup plus grand de qubits dans le circuit de décodage (erreur catastrophique). Il existe une condition nécessaire et suffisante pour échapper à l'erreur catastrophique qui est que les portes du circuit de décodage doivent être groupées en couches telles que les portes d'une même couche commutent entre elles (figure 9). En effet, l'erreur ne peut se propager qu'à l'aide de portes qui ne commutent pas entre elles. Par suite, pour une erreur de taille finie un circuit de décodage vérifiant la condition précédente impose qu'après l'application d'une couche de portes seulement un nombre fini de qubits sont potentiellement infectés. Concrètement, le circuit de décodage est obtenu en inversant le circuit de codage, autrement dit en permutant en sens inverse l'ordre d'exécution des portes sur chaque qubit. La construction du code consiste donc à mettre en place le circuit de codage initial de la figure 9 puis de le transformer (changer l'ordre des portes qui ne commutent pas) de manière à obtenir la structure qui assure la non-catastrophicité. On dérive enfin par inversion le circuit de décodage et on obtient finalement le code montré sur la figure 9 qui permet aussi bien un encodage en ligne qu'un décodage en ligne **[8]**.

II.9.7 Estimation de l'erreur

Un code correcteur d'erreur doit permettre au récepteur d'identifier l'erreur de canal la plus probable. On élabore à cette fin un algorithme d'estimation d'erreur quantique qui est l'analogue de l'algorithme de Viterbi utilisé dans le cas classique. Ce dernier donne pour tout canal sans mémoire une estimation d'erreur au maximum de vraisemblance ayant une complexité linéaire avec le nombre de bits encodés. Dans le cas quantique l'algorithme déduit l'erreur la plus probable à partir des syndromes qui sont les états finaux des qubits ancillas. On procède de la manière suivante : On prépare un qubit ancilla à l'état $|0\rangle$, on applique sur lui H puis un des générateurs S_i du groupe stabilisateur suivant d'une autre transformation H, et on mesure finalement son état sur la base $\{|O\rangle,|1\rangle\}$. L'algorithme traite en fait un petit nombre de syndromes à la fois et déduit une liste d'erreurs les plus probables qui est révisée au fur et à mesure jusqu'au traitement de tous les syndromes [8].

II.9.8 Conclusion

Les codes correcteurs d'erreurs quantiques ouvrent de grandes perspectives à l'information quantique, particulièrement aux communications quantiques qui demandent un nombre restreint de qubits en comparaison avec le calcul quantique. Parmi ces codes, les codes convolutifs quantiques qui sont une adaptation de leurs homologues classiques présentent l'intérêt d'un codage, détection et correction d'erreur et décodage en ligne des qubits. Cette particularité les rend convenable au traitement quantique de l'information car elle permet de gagner du temps évitant ainsi le phénomène de décohérence. La mise en pratique de ces codes n'étant pas encore possible, il serait intéressant de les implémenter sur des ordinateurs classique afin de tester leur efficacité. Le chapitre III décrit la simulation sur Maple d'un code convolutif à cinq qubits qui a fait l'objet d'une publication [R5].

Chapitre III :

Simulation d’un Code Convolutif à Cinq Qubits

III.1 Générateurs

Nous allons présenter dans ce chapitre notre simulation par le programme Feynman du code convolutif à cinq qubits décrit dans la référence **[7]**[8]. Ce code utilise cinq qubits (n=5) pour protéger l'information contenu dans l'un d'eux (k=1, taux de k/n=1/5). On définit pour ce code un groupe stabilisateur composé de groupements générateurs dont le premier élément $\{G_1 = M_i\,, i = 1 \ldots .4\}$ contient les quatre générateurs [8] :

M_1=*ZXXZIIIIIII* ; M_2=*IZXXZIIIIII* ; M_3=*IIZXXZIIIII*
M_4=*IIIZXXZIIII*

Les autres générateurs sont donnés par :

$$M_{4i+j} = I^{\otimes 5i} \otimes M_j \quad \text{avec i} > 0 \;,\; 1 \leq j \leq 4 \text{ et } M_\infty = \ldots IIIIZX$$

On note que tous les générateurs du code ont le même poids égal à quatre. De plus, la position de chaque opérateur de Pauli dans un générateur quelconque M_i est décalée cinq fois vers la droite dans le générateur M_{i+4}. On remarque que tous les générateurs sont indépendants car ils commutent entre eux puisque nous avons pour chaque qubits Q_i **[7]**[8] : $[X_i,Y_i] = [X_i,Z_i] = [Y_i,Z_i] \neq 0$ *et* $[X_i,X_i] = [Y_i,Y_i] = [Z_i,Z_i] \neq 0$.

III.2 Circuit de codage

La référence [4] donne le circuit de codage d'un code convolutif à cinq qubits repris sur la figure 9. Le circuit est exécuté de la gauche à la droite et chaque ligne horizontale représente un qubit sur lequel sont successivement appliquées différentes portes. Les ancillas sont initialement à l'état $|0\rangle$ et les qubits portant l'information utile à l'état superposé $|Q_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$. L'action d'une porte sur un qubit est représentée par une boite placée sur la ligne horizontale correspondante. Lorsque la boite est reliée à un autre qubit, cela indique une application conditionnelle de la porte associée où ce qubit agit comme contrôleur (la porte n'est actionnée que si sa valeur est 1). Du fait de sa spécificité, un code convolutif propage l'information portée par un qubit à ses successeurs. Cette propagation de l'information peut être un problème dans le circuit de décodage : une erreur affectant un nombre fini de qubit dans le canal bruité se propage à un nombre infini de qubits. Afin de contrer ces erreurs catastrophiques, les portes dans les circuits de codage et décodage sont arrangées en un nombre fini de couches dans lesquelles elles commutent les unes avec les autres. Cette structure en couches est une condition nécessaire et suffisante qui évite les erreurs catastrophiques **[7]**[8] . L'annexe H-1 montre la simulation du circuit de codage faite par le programme Feynman.

III.3 Détection et correction d'erreur

Pour corriger une erreur simple ou double sur qubit 2 à qubit 12 (voir figure 9), les syndromes sont mesurés pour les générateurs M_1 à M_{10} suivants :

M_1=ZXXZIIIIIII ; M_2=IZXXZIIIIII ; M_3=IIZXXZIIIII
M_4=IIIZXXZIIII ; M_5=IIIIIZXXZIII ; M_6=IIIIIIZXXZII
M_7=IIIIIIIZXXZI ; M_8=IIIIIIIIZXXZ ; M_9=IIIIIIIIIZXXZ
M_{10}=IIIIIIIIIIZXXZ ; M_{11}=IIIIIIIIIIIZXXZI ; M_{12}=IIIIIIIIIIIIZXXZ

On note que les générateurs M_1 à M_4 agissent du premier au septième qubit, alors que les générateurs M_5 à M_8 agissent du sixième au douzième qubits. Les deux groupes de générateurs s'appliquent sur sept qubits avec en commun deux qubits (le sixième et le septième). Les générateurs M_9 à M_{12} agissent du onzième au dix-septième qubits en ayant deux qubits en commun (le onzième et le douzième) avec le groupe précédent (M_5 à M_8). C'est une propriété générale des codes convolutifs d'avoir des générateurs divisés en groupes agissant tous sur un même nombre de qubits avec un recouvrement de m qubits entre deux groupes successifs. Nous avons donc pour le code à cinq qubits n=5, k=1, m=2 et nous l'appellerons le code (5,1,2) [6][7] . En général, un code convolutif quantique (n,k,m) possède un groupe stabilisateur S donné par [4] : $S = sp\left\{M_{i,j} = I^{\otimes j\times n} \otimes M_{0,j}\ ,\ \ 1 \le i \le n-k\ , 0 \le j\right\}$ où $M_{0,j} \in G_{n+m}$ et $M_{i,j}$ sont indépendants et commutent les uns avec les autres [5].

III.4 Mesure d'extraction des syndromes

Nous expliquons ici-bas la détection expérimentale d'erreur réalisée par l'extraction du syndrome [8]. C'est une procédure de mesure non destructive car elle ne perturbe pas l'état codé du système. Afin de faciliter la compréhension, nous allons utiliser les mêmes symboles que ceux de la simulation du code montrée dans l'annexe H-3. Nous commençons par rajouter à l'état à mesurer $|Q27\rangle$ reçu au décodeur, un nouveau qubit initialement à l'état $|0\rangle$ puis transformé en un état superposé par une porte d'Hadamard H. L'état obtenu $|Q28\rangle$ est le produit tensoriel de $|Q27\rangle$ par l'état superposé du qubit rajouté :

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \quad (1)$$

$$|Q28\rangle = |+\rangle|Q27\rangle = \frac{1}{\sqrt{2}}(|0\rangle|Q27\rangle + |1\rangle|Q27\rangle) \quad (2)$$

Le générateur M_i est conditionnellement appliqué sur $|Q28\rangle$:

$$|Q28b\rangle = M_i|Q28\rangle = \frac{1}{\sqrt{2}}(|0\rangle|Q27\rangle + M_i|1\rangle|Q27\rangle) \quad (3)$$

La Valeur propre du générateur M_i est +1 ou -1 pour une erreur E affectant l'état codé $|Q25\rangle$ envoyé par l'encodeur, selon que M_i commute ou anticommute avec E :

$$M_i|Q27\rangle = M_iE|Q25\rangle = \pm EM_i|Q25\rangle = \pm E|Q25\rangle \quad (4)$$

Puisque $M_i|Q25\rangle = |Q25\rangle$ et $|Q27\rangle = \pm E|Q25\rangle$ alors :

$$M_i|Q27\rangle = \pm|Q27\rangle \quad (5)$$

On obtient donc à partir de (3) et (4) :

$$|Q28b\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)|Q27\rangle) = \pm|Q27\rangle \quad (6)$$

On applique la porte H_1 sur le premier qubit pour obtenir un état séparable du système contenant l'état codé inchangé :

$$|Q281c\rangle = H_1|Q281b\rangle = (|0\rangle \text{ ou } |1\rangle)|Q27\rangle \quad (H_1|\pm\rangle = |0\rangle \text{ ou } |1\rangle) \quad (7)$$

On peut identifier l'état du premier qubit en appliquant sur lui la porte Z :

$$|Q281\rangle = Z_1|Q281c\rangle = Z_1|0\rangle|Q27\rangle \text{ ou } Z_1|1\rangle)|Q27\rangle \quad (8)$$

Puisque $Z_1|0\rangle = |0\rangle$ et $Z_1|1\rangle = -|1\rangle$, on obtient finalement :

$|Q281\rangle = |Q281c\rangle$ (Syndrome 0) ou $|Q281\rangle = -|Q281c\rangle$ (Syndrome 1)

III.5 Détermination théorique des syndromes

Les syndromes sont déterminés en utilisant les commutateurs des portes X_i, Y_i et Z_i appliquées sur le qubit « i » suivants :

$$[X_i,Y_i] = [X_i,Z_i] = [Y_i,Z_i] \neq 0 \quad ; \quad [X_i,X_i] = [Y_i,Y_i] = [Z_i,Z_i] \neq 0 \quad (9)$$

On sait par exemple qu'une erreur X_i anticommute avec un générateur M s'il contient un opérateur Y ou Z à sa $i^{ème}$ position. Une erreur X_iZ_i anticommute avec un générateur M s'il contient des opérateurs Y ou Z à la $i^{ème}$ position ou bien des opérateurs X ou Y à la $j^{ème}$ position. Les générateurs M_{11} et M_{12} ne sont pas concernés car ils agissent du qubit 13 au qubit 17. Les tableaux 3a, 3b et 3c ci-dessous, montrent les syndromes pour toutes les erreurs possibles (253 erreurs) sur un ou deux qubits dans le groupe allant du premier au onzième qubit. Chaque ligne donne le syndrome pour les erreurs E contenues dans la première colonne. Les lignes sont disposées de manière à diriger l'algorithme d'estimation d'erreur présenté dans l'appendice 8.4. Les valeurs en gras dans les syndromes indiquent les générateurs dont les valeurs propres doivent être mesurées afin de détecter l'erreur de canal E. Cette procédure aide à contrer le phénomène de décohérence.

E	Syndromes	E	Syndromes
Y_3,Z_2Z_4	**1111**000000	X_3Z_8	**1**00**1**0**11**000
Z_2X_5	**111**0**1**00000	X_3X_9	**1**00**1**0**10**0**1**0
Y_2,Z_1Z_3	**1110000**000	Z_1X_6	**1**00**1**0**1**000
Z_2X_6	**11**0**1**0**1**0000	X_3Z_9	**1**00**1**00**11**00
Z_2Z_5,X_1X_3,X_3X_4	**1101**0**0**0000	X_3X_{10}	**1**00**1**00**1**0**1**0
Z_2Z_7	**11**00**1**10000	X_3X_7	**1**00**1**0**0100**0
Z_2X_8	**11**00**1**0**0**100	X_3X_{11}	**1**00**1**000**1**0**1**
Z_2Z_6	**110**0**1**00**0**00	X_3Z_{10}	**1**00**1**0**0100**
Z_2Z_8	**11**0000**11**000	X_3Z_{11}	**1**00**1**00**0**0**1**0
Z_2X_9	**110001**0000	X_3,Z_1Z_5	**1001000000**
Z_2Z_9	**11**0000**1**100	Z_1Z_7	**100011**0000
Z_2X_{10}	**11**0000**1**0**1**0	Z_1X_8	**100**0**1**00100
Z_2X_7	**11**0000**1000**	Z_1Z_6	**10001**0**0**00
Z_2X_{11}	**11000001**0**1**	Z_1Z_8	**1000011000**
Z_2Z_{10}	**11**0000**10**0	Z_1X_9	**100010**0**1**0
Z_2Z_{11}	**11**0000**0**0**1**0	X_3X_6	**100010**000
Y_1,Z_2,Z_1X_4	**1100000000**	Z_1Z_9	**100**0**11**00
Z_1Z_4,X_2X_3	**1011**000000	Z_1X_{10}	**100**0**1**0**1**0
X_3X_5	**1011**00000	Z_1X_7	**100**0**0100**0
Z_1X_5	**101**0**1**00000	Z_1Z_{10}	**100000**0**11**0
Z_2Z_3,X_3Z_4,Z_1X_2	10**100**00000	Z_1X_{11}	**100000**0**10**0
X_3Z_7	100**111**0000	Z_1Z_{11}	**100**0**0**0**0**1**0**
X_3X_8	100**11**0**0**100	$Z_1,X_1Z_2,$	**1000000000**
X_3Z_6	100**11**0**0**000	X_3Z_5,Z_2X_4	**1000000000**

Tableau 3a : Valeurs des syndromes pour les erreurs de canal sur un ou deux qubits parmi un groupe de onze qubits reçus et traités par le décodeur. Les valeurs en gras désignent les générateurs qui doivent être mesurés pour détecter l'erreur E correspondante.

E	Syndromes	E	Syndromes
Z_3X_6	0**111**0**1**0000	Z_4Z_{10}	00**11**00**1**0**0**
Y_4,X_1Z_4,Z_3Z_5	**0111**0**0**000	Z_4Z_{11}	00**11**00**0**1**0**
Z_3Z_7	0**11**0**11**0000	Z_4,X_2Z_5	**0011**0**0000**
Z_3X_8	0**11**0**1**00**1**00	X_5Z_8	00**1**0**111**000
X_1X_5,X_4X_5,Z_3Z_6	**0110100**000	X_5X_9	0**0101100**1**0**
Z_3Z_8	0**11**00**11**000	X_2Z_7	**0010110000**
Z_3X_9	0**11**00**1**0000	X_5Z_9	00**1**0**1**0**11**00
Z_3Z_9	0**11**0000**11**00	X_5X_{10}	00**1**0**1**0**1**0
Z_3X_{10}	0**11**0000**1010**	X_5X_7	00**1**0**1010**0
Z_3X_7	0**11**0000**1**000	X_5Z_{10}	00**1**0**1**00**1**0
Z_3X_{11}	0**11**000**1**0**1**	X_5X_{11}	00**1**0**1**00**1**01
Z_3Z_{10}	0**110**0**0**1**0**0	X_2X_8	**0010100100**
Z_3Z_{11}	0**11**0000**1**0	X_5Z_{11}	0**0101**00**10**
Z_3,X_1X_2,X_2X_4	0**11000000**0	X_5,X_2Z_6	**0010100**000
X_1X_6,X_4X_6	**0101**0**1**0000	X_2Z_8	0**0100111**000
$X_1Z_5,X_4Z_5,Z_2X_3,Z_3Z_4$	**0101**00000	X_2X_9	00**1001**0**1**0
X_1Z_7,X_4Z_7	**0100**1**1**0000	X_5Z_7,Z_4X_6	00**1001000**0
X_1X_8,X_4X_8	**0100**1**0**0**1**00	X_2Z_9	0**0100**0**11**00
X_1Z_6,X_4Z_6,Z_3X_5	**0100100**000	X_2X_{10}	0**0100**0**1**0**1**0
X_1Z_8,X_4Z_8	**0100011**000	X_2X_7	0**0100010**0**0**
X_1X_9,X_4X_9	**0100010**0**1**0	X_2Z_{10}	0**0100**00**100**
X_1Z_9,X_4Z_9	0**10**0000**11**00	X_2X_{11}	0**0100**00**1**0**1**
X_1X_{10},X_4X_{10}	**0100**0**1**0**10**	X_5X_8	0**0100**0**1**0**0**
X_1X_7,X_4X_7	**0100**0**1**00**0**	X_2Z_{11}	0**01**0000**010**
X_1Z_{10},X_4Z_{10}	**01**00000**100**	$X_2,X_1Z_3,X_5Z_6,Z_3X_4,Z_4Z_5$	**0010000000**
X_1X_{11},X_4X_{11}	**0100**0000**1**0**1**	X_6X_8	000**111**0100
X_1Z_{11},X_4Z_{11}	**0100**0000**1**0	Y_6,Z_5Z_7	**00011100**00
X_4,X_1,X_2Z_3,Z_1Z_2	**0100000000**	Z_5X_8	**0011**00**1**00
X_5X_6,Z_4Z_7	00**1111**0000	X_6Z_7,Z_4X_5,Z_5Z_6	**00110000**0
Z_4X_8	00**111001**00	X_6Z_9	000**1011**00
Y_5,Z_4Z_6	00**111000**00	X_6X_{10}	000**1011**0**1**0
Z_4Z_8	00**11011**000	X_6X_7,Z_5Z_8	**0001011000**
X_2X_6,Z_4X_9	0**0110100**00	X_6X_{11}	000**1**0**1**0**1**0**1**
Z_4Z_9	00**11001100**	X_6Z_{10}	000**1010**0**0**
Z_4X_{10}	00**11001**0**1**0	X_6Z_{11}	000**1010**0**1**0
Z_4X_7	00**11001000**	X_6,Z_5X_9	**0001010000**
Z_4X_{11}	00**11000101**	Z_5Z_9	**0**000**1011**00

Tableau 3b : Valeurs des syndromes pour les erreurs de canal sur un ou deux qubits parmi un groupe de onze qubits reçus et traités par le décodeur. Les valeurs en gras désignent les générateurs qui doivent être mesurés pour détecter l'erreur E correspondante.

E	Syndromes	E	Syndromes
Z_5X_{10}	**0**0010**0101**0	Z_8X_{11}	0000**1110**1
X_6Z_8,Z_5X_7	**0001001000**	Y_9,Z_8Z_{10}	000**0111000**
Z_5X_{11}	00**1000101**	X_9X_{10},X_7X_9	000**0110**10
Z_5Z_{10}	00**1000100**	Z_8,Z_8Z_{11}	**0000110**10
Z_5Z_{11}	00**1000010**	X_9X_{11}	000**0101**01
Z_5,X_6X_9,X_2Z_4,Z_1X_3	**0001000000**	X_9Z_{10},Z_7X_8,Z_8Z_9	000**0101000**
Y_8,Z_7Z_9	0000**111**00	X_9,X_9Z_{11},Z_8X_{10}	000**0100**10
Z_7X_{10}	00**0011010**	X_7Z_8,Z_5X_6,Z_6Z_7	**0000100**00
Y_7,Z_6Z_8	00**0011000**	$X_{10}X_{11}$	000000**1111**
Z_7X_{11}	0000**110101**	Y_{10},Z_9Z_{11}	0000**01110**
X_8X_9,Z_7Z_{10}	000**0110100**	X_7X_{11}	0000**01101**
Z_7Z_{11}	0000**110**10	Z_9,X_7Z_{10}	**0000011000**
Z_7,Z_6X_9	**0000110000**	X_{10},X_7Z_{11}	**0000010**10
X_8X_{10}	0000**10111****0**	Z_9X_{11}	000000**100**1
X_7X_8,Z_6Z_9	00**0010110**0	$X_7,Z_8X_9,X_{10}Z_{11},Z_9Z_{10}$	**0000010000**
Z_6X_{10}	00**0010101**0	Y_{11}	000000**111**
X_8Z_9,Z_6X_7,Z_7Z_8	00**0010100**0	$Z_9X_{10},Z_{10}Z_{11}$	0000**00110**
X_8Z_{11}	0000100**11**0	X_{11}	0**000001**01
Z_6X_{11}	00**0010010**1	Z_{10},X_7Z_9,Z_6X_8	**0000000100**
X_8,Z_6Z_{10}	**0000100100**	Z_{11},X_7X_{10}	0000000010
Z_6Z_{11}	0000**1000**10	$Z_{10}X_{11}$	0000**00001**
X_8X_{11}	0000100**001**	X_1X_4	**0000000000**
$Z_6,X_2X_5,Z_7X_9,X_8Z_{10}$	0**0010000**0	Pas d'erreur	**0000000000**

Tableau 3c : Valeurs des syndromes pour les erreurs de canal sur un ou deux qubits parmi un groupe de onze qubits reçus et traités par le décodeur. Les valeurs en gras désignent les générateurs qui doivent être mesurés pour détecter l'erreur E correspondante.

III.6 Simulation

Nous avons simulé sur Maple le code à cinq qubits en utilisant le programme Feynman version 4 (2008) décrit dans [9][10][11][12] et disponible dans [12]. Ce programme est un ensemble de procédures destinées à la définition et à la manipulation d'un système à n qubits et des portes agissant sur eux. L'annexe H-1 exhibe la simulation du circuit de codage montré sur la figure 9. On note que le premier qubit n'est pas envoyé à travers le canal car aucune porte ne s'applique sur lui [5]. On remarque aussi que jusqu'à l'état $|Q8\rangle$ la procédure d'encodage ne concerne que cinq qubits (qubit 2 à qubit 6), alors que celle allant de l'état $|Q9\rangle$ à $|\ Q20\rangle$

concerne six qubits. L'état $|Q21\rangle$ qui n'est pas encore l'état codé est un produit tensoriel des états $|Q8\rangle$ et $|Q20\rangle$ correspondants respectivement aux groupes à cinq et six qubits. L'état codé qui sera transmis dans le canal est déduit en appliquant la porte restante controlled-Z (CZ) partagé par les deux groupes de qubits précédents. Cette procédure évite de calculer le produit de plusieurs grandes matrices et permet donc de réduire le temps d'exécution. L'état final codé $|Q26\rangle$ correspond au groupe allant du second au dix-septième qubits. Afin de vérifier que le circuit de codage simulé donne un état codé correct, on mesure dans l'annexe H-2 les Valeurs propres des générateurs (M_1 à M_8) pour l'état $|Q25\rangle$ correspondant au système de qubits allant du premier au onzième. Les messages « M_i true » obtenus à la sortie indiquent que la relation ($M_i|Q25\rangle = |Q25\rangle$, $1 \leq i \leq 8$) est vérifiée pour les huit générateurs, ce qui prouve la justesse du circuit de codage simulé. L'extraction des syndromes expliquée dans la section V-4 et simulée dans l'appendice H-3 a été effectuée pour les générateurs M_1 à M_8. L'appendice H-4 contient la simulation de la correction pour une erreur simple et double dans le groupe d'erreur allant de qubit 1 à qubit 11. Les différents syndromes sont extraits en suivant l'ordre de disposition des erreurs dans les tables 2, 3 et 4 dans le but d'identifier plus rapidement les erreurs de canal possibles. L'erreur la plus vraisemblable est choisie en tenant compte du fait par exemple que la perturbation d'un qubit unique est plus probable que celle de deux qubits lors de la transmission. Enfin, l'état codé $|Q29\rangle$ du système allant du premier au onzième qubits est rétabli dans son état initial transmis par l'émetteur en appliquant la porte associée à l'erreur détectée par la mesure des syndromes. Une procédure utilisant les générateurs M_9 à M_{16} démarre pour détecter l'erreur dans le groupe de qubits suivants allant du douzième au vingt-troisième. Une fois cette détection déclenchée, on commence instantanément le décodage du groupe de qubits précédents corrigé. Le circuit de décodage simulé dans l'appendice H-5 est le circuit de codage de la figure 9 mais inversement exécuté. Pour une meilleure compréhension, on a divisé la simulation par couches de portes commutant entre elles dans la même couche. Afin de réduire le temps d'exécution, seule une porte est exécutée à la fois sur un qubit donné du système à onze qubits. On obtient finalement l'état initial $|Q67\rangle = |Q25\rangle$ transmis qui permet de récupérer en supprimant les ancillas, les états $|Q_1\rangle\ et\ |Q_2\rangle$ des deux qubits en position 4 et 9 portant l'information utile.

III.6.1 Fidélité

La fidélité est le recouvrement $F=<\Psi_t|\rho_m|\Psi_t>$ entre la fonction d'onde $|\Psi_t> = |Q_1> \otimes |Q_2>$ qui est le produit tensoriel des états deux qubits utiles transmis et $\rho_m=|\Psi_m><\Psi_m|$ qui est la matrice densité de l'état mesuré $|\Psi_m> = |Q_{1m}> \otimes |Q_{2m}>$. Si une erreur double se produit, l'état $|\Psi_m>$ est obtenu en appliquant (après mesure du syndrome et avant décodage) l'opérateur correspondant à l'erreur sur un seul qubit ayant le même syndrome. Par exemple, si une erreur $E=X_5Z_6$ se produit, elle sera corrigée par l'application de l'opérateur X_2 qui permet de déduire la fidélité $F= |2\alpha^2 -1|^2 <1$. Par contre, si la double erreur est $E=X_1Z_3$ alors la fidélité sera égale à F=1. Lorsque certaines erreurs n'ont pas de syndrome en commun avec des erreurs sur un qubit , on les considère comme équiprobables. Par exemple, les erreurs (X_1X_6, X_4X_6) ont le même syndrome et peuvent être recouverts par application de l'opérateur X_4X_6 lorsque l'erreur X_1X_6 s'est produite ou inversement. Les facteurs $\alpha_i=cos(\theta_i/2)$ et $\beta_i=e^{i\phi i}sin(\theta_i/2)$ illustrés dans la sphère de Bloch par les angles sphériques (θ_i,ϕ_i) permettent d'exprimer la fidélité $F(\theta_i,\Phi i)$ en termes de ces angles. Le tableau 4 montre quelques erreurs avec la même fidélité et le tableau 5 la fidélité F calculée

pour des erreurs ayant le même syndrome. Le tableau 6 exhibe la fidélité $F(\theta,\phi)$ et la fidélité moyenne F_a pour toutes les erreurs possibles sur les états $(|Q_1>, |Q_2>)$ des deux qubits utiles. On note que si une erreur X_5X_6 se produit et qu'elle est recouverte par l'opérateur Z_4Z_7 (même syndrome), ou inversement, alors les deux qubits utiles seront infectés après décodage donnant une fidélité égale à $F_a=1/9$. Cependant, la fidélité peut être égale à $F_a=1$ si l'opérateur de recouvrement correspond à l'erreur. La fidélité moyenne est calculée par intégration sur (θ,ϕ) :

$$Fa = (1/4)\iint F(\theta,\phi)\sin(\theta)d\theta d\phi \;;\; 0 < \theta < \pi \text{ et } 0 < \phi < 2\pi \qquad (10)$$

E	$F(\alpha_1,\beta_1,\alpha_2,\beta_2)$
x_1z_3,z_3x_4	1
$x_2z_6,x_5z_6,x_1x_2,x_2x_4$	$\lvert 2\alpha_1^2-1\rvert^2$
$z_5x_9,z_8x_9,x_{10}z_{11},x_7z_{11}$	$\lvert 2\alpha_2^2-1\rvert^2$
z_1z_5,z_4z_5	$\lvert \alpha_1\beta_1^*+\beta_1\alpha_1^*\rvert^2$
z_9z_{10},z_6z_{10}	$\lvert \alpha_2\beta_2^*+\beta_2\alpha_2^*\rvert^2$
x_1z_2,z_1z_3	$\lvert \alpha_1\beta_1^*-\beta_1\alpha_1^*\rvert^2$
x_5x_6,z_4z_7	1 ou $\lvert \alpha_1\beta_1^*-\beta_1\alpha_1^*\rvert^2$ $\lvert \alpha_2\beta_2^*-\beta_2\alpha_2^*\rvert^2$

Tableau 4 : Quelques erreurs ayant la même fidélité.

E	$F(\alpha_1,\beta_1,\alpha_2,\beta_2)$
x_1,x_4,x_2z_3,z_1z_2	$1,1,1 ou \lvert 2\alpha_1^2-1\rvert^2, \lvert \alpha_1\beta_1^*-\beta_1\alpha_1^*\rvert^2 ou \lvert \alpha_1\beta_1^*+\beta_1\alpha_1^*\rvert^2$
$x_2,x_1z_3,z_3x_4,x_5z_6,z_4z_5$	$1,1,1,\lvert 2\alpha_1^2-1\rvert^2,\lvert \alpha_1\beta_1^*+\beta_1\alpha_1^*\rvert^2$
x_3,z_1z_5	$1,\lvert \alpha_1\beta_1^*+\beta_1\alpha_1^*\rvert^2$
x_5,x_2z_6	$1,\lvert 2\alpha_1^2-1\rvert^2$
x_6,z_5x_9	$1,\lvert 2\alpha_2^2-1\rvert^2$
$x_7,z_8x_9,x_{10}z_{11},z_9z_{10}$	$1,\lvert 2\alpha_2^2-1\rvert^2,\lvert 2\alpha_2^2-1\rvert^2,\lvert \alpha_2\beta_2^*+\beta_2\alpha_2^*\rvert^2$
x_8,z_6z_{10}	$1,\lvert \alpha_2\beta_2^*+\beta_2\alpha_2^*\rvert^2$
x_9,x_9z_{11}	$1,\lvert 2\alpha_2^2-1\rvert^2$
x_{10},x_7z_{11}	$1,\lvert 2\alpha_2^2-1\rvert^2$
x_{11}	1
z_1,x_1z_2,x_3z_5,z_2x_4	$1,\lvert \alpha_1\beta_1^*-\beta_1\alpha_1^*\rvert^2$
z_3,x_1x_2,x_2x_4	$1,1,\lvert 2\alpha_1^2-1\rvert^2$
y_2,z_1z_3	$1,\lvert \alpha_1\beta_1^*-\beta_1\alpha_1^*\rvert^2$
x_1x_5,x_4x_5,z_3z_6	$1,\lvert 2\alpha_1^2-1\rvert^2,\lvert 2\alpha_1^2-1\rvert^2$

Tableau 5 : Fidélité F calculée pour des erreurs ayant le même syndrome.

E	$\|Q_1\rangle \otimes \|Q_2\rangle$	$F(\theta,\phi)$	F_a
$No\ error$	$\langle\alpha_1,\beta_1\rangle\langle\alpha_2,\beta_2\rangle$	1	1
X_1	$\langle\beta_1,\alpha_1\rangle\langle\alpha_2,\beta_2\rangle$	$\|\alpha_1\beta_1^*+\beta_1\alpha_1^*\|^2=\|sin\theta_1 cos\phi_1\|^2$	$1/3$
Z_1	$\langle\alpha_1,-\beta_1\rangle\langle\alpha_2,\beta_2\rangle$	$\|2\alpha_1^2-1\|^2=cos^2\theta_1$	$1/3$
Y_1	$\imath\langle-\beta_1,\alpha_1\rangle\langle\alpha_2,\beta_2\rangle$	$\|\alpha_1\beta_1^*-\beta_1\alpha_1^*\|^2=\|sin\theta_1 sin\phi_1^2\|$	$1/3$
X_2	$\langle\alpha_1,\beta_1\rangle\langle\beta_2,\alpha_2\rangle$	$\|\alpha_2\beta_2^*+\beta_2\alpha_2^*\|^2=\|sin\theta_2 cos\phi_2\|^2$	$1/3$
Z_2	$\langle\alpha_1,\beta_1\rangle\langle\alpha_2,-\beta_2\rangle$	$\|2\alpha_2^2-1\|^2=cos^2\theta_2$	$1/3$
Y_2	$\imath\langle\alpha_1,\beta_1\rangle\langle-\beta_2,\alpha_2\rangle$	$\|\alpha_2\beta_2^*-\beta_2\alpha_2^*\|^2=\|sin\theta_2 sin\phi_2\|^2$	$1/3$
X_1X_2	$\langle\beta_1,\alpha_1\rangle\langle\beta_2,\alpha_2\rangle$	$\|sin\theta_1 cos\phi_1\|^2\|sin\theta_2 cos\phi_2\|^2$	$1/9$
X_1Z_2	$\langle\beta_1,\alpha_1\rangle\langle\alpha_2,-\beta_2\rangle$	$\|sin\theta_1 cos\phi_1\|^2 cos^2\theta_2$	$1/9$
X_1Y_2	$\imath\langle\beta_1,\alpha_1\rangle\langle-\beta_2,\alpha_2\rangle$	$\|sin\theta_1 cos\phi_1\|^2\|sin\theta_2 cos\phi_2\|^2$	$1/9$
Z_1X_2	$\langle\alpha_1,-\beta_1\rangle\langle\beta_2,\alpha_2\rangle$	$cos^2\theta_1\|sin\theta_2 cos\phi_2\|^2$	$1/9$
Z_1Z_2	$\langle\alpha_1,-\beta_1\rangle\langle\alpha_2,-\beta_2\rangle$	$cos^2\theta_1 cos^2\theta_2$	$1/9$
Z_1Y_2	$\imath\langle\alpha_1,-\beta_1\rangle\langle-\beta_2,\alpha_2\rangle$	$cos^2\theta_1\|sin\theta_2 sin\phi_2\|^2$	$1/9$
Y_1X_2	$\imath\langle-\beta_1,\alpha_1\rangle\langle\beta_2,\alpha_2\rangle$	$\|sin\theta_1 sin\phi_1\|^2\|sin\theta_2 cos\phi_2\|^2$	$1/9$
Y_1Z_2	$\imath\langle-\beta_1,\alpha_1\rangle\langle\alpha_2,-\beta_2\rangle$	$\|sin\theta_1 sin\phi_1\|^2 cos^2\theta_2$	$1/9$
Y_1Y_2	$-\langle-\beta_1,\alpha_1\rangle\langle-\beta_2,\alpha_2\rangle$	$\|sin\theta_1 sin\phi_1\|^2\|sin\theta_2 sin\phi_2\|^2$	$1/9$

Tableau 6 : La fidélité $F(\theta,\phi)$ et la fidélité moyenne F_a pour différentes erreurs possibles sur les deux qubits (Q_1,Q_2) envoyés contenant l'information utile.

IV.6.2 Généralisation

La propriété convolutive du code permet de généraliser les résultats précédents obtenus pour le premier groupe traité composé de onze qubits à tout le flux de qubits qui seront envoyés. En pratique, une fois le premier groupe traité (mesure de syndromes et recouvrement), le récepteur procède à son décodage et à la suppression des ancillas pour accéder au deux états de qubits utiles ($|Q_1\rangle, |Q_2\rangle$). Il entame alors instantanément le même traitement au second groupe (qubit 12 à qubit 22) jusqu'à accéder aux deux états utiles suivants qui sont ($|Q_3\rangle, |Q_4\rangle$) et ainsi de suite jusqu'à ($|Q_{p-1}\rangle, |Q_p\rangle$) si p est le nombre total de qubit utiles. Notons que le récepteur ne doit pas décoder le qubit numéro 11 du premier groupe avant d'avoir achevé le traitement du second groupe où il est utilisé comme contrôleur et cible. Pour un ensemble composé de k groupes contenant un total n=2k de qubits utiles, le qubit $Q_{2(5m+1)}$ avec m=1,2,….k est commun aux groupes successifs m et (m+1) mais doit être décodé avec le groupe (m+1). La table 7 montre pour un groupe donné de qubits (Q_l à Q_{l+10}, l=2,..,5n-8) la fidélité obtenue par la procédure décrite ici- bas.

E	$F_i(\alpha_i,\beta_i)$	F_{a_i}
$(X_j,Z_j,Y_j),(2 \preceq j \leq 12,$ $l \preceq j \leq l+10,\ l=12,22,..)$	1	1
$(X_jX_k,Z_jZ_k,X_jZ_k),(2 \preceq j,k \leq 12,$ $l \preceq j,k \leq l+10,\ l=12,22,..)$	$1\ ou\ \left\|2\alpha_i^2-1\right\|^2$ ou $\left\|\alpha_i\beta_i^* \pm \beta_i\alpha_i^*\right\|^2$ $i=1/2,3/4,...,(n-1)/n$	$1\ ou\ \frac{1}{3}$
$X_{m+6}X_{m+7}, Z_{m+5}Z_{m+8},$ $m=-1,5,10,...,5(n-1), n \succeq 2$	$1\ ou\ \left\|\alpha_i\beta_i^*-\beta_i\alpha_i^*\right\|^2\left\|\alpha_{i+1}\beta_{i+1}^*-\beta_{i+1}\alpha_{i+1}^*\right\|^2$	$1\ ou\ \frac{1}{9}$

Tableau 7 : Fidélité $F(\alpha_i,\beta_i)$ et fidélité moyenne Fa_i pour erreur sur deux qubits dans un groupe de onze qubits contenant deux qubits utiles.

Notre modèle considère les erreurs de canal sur un ou deux qubits comme les plus probables et celles sur trois qubits et plus comme très improbables. Nous déduisons de la table 4 que pour chaque groupe contenant deux qubits utiles, l'un des deux est recouverts dans la majorité des cas. Les deux qubits utiles *(Q_i , Q_{i+1})* sont tous les deux infecté à la fin du décodage, seulement si l'erreur de canal produite est $X_{m+6}X_{m+7}$ ou $Z_{m+5}Z_{m+8}$, *m=-1,5,10,…,5(n-1).*

La fidélité calculée pour le i^{eme} groupe de onze qubits contenant deux qubits utiles *(Q_i , Q_{i+1})* est donnée par l'expression suivante :

$$F_i = \langle\psi_t|\psi_m\rangle\langle\psi_m|\psi_t\rangle = \left|\langle Q_{t_i}|Q_{m_i}\rangle\langle Q_{t_{i+1}}|\,Q_{m_{(i+1)}}\rangle\right|^2 \quad (11)$$

Pour n qubits utiles transmis, la fidélité est donnée par l'expression :

$$F = \Pi_i F_i \left|\langle Q_{t_i}|Q_{m_i}\rangle\langle Q_{t_{i+1}}|\,Q_{m_{(i+1)}}\rangle\right|^2 \quad i=1,3,..,n-1 \quad (12)$$

La fidélité moyenne totale est égale à :

$$F_a = \Pi_i F_{a_i}\ ,\quad F_{a_i} = 1\ \ ou\ \ \frac{1}{3}\ \ ou\ \ \frac{1}{9}\ \ , i=1,3,\ldots,n-1 \quad (13)$$

Supposons qu'un nombre n_1 de groupes à onze qubits traités soient recouverts avec une fidélité moyenne $Fa_i=1/3$ et qu'un nombre n_2 soient recouverts avec une fidélité moyenne $Fa_i=1/9$. Alors, les $((n/2)-n_1-n_2)$ groupes restants sont recouverts avec une fidélité $Fa_i=1$ et la fidélité moyenne pour l'ensemble du flux transmis est égale à :

$$F_a = (1)^{\left(\frac{n}{2}-n_1-n_2\right)}\left(\frac{1}{3}\right)^{n_1}\left(\frac{1}{9}\right)^{n_2} \quad (14)$$

On définit les probabilités P_1 et P_2 correspondant respectivement aux fractions de groupes de qubits recouverts avec les fidélités moyennes $Fa_i = 1/3$ et $Fa_i = 1/9$ par les relations suivantes :

$$P_1 = \frac{n_1}{(n/2)} \qquad \text{et} \qquad P_2 = \frac{n_2}{(n/2)} \tag{15}$$

On obtient finalement la fidélité moyenne en fonction de P_1 et P_2 :

$$F_a(P_1, P_2) = (1)^{\frac{n}{2}(1-P_1-P_2)} \left(\frac{1}{3}\right)^{nP_1} \left(\frac{1}{9}\right)^{\frac{n}{2}P_2}$$

$$F_a(P_1, P_2) = \left(\frac{1}{3^n}\right)^{\frac{P_1}{2}+P_2} \tag{16}$$

La table 7 permet de faire une comparaison entre P_1 et P_2 . En effet, la première ligne concerne trente trois erreurs simples (sur un groupe de onze qubits transmis) auxquelles il faut rajouter une des deux erreurs doubles de la dernière ligne qui donnent une fidélité égale à un.

La ligne du milieu concerne des erreurs doubles qui donnent trois expressions de la fidélité dont l'une vaut 1. On peut donc supposer que les 2/3 de ces doubles erreurs donneront une fidélité moyenne égale à 1/3. Le nombre total d'erreurs simples et doubles sur le groupe de onze qubits étant de 253 on déduit que le nombre de double erreur donnant une fidélité égale à 1/3 est égal à (253-34)x2/3=146. Selon la dernière ligne de la table 7, seule une erreur double parmi les deux donnera une fidélité égale à 1/9 car l'autre sera corrigée par elle-même. Donc une erreur double sur 253 donne une fidélité égale à 1/9. En conclusion, on peut déduire $P_1 \gtrsim 146$, ce qui donne :

$$F_a(P_1) = \left(\frac{1}{3^n}\right)^{P_1\left(\frac{1}{2}+\frac{1}{146}\right)} \cong \left(\frac{1}{3}\right)^{\frac{n}{2}P_1} \tag{17}$$

La figure 10 montre l'évolution de la fidélité moyenne pour l'intervalle de probabilité ($0 \leq p_1 = p \leq 1$, $p_2 \cong 0$) et différentes valeurs du nombre total n de qubits utiles transmis. On observe qu'elle décroit rapidement lorsque P croit et s'évanouit de plus en plus vite lorsque n augmente. En conclusion, la fidélité est proche de l'unité pour de très petites valeurs de P et elle est meilleure lorsque n est plus petit pour une valeur fixe de P. Par exemple, pour $F = \left(\frac{1}{3}\right)^{\frac{n}{2}P_1} > \frac{2}{3}$ on déduit la condition : $P_1 = \frac{n_1}{(n/2)} < (1 - \frac{ln2}{ln3})\frac{2}{n}$ et si n=10^3 on a $P_1 < 0.74\ 10^{-3}$. Ce qui implique que sur 10^4 groupes de onze qubits traités, seuls environ sept groupes contiennent un qubit utile sur deux non désinfecté.

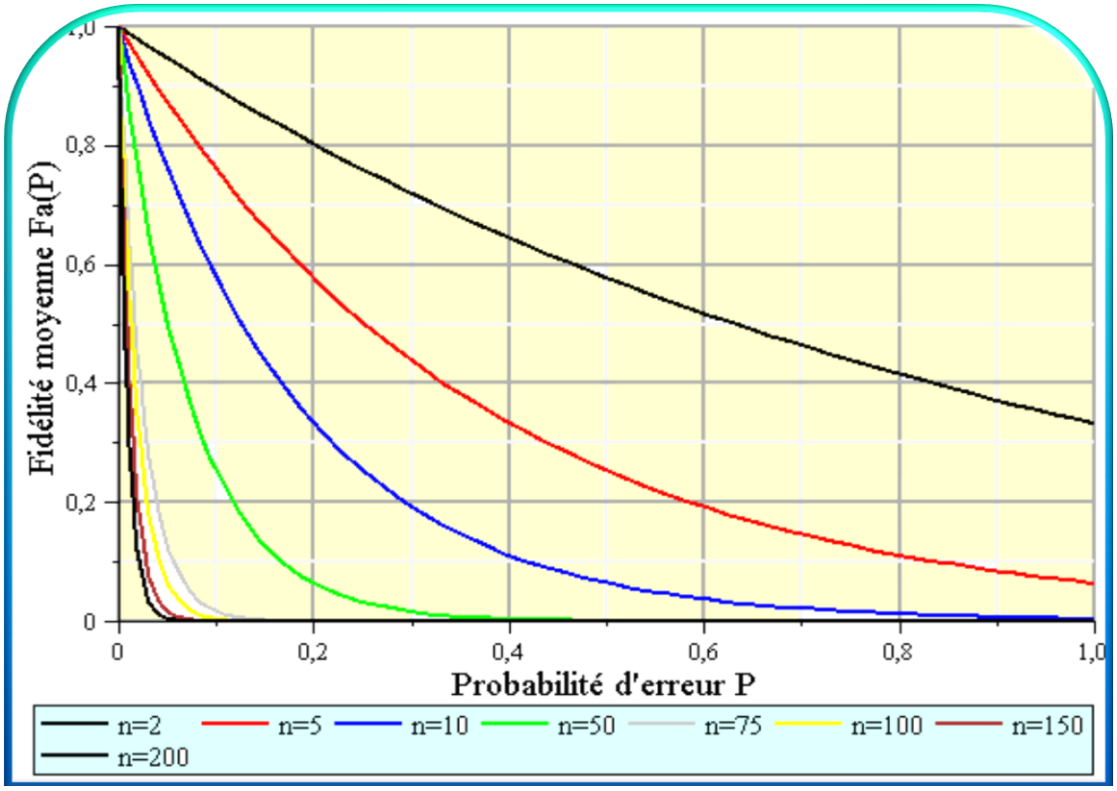

Figure 10 : Evolution de la fidélité en fonction de la probabilité P qu'une erreur affecte deux qubits durant la transmission pour différentes valeurs du nombre total n de qubits portant l'information utile.

III-7 Conclusion

Les résultats de la simulation d'un code convolutif à cinq qubits obtenus dans ce chapitre démontrent clairement l'exigence d'utiliser des canaux de transmission faiblement bruités afin d'atteindre une fiabilité acceptable de l'information transmise. Cette fiabilité est d'autant plus basse que le nombre de qubits transmis est plus élevé. Nous pouvons conclure, au moins pour le code convolutif étudié, que l'efficacité de ce type de code est intéressante lorsque des messages de courte ou moyenne longueur sont envoyés par des canaux à faible interaction avec le monde extérieur. Le chapitre suivant traite d'un protocole de communication quantique dans lequel un secret est transmis à travers des canaux bruités par un petit nombre de qubits. En conséquence, un autre type de code sera utilisé qui sont trois codes en blocs car l'information utile à transmettre n'est pas un flux mais portée par un seul qubit. Le but est de comparer l'efficacité des trois codes à travers la détermination de la fidélité.

Chapitre IV :

Le Partage de Secret Quantique

IV.1 Introduction

Nous investiguons dans ce travail un protocole particulier de cryptographie quantique qui est le partage d'un secret stocké dans l'état intriqué d'un système de n qubits appelé état de graphe. Ces qubits sont envoyés chacun dans un canal par un émetteur et reçus par n récepteurs dont un nombre k vont collaborer afin que l'un d'eux puisse accéder au secret. Nous allons traiter ici le cas d'un secret enregistré dans l'état d'un ensemble de cinq qubits appelé état de graphe et envoyé à cinq récepteurs dont trois seulement accéderont au secret, les deux autres étant considérés comme des espions. L'originalité du travail est l'utilisation de codes correcteurs d'erreur quantiques à cause de la présence de bruit dans les canaux de transmission. Ainsi, nous allons utiliser trois codes respectivement à cinq, sept et neuf qubits et comparer la fidélité du secret mesuré par rapport au secret envoyé. Il est connu que ces trois codes corrigent toujours, avec une fidélité égale à un, une erreur quelconque sur l'un des cinq, sept ou neuf qubits envoyés. Cependant, si deux qubits ou plus sont perturbés dans un canal, alors la correction donnera une fidélité qui dépend du code utilisé. Afin de réduire la complexité du problème on traitera le cas où deux qubits sont infectés dans chacun des canaux. L'utilisation de l'état de graphe se justifie par le fait qu'il est très utile pour plusieurs protocoles quantiques comme le partage de secret, le calcul basé sur la mesure, la correction d'erreur, la téléportation et les communications quantiques. Ainsi, il pourrait être à l'avenir un bon outil pour unifier ces protocoles en un seul formalisme**.** Par exemple, un résultat secret de calcul quantique est enregistré dans un état de graphe puis protégé par un code et envoyé à travers des canaux bruités. Par ailleurs, les états de graphes ont une représentation graphique qui offre une image intuitive du flux d'information transmis **[**14]. Enfin, notre modeste contribution à cette tache a fait l'objet de travaux décrits dans [R2] [R3] et [R4].

IV.2 Partage de secret avec un état de graphe à cinq qubits

L'état de graphe à cinq qubits symbolisé pa $|G\rangle$ est donné par l'équation (18) et schématisé dans la figure 11 où les sommets représentent les qubits et les liaisons les portes controlled-Z. L'état de graphe $|\Psi_G\rangle$ donné par l'expression (19) contient le secret $|\psi_S\rangle = \alpha|0\rangle + \beta|1\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}sin\left(\frac{\theta}{2}\right)|1\rangle$ transmis par un émetteur appelé « dealer » à cinq récepteurs appelés « joueurs ». La construction par l'émetteur de l'état de graphe $|\psi_G\rangle$ se fait en plusieurs étapes. D'abord, il dispose de cinq qubits se trouvant à l'état global initial $|\psi_0\rangle = |00000\rangle$ sur lesquels il applique la porte H à chacun d'eux puis la porte conditionnelle CZ sur les qubits [1,2]; [2,3]; [3,4]; [4,5]; [5,1] pour obtenir l'état de graphe **[**14] :

$$|\,G\rangle = \left(\Pi_{1\le i\le 4} CZ_{[i,i+1]}|+\rangle^{\otimes 5}\right) \qquad (18)$$

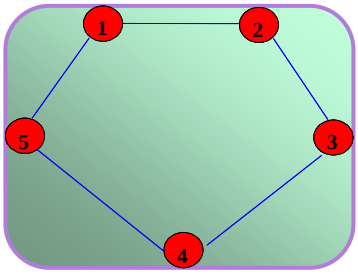

Figure 11 : Etat de graphe à cinq qubits $|G\rangle$ **[**14] **.**

L'émetteur réalise alors une intrication entre un qubit additionnel appelé D et chacun des cinq qubits puis rajoute au système obtenu le qubit S contenant le secret $|\Psi_S\rangle$ (la procédure est detailée dans la référence [14]) . Il procède alors à une mesure de Bell sur les deux qubits D and S pour obtenir l'état final à transmettre [14] :

$$|\Psi_G\rangle = \alpha|G\rangle + \beta[\Pi_{1\leq i\leq 5} Z_i]|G\rangle \quad (19)$$

On obtient dans la notation de Dirac la superposition d'états suivante :

$$\begin{aligned}|\Psi_G\rangle = \left(\frac{\sqrt{2}}{8}\right)\{(\alpha+\beta)[\,&|10100\rangle + |10010\rangle + |10111\rangle + |01111\rangle \\ &+|11101\rangle + |00000\rangle + |00011\rangle + |11000\rangle + |10001\rangle + |01100\rangle \\ &+|00101\rangle + |01010\rangle] + (\alpha\text{-}\beta)\,[|11010\rangle + |10110\rangle + |10101\rangle + |10000\rangle] \\ &+ (-\alpha+\beta)\,[\,|01011\rangle + |01101\rangle + |00001\rangle + |10011\rangle + |01000\rangle + |11111\rangle \\ &+|00100\rangle + |01110\rangle + |00111\rangle + |11100\rangle + |11001\rangle] - (\alpha+\beta) \\ &[|11011\rangle + |00110\rangle + |01001\rangle + |11110\rangle + |00010\rangle]\}\end{aligned} \quad (20)$$

IV.2.1 Transmission par canaux non bruités

Commençons par traiter le cas où les cinq qubits sont transmis par des canaux non bruités. L'état de graphe $|\Psi_G\rangle$ peut être décomposé en termes d'états de Bell $|B_{ij}\rangle_{13}$ et $|B_{ij}\rangle_{45}$ **[14]** :

$$\begin{aligned}|\Psi_G\rangle = \left(\frac{1}{2}\right)\{&|B_{00}\rangle_{13}[\alpha|+\rangle + \beta|-\rangle]_2|B_{01}\rangle_{45} + |B_{01}\rangle_{13}[\alpha|+\rangle - \beta|-\rangle]_2|B_{10}\rangle_{45} + \\ &|B_{10}\rangle_{13}[\alpha|-\rangle - \beta|+\rangle]_2|B_{00}\rangle_{45} + |B_{11}\rangle_{13}[\alpha|-\rangle + \beta|+]_2|B_{11}\rangle_{45}\}\end{aligned} \quad 21)$$

Les états de Bell sont données par :

$$\begin{aligned}|B_{00}\rangle = \tfrac{|00\rangle+|11\rangle}{\sqrt{2}} \quad ; \quad |B_{01}\rangle = \tfrac{|00\rangle-|11\rangle}{\sqrt{2}} \quad ; \\ |B_{10}\rangle = \tfrac{|01\rangle+|10\rangle}{\sqrt{2}} \quad ; \quad |B_{11}\rangle = \tfrac{|01\rangle-|10\rangle}{\sqrt{2}}\end{aligned} \quad (22)$$

Le secret doit être accessible seulement aux joueurs 1, 2 et 3, les joueurs 4 et 5 étant considérés comme des espions. Les joueurs 1 et 3 mesurent leur qubits dans la base de Bell et transmettent le résultat au joueur 2 qui applique en conséquence sur son qubit l'une des portes R_G dans le tableau 8 qui lui permet d'accéder au secret.

$\|B_{ij}\rangle_{13}$	$\|B_{00}\rangle$	$\|B_{01}\rangle$	$\|B_{10}\rangle$	$\|B_{11}\rangle$
R_g	H	ZH	ZXH	XH

Tableau 8 : Portes de recouvrement de secret R_G utilisées par le joueur 2 selon l'état de Bell $|B_{ij}\rangle_{13}$ mesuré par les joueurs 1 et 3.

Nous décrivons ici-bas la procédure d'accession au secret utilisée par les joueurs 1, 2 et 3. L'équation (21) peut être écrite de la manière suivante :

$$|\Psi_G\rangle = |B_{00}\rangle_{13}|\Psi_a\rangle_{245} + |B_{01}\rangle_{13}|\Psi_b\rangle_{245} + |B_{10}\rangle_{13}|\Psi_c\rangle_{245} + |B_{11}\rangle_{13}|\Psi_d\rangle_{245} \quad (23a)$$

Avec $|\Psi_a\rangle_{245} = \frac{1}{2}[\alpha|+\rangle + \beta|-\rangle]_2|B_{01}\rangle_{45}$; $|\Psi_b\rangle_{245} = \frac{1}{2}[\alpha|+\rangle - \beta|-\rangle]_2|B_{10}\rangle_{45}$

$$|\Psi_c\rangle_{245} = \frac{1}{2}[\alpha|-\rangle - \beta|+\rangle]_2|B_{00}\rangle_{45} \; ; |\Psi_d\rangle_{245} = \frac{1}{2}[\alpha|-\rangle + \beta|+\rangle]_2|B_{11}\rangle_{45} \quad (23b)$$

La mesure dans la base de Bell $\{|B_{ij}\rangle_{13}\}$ des deux qubits 1 et 3 ne laissera qu'un seul terme dans la superposition (23a), ce qui donne la matrice densité :

$$\rho_{1..5} = \left(\frac{1}{4}\right)(|B_{ij}\rangle\langle B_{ij}|)_{13}\,(|\psi_x\rangle\langle\psi_x|)_{245} = \left(\frac{1}{4}\right)(\rho_{ij})_{13}(\rho_x)_{245} \quad (24)$$

Avec x = a, b, c ou d. La trace partielle sur qubits 4 et 5 donne la matrice densité :

$$\rho_2' = |\psi_2'\rangle\langle\psi_2'| = P_{tr}[(\rho_x)_{245}]_{(4,5)} \quad (25)$$

Le joueur 2 applique la porte R_G qui convient et accède au secret :

$$\rho_2 = R_g^* \rho_2' R_g \qquad \text{ou} \qquad |\Psi_2\rangle = R_g|\psi_2'\rangle \quad (26)$$

IV.2.2 Erreur de canal X, Y ou Z sur les qubits transmis

On considère le cas où les qubits envoyés subissent une erreur de canal X, Y ou Z. En appliquant la procédure de la section précédente on obtient pour chaque erreur de canal sur les qubits 1, 2 et 3 un secret mesuré entaché d'erreur contenu dans le tableau 9. On déduit de la relation (23a) et de la procédure d'accession au secret que les erreurs sur les qubits 4 et 5 n'ont aucune incidence sur le secret mesuré.

$Error$	$\|\Psi^E\rangle_2$
X_1, X_3, Y_2	$\alpha\|1\rangle - \beta\|0\rangle$
Z_1, X_2, Z_3	$\alpha\|0\rangle - \beta\|1\rangle$
Z_2, Y_1, Y_3	$\alpha\|1\rangle + \beta\|0\rangle$

Tableau 9 : Secret mesuré entaché d'erreur $|\psi_2^E\rangle$ en fonction de l'erreur de canal sur les qubits 1 , 2 et 3.

On voit donc que la première ligne d'erreur induit une erreur Y sur le qubit secret et les lignes deux et trois une erreur Z et X respectivement.

IV.2.3 Fidélité

La fidélité est une des quantités mathématiques qui permet de savoir le degré de rapprochement entre deux états quantiques représentés par leur matrice densité σ et ρ en mesurant la distance entre eux [1] :

$$F(\sigma,\rho) = \left|Tr\left(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)\right|^2 \quad (27)$$

Dans le cas d'un état pure $\sigma = |\psi\rangle\langle\psi|$ et d'un état arbitraire ρ, la fidélité est le recouvrement entre ces deux états [1] :

$$F(|\psi\rangle, \rho)=\langle\psi|\rho|\psi\rangle \quad (28)$$

Dans ce travail, on mesure le recouvrement entre le secret envoyé $\sigma_S = |\psi_S\rangle\langle\psi_S|$ et celui mesuré par le joueur 2 $\rho_2 = |\psi_2\rangle\langle\psi_2|$. Nous décrivons ici-bas la procédure donnant la fidélité dans le cas où une erreur de Pauli quelconque E= σ_0, σ_x, σ_y ou σ_z perturbe l'état $|\psi_G\rangle$ dans le canal de transmission. En observant l'équation (23a) on constate qu'elle conserve toujours la même forme quelque soit l'erreur de canal affectant les qubits envoyé. En effet, si une erreur E perturbe les qubits transmis alors l'état global des cinq qubits devient à la réception :

$$|\psi_G^E\rangle = |B_{00}\rangle_{13}|\psi_a^E\rangle_{245} + |B_{01}\rangle_{13}|\psi_b^E\rangle_{245} + |B_{10}\rangle_{13}|\psi_c^E\rangle_{245} + |B_{11}\rangle_{13}|\psi_d^E\rangle_{245} \quad (29)$$

$|\psi_{a,b,cd}^E\rangle_{245}$ sont les états des qubits (2,4,5) altérés par les erreurs de canal.

On note que $|\psi^{\mathrm{E}}_{\mathrm{a,b,cd}}\rangle_{245} \neq \mathrm{E}|\psi_{\mathrm{a,b,cd}}\rangle_{245}$ car les erreurs peuvent affecter aussi bien les qubits (1,3) que les qubits (2,4,5). En fait, si une erreur perturbe les qubits (1,3) ou (4,5) alors leur état global va simplement changer en un autre état de Bell. De même, si le qubit 2 est perturbé alors son état va prendre l'une des autres formes apparaissant dans l'équation (23a) qui conserve alors sa forme globale. Après mesure sur l'état de Bell des qubits (1,3), seul un terme persiste dans la superposition (29) :

$$|\psi_G^E\rangle' = \frac{1}{2}|\mathrm{B_{ij}}\rangle_{13}|\psi^{\mathrm{E}}_{\mathrm{x}}\rangle_{245} \quad (30)$$

La matrice densité correspondante est :

$$\rho^E_{1..5} = \left(\frac{1}{4}\right)(|\mathrm{B_{ij}}\rangle\langle\mathrm{B_{ij}}|)_{13}\,(|\psi^{\mathrm{E}}_{\mathrm{x}}\rangle\langle\psi^{\mathrm{E}}_{\mathrm{x}}|)_{245} = = \left(\frac{1}{4}\right)(\rho_{ij})_{13}(\rho_x^E)_{245} \quad (31)$$

La trace partielle sur les qubits (4,5) donne la matrice densité de qubit 2 :

$$\rho_2'^{E} = |\psi_2'^{E}\rangle\langle\psi_2'^{E}| = P_{tr}[(\rho_x^E)_{245}]_{(4,5)} \quad (32)$$

La matrice densité de l'état secret entaché d'erreur mesuré par le joueur 2 est alors :

$$\rho_2^E = R_g^* \rho_2'^{E} R_g = |\psi_2^E\rangle\langle\psi_2^E| \quad (33)$$

On multiplie (33) par l'état secret $|\psi_S\rangle = \alpha|0\rangle + \beta|1\rangle$ pour obtenir la fidélité :

$$F(\theta,\phi)=\langle\psi_S|\rho_2^E|\psi_S\rangle \quad (34)$$

Le tableau 10a donne la fidélité F(θ,ϕ) calculée par le programme Feynman pour toutes les erreurs sur les qubits i=1,2 ou 3. La figure 12 montre la fidélité F(θ,ϕ) avec $0 \leq \theta \leq \pi$ et $\phi = 0$ ou $\pi/2$ lorsque différentes erreurs se produisent durant la transmission dans un, deux ou trois canaux. On note par exemple que si le secret est $|\psi_S\rangle = \frac{\sqrt{2}}{2}(\alpha|0\rangle + \beta|1\rangle)$, alors la fidélité moyenne est la meilleure (F_a=1) pour l'erreur X_1 sur qubit 1 et la plus mauvaise (F_a=0) pour l'erreur Z_1 sur le même qubit.

$Error$	$\|\Psi\rangle_2$	$F(\theta,\phi)$	F_a
ε_a	$\alpha\|1\rangle - \beta\|0\rangle$	$\|sin(\theta)sin\phi\|^2$	$1/3$
ε_b	$\alpha\|0\rangle - \beta\|1\rangle$	$cos^2(\theta)$	$1/3$
ε_c	$\alpha\|1\rangle + \beta\|0\rangle$	$\|sin(\theta)cos\phi\|^2$	$1/3$
ε_d	$\alpha\|0\rangle + \beta\|1\rangle$	1	1

Tableau 10a : Secret mesuré $|\Psi_2\rangle$, fidélité F(θ,ϕ) et F_a selon l'erreur de canal.

ε_a	$X_1, X_3, Y_2, X_1X_2Z_3, Z_1X_2X_3, Y_1X_2, Y_1Z_3, Z_1Y_3, X_2Y_3,$ $Y_1Y_2Y_3, Y_1Z_2X_3, X_1Y_2X_3, X_1Z_2Y_3, Z_1Y_2Z_3$
ε_b	$Z_1, X_2, Z_3, X_1Z_2, Z_2X_3, X_1X_2X_3, Z_1X_2Z_3, Y_1Y_2, Y_1X_3, Y_2Y_3,$ $X_1Y_3, Y_1X_2Y_3, Y_1Z_2Z_3, X_1Y_2Z_3, Z_1Y_2X_3, Z_1Z_2Y_3$
ε_c	$Z_2, Y_1, Y_3, X_1X_2, X_2X_3, Z_2Z_3, X_1Z_3, Z_1Z_2, Z_1X_3, Z_1Z_2Z_3, X_1Z_2X_3,$ $Y_2Z_3, Z_1Y_2, Y_1Y_2X_3, Y_1X_2Z_3, Y_1Z_2Y_3, X_1Y_2Y_3, Z_1X_2Y_3$
ε_d	$X_1X_3, Z_1Z_3, Z_1X_2, X_2Z_3, X_1Z_2Z_3, Z_1Z_2X_3, Y_1Y_3, Y_1Z_2, Y_2X_3,$ $X_1Y_2, Z_2Y_3, Y_1Y_2Z_3, Y_1X_2X_3, Z_1Y_2Y_3, X_1X_2Y_3,$

Tableau 10b : Groupes d'erreurs de canal sur un, deux ou trois qubits donnant le même secret mesuré et donc la même fidélité.

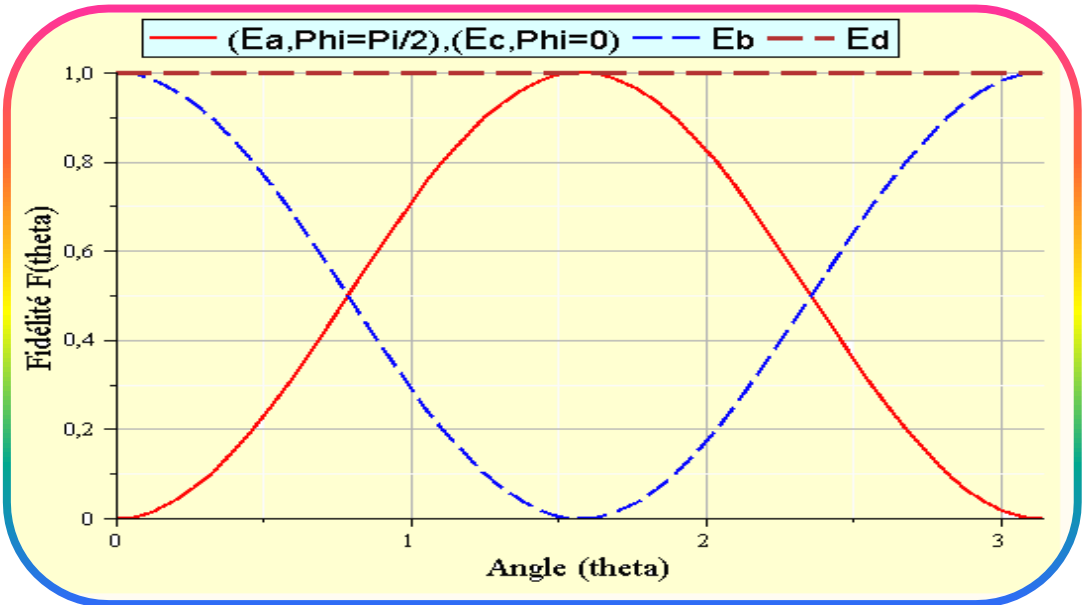

Figure 12 : Fidélité F(θ,ϕ) avec $0 \leq \theta \leq \pi$, $\phi = \pi/2$ pour le groupe d'erreur ε_a et $\phi = 0$ pour le groupe d'erreur ε_c. On note que pour le groupe d'erreur ε_d la fidélité est égale à 1 pour $0 \leq (\theta,\phi) \leq \pi$.

On déduit de la figure 12 que pour les groupe ε_a et ε_c la fidélité est la meilleure (F=1) si le secret envoyé est $|\psi_S\rangle = \frac{\sqrt{2}}{2}(\alpha|0\rangle + \beta|1\rangle)$ et la plus basse (F=0) si $|\psi_S\rangle = |0\rangle$ ou $|1\rangle$ qui sont des bits classiques. La situation est inversée pour le groupe ε_b .

IV.2.4 Rotation $R_x(x)$ et $R_z(x)$ sur les qubits transmis

Les cinq qubits transmis peuvent aussi être affectés par une rotation x autour de l'axe ox ou oz dans la sphère de Bloch. Ces rotations correspondent à des portes quantiques qui déplacent les vecteurs état vers un point donné de la sphère et sont représentées par les matrices :

$$R_x(x) = \begin{pmatrix} \cos\left(\frac{x}{2}\right) & -i\sin\left(\frac{x}{2}\right) \\ -i\sin\left(\frac{x}{2}\right) & \cos\left(\frac{x}{2}\right) \end{pmatrix} \quad ; \quad R_z(x) = \begin{pmatrix} e^{-i\frac{x}{2}} & 0 \\ 0 & -e^{i\frac{x}{2}} \end{pmatrix} \tag{35}$$

Les tableaux 11 donnent l'état de graphe global modifié par les rotations $R_x(x)$ et $R_z(x)$ sur les qubits i=1,2,3 et les tableaux 12 l'état secret du qubit 2 déterminé par la procédure décrite dans la section VI-2-1. Le tableau 13 montre l'expression de la fidélité pour chaque rotation et la figure 13 illustre l'évolution de cette fidélité en fonction de la valeur x de la rotation. On constate que la fidélité moyenne est décroissante pour $0 \le x \le \pi$ et croissante pour $\pi \le x \le 2\pi$. La plus basse fidélité $F_a(x=\pi)=1/3$ correspond à une erreur X ou Z traitée dans la section VI.2.1.

$Error$	$\|\psi_G\rangle$
$Rx_1(x)$	$\left(\frac{1}{2}\right)\{(B_{00})_{13}\|\psi_a^{x_1}\rangle_{245} + (B_{01})_{13}\|\psi_b^{x_1}\rangle_{245}$ $+ (B_{10})_{13}\|\psi_c^{x_1}\rangle_{245} + (B_{11})_{13}\|\psi_d^{x_1}\rangle_{245}\}$
$Rx_2(x)$	$\left(\frac{1}{2}\right)(B_{00})_{13}\left[e^{-ix/2}\alpha\|+\rangle + e^{ix/2}\beta\|-\rangle\right]_2(B_{01})_{45}$ $+\left(\frac{1}{2}\right)(B_{01})_{13}\left[e^{-ix/2}\alpha\|+\rangle - e^{ix/2}\beta\|-\rangle\right]_2(B_{10})_{45}$ $+\left(\frac{1}{2}\right)(B_{10})_{13}\left[e^{ix/2}\alpha\|-\rangle - e^{-ix/2}\beta\|+\rangle\right]_2(B_{00})_{45}$ $+\left(\frac{1}{2}\right)(B_{11})_{13}\left[e^{ix/2}\alpha\|-\rangle + e^{-ix/2}\beta\|+\rangle\right]_2(B_{11})_{45}$
$Rx_3(x)$	$\left(\frac{1}{2}\right)\{(B_{00})_{13}\|\psi_a^{x_3}\rangle_{245} + (B_{01})_{13}\|\psi_b^{x_3}\rangle_{245}$ $+ (B_{10})_{13}\|\psi_c^{x_3}\rangle_{245} + (B_{11})_{13}\|\psi_d^{x_3}\rangle_{245}\}$

Tableau 11a: Etat de graphe perturbé par une rotation $R_{xi}(x)$ sur qubit 1, 2 ou 3.

$\|\psi_a^{x_1}\rangle_{245}$, $\|\psi_a^{x_3}\rangle_{245}$ $\|\psi_b^{x_1}\rangle_{245}$	$-C_1\|111\rangle + C_2\|000\rangle - C_1^*\|100\rangle + C_2^*\|011\rangle$ $C_1\|010\rangle + C_2\|101\rangle - C_1^*\|001\rangle - C_2^*\|110\rangle$
$\|\psi_b^{x_3}\rangle_{245}$ $\|\psi_c^{x_1}\rangle_{245}$, $\|\psi_c^{x_3}\rangle_{245}$ $\|\psi_d^{x_1}\rangle_{245}$ $\|\psi_d^{x_3}\rangle_{245}$	$C_1\|001\rangle + C_2\|110\rangle - C_1^*\|010\rangle - C_2^*\|101\rangle$ $C_1\|000\rangle - C_2\|111\rangle - C_1^*\|011\rangle + C_2^*\|100\rangle$ $-C_1\|101\rangle - C_2\|010\rangle - C_1^*\|110\rangle - C_2^*\|001\rangle$ $C_1\|110\rangle + C_2\|001\rangle + C_1^*\|101\rangle + C_2^*\|010\rangle$
C_1	$(1/4)[(a+b)sin(x/2) + i(a-b)cos(x/2)]$
C_2	$(1/4)[(a-b)sin(x/2) + i(a+b)cos(x/2)]$

Tableau 11b : Termes apparaissant dans le tableau 11a.

$Error$	$\|\psi\rangle$
$Rz_1(x)$	$\left(\frac{1}{2}\right)\{(B_{00})_{13}\|\psi_a^{z_1}\rangle_{245}+(B_{01})_{13}\|\psi_b^{z_1}\rangle_{245}$ $\left(\frac{1}{2}\right)\{(B_{00})_{13}\|\psi_c^{z_1}\rangle_{245}+(B_{01})_{13}\|\psi_d^{z_1}\rangle_{245}$
$Rz_2(x)$	$\left(\frac{1}{2}\right)(B_{00})_{13}[C_a^*\|+\rangle+C_b^*\|-\rangle]_2(B_{01})_{45}$ $+\left(\frac{1}{2}\right)(B_{01})_{13}[C_a\|+\rangle-C_b\|-\rangle]_2(B_{00})_{45}$ $+\left(\frac{1}{2}\right)(B_{10})_{13}[-C_b\|+\rangle+C_a\|-\rangle]_2(B_{00})_{45}$ $+\left(\frac{1}{2}\right)(B_{11})_{34}[C_b^*\|+\rangle+C_a^*\|-\rangle]_2(B_{11})_{45}$
$Rz_3(x)$	$\left(\frac{1}{2}\right)\{(B_{00})_{13}\|\psi_a^{z_3}\rangle_{245}+(B_{01})_{13}\|\psi_b^{z_3}\rangle_{245}$ $\left(\frac{1}{2}\right)\{(B_{00})_{13}\|\psi_c^{z_3}\rangle_{245}+(B_{01})_{13}\|\psi_d^{z_3}\rangle_{245}$

Tableau 11c : L'état de graphe perturbé par une rotation $R_{zi}(x)$ sur qubit i=1,2,3.

$\|\psi_a^{z_1}\rangle_{245}$	$C_3[\|000\rangle-\|011\rangle]-C_4[\|110\rangle+\|101\rangle]+$ $C_5[\|100\rangle-\|111\rangle]+C_6[-\|010\rangle-\|001\rangle]$
$\|\psi_b^{z_1}\rangle_{245}$	$C_3[\|101\rangle+\|110\rangle]+C_4[-\|000\rangle+\|011\rangle]+$ $C_5[\|010\rangle-\|001\rangle]+C_6[-\|100\rangle+\|111\rangle]$
$\|\psi_c^{z_1}\rangle_{245}$	$-C_3[\|100\rangle+\|111\rangle]+C_4[\|001\rangle-\|101\rangle]+$ $C_5[\|000\rangle+\|011\rangle]+C_6[\|110\rangle-\|101\rangle]$
$\|\psi_a^{z_1}\rangle_{245}$	$C_3[\|001\rangle-\|010\rangle]-C_4[\|100\rangle+\|111\rangle]+$ $C_5[\|110\rangle-\|101\rangle]+C_6[\|000\rangle+\|011\rangle]$
C_3, C_5	$(1/4)(a+b)cos(x/2), (1/4)(a-b)cos(x/2)$
C_4, C_6	$(i/4)(a+b)sin(x/2), (i/4)(a-b)sin(x/2)$

Tableau 11d : Termes apparaissant dans le tableau 11c**.**

$Error$	$\left(\left\|\psi_2^E\right\rangle, \rho_2^E\right)$
$Rx_{1,3}(x)$	$\rho_2 = k_{x_1}\|0\rangle\langle 0\| + k_{x_2}\|0\rangle\langle 1\| + k_{x_3}\|1\rangle\langle 0\| + k_{x_4}\|1\rangle\langle 1\|$
$Rx_2(x)$	$\|\psi_2\rangle = e^{\mp ix/2}\alpha\|0\rangle + e^{\pm ix/2}\beta\|1\rangle$
$Rz_{1,2}(x)$	$\rho_2 = k_{z_1}\|0\rangle\langle 0\| + k_{z_2}\|0\rangle\langle 1\| + k_{z_3}\|1\rangle\langle 0\| + k_{z_4}\|1\rangle\langle 1\|$
$Rz_2(x)$	$\|\psi_2\rangle = C_a^{(*)}\|0\rangle + C_b^{(*)}\|1\rangle$

Tableau 12a : L'état secret affecté par une rotation sur les qubits 1,2, 3.

k_{x_1}, k_{z_1}	$a^2cos^2(x/2) + b^2sin^2(x/2)$
k_{x_2}, k_{z_2}	$ab^*cos^2(x/2) - a^*bsin^2(x/2)$
k_{x_3}, k_{z_3}	$a^*bcos^2(x/2) - ab^*sin^2(x/2)$
$k_{x_4}, \ k_{z_4}$	$b^2cos^2(x/2) + a^2sin^2(x/2)$
C_a	$acos(x/2) + ibsin(x/2)$
C_b	$bcos(x/2) + iasin(x/2)$

Tableau 12b : Termes apparaissant dans le tableau 12a**.**

Error	$F(x,\theta,\phi)$	$F_a(x)$
$R_{x_{1,3}}(x)$	$cos^2(\frac{x}{2})[1-\lvert sin\theta sin\phi\rvert^2]+\lvert sin\theta sin\phi\rvert^2$	$\frac{1}{3}[1+2cos^2(\frac{x}{2})]$
$R_{x_2}(x), R_{z_{1,3}}(x)$	$1+sin^2\theta[cos^2(\frac{x}{2})-1]$	$\frac{1}{3}[1+2cos^2(\frac{x}{2})]$
$R_{z_2}(x)$	$cos^2(\frac{x}{2})[1-\lvert sin(\theta)cos\phi\rvert^2]+\lvert sin(\theta)cos\phi\rvert^2$	$\frac{1}{3}[1+2cos^2(\frac{x}{2})]$

Tableau 13 : Fidélité F(x,θ,ϕ) pour chaque rotation $R_x(x)$ et $R_z(x)$ sur qubit "i". On note que la fidélité moyenne $F_a(x)$ est la même pour toutes les rotations.

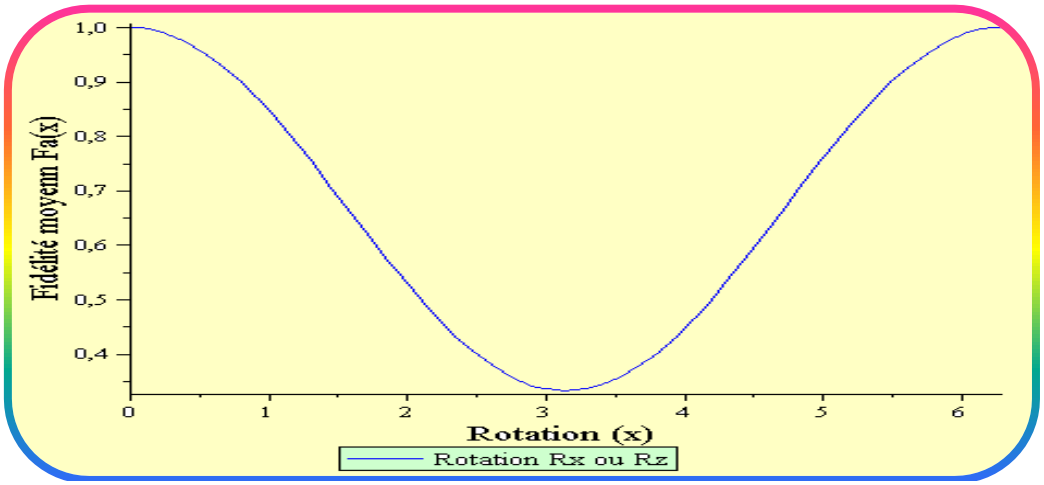

Figure 13 : Evolution de la fidélité moyenne $F_a(x)$ en fonction de la valeur x de la rotation $R_x(x)$ ou $R_z(x)$ sur l'un des qubits 1, 2 ou 3.

IV.2.5 Transmission par canaux dépolarisants

Le canal dépolarisant est un modèle particulier de bruit perturbateur de système quantique. Dans ce processus, la matrice densité globale ρ correcte transmise est remplacée par une densité combinée ρ(P) fonction de la probabilité P qu'une erreur de Pauli $E_{ij} = (\sigma_{1j}=\sigma_{xj}$, $\sigma_{2j}=\sigma_{yj}$ ou $\sigma_{3j}=\sigma_{zj})$ ou perturbe un qubit « j » dans un système à n-qubits. Pour un système à qubit unique la matrice densité perturbée atteignant le récepteur est donnée par l'expression (36a) [1] et pour un système à n qubits elle peut être généralisée par l'expression (36b) :

$$\rho_1(P) = (1-P)\rho + \frac{P}{3}[X\rho X + Y\rho Y + Z\rho Z] \qquad (36a)$$

$$\rho_n(P) = (1-P)^n\rho + \ldots\frac{P^k}{3^k}(1-P)^{n-k}[\sum_{1\le i\le 3}^{1\le j_l\le n}(\Pi_{1\le i\le k}\,\sigma^*_{ij_l})]\rho\,(\Pi_{1\le i\le k}\,\sigma^*_{ij_l}) + \ldots\frac{P^n}{3^n}[\sum_{1\le i\le 3}^{1\le j_l\le n}(\Pi_{1\le i\le k}\,\sigma^*_{ij_l})]\rho\,(\Pi_{1\le i\le k}\,\sigma^*_{ij_l}) \qquad (36b)$$

On remarque que la matrice densité perturbée par le canal dépolarisant est une sommation de termes correspondant chacun à la perturbation du système de qubit par une erreur donnée.

Notons que le premier terme $(1\text{-P})^n\rho$ exprime le cas où tous les qubits atteignent le récepteur sain et sauf. Considérons maintenant le cas où l'état de graphe à cinq qubits contenant le secret est envoyé par l'émetteur à travers cinq canaux dépolarisants. On va supposer que la probabilité P qu'une erreur quelconque perturbe un qubit est la même dans les cinq canaux. On traitera le problème comme si l'émetteur utilise pour envoyer son secret un canal dépolarisant unique exprimé par la relation (36b). On va décrire ici-bas la procédure de calcul de la fidélité moyenne $F_a(P)$ en considérant toutes les erreurs de canal possibles sur qubit 1, 2 et 3. Commençons par écrire la matrice densité du système de cinq qubits perturbés par les canaux dépolarisants et reçus par les cinq joueurs :

$$\rho_{1..5}^{E}(P) = (1-P)^5\rho_{1..5} + \frac{P}{3}(1-P)^4[\rho_{1..5}^{E_1} + \rho_{1..5}^{E_2} + \rho_{1..5}^{E_3} + \rho_{1..5}^{E_4} + \rho_{1..5}^{E_5}] \frac{P^2}{3^2}(1-P)^3[\rho_{1..5}^{E_1E_2} + \rho_{1..5}^{E_1E_3} + \rho_{1..5}^{E_1E_4} + \rho_{1..5}^{E_1E_5} + \rho_{1..5}^{E_2E_3} + \rho_{1..5}^{E_2E_4} + \rho_{1..5}^{E_2E_5} + \rho_{1..5}^{E_3E_4} + \rho_{1..5}^{E_3E_5} + \rho_{1..5}^{E_4E_5}] + \frac{P^3}{3^3}(1-P)^2[\rho_{1..5}^{E_1E_2E_3} + \rho_{1..5}^{E_1E_2E_4} + \rho_{1..5}^{E_1E_2E_5} + \rho_{1..5}^{E_1E_3E_4} + \rho_{1..5}^{E_1E_3E_5} + \rho_{1..5}^{E_1E_4E_5} + \rho_{1..5}^{E_2E_3E_4} + \rho_{1..5}^{E_2E_3E_5} + \rho_{1..5}^{E_2E_4E_5} + \rho_{1..5}^{E_3E_4E_5}] + \frac{P^4}{3^4}(1-P)[\rho_{1..5}^{E_1E_2E_3E_4} + \rho_{1..5}^{E_1E_2E_3E_5} + \rho_{1..5}^{E_1E_2E_4E_5} + \rho_{1..5}^{E_1E_3E_4E_5} + \rho_{1..5}^{E_2E_3E_4E_5}] + \frac{P^5}{3^5}\rho_{1..5}^{E_1E_2E_3E_4E_5} \quad (37)$$

Dans cette expression $\rho_{1..5}^{E_i}$ est la matrice densité du système infectée par une erreur de Pauli sur un seul qubit « i » :

$$\rho_{1..5}^{E_i} = X_i\rho_{1..5}X_i + Y_i\rho_{1..5}Y_i + Z_i\rho_{1..5}Z_i \quad (38)$$

Les symboles $\rho_{1..5}^{E_iE_j}$, $\rho_{1..5}^{E_iE_jE_j}$, $\rho_{1..5}^{E_iE_jE_kE_l}$, et $\rho_{1..5}^{E_iE_jE_kE_lE_m}$ sont des sommations de 8, 27, 81 et 243 termes et représentent la matrice densité affectée par des erreurs sur deux, trois, quatre et cinq qubits respectivement. Après mesure sur les états de Bell des qubits (1,3) on obtient la matrice densité du système de qubits (2,4,5) :

$$\rho_{245}^{E}(P) = (1-P)^5\rho_{245} + \frac{P}{3}(1-P)^4[\rho_{245}^{E_1} + \rho_{245}^{E_2} + \rho_{245}^{E_3} + \rho_{245}^{E_4} + \rho_{245}^{E_5}] + \frac{P^2}{3^2}(1-P)^3[\rho_{245}^{E_1E_2} + \rho_{245}^{E_1E_3} + \rho_{245}^{E_1E_4} + \rho_{245}^{E_1E_5} + \rho_{245}^{E_2E_3} + \rho_{245}^{E_2E_4} + \rho_{245}^{E_2E_5} + \rho_{245}^{E_3E_4} + \rho_{245}^{E_3E_5} + \rho_{245}^{E_4E_5}] + \frac{P^3}{3^3}(1-P)^2[\rho_{245}^{E_1E_2E_3} + \rho_{245}^{E_1E_2E_4} + \rho_{245}^{E_1E_2E_5} + \rho_{245}^{E_1E_3E_4} + \rho_{245}^{E_1E_3E_5} + \rho_{245}^{E_1E_4E_5} + \rho_{245}^{E_2E_3E_4} + \rho_{245}^{E_2E_3E_5} + \rho_{245}^{E_2E_4E_5} + \rho_{245}^{E_3E_4E_5}] + \frac{P^4}{3^4}(1-P)[\rho_{245}^{E_1E_2E_3E_4} + \rho_{245}^{E_1E_2E_3E_5} + \rho_{245}^{E_1E_2E_4E_5} + \rho_{1..5}^{E_1E_3E_4E_5} + \rho_{245}^{E_2E_3E_4E_5}] + \frac{P^5}{3^5}\rho_{245}^{E_1E_2E_3E_4E_5} \quad (39a)$$

Avec $\rho_{245} = (\rho_a)_{245}, (\rho_b)_{245}, (\rho_c)_{245}$ ou $(\rho_d)_{245}$ et
$\rho_{245}^{E} = (\rho_a^{E})_{245}, (\rho_b^{E})_{245}, (\rho_c^{E})_{245}$ ou $(\rho_d^{E})_{245}$

Après traçage partielle sur qubits (4,5) et multiplication par la porte R_G , on obtient la matrice densité de qubit 2 mesurée par le joueur 2 :

$$\rho_2^E(P) = (1-P)^5\rho_2 + \frac{P}{3}(1-P)^4\left[\rho_2^{E_1} + \rho_2^{E_2} + \rho_2^{E_3} + \rho_2^{E_4} + \rho_2^{E_5}\right] + \frac{P^2}{3^2}(1-P)^3\left[\rho_2^{E_1E_2} + \rho_2^{E_1E_3} + \rho_2^{E_1E_4} + \rho_2^{E_1E_5} + \rho_2^{E_2E_3} + \rho_2^{E_2E_4} + \rho_2^{E_2E_5} + \rho_2^{E_3E_4} + \rho_2^{E_3E_5} + \rho_2^{E_4E_5}\right] + \frac{P^3}{3^3}(1-P)^2\left[\rho_2^{E_1E_2E_3} + \rho_2^{E_1E_2E_4} + \rho_2^{E_1E_2E_5} + \rho_2^{E_1E_3E_4} + \rho_2^{E_1E_3E_5} + \rho_2^{E_1E_4E_5} + \rho_2^{E_2E_3E_4} + \rho_2^{E_2E_3E_5} + \rho_2^{E_2E_4E_5} + \rho_2^{E_3E_4E_5}\right] + \frac{P^4}{3^4}(1-P)\left[\rho_2^{E_1E_2E_3E_4} + \rho_2^{E_1E_2E_3E_5} + \rho_2^{E_1E_2E_4E_5} + \rho_2^{E_1E_3E_4E_5} + \rho_2^{E_2E_3E_4E_5}\right] + \frac{P^5}{3^5}\rho_2^{E_1E_2E_3E_4E_5} \quad (39b)$$

Avec $\rho_2 = |\psi_s\rangle\langle\psi_s|$ le secret envoyé et $\rho_2^E = (\rho_a^E)_2, (\rho_b^E)_2, (\rho_c^E)_2$ ou $(\rho_d^E)_2$ est le secret perturbé par l'erreur E = E_i , E_i E_j , E_i E_j E_k, E_i E_j $E_k$$E_l$

On multiplie par $|\psi_s\rangle$ et on intègre sur (θ,ϕ) pour obtenir la fidélité :

$$\langle\psi_S|\rho_2^E|\psi_S\rangle = (1-P)^5\rho_2 + \frac{P}{3}(1-P)^4\left[F_a^{E_1} + F_a^{E_2} + F_a^{E_3} + F_a^{E_4} + F_a^{E_5}\right] + \frac{P^2}{3^2}(1-P)^3\left[F_a^{E_1E_2} + F_a^{E_1E_3} + F_a^{E_1E_4} + F_a^{E_1E_5} + F_a^{E_2E_3} + F_a^{E_2E_4} + F_a^{E_2E_5} + F_a^{E_3E_4} + F_a^{E_3E_5} + F_a^{E_4E_5}\right] + \frac{P^3}{3^3}(1-P)^2\left[F_a^{E_1E_2E_3} + F_a^{E_1E_2E_4} + F_a^{E_1E_2E_5} + F_a^{E_1E_3E_4} + F_a^{E_1E_3E_5} + F_a^{E_1E_4E_5} + F_a^{E_2E_3E_4} + F_a^{E_2E_3E_5} + F_a^{E_2E_4E_5} + F_a^{E_3E_4E_5}\right] + \frac{P^4}{3^4}(1-P)\left[F_a^{E_1E_2E_3E_4} + F_a^{E_1E_2E_3E_5} + F_a^{E_1E_2E_4E_5} + F_a^{E_2E_3E_4E_5}\right] + \frac{P^5}{3^5}F_a^{E_1E_2E_3E_4} \quad (40)$$

On peut écrire (40) comme :

$$F_a(p) = \langle\psi_S|\rho_2^E\left|\psi_S\right\rangle = (1-P)^5 + \frac{P}{3}(1-P)^4\,[A] + \frac{P^2}{3^2}(1-P)^3\,[B] + \frac{P^3}{3^3}(1-P)^2[C] + \frac{P^4}{3^4}(1-P)\,[D] + \frac{P^5}{3^5}\,[E] \quad (41)$$

On déduit des tableaux 10a et 10b les valeurs F_a^E contenues dans le tableau 14 et donc les valeurs des facteurs A, B, C, D et E dans (41).

$F_a^{E_1}, F_a^{E_2}, F_a^{E_3}$	$(3\times\frac{1}{3}) = 1$
$F_a^{E_4}, F_a^{E_5}$	$(3\times 1) = 3$
$F_a^{E_1E_2}, F_a^{E_1E_3}, F_a^{E_2E_3}$	$(6\times\frac{1}{3}) + (3\times 1) = 5$
$F_a^{E_1E_4}, F_a^{E_1E_5}, F_a^{E_2E_4}, F_a^{E_2E_5}, F_a^{E_3E_4}, F_a^{E_3E_5}$	$(9\times\frac{1}{3}) = 3$
$F_a^{E_4E_5}$	$(9\times 1) = 9$
$F_a^{E_1E_2E_3}$	$(21\times\frac{1}{3}) + (6\times 1) = 13$
$F_a^{E_1E_2E_4}, F_a^{E_1E_3E_4}, F_a^{E_2E_3E_4}, F_a^{E_1E_2E_5}, F_a^{E_1E_3E_5}, F_a^{E_2E_3E_5}$	$[(6\times 3)\times\frac{1}{3}] + [(3\times 3)\times 1] = 15$
$F_a^{E_1E_4E_5}, F_a^{E_2E_4E_5}, F_a^{E_3E_4E_5}$	$(3\times 9)\times\frac{1}{3} = 9$
$F_a^{E_1E_2E_3E_4}, F_a^{E_1E_2E_3E_5}$	$[(21\times 3)\times\frac{1}{3}] + [(6\times 3)\times 1] = 39$
$F_a^{E_1E_2E_4E_5}, F_a^{E_1E_3E_4E_5}, F_a^{E_2E_3E_4E_5}$	$(6\times 9)\times\frac{1}{3} + (3\times 9)\times 1 = 45$
$F_a^{E_1E_2E_3E_4E_5}$	$(21\times 9)\times\frac{1}{3} + (6\times 9)\times 1 = 117$

Tableau 14 : Valeurs des termes F_a^E dans l'expression (40) pour les erreurs E possibles sur les cinq qubits envoyés.

Le calcul donne : A=9 , B=42 , C=130 , D=213 , E=117 (42)

L'expression (41) devient alors :

$$F_a(p) = (1\text{-}P)^5+3P(1\text{-}P)^4+\frac{14}{3}P^2(1\text{-}P)^3+\frac{130}{27}P^3(1\text{-}P)^2+\frac{71}{27}P^4(1\text{-}P)+\frac{13}{27}P^5 \quad (43)$$

Enfin l'expression finale de la fidélité :

$$F_a(p) = 1 - 2P + \frac{8}{3}P^2 - \frac{32}{27}P^3 \quad (44)$$

IV.2.6 Protection par le code à cinq qubits

On va décrire la protection des qubits transportant le secret par le code à cinq qubits. Ce code décrit dans [15] utilise cinq qubits pour protéger l'un d'eux qui se trouve dans un état superposé. Ainsi, si une erreur X, Y ou Z affecte l'un des cinq qubits (le qubit à protéger et quatre ancillas) envoyés dans un canal donné, alors le code corrige cette erreur et permet donc au récepteur d'accéder à l'état correct du qubit protégé. Cependant, si deux qubits ou plus parmi les cinq envoyés dans un canal donné sont atteints d'erreur lors de la transmission, alors le code permet d'accéder à un état protégé qui peut être entaché d'erreur donnant une fidélité inférieure à 1.

IV.2.6.1 Erreur sur deux qubits dans chaque canal bruité

L'emetteur protège chacun des qubits (1,2,3) avec quatre ancillas comme illustré sur la figure 14 et les envoie à travers trois canaux bruités qui introduisent des erreurs X, Y ou Z avec une probabilité P=1.

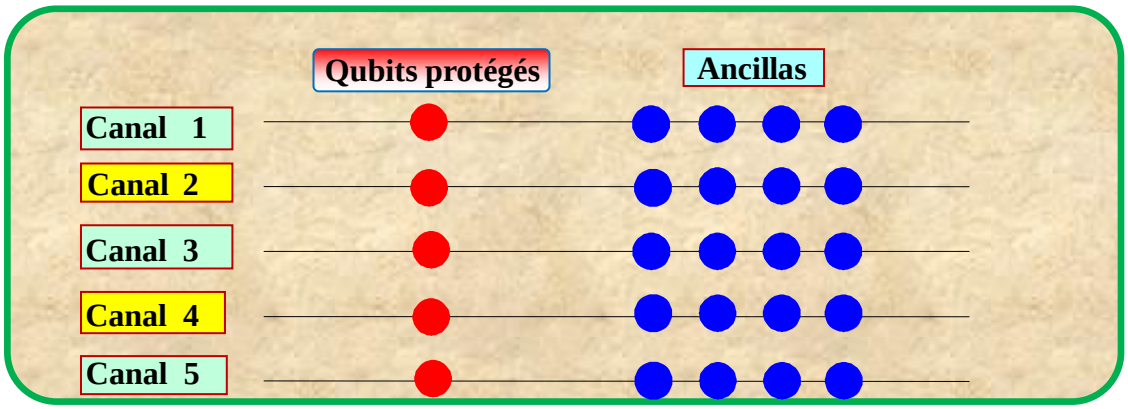

Figure 14 : Protection par le code à cinq qubits.

On note qu'en général l'emetteur protège les cinq canaux de transmission car il ignore lesquels des cinq joueurs accéderont au secret. Nous allons voir ici-bas l'effet du code sur l'état de graphe $|\Psi_G\rangle$ de l'équation (20) qui peut être écrit comme suit :

$$|\Psi_G\rangle = \left(\frac{\sqrt{2}}{8}\right)\{[\alpha|0\rangle + \beta|1\rangle]_i|\psi_a\rangle_{jklm} + [\alpha|0\rangle - \beta|1\rangle]_i|\psi_b\rangle_{jklm} + [\beta|0\rangle + \alpha|1\rangle]_i|\psi_c\rangle_{jklm} + [\beta|0\rangle - \alpha|1\rangle]_i|\psi_d\rangle_{jklm}] \quad (45)$$

[i=1, (j,k,l,m)=(2,3,4,5)] ; [i=2, (j,k,l,m)=(1,3,4,5)] ; [i=3,(j,k,l,m)=(1,2,4,5)] (46)

Les états $|\psi_a\rangle_{jklm}$, $|\psi_b\rangle_{jklm}$, $|\psi_c\rangle_{jklm}$ et $|\psi_d\rangle_{jklm}$ ont différentes expressions selon la valeur de 'i'. On supposera que l'émetteur sait que les joueurs (1,2,3) vont collaborer pour accéder au secret. Par suite, les qubits envoyés aux joueurs (4,5) ne seront pas protégés car les erreurs les affectant n'ont pas d'incidence sur le secret recueilli. L'émetteur rajoute quatre ancillas à l'état $|0\rangle$ dans chacun des canaux 1, 2 et 3 et applique le circuit de codage du code à cinq qubits simulé dans l'annexe G. On obtient l'état de graphe codé $|\Psi_{G_1}\rangle$ envoyér où $|0_l\rangle$ et $|1_l\rangle$ sont les qubits logiques donnés dans [1] et l'annexe G :

$$|\Psi_{G_1}\rangle = \left(\frac{\sqrt{2}}{8}\right)\{[\alpha|0_l\rangle + \beta|1_l\rangle]_i|\psi_a\rangle_{jklm} + [\alpha|0_l\rangle - \beta|1_l\rangle]_i|\psi_b\rangle_{jklm} + [\beta|0_l\rangle + \alpha|1_l\rangle]_i|\psi_c\rangle_{jklm} + [\beta|0_l\rangle - \alpha|1_l\rangle]_i|\psi_d\rangle_{jklm}] \quad (47)$$

Après mesure des syndromes, correction et décodage, les joueurs (1,2,3) suppriment les ancillas. Si un des qubit 'i=1,2 ou 3' est infecté par une erreur $E_i = X_i$, Y_i ou Z_i alors l'état de graphe devient :

$$|\Psi_G^{E_i}\rangle = \left(\frac{\sqrt{2}}{8}\right)\{E_i[\alpha|0\rangle + \beta|1\rangle]_i|\psi_a\rangle_{jklm} + E_i[\alpha|0\rangle - \beta|1\rangle]_i|\psi_b\rangle_{jklm} + E_i[\beta|0\rangle + \alpha|1\rangle]_i|\psi_c\rangle_{jklm} + E_i[\beta|0\rangle - \alpha|1\rangle]_i|\psi_d\rangle_{jklm}] \quad (48)$$

Le tableau 15 donne les syndromes S des erreurs sur un et deux qubits que nous avons déterminés pour le code à cinq qubits. Une erreur double est corrigée comme une erreur simple ayant le même syndrome. La dernière colonne donne l'erreur E_i affectant le qubit à protéger 'i' après décodage obtenue par le programme Feynman.

$Error$	S	E_i
$X_i, (Z_{a_2}Z_{a_3}), (X_{a_3}Z_{a_4}, Z_{a_1}X_{a_2})$	0101	$I_i, (X_i), (Z_i)$
$X_{a_1}, (Z_{a_3}Z_{a_4}), (Z_iX_{a_4}, Z_{a_2}X_{a_3})$	0010	$I_i, (X_i), (Z_i)$
$X_{a_2}, (Z_iZ_{a_4}), (X_iZ_{a_1}, Z_{a_3}X_{a_4})$	1001	$I_i, (X_i), (Z_i)$
$X_{a_3}, (Z_iZ_{a_1}), (X_iZ_{a_4}, X_{a_1}Z_{a_2})$	0100	$I_i, (X_i), (Z_i)$
$X_{a_4}, (Z_{a_1}Z_{a_2}), (X_{a_2}Z_{a_3}, Z_iX_{a_1})$	1010	$I_i, (X_i), (Z_i)$
$Z_i, (X_{a_1}X_{a_4}), (X_{a_2}Z_{a_4}, Z_{a_1}X_{a_3})$	1000	$I_i, (X_i), (Z_i)$
$Z_{a_1}, (X_iX_{a_2}), (Z_iX_{a_3}, Z_{a_2}X_{a_4})$	1100	$I_i, (X_i), (Z_i)$
$Z_{a_2}, (X_{a_1}X_{a_3}), (X_iZ_{a_3}, Z_{a_1}X_{a_4})$	0110	$I_i, (X_i), (Z_i)$
$Z_{a_3}, (X_{a_2}X_{a_4}), (X_iZ_{a_2}, X_{a_1}Z_{a_4})$	0011	$I_i, (X_i), (Z_i)$
$Z_{a_4}, (X_iX_{a_3}), (X_{a_1}Z_{a_3}, Z_iX_{a_2})$	0001	$I_i, (X_i), (Z_i)$
$Y_i, (X_{a_2}X_{a_3}, Z_{a_1}Z_{a_4})$	1101	$I_i, (Y_i)$
$Y_{a_1}, (X_{a_3}X_{a_4}, Z_iZ_{a_2})$	1110	$I_i, (Y_i)$
$Y_{a_2}, (X_iX_{a_4}, Z_{a_1}Z_{a_3})$	1111	$I_i, (Y_i)$
$Y_{a_3}, (X_iX_{a_1}, Z_{a_2}Z_{a_4})$	0111	$I_i, (Y_i)$
$Y_{a_4}, (X_{a_1}X_{a_2}, Z_iZ_{a_3})$	1011	$I_i, (Y_i)$

Tableau 15 : Erreur E_i sur le qubit 'i' à protéger par le code à cinq qubits en fonction des erreurs de canal avec a_j le "j^{eme}" ancilla avec j=1,2,3,4.

IV.2.6.2 Double erreur dans chaque canal dépolarisant

On considère ici trois double erreurs E_kE_l, E_mE_n et E_oE_p se produisant respectivement dans les canaux 1, 2 et 3 sur six qubits quelconques (k,l,m,n,o,p) et corrigées comme les trois erreurs simples ayant le même syndrome. Les qubits (4,5) ne sont pas protégés et peuvent donc être infectés par une erreur X, Y ou Z. Si la probabilité qu'une erreur de canal perturbe un qubit est égale à P, alors la matrice densité du système de cinq qubits reçus par les joueurs est :

$$\rho^{E}_{(123a)(45)} = (1-P)^8\rho_{(123a)(45)} + \frac{P}{3}(1-P)^7\left[\Sigma\rho^{E_x}_{(123a)(45)}\right] + \frac{P^2}{3^2}(1-P)^6 [\Sigma\rho^{E_xE_y}_{(123a)(45)}] + \frac{P^3}{3^3}(1-P)^5\left[\Sigma\rho^{E_xE_yE_z}_{(123a)(45)}\right] + \frac{P^4}{3^4}(1-P)^4\left[\Sigma\rho^{E_xE_yE_zE_u}_{(123a)(45)}\right] + \frac{P^5}{3^5}(1-P)^3\left[\Sigma\rho^{E_xE_yE_zE_uE_v}_{(123a)(45)}\right] + \frac{P^6}{3^6}(1-P)^2\left[\Sigma\rho^{E_xE_yE_zE_uE_vE_w}_{(123a)(45)}\right] + \frac{P^7}{3^7}(1-P)\left[\Sigma\rho^{E_xE_yE_zE_uE_vE_wE_4}_{(123a)(45)}\right] + \frac{P^8}{3^8}\left[\Sigma\rho^{E_kE_lE_mE_nE_oE_pE_4E_5}_{(123a)(45)}\right] \quad (49a)$$

La notation (123a) représente les qubits 1, 2 et 3 protégés par les ancillas. La sommation concernant une erreur simple E_x est donnée par :

$$\Sigma\rho^{E_x}_{(123a)(45)} = \rho^{E_k}_{(123a)(45)} + \rho^{E_l}_{(123a)(45)} + \rho^{E_m}_{(123a)(45)} + \rho^{E_n}_{(123a)(45)} + \rho^{E_o}_{(123a)(45)} + \rho^{E_p}_{(123a)(45)} + \rho^{E_4}_{(123a)(45)} + \rho^{E_5}_{(123a)(45)} \quad (49b)$$

Avec

$$\rho^{E_k}_{(123a)(45)} = \rho^{E_x}_{(123a)(45)} + \rho^{E_y}_{(123a)(45)} + \rho^{E_z}_{(123a)(45)}$$

$$\rho^{X_k}_{(123a)(45)} = X_k^*\,\rho_{(123a)(45)}X_k \quad (49c)$$

Les sommations $\Sigma\rho^{E_x}_{(123a)(45)}$, $\Sigma\rho^{E_xE_y}_{(123a)(45)}$, $\Sigma\rho^{E_xE_yE_z}_{(123a)(45)}$, $\Sigma\rho^{E_xE_yE_zE_u}_{(123a)(45)}$, $\Sigma\rho^{E_xE_yE_zE_uE_v}_{(123a)(45)}$ $\Sigma\rho^{E_xE_yE_zE_uE_vE_w}_{(123a)(45)}$ et $\rho^{E_xE_yE_zE_uE_vE_wE_4}_{(123a)(45)}$ sont la somme respectivement de 8X3, $28X3^2$, $56X3^3$, $70X3^4$, $56X3^5$, $28X3^6$ et $8X3^7$ termes. L'expression $\Sigma\rho^{E_kE_lE_mE_nE_oE_pE_4E_5}_{(123a)(45)}$ est la sommation de 3^8 termes. Après décodage et suppression des ancillas, on utilise le tableau 15 pour obtenir à partir le l'expression (49a) l'état de graphe perturbé reçu par les cinq joueurs :

$$\rho^{E}_{1..5} = [(1-P)^8 + 18\frac{P}{3}(1-P)^7 + 108\frac{P^2}{9}(1-P)^6 + 216\frac{P^3}{27}(1-P)^5]\rho_{1..5} + \left[3\frac{P^2}{9}(1-P)^6 + 36\frac{P^3}{27}(1-P)^5 + 108\frac{P^4}{81}(1-P)^4\right][\rho^{E_1}_{1..5} + \rho^{E_2}_{1..5} + \rho^{E_3}_{1..5}] [9\frac{P^4}{81}(1-P)^4 + 54\frac{P^3}{243}(1-P)^3][\rho^{E_1E_2}_{1..5} + \rho^{E_1E_3}_{1..5} + \rho^{E_2E_3}_{1..5}] + [\frac{P^6}{27}(1-P)^2][\rho^{E_1E_2E_3}_{1..5}] + [\frac{P}{3}(1-P)^7 + 18\frac{P^2}{9}(1-P)^6 + 108\frac{P^3}{27}(1-P)^5 + 216\frac{P^4}{81}(1-P)^4][\rho^{E_4}_{1..5} + \rho^{E_5}_{1..5}] + [\frac{P^2}{9}(1-P)^6 + 18\frac{P^3}{27}(1-P)^5 + 108\frac{P^4}{81}(1-P)^4 + 216\frac{P^5}{243}(1-P)^3][\rho^{E_4E_5}_{1..5}] + [3\frac{P^3}{27}(1-P)^5 + 36\frac{P^4}{81}(1-P)^4 + 108\frac{P^5}{243}(1-P)^3][\rho^{E_1E_4}_{1..5} + \rho^{E_1E_5}_{1..5} + \rho^{E_2E_4}_{1..5} + \rho^{E_2E_5}_{1..5} + \rho^{E_3E_4}_{1..5} + \rho^{E_3E_5}_{1..5}] + [3\frac{P^4}{81}(1-P)^4 + 36\frac{P^5}{243}(1-P)^3 + 108\frac{P^6}{3^6}(1-P)^3] [\rho^{E_1E_4E_5}_{1..5} + \rho^{E_2E_4E_5}_{1..5} + \rho^{E_3E_4E_5}_{1..5}] + [9\frac{P^5}{243}(1-P)^3 + 54\frac{P^6}{3^6}(1-P)^2][\rho^{E_1E_2E_4}_{1..5} + \rho^{E_1E_2E_5}_{1..5} + \rho^{E_1E_3E_4}_{1..5} + \rho^{E_1E_3E_5}_{1..5} + \rho^{E_2E_3E_4}_{1..5} + \rho^{E_2E_3E_5}_{1..5}] + [9\frac{P^6}{3^6}(1-P)^2 + 54\frac{P^7}{3^7}(1-P)]$$

$$\left[\rho_{1..5}^{E_1E_2E_4E_5} + \rho_{1..5}^{E_1E_3E_4E_5} + \rho_{1..5}^{E_2E_3E_4E_5}\right] + \left[27\frac{P^7}{3^7}(1-P)\right]\left[\rho_{1..5}^{E_1E_2E_3E_4} + \rho_{1..5}^{E_1E_2E_3E_5}\right] + 27\frac{P^8}{3^8}\left[\rho_{1..5}^{E_1E_2E_3E_4E_5}\right] \quad (50)$$

Après mesure sur les états de Bell des qubits (1,3), traçage partiel sur les qubits (4,5), multiplication par la porte de recouvrement R_G et l'état secret $|\Psi_s\rangle$ et intégration sur les angles, on obtient la fidélité moyenne en fonction de P :

$$F_a(P) = \left[(1-P)^8 + 18\frac{P}{3}(1-P)^7 + 108\frac{P^2}{9}(1-P)^6 + 216\frac{P^3}{27}(1-P)^5 + 3\frac{P^2}{9}(1-P)^6 + 36\frac{P^3}{27}(1-P)^5 + 108\frac{P^4}{81}(1-P)^4\right] + \left[9\frac{P^4}{81}(1-P)^4 + 54\frac{P^3}{243}(1-P)^3\right]\left[F_a^{E_1E_2} + F_a^{E_1E_3} + F_a^{E_2E_3}\right] + \left[\frac{P^6}{27}(1-P)^2\right]\left[F_a^{E_1E_2E_3}\right] + \left[\frac{P}{3}(1-P)^7 + 18\frac{P^2}{9}(1-P)^6 + 108\frac{P^3}{27}(1-P)^5 + 216\frac{P^4}{81}(1-P)^4\right]\left[F_a^{E_4} + F_a^{E_5}\right] + \left[\frac{P^2}{9}(1-P)^6 + 18\frac{P^3}{27}(1-P)^5 + 108\frac{P^4}{81}(1-P)^4 + 216\frac{P^5}{243}(1-P)^3\right]\left[F_a^{E_4E_5}\right] + \left[3\frac{P^3}{27}(1-P)^5 + 36\frac{P^4}{81}(1-P)^4 + 108\frac{P^5}{243}(1-P)^3\right]\left[F_a^{E_1E_4} + F_a^{E_1E_5} + F_a^{E_2E_4} + F_a^{E_2E_5} + F_a^{E_3E_4} + F_a^{E_3E_5}\right] + \left[3\frac{P^4}{81}(1-P)^4 + 36\frac{P^5}{243}(1-P)^3 + 108\frac{P^6}{3^6}(1-P)^3\right]\left[F_a^{E_1E_4E_5} + F_a^{E_2E_4E_5} + F_a^{E_3E_4E_5}\right] + \left[9\frac{P^5}{243}(1-P)^3 + 54\frac{P^6}{3^6}(1-P)^2\right]\left[F_a^{E_1E_2E_4} + F_a^{E_1E_2E_5} + F_a^{E_1E_3E_4} + F_a^{E_1E_3E_5} + F_a^{E_2E_3E_4} + F_a^{E_2E_3E_5}\right] + \left[9\frac{P^6}{3^6}(1-P)^2 + 54\frac{P^7}{3^7}(1-P)\right]\left[F_a^{E_1E_2E_4E_5} + F_a^{E_1E_3E_4E_5}\right] + \left[F_a^{E_2E_3E_4E_5}\right] + 27\frac{P^7}{3^7}(1-P)\left[F_a^{E_1E_2E_3E_4} + F_a^{E_1E_2E_3E_5}\right] + 27\frac{P^8}{3^8}\left[F_a^{E_1E_2E_3E_4E_5}\right] \quad (51)$$

On substitue dans (51) les valeurs du tableau 14 on obtient :

$$F_a(P) = \left[(1-P)^8 + 18\frac{P}{3}(1-P)^7 + 108\frac{P^2}{9}(1-P)^6 + 216\frac{P^3}{27}(1-P)^5 + 3\frac{P^2}{9}(1-P)^6 + 36\frac{P^3}{27}(1-P)^5 + 108\frac{P^4}{81}(1-P)^4\right][3] + \left[9\frac{P^4}{81}(1-P)^4 + 54\frac{P^3}{243}(1-P)^3\right][15] + \left[\frac{P^6}{27}(1-P)^2\right][13] + \left[\frac{P}{3}(1-P)^7 + 18\frac{P^2}{9}(1-P)^6 + 108\frac{P^3}{27}(1-P)^5 + 216\frac{P^4}{81}(1-P)^4\right][6] + \left[\frac{P^2}{9}(1-P)^6 + 18\frac{P^3}{27}(1-P)^5 + 108\frac{P^4}{81}(1-P)^4 + 216\frac{P^5}{243}(1-P)^3\right][9] + \left[3\frac{P^3}{27}(1-P)^5 + 36\frac{P^4}{81}(1-P)^4 + 108\frac{P^5}{243}(1-P)^3\right][18] + \left[3\frac{P^4}{81}(1-P)^4 + 36\frac{P^5}{243}(1-P)^3 + 108\frac{P^6}{3^6}(1-P)^3\right][27] + \left[9\frac{P^5}{243}(1-P)^3 + 54\frac{P^6}{3^6}(1-P)^2\right][90] + \left[9\frac{P^6}{3^6}(1-P)^2 + 54\frac{P^7}{3^7}(1-P)\right][135] + 27\frac{P^7}{3^7}(1-P)\left[78\right] + 27\frac{P^8}{3^8}[117] \quad (52)$$

Le calcul donne finalement :

$$F_a(P) = (1-P)^8 + 8P(1-P)^7 + 26P^2(1-P)^6 + 44P^3(1-P)^5 + \frac{128}{3}P^4(1-P)^4 + \frac{80}{3}P^5(1-P)^3 + \frac{346}{27}P^6(1-P)^2 + \frac{116}{27}P^7(1-P) + \frac{13}{27}P^8 \quad (53)$$

IV.2.7 Protection par le code de Steane à sept qubits

Ce code décrit dans [16][17] utilise sept qubits pour protéger l'un d'entre eux en état superposé contre une erreur X, Y ou Z. Les tableaux 16 montrent pour chaque erreur de canal simple ou double, l'erreurs E_i affectant le qubit protégé après correction que nous avons déterminés à l'aide du programme Feynman.

E	S	E_i	E	S	E_i
$X_1, (X_2X_3, X_4X_5, X_6X_7)$	000001	$I_i, (X_i)$	Y_1	001001	I_i
$X_2, (X_1X_3, X_4X_6, X_5X_7)$	000010	$I_i, (X_i)$	Y_2	010010	I_i
$X_3, (X_1X_2, X_5X_6, X_4X_7)$	000011	$I_i, (X_i)$	Y_3	011011	I_i
$X_4, (X_1X_5, X_2X_6, X_3X_7)$	000100	$I_i, (X_i)$	Y_4	100100	I_i
$X_5, (X_1X_4, X_2X_7, X_3X_6)$	000101	$I_i, (X_i)$	Y_5	101101	I_i
$X_6, (X_1X_7, X_2X_4, X_3X_5)$	000110	$I_i, (X_i)$	Y_6	110110	I_i
$X_7, (X_1X_6, X_2X_5, X_3X_4)$	000111	$I_i, (X_i)$	Y_7	111111	I_i

Tableau 16a : Erreurs de canal simples et doubles E ayant même syndrome S et l'erreur associée E_i sur le qubit protégé après correction par un opérateur X_k, Y_k ou Z_k (k=1 ,...,7).

$Errors$	S	E_i
$Z_1, (Z_6Z_7, Z_2Z_3, Z_4Z_5)$	001000	$I_i, (Z_i)$
$Z_2, (Z_1Z_3, Z_4Z_6, Z_5Z_7)$	010000	$I_i, (Z_i)$
$Z_3, (Z_4Z_7, Z_1Z_2, Z_5Z_6)$	011000	$I_i, (Z_i)$
$Z_4, (Z_3Z_7, Z_1Z_5, Z_2Z_6)$	100000	$I_i, (Z_i)$
$Z_5, (Z_2Z_7, Z_1Z_4, Z_3Z_6)$	101000	$I_i, (Z_i)$
$Z_6, (Z_1Z_7, Z_2Z_4, Z_3Z_5)$	110000	$I_i, (Z_i)$
$Z_7, (Z_1Z_6, Z_2Z_5, Z_3Z_4)$	111000	$I_i, (Z_i)$

Tableau 16b : Erreurs de canal simples et doubles E ayant même syndrome S et l'erreur associée E_i sur le qubit protégé après correction par un opérateur Z_k.

$Errors$	S	$Errors$	S	$Errors$	S
X_1Z_4	100001	Z_1X_4	001100	Z_1X_3	001011
X_1Z_5	101001	Z_2X_4	010100	X_1Z_2	010001
X_1Z_6	110001	Z_3X_4	011100	X_1Z_3	011001
X_1Z_7	111001	Z_1X_5	001101	X_2Z_1	001010
X_2Z_7	111010	Z_2X_5	010101	X_2Z_3	011010
X_3Z_4	100011	Z_1X_6	001110	X_2Z_4	100010
X_3Z_6	110011	Z_2X_6	010110	X_2Z_5	101010
X_3Z_7	111011	Z_3X_6	011110	X_2Z_6	110010
X_4Z_7	111100	Z_1X_7	001111	Z_2X_3	010011
X_5Z_7	111101	Z_2X_7	010111	X_4Z_5	101100
X_6Z_5	101110	Z_3X_7	011111	X_4Z_6	110100
X_6Z_7	111110	Z_4X_5	100101	Z_4X_6	100110
X_5Z_6	110101	Z_3X_5	011101	X_3Z_5	101011

Tableau 16c : Erreurs de canal doubles laissant le qubit protégé non perturbé.

IV.2.8 Protection par le code de Shor à neuf qubits

Ce code décrit dans **[1]** utilise neuf qubits pour protéger l'un d'entre eux en état superposé contre une erreur X, Y ou Z. Les tableaux 15 montrent pour chaque erreur de canal simple ou double, l'erreurs E_i affectant le qubit protégé après correction que nous avons déterminés à l'aide du programme Feynman.

E	S	E_i
X_1, X_2X_3	10000000	I_i, Z_i
X_2, X_1X_3	11000000	I_i, Z_i
X_3, X_1X_2	01000000	I_i, Z_i
X_4, X_5X_6	00100000	I_i, Z_i
X_5, X_4X_6	00110000	I_i, Z_i
X_6, X_4X_5	00010000	I_i, Z_i
X_7, X_8X_9	00001000	I_i, Z_i
X_8, X_7X_9	00001100	I_i, Z_i
X_9, X_7X_8	00000100	I_i, Z_i

Tableau 17a : Erreurs de canal simples et doubles E ayant même syndrome S et l'erreur associée E_i sur le qubit protégé après correction par un opérateur X_k.

E	S	E_i
$Y_1, X_1Z_{2,3}$	10000010	I_i
$Y_2, X_2Z_{1,3}$	11000010	I_i
$Y_3, X_3Z_{1,2}$	01000010	I_i
$Y_4, X_4Z_{5,6}$	00100011	I_i
$Y_5, X_5Z_{4,6}$	00110011	I_i
$Y_6, X_6Z_{4,5}$	00010011	I_i
$Y_7, X_7Z_{8,9}$	00001001	I_i
$Y_8, X_8Z_{7,9}$	00001101	I_i
$Y_9, X_9Z_{7,8}$	00000101	I_i

Tableau 17b : Erreurs de canal simples et doubles E ayant même syndrome S et l'erreur associée E_i sur le qubit protégé après correction par un opérateur Y_k.

$Errors$	S	E_i
$(Z_1, Z_2, Z_3), (Z_4Z_{7,8,9}, Z_5Z_{7,8,9}, Z_6Z_{7,8,9})$	00000010	$(I_i), (X_i)$
$(Z_4, Z_5, Z_6), (Z_1Z_{7,8,9}, Z_2Z_{7,8,9}, Z_3Z_{7,8,9})$	00000011	$(I_i), (X_i)$
$(Z_7, Z_8, Z_9), (Z_1Z_{4,5,6}, Z_2Z_{4,5,6}, Z_3Z_{4,5,6})$	00000001	$(I_i), (X_i)$
$(Z_1Z_{2,3}, Z_2Z_3, Z_4Z_{5,6}, Z_5Z_6, Z_7Z_{8,9}, Z_8Z_9)$	00000000	(I_i)

Tableau 17c : Erreurs de canal E ayant même syndrome S et l'erreur E_i sur le qubit protégé après correction par un opérateur Z_k.

E	S	E	S
$X_1Z_{4,5,6}$	10000011	$X_4Z_{1,2,3}$	00100010
$X_1Z_{7,8,9}$	10000001	$X_5Z_{1,2,3}$	00110010
$X_2Z_{7,8,9}$	11000001	$X_6Z_{1,2,3}$	00010010
$X_2Z_{4,5,6}$	11000011	$X_7Z_{1,2,3}$	00001010
$X_3Z_{4,5,6}$	01000011	$X_8Z_{1,2,3}$	00001110
$X_3Z_{7,8,9}$	01000001	$X_9Z_{1,2,3}$	00000110
$X_4Z_{7,8,9}$	00100001	$X_7Z_{4,5,6}$	00001011
$X_5Z_{7,8,9}$	00110001	$X_8Z_{4,5,6}$	00001111
$X_6Z_{7,8,9}$	00010001	$X_9Z_{4,5,6}$	00000111

Tableau 17d: Erreurs de canal doubles $E=X_kZ_l$ laissant le qubit protégé non perturbé.

E	S	E	S	E	S
X_1X_4	10100000	X_2X_7	11001000	X_4X_7	00101000
X_1X_5	10110000	X_2X_8	11001100	X_4X_8	00101100
X_1X_6	10010000	X_2X_9	11000100	X_4X_9	00100100
X_1X_7	10001000	X_3X_4	01100000	X_5X_7	00111000
X_1X_8	10001100	X_3X_5	01110000	X_5X_8	00111100
X_1X_9	10000100	X_3X_6	01010000	X_5X_9	00110100
X_2X_4	11100000	X_3X_7	01001000	X_6X_7	00011000
X_2X_5	11110000	X_3X_8	01001100	X_6X_8	00011100
X_2X_6	11010000	X_3X_9	01000100	X_6X_9	00010100

Tableau 17e: Erreurs de canal doubles $E=X_kX_l$ laissant le qubit protégé non perturbé.

IV.2.9 Comparaison des trois codes

La procédure donnant la fidélité moyenne décrite dans la section VI.2.5 pour le code à cinq qubits est la même pour les autres codes. La différence vient du nombre n de doubles erreurs de canal ayant un syndrome exclusif permettant leur recouvrement qui laisse le qubit protégé dans un état non perturbé (fidélité égale à 1).

On suppose que les erreurs de canal triple et plus sont très improbables. On déduit des tableaux 13, 14 et 15 et pour chaque code les fractions d'erreurs double recouvrables :

$$\frac{n_5}{N_5} = 0 \;\; ; \;\; \frac{n_7}{N_7} = \frac{39}{81} \;\; ; \;\; \frac{n_9}{N_9} = \frac{108}{144} \qquad (54)$$

Avec N_5=40, N_7=81 et N_9=144 le nombre total de double erreur respectivement pour les codes à cinq, sept et neuf qubits. On peut déduire la fidélité moyenne en substituant la valeur F_a=1/3 dans le tableau 10a par une valeur moyenne f_n, ce qui donne pour chaque code :

$$f_5 = \frac{1}{3}\ ;\ f_7 = \frac{(n_7\times 1+(N_7-n_7)\times\frac{1}{3}}{81} = \frac{53}{81}\ ;\ f_9 = \frac{(n_9\times 1+(N_9-n_9)\times\frac{1}{3}}{144} = \frac{5}{6} \qquad (55)$$

On substitue dans le tableau 14 la valeur 1/3 par la valeur moyenne f_n, sauf dans la dernière ligne car pour P=1 toutes les erreurs sont non recouvrables quelque soit le code utilisé. L'équation (52) devient alors fonction de f_n :

$$F_a(P) = [\,(1-P)^8 + 18\,\frac{P}{3}(1-P)^7 + 108\,\frac{P^2}{9}(1-P)^6 + 216\,\frac{P^3}{27}(1-P)^5 + 3\,\frac{P^2}{9}(1-P)^6 + 36\,\frac{P^3}{27}(1-P)^5 + 108\,\frac{P^4}{81}(1-P)^4\,][\,9f_n\,] + [\,9\frac{P^4}{81}(1-P)^4 + 54\,\frac{P^3}{243}(1-P)^3\,][\,18f_n + 6\,] + [\,\frac{P^6}{27}(1-P)^2\,][\,21f_n + 6\,] + [\,\frac{P}{3}(1-P)^7 + 18\,\frac{P^2}{9}(1-P)^6 + 108\frac{P^3}{27}(1-P)^5 + 216\frac{P^4}{81}(1-P)^4\,][\,6\,] + [\,\frac{P^2}{9}(1-P)^6 + 18\,\frac{P^3}{27}(1-P)^5 + 108\frac{P^4}{81}(1-P)^4 + 216\frac{P^5}{243}(1-P)^3\,][\,9\,] + [\,3\frac{P^3}{27}(1-P)^5 + 36\frac{P^4}{81}(1-P)^4 + 108\frac{P^5}{243}(1-P)^3\,][54f_n\,] + [3\frac{P^4}{81}(1-P)^4 + 36\frac{P^5}{243}(1-P)^3 + 108\frac{P^6}{3^6}(1-P)^3\,][\,81f_n\,] + [\,9\frac{P^5}{243}(1-P)^3 + 54\frac{P^6}{3^6}(1-P)^2\,][\,54(2f_n+1)\,] + [\,9\frac{P^6}{3^6}(1-P)^2 + 54\frac{P^7}{3^7}(1-P)\,][81(2f_n+1)] + 27\frac{P^7}{3^7}(1-P)\,][18(7f_n+2)] + 27\frac{P^8}{3^8}[117] \qquad (56)$$

Le calcul donne finalement :

$$F_a(P) = (1-P)^8 + 8P(1-P)^7 + (3f_n+25)P^2(1-P)^6 + (18f_n+38)P^3(1-P)^5 + (41f_n+29)P^4(1-P)^4 + (44f_n+12)P^5(1-P)^3 + \frac{(205f_n+47)}{9}P^6(1-P)^2 + \frac{(50f_n+22)}{9}P^7(1-P) + \frac{13}{27}P^8 \qquad (57)$$

Le tableau 18 résume les expressions de la fidélité déterminées précédemment et la figure 15 compare cette fidélité sans et avec correction par les trois codes. Elle montre logiquement que la fidélité moyenne décroit lorsque la probabilité d'erreur P croit que les qubits transmis soient protégés ou non par un code. De plus, on constate qu'elle décroit plus lentement avec P lorsqu'un code est utilisé que dans le cas de non protection. On voit aussi qu'elle est la meilleure pour toutes valeurs de P lorsque la protection est réalisée par le code à neuf qubits. De même, la protection avec le code à sept qubits est meilleure pour toutes les valeurs de P que celle avec le code à cinq qubits. La raison est que dans le cas du code à cinq qubits toutes les doubles erreurs de canal laissent le qubit protégé perturbé après correction et décodage. Les deux autres codes offrent une protection meilleure car un certain nombre de double erreur de canal peuvent être recouvertes. Cependant, il faut noter que dans ce travail on a considéré très improbables les erreurs sur trois qubits et plus parmi les cinq, sept ou neuf transmis par canal. Ainsi, la mesure de syndrome (code à sept et neuf qubits) permet le recouvrement de certaines double erreurs. Enfin, on constate que si la probabilité d'erreur est égale à P=1 alors la fidélité moyenne Fa(P=1) = 13/27= 0.4815 est la même pour les trois codes.

Code	$F_a(P)$
C_0	$1-2P+\frac{8}{3}P^2-\frac{32}{27}P^3$
C_n	$(1-P)^8+8P(1-P)^7+(3f_n+25)P^2(1-P)^6+(18f_n+38)P^3(1-P)^5+(41f_n+29)P^4(1-P)^4+(44f_n+12)P^5(1-P)^3+(\frac{205f_n+47}{9})P^6(1-P)^2+(\frac{50f_n+22}{9})P^7(1-P)+\frac{13}{27}P^8$
C_5	$(1-P)^8+8P(1-P)^7+26P^2(1-P)^6+44P^3(1-P)^5+\frac{128}{3}P^4(1-P)^4$ $\frac{80}{3}P^5(1-P)^3+\frac{346}{27}P^6(1-P)^2+\frac{116}{27}P^7(1-P)+\frac{13}{27}P^8$
C_7	$(1-P)^8+8P(1-P)^7+\frac{728}{27}P^2(1-P)^6+\frac{448}{9}P^3(1-P)^5+\frac{4522}{81}P^4(1-P)^4$ $\frac{3304}{81}P^5(1-P)^3+\frac{14672}{729}P^6(1-P)^2+\frac{4432}{729}P^7(1-P)+\frac{13}{27}P^8$
C_9	$(1-P)^8+8P(1-P)^7+\frac{55}{2}P^2(1-P)^6+53P^3(1-P)^5+\frac{379}{6}P^4(1-P)^4$ $\frac{146}{3}P^5(1-P)^3+\frac{1307}{54}P^6(1-P)^2+\frac{191}{27}P^7(1-P)+\frac{13}{27}P^8$

Tableau 18 : Fidélité sans et avec correction par les trois codes. Les symboles C_0 et C_n représentent respectivement la transmission sans protection et le code à n qubits.

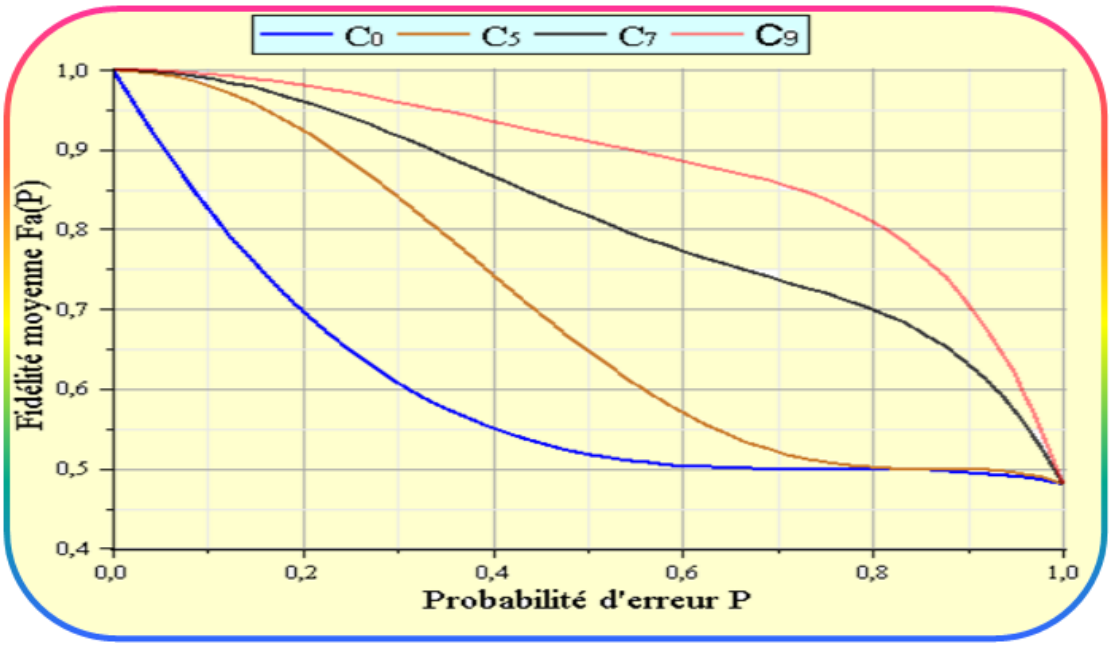

Figure 15 : Evolution de la fidélité moyenne avec la probabilité d'erreur de canal dépolarisant, sans et avec protection par trois codes.

IV.3 Conclusion

Les résultats de ce chapitre démontrent la nécessite de protéger les qubits servant à la transmission de secret par canaux bruités. Bien que nous ayons montré que certaines erreurs de canal n'affectent pas le secret transmis il n'y a à notre connaissance aucun moyen pratique de contrôler l'interaction d'un canal avec le monde extérieur afin de le protéger d'un type particulier d'erreur. D'autre part, ce travail montre l'utilité des états de graphes qui permettent d'unifier le partage de secret et les codes correcteurs.

Conclusion Générale et Perspectives

Conclusion générale et perspectives

Nous avons investigué dans ce travail un code convolutif quantique à cinq qubits. Nous avons décrit l'implantation de ce code sur un ordinateur classique en simulant le circuit de codage, la procédure de détection et correction d'erreur et le circuit de décodage. La simulation a porté sur un premier groupe de onze qubits transmis mais les résultats ont été généralisés à tout le flux envoyé dans le canal grâce à la propriété convolutive du code. La simulation du circuit de codage des onze premier qubits a permis de construire l'état codé en un temps assez court (quelques secondes). L'originalité dans notre procédure de détection et correction d'erreur est qu'elle ne procède pas à la détermination des syndromes dans leur intégralité, mais effectue seulement la mesure d'un nombre restreint de générateurs, suffisant pour identifier l'erreur de canal la plus probable et la corriger. Cette démarche aide à contrer le phénomène de décohérence par un gain de temps dans le traitement du flux de qubits par le récepteur qui permet d'accéder plus vite à l'information utile. Enfin, nous pouvons conclure à partir de ce travail qu'un code convolutif quantique ne permet d'extraire de manière fiable un flux d'information transmis de manière continue dans un canal bruité que si la probabilité d'erreur dans ce canal est très faible. La deuxième partie de cette thèse a été consacrée au partage de secret quantique à travers des canaux dépolarisants. Ainsi, trois codes correcteurs quantiques ont été utilisés et les résultats montrent clairement que le code à neuf qubits donne la meilleure fidélité quelque soit la probabilité d'erreur dans le canal, suivi par le code à sept puis à cinq qubits. Cette conclusion confirme le travail de simulation fait dans la référence [18] où les erreurs ont été introduites dans le processus de correction lui même. On peut déduire que plus le nombre de qubits protecteurs est élevé mieux est la fiabilité de l'information transmise par le canal bruité. La raison est que le code à neuf qubits donne lieu à un plus grand nombre de doubles erreurs de canal qui laisse le qubit protégé intact après correction. En réalité, nous avons considéré seulement les erreurs simples et doubles ce qui fait qu'une plus grande fraction de doubles erreurs possède un syndrome exclusif qui permet leur recouvrement par le code à neuf qubits. Nous avons supposé que la probabilité d'erreur de canal sur trois qubits et plus sont tellement négligeables qu'elles n'influent pas sur les résultats et conclusion obtenue.

Les perspectives théoriques de ce travail résident en premier dans l'investigation des codes quantiques utilisés dans le cas ou plus de deux qubits sont infectés lors de la transmission. En second lieu, il serait intéressant d'étudier le partage de plusieurs secrets en utilisant plus que cinq qubits transmis par des canaux bruités. Le but étant d'utiliser les états de graphes pour construire un formalisme général qui unifie les codes correcteurs avec d'une part le calcul quantique et d'autre part les communications quantiques telles que le partage de secret et la téléportation. Concernant les perspectives expérimentales, il est clair que les communications quantiques ont plus de chance de se développer que le calcul quantique qui exige un nombre de qubits infiniment plus élevé entrainant des difficultés expérimentales actuellement insurmontables. Néanmoins, un problème majeur se pose est que les communications quantiques du fait de leur confidentialité accrue constitue un domaine d'application militaire et dans le monde des finances. En conséquence, il est difficile de trouver des laboratoires étrangers ouverts à la collaboration ou même de la documentation disponible qui décrit en détail les expériences réalisées.

Références bibliographiques

Références bibliographiques

[1] M.A.Nielsen, I.L.Chuang: "Quantum computation and quantum information",Cambridge University Press, UK, 2000.

[2] C.C.Tannoudji, B.Diu, F.Laloë, "Mécanique quantique", Tome 1 et 2, Collection Enseignement des sciences, ISSN 0768-0341, Ed Hermannm, 1973.

[3] Eleanor Rieeel and W.Polak, "An introduction to quantum computing for non-physicists", permissions@acm.org, 2000.

[4] Daniel Gottesman, "An Introduction to Quantum Error Correction",arXiv:0904.2557v1, [quant-ph], 16 Apr 2009.

[5] H.Olivier, J.P Tillich, "Quantum Convolutional code: Fundamentals ", arXiv:quant-ph/0401134v11, 2004.

[6] Mark McMahonWilde,"Quantum Coding with Entanglement", arXiv:0806.4214v1,[quant-ph], 25 Jun 2008.

[7] H.Olivier, "Elements of quantum information theory, decoherence and error correcting codes", thesis, INRIA-CODES, 2004.

[8] H.Olivier, J.P Tillich,"Description of a quantum convolutional code ", arXiv:quant-ph/0304189v2, 15 May 2003

[9] T.Radtke, S.Fritzsche: .Simulation of n-qubits quantum systems., I. Quantum gates and registers,CPC,Vol 173,Issues1.2, 2005, Pages 91.113.

[10] T.Radtke, S.Fritzsche: Simulation of n-qubits quantum systems, II.Quantum states, CPC, Volume 175, Issue 2, 2006, Pages 145.166.

[11] T.Radtke, S.Fritzsche: Simulation …, III. Quantum operations, CPC, Vol 176, Issues 9.10, 2007, Pages 617.633.

[12] T.Radtke, S.Fritzsche: Simulation ..., IV. Parametrizations of quantum states, CPC, Vol 179, Issue 9, 2008, Pages 647.664.

[13] CPC Program Lib, Queen.s University of Belfast, N.Ireland, 2008.

[14] Graph States for Quantum Secret Sharing, Damian Markham and Barry C. Sanders, Phys. Rev. A 78, 042309 (2008).

[15] Raymond Laflamme and co "Perfect Quantum Error Correcting Code", Physic Review Letters, Volume 77,Number 1,198-201, july 1996.

[16] A. M. Steane. "Multiple particle interference...".Proc. R. Soc. Lond. A, 452:2551.2576, 1996. quant-ph/9601029.

[17] A.G.Fowler, "Constructing arbitrary Steane code….gates", Quantum Information and Computation,11: 867-873 (2011).

[18] Jumpei Niwa, Keiji Matsumoto, Hiroshi Imai, "Simulating the Effects of Quantum Error-correction Schemes",arXiv:quant-ph/0211071v1 13 Nov 2002.

[19] « *Rapid solutions of problems by quantum computation* », *Proceedings of the Royal Society of London A*, vol. 439, 1992, p. 553

[20] C. H. Bennett et al. Teleporting an unknown quantum state via dual classical and EPR channels. Phys. Rev. Lett. 70, 1895–1899 (1993)

[21] RB Griffiths 'Quantum Error Correction - CMU Quantum Theory group', *quantum.phys.cmu.edu/QCQI/qitd213.pdf* , Avril 2012.

[22] J.Kempe **'**Quantum Algorithms', Summer School on Theory and Technology in Quantum Information, Communication, Computation and Cryptography, w*ww.cs.tau.ac.il/.../QUANTUM.../kempe-notes06.pdf*2006

[23] SHANNON C. E., « A Mathematical Theory of Communication », The Bell System Technical Journal, vol. 27, pp. 379-423, 623-656, juillet-octobre 1948.

[24] P. Elias, "Coding for noisy channels,"IRE Conv. Rec., pt.4, pp.37–46,Mar. 1955

[25] BERROU C., PYNDIAH R., JEZEQUEL M., GLAVIEUX A., ADDE P., « La double correction des Turbo-Codes », *La Recherche*, n°315, pp. 34-37, décembre 1998.

[26] BERROU C., « Les turbo codes convolutifs », ENST Bretagne, mars 1999.

[27] INGVARSON O. et SVENELL H., « Error performance of turbo codes » (Master's Thesis, 18/12/98), http://www.df.lth.se/~pi/exjobbet/

[28] Rohit Khandekar, "Notes on quantum error correcting codes", University of California, Berkley, 2004.

[29] John Preskill, "Chap 7: Quantum error correction". http://www.theory.caltech.edu/people/preskill/ph229/.

[30] Adriano Barenco, Charles H.Bennet and co, "Elementary gates for quantum computation", Phys rev A, 1995.

[31] A.Viterbi "Error bounds for convolutional codes……...", *IEEE transactions on Information Theory* Volume IT-13, pages 260-269, Avril, 1967.

Contributions de l'auteur

[R1] Publication de l'article intitulé : « Simulation of the Shor's nine-qubits code using Feynman program» sur le site électronique MapleSoft: http://go.microsoft.com/fwlink/?LinkId=69157

[R2] Communication par poster intitulée «Partage de Secret Quantique avec Correction d'erreur » au workshop sur les communications et l'information quantiques organisé à Paris par GDR-IQFA (CNRS). http://gdriqfa.unice.fr/.

[R3] Publication de l'article intitulé : « Quantum Secret Sharing with Error Correction» sur le journal « Communication in Theoretical Physics », http://www.iop.org/EJ/journal/ctp http://ctp.itp.ac.cn

[R4] Communication orale «Quantum Secret Sharing with Noisy channels » à la conférence FCS2012 (FOUNDATIONS OF COMPUTER SCIENCE), Las Vegas USA. www.world-academy-of-science.org

[R5] Publication de l'article intitulé : « Simulation of a five-qubits convolutional code» : http://go.microsoft.com/fwlink/?LinkId=69157

Annexes

Annexe A : Exemple de calcul quantique : l'algorithme de Deutsch

On dispose d'une fonction f : {0,1}→{0,1} et on cherche à déterminer si elle est constante (f(0)=f(1)) ou balancée (f(0)#f(1)). Elle est représentée par l'opérateur unitaire U_f : $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$. L'algorithme décrit dans [19] est réalisé par le circuit suivant à deux qubits initialisés à $|0\rangle$ et $|1\rangle$ respectivement :

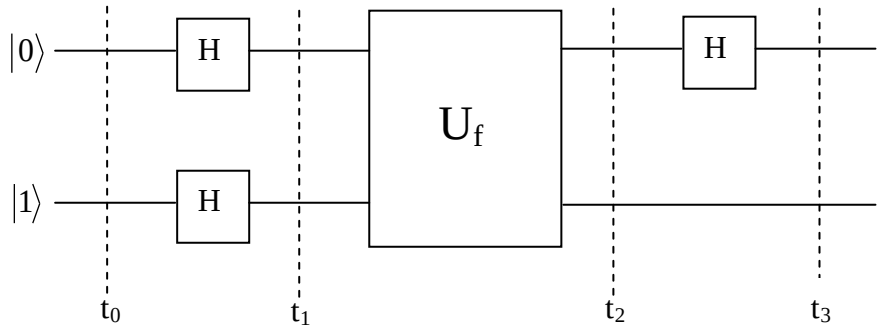

Figure A : Circuit quantique de l'algorithme de Deutsch [22].

Décrivons ici-bas le protocole quantique qui réalise cet algorithme :
Etat initial séparable du système à deux qubits à l'instant $t=t_0$:

$$|\phi_0\rangle = |0\rangle|1\rangle$$

Application de H à chaque qubit :

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

Application de U_f :

$$|\phi_2\rangle = \frac{1}{2}(|0\rangle|f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle)$$

Application de H sur le premier qubit :

$$|\phi_3\rangle = \frac{1}{2^{3/2}}((|0\rangle + |1\rangle)(|f(0)\rangle - |1 \oplus f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |1 \oplus f(1)\rangle))$$

Si f(0)=f(1) :

$$|\phi_3\rangle = \frac{1}{2^{1/2}}|0\rangle(|f(0)\rangle - |1 \oplus f(0)\rangle) = \frac{1}{2^{1/2}}(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle)$$

Si f(0)#f(1) :

$$|\phi_3\rangle = \frac{1}{2^{3/2}}((|0\rangle + |1\rangle)(|f(0)\rangle - |f(1)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |f(0)\rangle))$$

$$|\phi_3\rangle = \frac{1}{2^{1/2}}|1\rangle(|f(0)\rangle - |f(1)\rangle) = \frac{1}{2^{1/2}}(-1)^{f(0)}|1\rangle(|0\rangle - |1\rangle)$$

On peut réécrire ces résultats sous la forme :

$$|\phi_3\rangle = \pm|f(0) \oplus f(1)\rangle\frac{1}{2^{1/2}}(|0\rangle - |1\rangle)$$

La dernière étape consiste à mesurer le premier qubit, si on trouve $|0\rangle$ alors f est constante et si on trouve $|1\rangle$ elle est balancée. La particularité de ce calcul est qu'une seule mesure suffit alors que dans le cas classique on doit mesurer f(0) et f(1) pour arriver au résultat.

Nous donnons dans cette annexe la simulation du problème de Deusch faite sur Maple avec le programme Feynman.

 # Chargement des packages

```
> with(Feynman):with(LinearAlgebra): Digits:=20;
```

 # Nomination de la procédure et liste de ses paramètres

```
Deutsch:=proc(n)
local Qo,Q1,Q2,Q3,Q4,f,Uf,Id,H,H1,H2,Z,cnot,Pa,A,val :
```

 # Portes quantiques simples et doubles à appliquer

```
H:=Feynman_quantum_operator("H"):Id:=Feynman_quantum_operator("I"):
Z:=Feynman_quantum_operator("Z"):
H1:=Feynman_evaluate("Kronecker product",H,H): H2:=Feynman_evaluate("Kronecker
product",H,Id):
```

 # Algorithme de Deush

```
if n=1 then Uf:=Feynman_evaluate("Kronecker product",-Id,Id): f:="f(x)=0":
end if: if n=2 then Uf:=Feynman_evaluate("Kronecker product",Id,Id): f:="f(x)=1":end if: if
n=3 then Uf:=Feynman_quantum_operator("cnot"):
f:="f(x)=x":end if: if n=4 then Uf:=Feynman_evaluate("Kronecker product",- Z,Id):
f:="f(x)=NOT(x)": end if: Q2:=Uf.Q1: Q3:=H2.Q2: Pa:=Feynman_evaluate("Kronecker
product",<1,0>.<1|0>,Id): Q4:=Pa.Q3: A:=<0,0,0,0>: val:=evalb(Equal(Q4,A)): if val=true
then print(" The function ",f, " is balanced "): else print(" The function ", f," is constant
"): end if; end proc:
```

 # Execution de la procédure

```
Deutsch(1); Deutsch(2);Deutsch(3);Deutsch(4);
```

```
Welcome to Feynman (April 2008)
" La fonction ", "f(x)=0", " est constante "
" La fonction ", "f(x)=1", " est constante "
" La fonction ", "f(x)=x", " est balancée "
" La fonction ", "f(x)=NOT(x)", " est balancée "
```

Annexe B : Téléportation

Nous donnons dans cette annexe la simulation de la téléportation faite sur Maple avec le programme Feynman.

```
# Chargement des packages
> with(Feynman): with(LinearAlgebra): Digits:=20;
# Nomination de la procédure et liste de ses paramètres
Teleport:=proc(n) : local Q,Qoa,Qob,Qoc,Qod,Qo,Q1,Q2,CN1,QId,H,H1,H2,
V,P1,P2,P3,P4,Q2a,Q2aa,Q2b,Q2bb,Q2c,Q2cc,Q2d,Q2dd,
Qx,Z,X,CN,Id,vb,Qz,Qxz:  Id:=Feynman_quantum_operator("I"):
# Portes quantiques simples et doubles à appliquer
H:=Feynman_quantum_operator("H"):H1:=Feynman_evaluate("Kronecker product",H,Id):
 H2:=Feynman_evaluate("Kronecker product",H,Id,Id): Z:=Feynman_quantum_operator("Z"):
X:=Feynman_quantum_operator("X"): CN:=Feynman_quantum_operator("cnot"):
CN1:=Feynman_evaluate("Kronecker product",CN,Id): Qoa:=<1,0>:
Qob:=Feynman_evaluate("Kronecker product",Qoa,Qoa):
# Téléportation
Qoc:=H1.Qob: Qod:=CN.Qoc:  Q:=<a,b>: Qo:=Feynman_evaluate("Kronecker product",Q,Qod):
Q1:=CN1.Qo: Q2:=H2.Q1: if n=1 then V:=<1,0,0,0>.<1|0|0|0>:
P1:=Feynman_evaluate("Kronecker product",V,Id):
Q2a:=P1.Q2:Q2aa:=Feynman_evaluate("Kronecker product",Qob/2,Q):
vb:=evalb(Equal(Q2a,Q2aa)):
if vb=true then print("The qubit teleported to Bob is Q=", Q);
else print("false"); fi; fi;if n=2 then V:=<0,1,0,0>.<0|1|0|0>:
P2:=Feynman_evaluate("Kronecker product",V,Id): Q2b:=P2.Q2:
Q2bb:=Feynman_evaluate("Kronecker product",<0,1/2,0,0>,X.Q):
vb:=evalb(Equal(Q2b,Q2bb)):
if vb=true then print("The qubit teleported to Bob is XQ=", X.Q);
else print("false") fi; fi; if n=3 then V:=<0,0,1,0>.<0|0|1|0>:
P3:=Feynman_evaluate("Kronecker product",V,Id): Q2c:=P3.Q2:
Q2cc:=Feynman_evaluate("Kronecker product",<0,0,1/2,0>,Z.Q):
vb:=evalb(Equal(Q2c,Q2cc)):
if vb=true then print("The qubit teleported to Bob is ZQ=",Z.Q);
else print("false") fi; fi; if n=4 then V:=<0,0,0,1>.<0|0|0|1>:
P4:=Feynman_evaluate("Kronecker product",V,Id): Q2d:=P4.Q2:
Q2dd:=Feynman_evaluate("Kronecker product",<0,0,0,1/2>,X.Z.Q):
vb:=evalb(Equal(Q2d,Q2dd)):
if vb =true then print(" The qubit teleported to Bob is XZQ=  ", X.Z.Q);
else print("false") fi; fi;  end proc;
# Execution de la procédure
Teleport(1);Teleport(2);Teleport(3);Teleport(4);
```

$$\text{" Le qubit téléporté vers Bob estQ=","} \begin{bmatrix} a \\ b \end{bmatrix} \quad \text{" Le qubit téléporté vers Bob est XQ=","} \begin{bmatrix} b \\ a \end{bmatrix}$$

$$\text{"Le qubit téléporté vers Bob est ZQ=","} \begin{bmatrix} a \\ -b \end{bmatrix} \quad \text{" Le qubit téléporté vers Bob est XZQ= ","} \begin{bmatrix} -b \\ a \end{bmatrix}$$

Annexe C : Code correcteur à deux qubits

Ce code décrit dans [20] corrige une erreur X sur un qubit en état superposé. Soit deux qubits respectivement dans les états $\psi = \alpha|0\rangle + \beta|1\rangle$ et $|0\rangle$. A l'instant t_0 le système se trouve dans l'état séparable $\psi_0 = (\alpha|0\rangle + \beta|1\rangle)|0\rangle$. En appliquant CNOT (le second qubit étant la cible) on produit à un instant $t_1 > t_0$ l'état intriqué $\psi_1 = \alpha|00\rangle + \beta|11\rangle$. On suppose qu'une erreur X se produit à un instant
$t > t_1$ sur le premier qubit comme illustré sur le circuit de codage suivant :

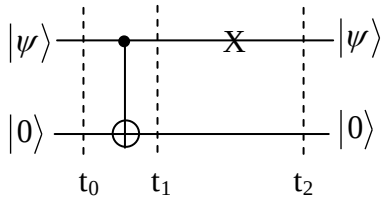

Figure C1 : Circuit quantique du code correcteur à deux qubits [21].

Notons que le symbole X indique une erreur probable alors que ce symbole entouré d'une boite carrée $\boxed{X}$ indique une erreur certaine. La probabilité d'erreur dépend de l'interaction du système avec l'environnement. La solution classique qui consiste à supprimer le bit altéré ne fonctionne pas dans le cas quantique. En effet, l'intrication des deux qubits fait que le qubit restant sera décrit par la matrice densité :

$$\rho = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| = |\alpha|^2\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + |\beta|^2\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}|\alpha|^2 & 0\\ 0 & |\beta|^2\end{pmatrix}$$

Cette matrice permet de déduire $\psi = \alpha|0\rangle \pm \beta|1\rangle$ pour le qubit supprimé avec donc une ambiguïté sur la phase de l'état initial. Considérons maintenant une autre solution illustrée sur la figure C2 qui consiste à utiliser deux autres qubits accessoires afin de mesurer sans le détruire l'état du système :

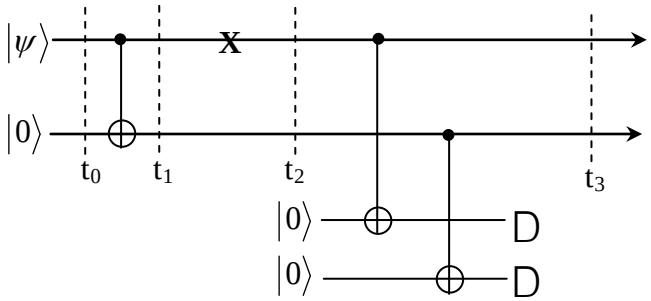

Figure C2 : Circuit quantique du code correcteur à deux qubits. Le symbole D désigne la détection de l'erreur sur qubit 1 par la mesure des deux qubits rajoutés [21].

A l'instant t_2 le système à quatre qubits est dans l'état séparable suivant $|\psi_2\rangle = (\alpha|10\rangle + \beta|01\rangle)|0\rangle|0\rangle = \alpha|1000\rangle + \beta|0100\rangle$ où nous avons introduit l'erreur sur le

premier qubit. L'application de CNOT sur le premier et le troisième qubits donne $|\psi_2'\rangle = \alpha|1010\rangle + \beta|0100\rangle$.

De même cette porte appliquée sur le second et dernier qubit donne $|\psi_3\rangle = \alpha|1010\rangle + \beta|0101\rangle$ où nous constatons la persistance de l'erreur sur le premier qubit. Cette méthode permet seulement d'être informé qu'il y'a eu erreur mais sans la corriger. En effet, la même procédure aurait donné en absence d'erreur un autre ket final : $|\psi_2\rangle = (\alpha|00\rangle + \beta|11\rangle)|0\rangle|0\rangle = \alpha|0000\rangle + \beta|1100\rangle$; $|\psi_2'\rangle = \alpha|0000\rangle + \beta|1110\rangle$ et enfin $|\psi_3\rangle = \alpha|0000\rangle + \beta|1111\rangle$. Donc, si la mesure des deux qubits rajoutés donne deux valeurs différentes, cela indique la présence d'erreur sur le premier qubit. Nous allons maintenant voir une autre méthode qui s'appuie sur la dissemblance qu'il y'a entre les termes de la superposition d'état selon que l'erreur s'est produite ou pas. Soient les deux kets du système des deux premiers qubits sans et avec erreur $|\psi_1\rangle = \alpha|00\rangle + \beta|11\rangle$; $|\psi_2'\rangle = \alpha|10\rangle + \beta|01\rangle$. La dissemblance entre les deux est que dans le premier les qubits ont la même valeur dans chaque terme de la superposition alors qu'ils sont différents dans le second. Cette dissemblance peut être représentée par l'opérateur produit Z_aZ_b où a et b désignent le premier et le second qubit. En effet, l'application de cet opérateur donne deux valeurs propres différentes selon qu'il y'a ressemblance ou dissemblance dans les termes de la superposition d'état. L'application de l'opérateur Z sur les état de base $|0\rangle$ et $|1\rangle$ donne :

$$Z|0\rangle = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = |0\rangle;\ Z|1\rangle = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\-1\end{pmatrix} = -|1\rangle$$ et en général

$Z|\psi\rangle = \alpha Z|0\rangle + \beta Z|1\rangle = \alpha|0\rangle - \beta|1\rangle$ c'est-à-dire $Z|+\rangle = |-\rangle$; $Z|-\rangle = |+\rangle$. L'application du produit Z_aZ_b sur les deux kets $|\psi_1\rangle$ et $|\psi_2'\rangle$ donne :

$$Z_aZ_b|\psi_1\rangle = \alpha Z_aZ_b|00\rangle + \beta Z_aZ_b|11\rangle = \alpha|00\rangle + \beta|11\rangle = |\psi_1\rangle$$
$$Z_aZ_b|\psi_2'\rangle = \alpha Z_aZ_b|10\rangle + \beta Z_aZ_b|01\rangle = -\alpha|10\rangle - \beta|11\rangle = -|\psi_2'\rangle$$

Nous avons donc une valeur propre +1 en absence d'erreur et -1 s'il y'a erreur. La correction de l'erreur se fait alors à l'aide d'un troisième qubit rajouté pour mesurer l'état du système des deux premiers qubits puis de corriger l'erreur si elle est détectée. La procédure est illustrée par le circuit suivant :

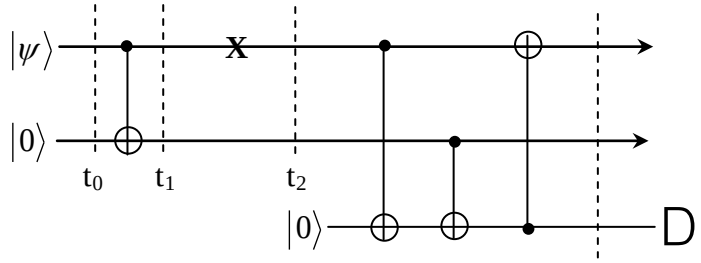

Figure C3 : Circuit quantique du code correcteur à deux qubits**.** Le symbole D désigne la détection de l'erreur par la mesure du qubit rajouté [21].

A l'instant t_2 le système des trois qubits est dans l'état séparable $\left|\psi_{2}^{'}\right\rangle = (\alpha|10\rangle + \beta|01\rangle)|0\rangle = \alpha|100\rangle + \beta|010\rangle$. L'application de CNOT sur le premier et troisième qubit donne :

$$CNOT\left|\psi_{2}^{'}\right\rangle = \alpha CNOT|100\rangle + \beta CNOT|010\rangle = \alpha|101\rangle + \beta|010\rangle.$$

L'application de CNOT sur le second et troisième qubit donne : $\left|\psi_{2}^{''}\right\rangle = \alpha CNOT|101\rangle + \beta CNOT|010\rangle = \alpha|101\rangle + \beta|011\rangle$. Enfin CNOT est appliquée entre le troisième et le premier qubit lequel est la cible : $\left|\psi_3\right\rangle = \alpha CNOT|101\rangle + \beta CNOT|011\rangle = \alpha|001\rangle + \beta|111\rangle = (\alpha|00\rangle + \beta|11\rangle)|1\rangle$

Nous obtenons finalement l'état final séparable du système à trois qubits $\left|\psi_3\right\rangle = \left|\psi_1\right\rangle|1\rangle$ où l'état initial $\left|\psi_1\right\rangle$ a été rétabli. Le changement de l'état du qubit de mesure de $|0\rangle$ en $|1\rangle$ indique la présence de l'erreur avant la correction. Remarquons qu'il n'est pas nécessaire de connaître l'état du qubit rajouté car en absence d'erreur la procédure donnerait :

$$\left|\psi_2\right\rangle = \left|\psi_1\right\rangle|0\rangle = (\alpha|00\rangle + \beta|11\rangle)|0\rangle = \alpha|000\rangle + \beta|110\rangle \ ;$$
$$CNOT|\psi_2\rangle = \alpha CNOT|000\rangle + \beta CNOT|110\rangle = \alpha|000\rangle + \beta|111\rangle \ ;$$
$$\left|\psi_2^{''}\right\rangle = \alpha CNOT|000\rangle + \beta CNOT|111\rangle = \alpha|000\rangle + \beta|110\rangle \ ;$$
$$\left|\psi_3\right\rangle = \alpha CNOT|000\rangle + \beta CNOT|110\rangle = \alpha|000\rangle + \beta|110\rangle = (\alpha|00\rangle + \beta|11\rangle)|0\rangle$$

L'état initial séparable $\left|\psi_3\right\rangle = \left|\psi_1\right\rangle|0\rangle$ étant donc conservé, on peut supprimer sans le mesurer le troisième qubit après utilisation. En réalité, il est possible de corriger l'erreur **X** précédente sans rajouter le troisième qubit comme on le constate sur le circuit suivant :

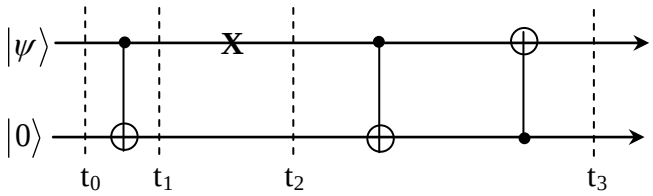

Figure C4 : Circuit quantique du code correcteur à deux qubits [21]**.**

A l'instant t_2 le système altéré est dans l'état $\left|\psi_{2}^{'}\right\rangle = \alpha|10\rangle + \beta|01\rangle$, la première porte CNOT donne $\left|\psi_{2}^{''}\right\rangle = \alpha|11\rangle + \beta|01\rangle$ et la seconde donne l'état final séparable $\left|\psi_3\right\rangle = \alpha|01\rangle + \beta|11\rangle = (\alpha|0\rangle + \beta|1\rangle)|1\rangle = \left|\psi_1\right\rangle|1\rangle$. Les deux dernières portes CNOT constitue un circuit de décodage correcteur d'erreur.

Nous donnons ici-bas la simulation du code à deux qubit :

 # Chargement des packages

```
> with(Feynman):with(LinearAlgebra):Digits := 14:
# Codage
Qo:=Feynman_evaluate("Kronecker product",<a,b>,<1,0>):
Qoa:=Feynman_evaluate("Kronecker product",<a,b>,<0,1>):
CN:=Feynman_quantum_operator("cnot"): Q1:=CN.Qo:
# Erreur
X:=Feynman_quantum_operator("X"):  Id:=Feynman_quantum_operator("I"):
X1:=Feynman_evaluate("Kronecker product",X,Id):Q2:=X1.Q1:
# Décodage et correctionQ2a:=CN.Q2:
N1:=Feynman_quantum_operator(2,"cnot",[2,1]):Q3:=CN1.Q2a:                    if
evalb(Equal(Q3,Qo))=true then print("pas d'erreur") end if;
if evalb(Equal(Q3,Qoa))=true then print("Error on first qubit corrected "); end if;
```

Welcome to Feynman (April 2008)

$$Qo := \begin{bmatrix} a \\ 0 \\ b \\ 0 \end{bmatrix} \qquad Qoa := \begin{bmatrix} 0 \\ a \\ 0 \\ b \end{bmatrix} \qquad Q3 := \begin{bmatrix} 0 \\ a \\ 0 \\ b \end{bmatrix}$$

"Error on first qubit corrected"

Annexe D : Code correcteur à trois qubits

D1 : Correction d'une erreur X par le code à trois qubits

Soit un code à trois qubits initialement dans les états $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle;\ |0\rangle\ et\ |0\rangle$ et illustré par le circuit suivant [21] **:**

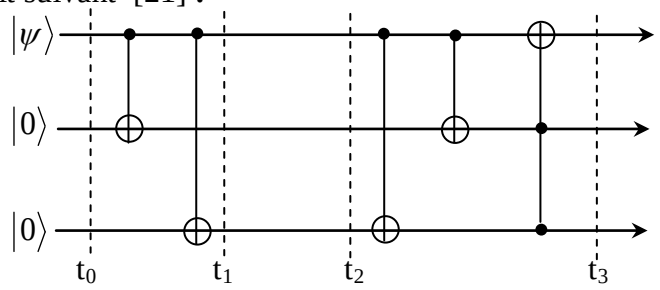

Figure D1: Circuit quantique du code correcteur à trois qubits [21]**.**

Nous avons l'état initial séparable à l'instant t_0 $|\psi_0\rangle = |\psi\rangle|0\rangle|0\rangle = \alpha|000\rangle + \beta|100\rangle$ qui devient à l'instant t_1 $|\psi_1\rangle = \alpha|000\rangle + \beta|111\rangle$. On suppose qu'une erreur **X** peut se produire sur

seulement l'un des trois qubits entre t_1 et t_2 et donner les quatre états $|\psi_2\rangle$ possibles où l'absence d'erreur est inclue: $\alpha|000\rangle + \beta|111\rangle$; $\alpha|100\rangle + \beta|011\rangle$; $\alpha|010\rangle + \beta|101\rangle$; $\alpha|001\rangle + \beta|110\rangle$

Montrons que ce code corrige l'erreur quelque soit sa localisation. Après erreur sur le premier qubit nous avons $|\psi_2\rangle = \alpha|100\rangle + \beta|011\rangle$ puis à la suite des deux CNOT $|\psi_2^{'}\rangle = \alpha|111\rangle + \beta|011\rangle$. La porte de TOFFOLI change la valeur de la cible seulement si les deux qubits contrôleurs ont la même valeur 1, ce qui donne ici $|\psi_3\rangle = \alpha|011\rangle + \beta|111\rangle = (\alpha|0\rangle + \beta|1\rangle)|11\rangle$. Nous avons donc rétabli l'état correct du premier qubit avec un basculement de la valeur des autres qui indique la présence de l'erreur. En cas d'erreur sur le second ou le troisième qubit cette procédure donnerait : $|\psi_2\rangle = \alpha|010\rangle + \beta|101\rangle$; $|\psi_2^{'}\rangle = \alpha|010\rangle + \beta|110\rangle$; $|\psi_3\rangle = \alpha|010\rangle + \beta|110\rangle = (\alpha|0\rangle + \beta|1\rangle)|10\rangle$

$|\psi_2\rangle = \alpha|001\rangle + \beta|110\rangle$; $|\psi_2^{'}\rangle = \alpha|001\rangle + \beta|101\rangle$; $|\psi_3\rangle = \alpha|001\rangle + \beta|101\rangle = (\alpha|0\rangle + \beta|1\rangle)|01\rangle$ Nous constatons qu'on obtient à chaque fois un état final séparable où le premier qubit est rétabli dans son état superposé initial. L'état des deux derniers qubits $|11\rangle$; $|10\rangle$; $|01\rangle$ indique à chaque fois la présence de l'erreur dans le premier, le second et le dernier qubit respectivement. Vérifions qu'en absence d'erreur l'état initial du système est conservé :

$|\psi_2\rangle = \alpha|000\rangle + \beta|111\rangle$; $|\psi_2^{'}\rangle = \alpha|000\rangle + \beta|100\rangle$; $|\psi_3\rangle = \alpha|000\rangle + \beta|100\rangle = (\alpha|0\rangle + \beta|1\rangle)|00\rangle$

D2 : Correction d'une erreur Z par le code à trois qubits

Nous allons utiliser un code à trois qubits pour corriger une erreur de phase Z sur le premier qubit entre t_1 et t_2 . Cette tache est accomplie par le circuit suivant :

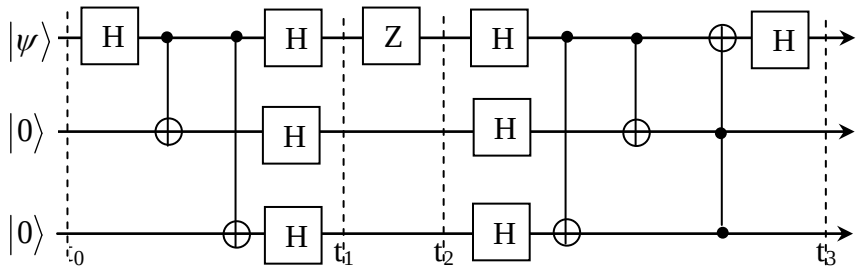

Figure D2 : Code à trois qubits pour la correction d'une erreur de phase [21]**.**

Décrivons ici-bas le protocole quantique qui corrige une erreur de phase.

Etat initial séparable à t=0 :

$$|\psi_0\rangle = |\psi\rangle|0\rangle|0\rangle = \alpha|000\rangle + \beta|100\rangle$$

Application de H_a sur le premier qubit :

$$|\psi_0^{'}\rangle = H_a|\psi\rangle|0\rangle|0\rangle = \alpha H_a|000\rangle + \beta H_a|100\rangle = \alpha|+00\rangle + \beta|-00\rangle$$

$$|\psi_0^{'}\rangle = \frac{1}{\sqrt{2}}(\alpha(|000\rangle + |100\rangle) + \beta(|000\rangle - |100\rangle)$$

Application des deux portes CNOT :

$$|\psi_0^{''}\rangle = \frac{1}{\sqrt{2}}(\alpha(|000\rangle + |111\rangle) + \beta(|000\rangle - |111\rangle) = \frac{1}{\sqrt{2}}((\alpha+\beta)|000\rangle + (\alpha-\beta)|111\rangle))$$

Triple application de H :

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}((\alpha+\beta)H_aH_bH_c|000\rangle + (\alpha-\beta)H_aH_bH_c|111\rangle))$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}((\alpha+\beta)|+++\rangle + (\alpha-\beta)|---\rangle))$$

Erreur de phase sur le premier qubit :

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}((\alpha+\beta)|-++\rangle + (\alpha-\beta)|+--\rangle))$$

Triple application de H :

$$|\psi_{2_2}^{'}\rangle = \frac{1}{\sqrt{2}}((\alpha+\beta)|100\rangle + (\alpha-\beta)|011\rangle))$$

Application des deux portes CNOT :

$$|\psi_2^{''}\rangle = \frac{1}{\sqrt{2}}((\alpha+\beta)|111\rangle + (\alpha-\beta)|011\rangle))$$

Application de TOFFOLI :

$$|\psi_2^{'''}\rangle = \frac{1}{\sqrt{2}}((\alpha+\beta)|011\rangle + (\alpha-\beta)|111\rangle))$$

Application de H sur le premier qubit :

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}((\alpha+\beta)|+11\rangle + (\alpha-\beta)|-11\rangle)) = \frac{1}{\sqrt{2}}(\alpha(|+\rangle+|-\rangle)+\beta(|+\rangle-|-\rangle))|11\rangle$$

Nous obtenons l'état final séparable :

$$|\psi_3\rangle = (\alpha|0\rangle + \beta|1\rangle)|11\rangle = |\psi\rangle|11\rangle$$

L'état du premier qubit est donc rétabli et le changement de l'état des deux autres qubits indique la présence de l'erreur. Ici-bas la simulation du code à deux qubit :

 # Chargement des packages

```
> with(Feynman): with(LinearAlgebra):Digits:=20:
```

 # Nomination de la procédure et liste de ses paramètres

```
code3qubit:=proc(n) local
Qo,CN,Qoa,CN1,Q1,T,Xo,Id,Xa,Xb,Xc,Q2a,Q3a,Q31,Q3aa,Ba,Bb,Bc,
va,vb,vc,X,Q2b,Q2c,Q3b,Q3bb,Q32,Q3c,Q3cc,Q33,Q2d,Q3d,Q3dd,Q34,Bd,vd:
```

 # Préparation des qubits

```
Qo:=Feynman_evaluate("Kronecker product",<a,b>,<1,0>,<1,0>):
```

 # Codage

```
CN:=Feynman_quantum_operator(3,"cnot",[1,2]):Qoa:=CN.Qo:
CN1:=Feynman_quantum_operator(3,"cnot",[1,3]):Q1:=CN1.Qoa:
T:=Feynman_quantum_operator(3,"ccn",[3,2,1]):
```

 # Erreur

```
X:=Feynman_quantum_operator("X"): Id:=Feynman_quantum_operator("I"):
Xa:= Feynman_evaluate("Kronecker product",X,Id,Id):
Xb:= Feynman_evaluate("Kronecker product",Id,X,Id): Xc:=Feynman_evaluate("Kronecker
product",Id,Id,X):
```

 # Décodage et correction

```
if n=1 then Q2a:=Xa.Q1:Q3a:=CN1.Q2a: Q3aa:=CN.Q3a: Q31:=T.Q3aa:
Ba:=Feynman_evaluate("Kronecker product",<a,b>,<0,1>,<0,1>):
va:=evalb(Equal(Q31,Ba)): if va=true then print("L'erreur sur le premier qubit est
corrigée");fi;fi; if n=2 then Q2b:=Xb.Q1: Q3b:=CN1.Q2b: Q3bb:=CN.Q3b: Q32:=T.Q3bb:
Bb:=Feynman_evaluate("Kronecker product",<a,b>,<0,1>,<1,0>):
vb:=evalb(Equal(Q32,Bb)): if vb=true then print("L'erreur sur le second qubit est corrigée");
fi; fi; if n=3 then Q2c:=Xc.Q1:Q3c:=CN1.Q2c: Q3cc:=CN.Q3c:
Q33:=T.Q3cc: Bc:=Feynman_evaluate("Kronecker product",<a,b>,<1,0>,<0,1>):
vc:=evalb(Equal(Q33,Bc)):  if vc=true then print("L'erreur sur le troisième qubit est
corrigée");fi;fi;if n=4 then Q2d:=Q1:Q3d:=CN1.Q2d:Q3dd:=CN.Q3d: Q34:=T.Q3dd;
Bd:=Feynman_evaluate("Kronecker product",<a,b>,<1,0>,<1,0>):
vd:=evalb(Equal(Q34,Bd)): if vd=true then print("No error");fi;fi; end proc;
```

 # Exécution de la procédure

```
code3qubit(1);code3qubit(2);code3qubit(3);code3qubit(4);
```

Welcome to Feynman (April 2008)

"L'erreur sur le premier qubit est corrigée

"L'erreur sur le second qubit est corrigée

"L'erreur sur le troisième qubit est corrigée

"Pas d'erreur"

Annexe E : Code correcteur de Shor à neuf qubits

Ce code décrit dans [1] et [R1], utilise neuf qubits pour corriger une seule erreur de type X, Y ou Z sur un seul qubit entre les instants t_2 et t_3. Il est schématisé par le circuit de la figure suivante [21] :

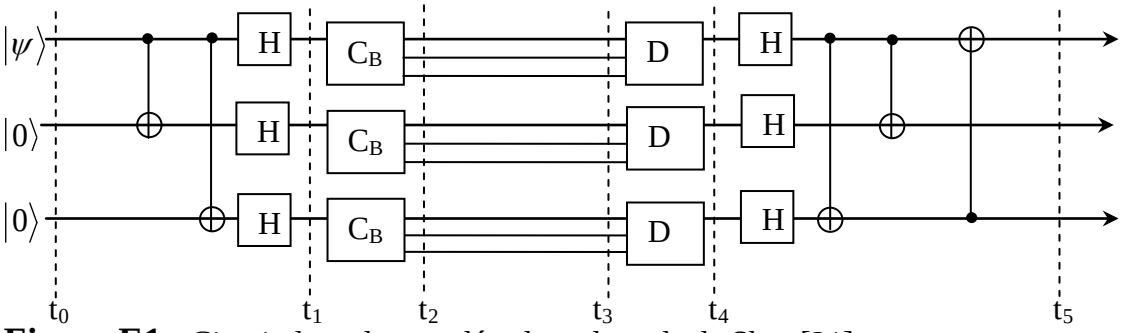

Figure E1 : Circuit de codage et décodage du code de Shor [21].

L'information utile est stockée sur le premier qubit d'état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Les huit autres qubits initialisés à $|0\rangle$ sont des accessoires utilisés dans le processus de correction des erreurs et peuvent après être supprimés. Les boites C_B et D_B sont appelées boites de codage et de décodage respectivement. Elles sont équivalentes aux circuits suivants :

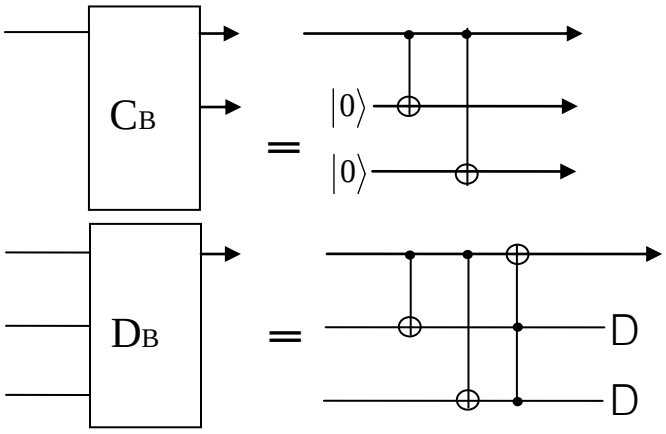

Figure E2 : Boites de codage (C_B) et décodage (D_B) [21] .

Nous allons décrire ici-bas le protocole qui corrige une erreur X, Y ou Z sur un qubit parmi les neuf utilisés dans le code de Shor. Déterminons l'état du système à l'instant t_2.

L'état initial séparable du système :

$$|\psi\rangle|0\rangle|0\rangle = \alpha|000\rangle + \beta|100\rangle$$

Application des deux portes CNOT :

$$|\psi_0\rangle = \alpha|000\rangle + \beta|111\rangle$$

Triple application de H :

$$|\psi_0^{'}\rangle = \alpha|+++\rangle + \beta|---\rangle$$

Rajout des six qubits :

$$\left|\psi_0^{''}\right\rangle = (\alpha\left|+00\right\rangle^{\otimes 3} + \beta\left|-00\right\rangle^{\otimes 3}) = \frac{1}{2^{3/2}}(\alpha(\left|000\right\rangle + \left|100\right\rangle)^{\otimes 3} + \beta(\left|000\right\rangle - \left|100\right\rangle^{\otimes 3}$$ Triple

application de la boite C_B :

$$\left|\psi_1\right\rangle = (\alpha\left|+00+00+00\right\rangle + \beta\left|-00-00-00\right\rangle) = \frac{1}{2^{3/2}}(\alpha(\left|000\right\rangle + \left|111\right\rangle)^3 + \beta(\left|000\right\rangle - \left|111\right\rangle)^3)$$

Erreur X sur le premier qubit

L'état global devient :

$$\left|\psi_2\right\rangle = \frac{1}{2^{3/2}}(\alpha(\left|100\right\rangle + \left|011\right\rangle)(\left|000\right\rangle + \left|111\right\rangle)^{\otimes 2} + \beta(\left|100\right\rangle - \left|011\right\rangle)(\left|000\right\rangle - \left|111\right\rangle)^{\otimes 2})$$

Application des deux portes CNOT de chaque boite D_B :

$$\left|\psi_2\right\rangle = \frac{1}{2^{3/2}}(\alpha(\left|111\right\rangle + \left|011\right\rangle)(\left|000\right\rangle + \left|100\right\rangle)^{\otimes 2} + \beta(\left|111\right\rangle - \left|011\right\rangle)(\left|000\right\rangle - \left|100\right\rangle)^{\otimes 2})$$

Application de la porte Toffoli de chaque boite D_B :

$$\left|\psi_2^{'}\right\rangle = \frac{1}{2^{3/2}}(\alpha(\left|011\right\rangle + \left|111\right\rangle)(\left|000\right\rangle + \left|100\right\rangle)^{\otimes 2} + \beta(\left|011\right\rangle - \left|111\right\rangle)(\left|000\right\rangle - \left|100\right\rangle)^{\otimes 2})$$

Triple application de H sur les trois premiers qubits :

$$\frac{1}{2^{3/2}}(\alpha(\left|+11\right\rangle + \left|-11\right\rangle)(\left|+00\right\rangle + \left|-00\right\rangle)^{\otimes 2} + \beta(\left|+11\right\rangle - \left|-11\right\rangle)(\left|+00\right\rangle - \left|-00\right\rangle)^{\otimes 2})$$

$$\alpha\left|011\right\rangle(\left|000\right\rangle)^{\otimes 2} + \beta\left|111\right\rangle(\left|100\right\rangle)^{\otimes 2} = (\alpha\left|000\right\rangle + \beta\left|111\right\rangle)\left|11\right\rangle(\left|00\right\rangle)^{\otimes 2}$$

Application des deux portes CNOT :

$$(\alpha\left|000\right\rangle + \beta\left|100\right\rangle)\left|11\right\rangle(\left|00\right\rangle)^{\otimes 2}$$

Application de la porte Toffoli :

$$(\alpha\left|000\right\rangle + \beta\left|100\right\rangle)\left|11\right\rangle(\left|00\right\rangle)^{\otimes 2} = (\alpha\left|0\right\rangle + \beta\left|1\right\rangle)\left|00\right\rangle\left|11\right\rangle(\left|00\right\rangle)^{\otimes 2} = \left|\psi\right\rangle\left|00\right\rangle\left|11\right\rangle(\left|00\right\rangle)^{\otimes 2}$$

On a donc rétabli l'état $\left|\psi\right\rangle$ du premier qubit qui porte l'information qui nous intéresse alors que le changement d'état de deux des huit qubits auxiliaires constitue le syndrome d'erreur.

Erreur Z sur le premier qubit

Avant erreur :

$$\left|\psi_1\right\rangle = \frac{1}{2^{3/2}}(\alpha(\left|000\right\rangle + \left|111\right\rangle)^{\otimes 3} + \beta(\left|000\right\rangle - \left|111\right\rangle)^{\otimes 3})$$

Après erreur :

$$\left|\psi_1^{'}\right\rangle = \frac{1}{2^{3/2}}(\alpha(\left|000\right\rangle + \left|-111\right\rangle)(\left|000\right\rangle + \left|111\right\rangle)^{\otimes 2} + \beta(\left|000\right\rangle - \left|-111\right\rangle)(\left|000\right\rangle - \left|111\right\rangle)^{\otimes 2})$$

$$\left|\psi_1^{'}\right\rangle = \frac{1}{2^{3/2}}(\alpha(\left|000\right\rangle - \left|111\right\rangle)(\left|000\right\rangle + \left|111\right\rangle)^{\otimes 2} + \beta(\left|000\right\rangle + \left|111\right\rangle)(\left|000\right\rangle - \left|111\right\rangle)^{\otimes 2})$$

Application des deux portes CNOT de chaque boite D_B :

$$\frac{1}{2^{3/2}}(\alpha(\left|000\right\rangle - \left|100\right\rangle)(\left|000\right\rangle + \left|100\right\rangle)^{\otimes 2} + \beta(\left|000\right\rangle + \left|100\right\rangle)(\left|000\right\rangle - \left|100\right\rangle)^{\otimes 2})$$

Application de la porte Toffoli de chaque boite D_B :

$$\frac{1}{2^{3/2}}(\alpha(\left|000\right\rangle - \left|100\right\rangle)(\left|000\right\rangle + \left|100\right\rangle)^{\otimes 2} + \beta(\left|000\right\rangle + \left|100\right\rangle)(\left|000\right\rangle - \left|100\right\rangle)^{\otimes 2})$$

Triple application de H sur les trois premiers qubits :

$$\frac{1}{2^{3/2}}(\alpha(\left|+00\right\rangle - \left|-00\right\rangle)(\left|+00\right\rangle + \left|-00\right\rangle)^{\otimes 2} + \beta(\left|+00\right\rangle + \left|-00\right\rangle)(\left|+00\right\rangle - \left|-00\right\rangle)^{\otimes 2})$$

$$\frac{1}{2^{3/2}}(\alpha(\left|+\right\rangle - \left|-\right\rangle)(\left|+\right\rangle + \left|-\right\rangle)^{\otimes 2} + \beta(\left|+\right\rangle + \left|-\right\rangle)(\left|+\right\rangle - \left|-\right\rangle)^{\otimes 2}\left|00\right\rangle^{\otimes 3}$$

$$(\alpha\left|1\right\rangle\left|0\right\rangle^{\otimes 2} + \beta\left|0\right\rangle\left|1\right\rangle^{\otimes 2})\left|00\right\rangle^{\otimes 3} = (\alpha\left|100\right\rangle + \beta\left|011\right\rangle)\left|00\right\rangle^{\otimes 3}$$

Application des deux portes CNOT :

$$(\alpha\left|111\right\rangle + \beta\left|011\right\rangle)\left|00\right\rangle^{\otimes 3}$$

Application de la porte Toffoli :

$$\left|\psi_3\right\rangle = (\alpha\left|011\right\rangle + \beta\left|111\right\rangle)\left|00\right\rangle^{\otimes 3} = (\alpha\left|0\right\rangle + \beta\left|1\right\rangle)\left|11\right\rangle\left|00\right\rangle^{\otimes 3}$$

Nous obtenons finalement :

$$\left|\psi_3\right\rangle = \left|\psi\right\rangle\left|11\right\rangle\left|00\right\rangle^{\otimes 3}$$

L'état du premier qubit est rétabli alors que le syndrome d'erreur se trouve sur les second et troisième qubit initiaux qui ont changé d'état. Les six qubits accessoires retrouvent quant à eux leur état initial $\left|0\right\rangle$.

Erreur Y sur le premier qubit

L'erreur Y produit les transformations suivantes :

$$Y\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = i\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = i\begin{pmatrix}-\beta\\ \alpha\end{pmatrix} \quad \text{donc} \quad Y\begin{pmatrix}1\\ 0\end{pmatrix} = i\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = i\begin{pmatrix}0\\ 1\end{pmatrix} \quad \text{et}$$

$Y\begin{pmatrix}0\\ 1\end{pmatrix} = i\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = i\begin{pmatrix}-1\\ 0\end{pmatrix}$ ou bien $Y\left|0\right\rangle = i\left|1\right\rangle$ et $Y\left|1\right\rangle = -i\left|0\right\rangle$.

Avant erreur :

$$\left|\psi_1\right\rangle = \frac{1}{2^{3/2}}(\alpha(\left|000\right\rangle + \left|111\right\rangle)^{\otimes 3} + \beta(\left|000\right\rangle - \left|111\right\rangle)^{\otimes 3})$$

$$\left|\psi_1\right\rangle = \frac{1}{2^{3/2}}(\alpha(\left|000\right\rangle + \left|111\right\rangle)(\left|000\right\rangle + \left|111\right\rangle)^{\otimes 2} + \beta(\left|000\right\rangle - \left|111\right\rangle)(\left|000\right\rangle - \left|111\right\rangle)^{\otimes 2})$$

Après erreur :

$$\left|\psi_1^{'}\right\rangle = \frac{1}{2^{3/2}}(\alpha(i\left|100\right\rangle - i\left|011\right\rangle)(\left|000\right\rangle + \left|111\right\rangle)^{\otimes 2} + \beta(i\left|100\right\rangle + i\left|011\right\rangle)(\left|000\right\rangle - \left|111\right\rangle)^{\otimes 2})$$

Application des deux portes CNOT de chaque boite D_B :

$$\frac{1}{2^{3/2}}(\alpha(i\left|111\right\rangle - i\left|011\right\rangle)(\left|000\right\rangle + \left|100\right\rangle)^{\otimes 2} + \beta(i\left|111\right\rangle + i\left|011\right\rangle)(\left|000\right\rangle - \left|100\right\rangle)^{\otimes 2})$$

Application de la porte Toffoli de chaque boite D_B :

$$\frac{1}{2^{3/2}}(\alpha(i\left|011\right\rangle - i\left|111\right\rangle)(\left|000\right\rangle + \left|100\right\rangle)^{\otimes 2} + \beta(i\left|011\right\rangle + i\left|111\right\rangle)(\left|000\right\rangle - \left|100\right\rangle)^{\otimes 2})$$ Triple application de H sur les trois premiers qubits :

$$\frac{1}{2^{3/2}}(\alpha(i\left|+11\right\rangle - i\left|-11\right\rangle)(\left|+00\right\rangle + \left|-00\right\rangle)^{\otimes 2} + \beta(i\left|+11\right\rangle + i\left|-11\right\rangle)(\left|+00\right\rangle - \left|-00\right\rangle)^{\otimes 2})$$

$$\frac{1}{2^{3/2}}(\alpha(i\left|+\right\rangle - i\left|-\right\rangle)(\left|+\right\rangle + \left|-\right\rangle)^{\otimes 2}\left|11\right\rangle\left|00\right\rangle^{\otimes 2} + \beta(i\left|+\right\rangle + i\left|-\right\rangle)(\left|+\right\rangle - \left|-\right\rangle)^{\otimes 2}\left|11\right\rangle\left|00\right\rangle^{\otimes 2})$$

$$\alpha i\left|1\right\rangle\left|0\right\rangle^{\otimes 2}\left|11\right\rangle\left|00\right\rangle^{\otimes 2} + \beta i\left|0\right\rangle\left|1\right\rangle^{\otimes 2}\left|11\right\rangle\left|00\right\rangle^{\otimes 2} = i(\alpha\left|100\right\rangle + \beta\left|011\right\rangle)\left|11\right\rangle\left|00\right\rangle^{\otimes 2}$$

Application des deux portes CNOT :

$$i(\alpha\left|111\right\rangle + \beta\left|011\right\rangle)\left|11\right\rangle\left|00\right\rangle^{\otimes 2}$$

Application de la porte Toffoli :

$$\left|\psi_3\right\rangle = i(\alpha\left|011\right\rangle + \beta\left|111\right\rangle)\left|11\right\rangle\left|00\right\rangle^{\otimes 2} = i\left|\psi\right\rangle\left|11\right\rangle\left|11\right\rangle\left|00\right\rangle^{\otimes 2}$$

L'état du premier qubit est rétabli alors que le syndrome d'erreur se trouve sur les second et troisième qubit initiaux et sur deux des six qubits accessoires.

E.1 Simulation du code de Shor (erreur sur un qubit)

Le code de Shor décrit dans **[1]** possède huit générateurs :

$M_1=Z_1Z_2$; $M_2=Z_2Z_3$; $M_3=Z_4Z_5$; $M_4=Z_5Z_6$; $M_5=Z_7Z_8$;
$M_6=Z_8Z_9$; $M_7=X_1X_2X_3X_4X_5X_6$; $M_8=X_4X_5X_6X_7X_8X_9$

 # Chargement des packages

```
>with(Feynman): with(LinearAlgebra): with(Typesetting): Digits := 20:
# Nomination de la procédure et liste de ses paramètres
Shor:=proc(Co,Cx,Cy,Cz,n,k)
local Psio,H,X,Y,Z,X1,Z1,X2,Z2,X3,Z3,X4,Z4,X5,Z5,X6,Z6,X7,Z7,
X8,Z8,X9, Z9,X16,X49,Id,CN,CN1,Psioa,Ha,Psiob,Psioc,Psiod, CN2,
CN3,CN4,CN5,CN6, CN7,E,Ex,Ey,Ez,Psi1,Psi2,Psi1a,Psi2a,Psi2b,
Psi2c,Psi2d, Psi2dd,Hb,Psi3a,Psi3, Psi3b,Psi33,T1,T2,T3,T4,A,P1,P2:
# Etat initial
Psio:=Feynman_evaluate("Kronecker product",<a,b>,<1,0>,<1,0>):
# Codage
H:=Feynman_quantum_operator("H"):
CN :=Feynman_quantum_operator(3,"cnot",[1,2]):
```

```
CN1:=Feynman_quantum_operator(3,"cnot",[1,3]):
Psioa :=CN1.CN.Psio:
Ha:=Feynman_quantum_operator("HHH"):
Psiob:=Ha.Psioa:
A:=Feynman_evaluate("Kronecker power",<1,0>,6):
Psioc:=Feynman_evaluate("Kronecker product",Psiob,A):
P1:=Feynman_quantum_operator("permute",[1,4,5,2,6,7,3,8,9]):
Psiod:=P1.Psioc:
CN2:=Feynman_quantum_operator(9,"cnot",[1,2]):
CN3:=Feynman_quantum_operator(9,"cnot",[1,3]):
CN4:=Feynman_quantum_operator(9,"cnot",[4,5]):
CN5:= Feynman_quantum_operator(9,"cnot",[4,6]):
CN6:=Feynman_quantum_operator(9,"cnot",[7,8]):
CN7:= Feynman_quantum_operator(9,"cnot",[7,9]):
Psi1a1:=CN6.Psiod:
Psi1a2:= CN4.Psi1a1:
Psi1a3:= CN2.Psi1a2:
Psi1a4:=CN7.Psi1a3:
Psi1a5:=CN5Psi1a4:
Psi1:=CN3.Psi1a5:
# Operateurs d'erreur
X:= Feynman_quantum_operator("X"):
Y:= Feynman_quantum_operator("Y"):
Z:=Feynman_quantum_operator("Z"):
Id:=Feynman_quantum_operator("IIIIIIIII"):
if n=0 then print("No error");
Ex:= Id:Ey:= Id:Ez:= Id:end if:
if n=1 then if Cx=1 then print("X error on first qubit");end if:
if Cy=1 then print("Y error on first qubit");end if:
if Cz=1 then print("Z error on first qubit");end if:
if Cx<1 and Cy<1 and Cz<1 then print("Error on first qubit");end if:
Ex:=Feynman_quantum_operator(9,"X",[1]):
Ey:=- I.Feynman_quantum_operator(9,"Y",[1])):
Ez:=Feynman_quantum_operator(9,"Z",[1]):end if:
if n=2 then if Cx=1 then print("X error on second qubit"):end if:
if Cy=1 then print("Y error on second qubit"):end if:
if Cz=1 then print("Z error on second qubit"):end if:
if Cx<1 and Cy<1 and Cz<1 then print("Error on second qubit"):end if:
Ex:=Feynman_quantum_operator(9,"X",[2]):
Ey:=-I.Feynman_quantum_operator(9,"Y",[2])):
Ez:= Feynman_quantum_operator(9,"Z",[2]):end if:
if n=3 then if Cx=1 then print("X error on third qubit");end if:
if Cy=1 then print("Y error on third qubit");end if:
if Cz=1 then print("Z error on third qubit");end if:
if Cx<1 and Cy<1 and Cz<1 then print("Error on third qubit");end if:
Ex:=Feynman_quantum_operator(9,"X",[3]):
Ey:=-I.Feynman_quantum_operator(9,"Y",[3])):
Ez:=Feynman_quantum_operator(9,"Z",[3]):end if:
if n=4 then if Cx=1 then print("X error on forth qubit");end if:
```

```
if Cy=1 then print("Y error on forth qubit");end if:
if Cz=1 then print("Z error on forth qubit");end if:
if Cx<1 and Cy<1 and Cz<1 then print("Error on forth qubit");end if:
Ex:= Feynman_quantum_operator(9,"X",[4]):
Ey:=-I.Feynman_quantum_operator(9,"Y", [4])):
Ez:= Feynman_quantum_operator(9,"Z",[4]):end if:
if n=5 then if Cx=1 then print("X error on fifth qubit");end if:
if Cy=1 then print("Y error on fifth qubit");end if:
if Cz=1 then print("Z error on fifth qubit");end if:
if Cx<1 and Cy<1 and Cz<1 then print("Error on fifth qubit");end if:
Ex:= Feynman_quantum_operator(9,"X",[5]):
Ey:=-I.Feynman_quantum_operator(9,"Y",[5])):
Ez:= Feynman_quantum_operator(9,"Z",[5]):end if:
if n=6 then if Cx=1 then print("X error on sixth qubit");end if:
if Cy=1 then print("Y error on sixth qubit");end if:
if Cz=1 then print("Z error on sixth qubit");end if:
if Cx<1 and Cy<1 and Cz<1 then print("Error on sixth qubit");end if:
Ex:= Feynman_quantum_operator(9,"X",[6]):
Ey:=-I.Feynman_quantum_operator(9,"Y",[6])):
Ez:=Feynman_quantum_operator(9,"Z",[6]):end if:
if n=7 then if Cx = 1 then print("X error on seventh qubit");end if:
if Cy=1 then print("Y error on seventh qubit");end if:
if Cz=1 then print("Z error on seventh qubit");end if:
if Cx<1 and Cy<1 and Cz<1 then print("Error on seventh qubit");end if:
Ex:= Feynman_quantum_operator(9,"X",[7]):
Ey:=-I, Feynman_quantum_operator(9,"Y",[7])):
Ez:= Feynman_quantum_operator(9,"Z",[7]):end if:
if n=8 then if Cx=1 then print("X error on eight qubit");end if:
if Cy=1 then print("Y error on eight qubit");end if:
if Cz=1 then print("Z error on eight qubit");end if:
if Cx<1 and Cy<1 and Cz<1 then print("Error on eight qubit");end if:
Ex:=Feynman_quantum_operator(9, "X", [8]):
Ey:=-I.Feynman_quantum_operator(9,"Y",[8])):
Ez:= Feynman_quantum_operator(9,"Z",[8]):end if:
if n=9 then if Cx=1 then print("X error on ninth qubit");end if:
if Cy=1 then print("Y error on ninth qubit");end if:
if Cz=1 then print("Z error on ninth qubit");end if:
if Cx<1 and Cy<1 and Cz<1 then print("Error on ninth qubit");end if:
Ex:=Feynman_quantum_operator(9,"X",[9]):
Ey:=-I.Feynman_quantum_operator(9,"Y",[9])):
Ez:= Feynman_quantum_operator(9,"Z",[9]):end if:
# Erreur
E:=Co.Id+Cx.Ex+Cy.Ey+Cz.Ez :
Psi2 :=E.Psi1:
if k = 0 then print("Correction before decoding");
# Gates for error detection and correction
Z1 := Feynman_quantum_operator(9,"Z",[1]):
Z2 := Feynman_quantum_operator(9,"Z",[2]):
Z3 := Feynman_quantum_operator(9,"Z",[3]):
```

```
Z4 := Feynman_quantum_operator(9, "Z", [4]):
Z5 := Feynman_quantum_operator(9, "Z", [5]):
Z6 := Feynman_quantum_operator(9, "Z", [6]):
Z7 := Feynman_quantum_operator(9, "Z", [7]):
Z8 := Feynman_quantum_operator(9,"Z",[8]):
Z9 := Feynman_quantum_operator(9, "Z", [9]):
X1:=Feynman_quantum_operator(9, "X", [1]):
X2:=Feynman_quantum_operator(9,"X",[2]):
X3:=Feynman_quantum_operator(9,"X",[3]):
X4 := Feynman_quantum_operator(9, "X", [4]):
X5 := Feynman_quantum_operator(9, "X", [5]):
X6:=Feynman_quantum_operator(9,"X",[6]):
X7:=Feynman_quantum_operator(9,"X",[7]):
X8:=Feynman_quantum_operator(9,"X",[8]):
X9:=Feynman_quantum_operator(9,"X",[9]):
X161:= Feynman_quantum_operator(9,"XXX",[1,2,3]):
X162:= Feynman_quantum_operator(9,"XXX",[4,5,6]):
X491:= Feynman_quantum_operator(9,"XXX",[4,5,6]):
X492:= Feynman_quantum_operator(9,"XXX",[7,8,9]):
```

 # Détection et correction d'erreur X

```
if evalb(Equal(Z1.Z2.Psi2,Psi2)) = true
and evalb(Equal(Z2.Z3.Psi2,Psi2))= true
and evalb(Equal(Z4.Z5.Psi2,Psi2))= true
and evalb(Equal(Z5.Z6.Psi2,Psi2))= true
and evalb(Equal(Z7.Z8.Psi2,Psi2))=true
and evalb(Equal(Z8.Z9.Psi2,Psi2)) = true then
Psi2a:=Psi2:end if:
if evalb(Equal (Z1.Z2.Psi2,Psi2))=false
and evalb(Equal(Z2.Z3.Psi2,Psi2)) = true then
Psi2a:=X1.Psi2:end if:
if evalb(Equal (Z1.Z2.Psi2,Psi2))=false
and evalb(Equal(Z2.Z3.Psi2,Psi2))=false then
Psi2a:=X2.Psi2: end if:
if evalb(Equal (Z1.Z2), Psi2), Psi2)) = true
and evalb(Equal(Z2, Z3), Psi2), Psi2)) = false
then Psi2a :=X3.Psi2 end if:
if evalb(Equal(Z4.Z5.Psi2, Psi2)) = false
and evalb(Equal(Z5.Z6.Psi2, Psi2)) = true then
Psi2a :=X4.Psi2:end if:
if evalb(Equal(Z4.Z5.Psi2, Psi2))=false
and evalb(Equal (Z5.Z6.Psi2, Psi2) = false then
Psi2a :=X5, Psi2) end if:
if evalb(Equal(Z4.Z5.Psi2), Psi2)) = true
and evalb(Equal (Z5.Z6.Psi2, Psi2) = false then
Psi2a :=X6.Psi2: end if:
if evalb(Equal(Z7.Z8.Psi2,Psi2))=false
and evalb(Equal(Z8.Z9,Psi2,Psi2))=true then
Psi2a:=X7.Psi2:end if:
if evalb(Equal(Z7.Z8.Psi2,Psi2))=false
```

```
and evalb(Equal(Z8.Z9.Psi2,Psi2)) = false then
Psi2a:=X8.Psi2: end if: if evalb(Equal(Z7.Z8.Psi2, Psi2))=true
and evalb(Equal(Z8.Z9.Psi2,Psi2))=false then
Psi2a:=X9.Psi2:end if:
# Détection et correction d'erreur Z
if evalb(Equal(X162.X161.Psi2a,Psi2a))=true
and evalb(Equal(X492.X491.Psi2a,Psi2a))=true then
Psi2b:=Psi2a:end if:
if evalb(Equal(X162.X161.Psi2a,Psi2a))=false
and evalb(Equal(X492.X491.Psi2a, Psi2a)) = true then
Psi2b1:=Z3.Psi2a:
Psi2b2:=Z2.Psi2b1:
Psi2b:=Z1.Psi2b2: end if:
if evalb(Equal(X162.X161.Psi2a, Psi2a))=false
and evalb(Equal(X492.X491.Psi2a,Psi2a))=false then
Psi2b1:=Z6.Psi2a:
Psi2b2:=Z5.Psi2b1:
Psi2b:=Z4.Psi2b2: end if:
if evalb(Equal(X162.X161.Psi2a, Psi2a))=true
and evalb(Equal(X492.X491.Psi2a,Psi2a))=false then
Psi2b1:=Z9.Psi2a:
Psi2b2:=Z8.Psi2b1:
Psi2b:=Z7.Psi2b2: end if:
end if:
if k=1 then print("Decoding without correction");
Psi2b:=Psi2:end if:
# Décodage
T1:=Feynman_quantum_operator(9,"ccn",[2,3,1]):
T2:=Feynman_quantum_operator(9,"ccn",[5,6,4]):
T3:=Feynman_quantum_operator(9,"ccn",[8,9,7]):
Psi2c1:=CN6.Psi2b:
Psi2c2:=CN4.Psi2c1:
Psi2c3:=CN2.Psi2c2:
Psi2d1:=CN7.Psi2c :
Psi2d2:=CN5.Psi2d1 :
Psi2d:=CN3.Psi2d2 :
Psi2dd1:=T3.Psi2d :
Psi2dd2:=T2.Psi2d1 :
Psi2dd:=T1.Psi2dd2 :
P2:= Feynman_quantum_operator("permute", [1,4,7,2,3,5,6,8,9]):
Psi3a:=P2.Psi2dd :
Hb := Feynman_quantum_operator(9,"HHH",[1,2,3]):
Psi3b:=Hb.Psi3a :
Psi31:=CN3.Psi3b :
Psi32:=CN2.Psi31 :
Psi3:=T1.Psi32 :
# Affichage de l'état final dans la notation de Dirac
Psi33:=simplify(Feynman_print(Psi3)):
print(Psi3afterdecoding = Psi33);
end proc:
```

E.2 : Code de Shor à neuf qubits (erreur sur deux qubit)

```
# Erreur sur deux qubits (Psi1 est l'état codé dans Annexe E-1)
X:= Feynman_quantum_operator("X");
Y:= Feynman_quantum_operator("Y");
Z:= Feynman_quantum_operator("Z");
Y:= -I.Feynman_quantum_operator("Y");
Id:= Feynman_quantum_operator("I");
# Erreur X et Z sur qubits 2 et 1 respectivement
Psi21 := Feynman_quantum_operator(9, "XZ", [2, 1]).Psi1;
# Correction par l'opérateur Y sur qubit 2 (même syndrome)
Psi2 :=Feynman_quantum_operator(9, "Y", [2]).Psi21;
# Décodage
T1:=Feynman_quantum_operator(9,"ccn",[2,3,1]):
T2:=Feynman_quantum_operator(9,"ccn",[5,6,4]):
T3:=Feynman_quantum_operator(9,"ccn",[8,9,7]):
Psi21:=CN6.Psi2:
Psi22:=CN4.Psi21:
Psi23:=CN2.Psi22:
Psi24:=CN7.Psi23 :
Psi25:=CN5.Psi24 :
Psi26:=CN3.Psi25 :
Psi27:=T3.Psi26 :
Psi28:=T2.Psi27 :
Psi29:=T1.Psi28 :
P2:= Feynman_quantum_operator("permute", [1,4,7,2,3,5,6,8,9]):
Psi30:=P2.Psi29 :
Hb :=Feynman_quantum_operator(9,"HHH",[1,2,3]):
Psi31:=Hb.Psi30 :
Psi32:=CN3.Psi31 :
Psi33:=CN2.Psi32 :
Psi3:=T1.Psi33 :
# Affichage de l'état final dans la notation de Dirac
Psi33:=simplify(Feynman_print(Psi3)):
print(Psi3doublerror = Psi33);
```

Output : Psi3doubleerrors = a|000000000> + b|100000000>

= (a|0>+b |1>)|00000000> = $|\Psi_1\rangle \ldots |\Psi_9\rangle$

On déduit donc l'état du qubit protégé $|\Psi_1\rangle = a\,|0\rangle + b\,|1\rangle$. Cette correction permet donc de recouvrir l'état initial de ce qubit, ce qui est mentionné sur le tableau 15b en seconde ligne par l'opérateur identité I_i.

Annexe F : Code de Steane à sept qubits

F.1 : Codage

Le circuit de codage de ce code est décrit dans les références [1][16] et [17] et ses six générateurs sont : $M_1=X_4X_5X_6X_7$; $M_2= X_2X_3X_6X_7$; $M_3=X_1X_3X_5X_7$
$M_4=Z_4Z_5Z_6Z_7$; $M_2= Z_2Z_3Z_6Z_7$; $M_6=Z_1Z_3Z_5Z_7$

 # Chargement des packages

```
> with(Feynman); with(LinearAlgebra); with(Typesetting); Digits := 20;
```

 # Etat initial

```
Psio:=Feynman_evaluate("Kronecker product", <a,b>,<1,0>,<1,0>,<1,0>,<1,0>,<1,0>,<1,0>) ;
```

 # Codage

```
H := Feynman_quantum_operator("H");
CN := Feynman_quantum_operator(7, "cnot", [1, 2]);
CN1 := Feynman_quantum_operator(7, "cnot", [1, 3]);
Psioa1 := CN.Psio; Psioa := CN1.Psioa1;
Ha := Feynman_quantum_operator(7, "HHH", [5, 6, 7]);
Psiob := Ha.Psioa; CN2 := Feynman_quantum_operator(7, "cnot", [7, 1]);
CN3 := Feynman_quantum_operator(7, "cnot", [7, 2]);
CN4 := Feynman_quantum_operator(7, "cnot", [7, 4]);
CN5 := Feynman_quantum_operator(7, "cnot", [6, 1]);
CN6 := Feynman_quantum_operator(7, "cnot", [6, 3]);
CN7 := Feynman_quantum_operator(7, "cnot", [6, 4]);
CN8 := Feynman_quantum_operator(7, "cnot", [5, 2]);
CN9 := Feynman_quantum_operator(7, "cnot", [5, 3]);
CN10 := Feynman_quantum_operator(7, "cnot", [5, 4]);
Psi1a := CN2.Psiob; Psi2a := CN3.Psi1a;
Psi3a := CN4.Psi2a; Psi4a := CN5.Psi3a;
Psi5a := CN6.Psi4a; Psi6a := CN7.Psi5a;
Psi7a := CN8.Psi6a; Psi8a := CN9.Psi7a;
Psi1 := CN10.Psi8a; Psi11:= Feynman_printPsi1; printPsiSteane = Psi11;
```

Output: On obtient en notation de Dirac l'état codé du système de sept qubits :

PsiSteane = (√2/4) [a|0000000> + a|0001111> + b|0010110> + b|0011001>+|0100101>+b|0101010>+a|0110011>+a|0111100>+b|1000011>+ b|1001100>+a|1010101>+a|1011010>+a|1100110>+a|1101001>+b|1110000>+b|111 1111>]

F.2 : Stabilisation de l'état codé par les générateurs

On vérifie ici que les générateurs M de ce code stabilisent l'état codé Psi1.

 # Application des générateurs

```
>Ga := Feynman_quantum_operator(7, "XXXX", [4,5,6,7]), Psi1);
Gb := Feynman_quantum_operator(7, "XXXX", [2,3,5,7]), Psi1);
Gc := Feynman_quantum_operator(7, "XXXX", [1,3,5,7]), Psi1);
Gd := Feynman_quantum_operator(7, "ZZZZ", [4,5,6,7]), Psi1);
```

```
Ge := Feynman_quantum_operator(7, "ZZZZ", [2,3,6,7]), Psi1);
Gf := Feynman_quantum_operator(7, "ZZZZ", [1,3,5,7]), Psi1);
Gaa := Feynman_print(Ga); Gbb := Feynman_print(Gb);
Gcc := Feynman_print(Gc); Gdd := Feynman_print(Gd);
Gee := Feynman_print(Ge); Gff := Feynman_print(Gf);
Psi11 := Feynman_print(Psi1); if Feynman_equal(Gaa, Psi11) = true then print("M1 true")
else print("M1 false") end if; if Feynman_equal(Gbb, Psi11) = true then print("M2 true") else
print("M2 false") end if;
if Feynman_equal(Gcc, Psi11) = true then print("M3 true") else print("M3 false") end if; if
Feynman_equal(Gdd, Psi11) = true then print("M4 true") else print("M4 false") end if; if
Feynman_equal(Gee, Psi11) = true then print("M5 true") else print("M5 false") end if; if
Feynman_equal(Gff, Psi11) = true then print("M6 true") else print("M6 false") end if;
```

Les messages obtenus en output assurent la justesse de l'état codé obtenu.

"M1 true" ; "M2 true" ; "M3 true"
"M4 true" ; "M5 true" ; "M6 true"

F.3 Double erreur de canal

Considérons l'exemple d'une erreur X sur qubits 1 et 2 corrigée comme une erreur simple X sur qubit 3 de même syndrome :

```
>X:= Feynman_quantum_operator("X");
Y:=Feynman_quantum_operator("Y"); Z:=Feynman_quantum_operator("Z");
Y:=-I.Feynman_quantum_operator("Y")); Id:=Feynman_quantum_operator("I");
Psi21:=Feynman_quantum_operator(7, "XX", [1, 2]). Psi1;
Psi2:= Feynman_quantum_operator(7, "X", [3]). Psi21;
```

F.4 Décodage

```
>Psi2a:=CN10.Psi2; Psi3a:=CN9.Psi2a; Psi4a :=CN8.Psi3a;
Psi5a:=CN7.Psi4a; Psi6a:=CN6.Psi5a; Psi7a := CN5.Psi6a;
Psi8a:= CN4.Psi7a;  Psi9a := CN3.Psi8a; Psi10a := CN2.Psi9a;
Psi11a := CN1.Psi10a; Psi12a := CN.Psi11a; Psi3 := Ha.Psi12a;
Psi33 := Feynman_print(Psi3); print(Psidec = Psi33);
Psioo := Feynman_print(Psio); Feynman_equal(Psioo.Psi33);
```

On obtient en output les deux états codés perturbé et non perturbé avec le message Fail qui indique leur différence:

Psidec = b |0010000> + a |1010000> ; Psioo = a |0000000> + b |1000000>
FAIL

L'état perturbé Psidec permet de déduire l'état du qubit protégé :

Psidec = (b|0>+a |1>)|010000>=$|\Psi_1>\ldots|\Psi_7>$, donc : $|\Psi_1>$= b|0>+a |1>=X (a|0>+b |1>).

Le qubit protégé a donc subi une erreur X comme indiqué sur la table 14a en seconde ligne.

Annexe G : Code à cinq qubits

Le circuit de codage de ce code est décrit dans les références [1] et [14] et ses quatre générateurs qui sont :

$$M_1 = X_1X_2Z_3Z_5 \ ; \ M_2= Z_1X_2X_3Z_4 \ ; \ M_3= Z_2X_3X_4Z_5 \ ; \ M_4= Z_1Z_3X_4X_5$$

G.1 : Codage

```
with(Feynman); with(LinearAlgebra); Digits := 20;
G0:=Feynman_evaluate("Kronecker product",<a,b>,<1,0>,<1,0>,<1,0>,<1,0>);
G1:=Feynman_quantum_operator(5,"HHHH",[2,3,4,5]),G0);
G2:=Feynman_quantum_operator(5,"cn",[2,1]).G1;
G3:=Feynman_quantum_operator(5,"H",[1]).G2;
G4:=Feynman_quantum_operator(5,"cn",[3,2]).G3;
G5:=Feynman_quantum_operator(5,"cn",[3,1]).G4;
G6:=Feynman_quantum_operator(5,"H",[2]).G5;
G7:=Feynman_quantum_operator(5,"cn",[4,3]).G6;
G8:=Feynman_quantum_operator(5,"cn",[4,2]).G7;
G9:=Feynman_quantum_operator(5,"HH",[2,3]).G8;
G10:=Feynman_quantum_operator(5,"cn",[5,4]).G9;
G11:=Feynman_quantum_operator(5,"cn",[5,3]).G10;
G12:=Feynman_quantum_operator(5,"cn",[5,1]).G11;
G13:=Feynman_quantum_operator(5,"HH",[1,3]).G12;
G133:=Feynman_print(G13);
```

On obtient en output l'état codé du système à cinq qubits :

G133 : = (1/4)[-|11111>b + |01000>b + |01011>b - |11011>a + |00011>a- |00101>a - |01001>a + |00100>b + |00110>a - |11100>b+|10000>b+|10001>a- |01010>a + |11000>a - |10011>b - |11101>a + |00000>a-|10100>a--|10111>a+ |11010>b - |11110>a + |00010>b - |00111>b + |00001>b - |10010>a - |11001>b +|10110>b + |01100>a +|01101>b - |01110>b - |01111>a+|10101>b]

Ou bien :

G133 : = (1/4)[a{- |11011> + |00011>-|00101> - |01001>+ |00110>+|10001>-|01010> + |11000>- |11101> + |00000>-|10100>-|10111>-|11110>-|10010>+|01100>- |01111>}+b{-|11111>+|01000>+|01011>+ |00100> - |11100>+|10000> - |10011> + |11010> +|00010>-|00111>+ |00001> -|11001> +|10110> +|01101> - |01110> + |10101>}]

On peut écrire G133 = (1/4)[a$|0_l\rangle$ + b$|1_l\rangle$] avec $|0_l\rangle$ et $|1_l\rangle$ les qubits logiques de ce code donnés par :

$|0_l\rangle$ = - |11011> + |00011>-|00101> - |01001>+ |00110>+|10001>-|01010> + |11000>- |11101> + |00000>-|10100>-|10111>-|11110>- |10010>+ |01100>- |01111>

$|1_l\rangle$ = -|11111>+|01000>+|01011>+ |00100> - |11100>+|10000> - |10011> + |11010> +|00010>-|00111>+ |00001> -|11001> +|10110> +|01101> - |01110> + |10101>

G.2 : Stabilisation

 # Application des générateurs

```
Ga := Feynman_quantum_operator(5, "XXZZ", [1, 2, 3, 5]), G13);
Gb := Feynman_quantum_operator(5, "ZXXZ", [1, 2, 3, 4]), G13);
Gc := Feynman_quantum_operator(5, "ZXXZ", [2, 3, 4, 5]), G13);
Gd := Feynman_quantum_operator(5, "ZZXX", [1, 3, 4, 5]), G13);
Gaa := Feynman_print(Ga); Gbb := Feynman_print(Gb);
Gcc := Feynman_print(Gc); Gdd := Feynman_print(Gd);
G133 := Feynman_print(G13); if Feynman_equal(Gaa, G133) = true then print("M1 true")
else print("M1 false") end if; if Feynman_equal(Gbb, G133) = true then print("M2 true") else
print("M2 false") end if; if Feynman_equal(Gcc, G133) = true then print("M3 true") else
print("M3 false") end if; if Feynman_equal(Gdd, G133) = true then print("M4 true") else
print("M4 false") end if
```

Les messages obtenus en output assurent la justesse de l'état codé obtenu :

Output :

"M1 true" ; "M2 true" ; "M3 true" ; "M4 true"

G.3 : Détection et correction d'erreur

Considérons l'exemple de la double erreur de canal X_4X_5 ayant le même syndrome que les erreurs Z_1Z_3 et Y_2 :

 # Détection

```
>G14:=Feynman_quantum_operator(5,"XX",[4,5]).G13;
G15 := Feynman_quantum_operator(5, "XXZZ", [1, 2, 3, 5]).G14;
G16 := Feynman_quantum_operator(5, "ZXXZ", [1, 2, 3, 4]), G14);
G17 := Feynman_quantum_operator(5, "ZXXZ", [2, 3, 4, 5]).G14;
G18 := Feynman_quantum_operator(5, "ZZXX", [1, 3, 4, 5]).G14;
G155:=Feynman_print(G15);G166:=Feynman_print(G16);
G177:=Feynman_print(G17);G188:=Feynman_print(G18);
G144:= Feynman_print(G14);if Feynman_equal(G155, -G144) = true and
Feynman_equal(G166, -G144) = true and Feynman_equal(G177, -G144) = true and
Feynman_equal(G188, G144) = true then print("Error Y2 or X4X5 or Z1Z3 uncorrected ")
end if;
```

On obtient en output le message donnant la liste d'erreurs possibles :

"Error Y2 or X4X5 or Z1Z3 uncorrected "

 # Correction comme l'erreur simple de même syndrome Y_2
G19 := I.Feynman_quantum_operator(5, "Y", [2])).G14 :

G.4 : Décodage

```
G20:=(Feynman_quantum_operator(5,"HH",[1,3]).G19);
G21:=Feynman_quantum_operator(5,"cn",[5,1]).G20;
G22:=(Feynman_quantum_operator(5,"cn",[5,3]).G21;
G23:=Feynman_quantum_operator(5,"cn",[5,4].G22;
G24:=Feynman_quantum_operator(5,"HH",[2,3]).G23;
G25:=Feynman_quantum_operator(5,"cn",[4,2]).G24;
G26:=Feynman_quantum_operator(5,"cn",[4,3]).G25;
G27:=Feynman_quantum_operator(5,"H",[2]).G26);
G28:=Feynman_quantum_operator(5,"cn",[3,1]).G27;
G29:=Feynman_quantum_operator(5,"cn",[3,2]).G28;
G30:=Feynman_quantum_operator(5,"H",[1]).G29;
G31 := (Feynman_quantum_operator(5, "cn", [2, 1]), G30);
G32 := (Feynman_quantum_operator(5, "HHHH", [2, 3, 4, 5]), G31);
G322 := Feynman_print(G32);
G00 := Feynman_print(G0); Feynman_equal(G322, G00);
```

On obtient en output les deux états codés perturbé et non perturbé avec le message Fail qui indique leur différence :

G322 := |00000>b-|10000>a ; G00 :=|00000>a+|10000>b ; Fail

L'état perturbé G322 permet de déduire l'état du qubit protégé :

G322 = (b|0>-a |1>)0000>=$|\Psi_1>\ldots|\Psi_5>$, donc :

$|\Psi_1>$= b|0>-a |1>=Y (a|0>+b |1>). Le qubit protégé a donc subi une erreur Y comme indiqué sur la table 12 à la ligne 12.

Annexe H : Code convolutif à cinq qubits

H.1 : Circuit de codage

Le circuit de codage est simulé en accord avec le diagramme schématique de la figure 9. Les boites H et Z représentent les portes Hadamard et Z respectivement. La porte H ne s'applique pas sur les états Q1, Q2 and Q3 car ces trois qubits portant l'information utile se présentent au codeur dans un état qui est déjà superposé. La simulation commence par appeler le programme Feynman qu'on a intégré comme librairie dans le logiciel Maple 11 et la subroutine Linear Algebra. L'état Q_0 est le produit tensoriel de l'état de cinq qubits (qubit 2 à qubit 12 sur la figure 9) initialement à l'état $|0\rangle$ (symbolisé par <1,0>) puis transformés en état superposé par l'application de la porte H puis Z. L'état global de cinq qubits Q_8 est obtenu après application de toutes les portes conditionnelles Controlled-X,Y ou Z à l'exception des deux dernières portes CZ sur qubit 6 (couche 5 et 6 respectivement dans figure 9). La cause est la présence d'une porte CZ sur qubit 6 (couche 4) avec qubit 4 comme contrôleur. On note que Q2 et Q3 sont obtenus après application de la porte conditionnelle Controlled-Y en deux parties (CN puis CZ). Le codage des qubits 7 à 12 est entamé par l'application de H et Z (couche 1 et 2) qui produit l'état Q9 à six qubits. L'état Q20 est produit en appliquant toute les portes conditionnelles sauf CZ sur qubit 7 (couche 5) à cause de la porte CZ sur qubit 6 (couche 5) où qubit 7 joue le rôle de contrôleur. Si on applique CZ sur qubit 7 dans la couche 5 son état changerait et entrainerait une erreur qui se propagerait jusqu'à l'état codé final. Afin d'achever le codage du groupe total de onze qubits on construit le produit tensoriel Q_{21} des états Q_8 et Q_{20}. On applique alors sur lui les quatre portes CZ restantes ([6,5] , [2,5] ,[7,6] et [3,5] dans respectivement les couches 4,5,5 et 6) pour obtenir l'état codé final Q_{25} du système intriqué à onze qubits. La même procédure est reprise pour le codage du qubit 13 à qubit 17 pour construire l'état Q26 à dix-sept qubits. Ici-bas la simulation avec en premier l'explication de quelques instructions utilisées :

H.1.1 Explications

Z:= Feynman_quantum_operator("Z"): Matrice de la porte Z.
H:=Feynman_quantum_operator("H"): Matrice de la porte Hadamard.
Qo: = Feynman_evaluate("Kronecker product",Z.H.<1,0>,Z.H.<1,0>,
H.<1,0>,<a1,b1>,H.<1,0>): Produit tensoriel des états de cinq qubits avec <1,0> = $|0\rangle$ et <a1,b1> = $a_1|0\rangle+b_1|1\rangle$.
Q1:=Feynman_quantum_operator(5,"cn",[5,4]).Qo: Porte conditionnelle Conrolled-not (cn) sur l'état à cinq qubits Q_0 qui produit l'état Q1. Le qubit 4 (cible) change de valeur si le qubit 5 (contrôleur) vaut 1.
Q2:=Feynman_quantum_operator(5,"cz",[1,4]).Q1: Porte conditionnelle Conrolled-Z (cz) sur l'état à cinq qubits Q_1 qui produit l'état Q_2. Le qubit 4 (cible) change de valeur si le qubit 1 (contrôleur) vaut 1.

H.1.2 : Simulation

```
> with(Feynman): with(LinearAlgebra): Digits:=20:
Z:= Feynman_quantum_operator("Z"): H:=Feynman_quantum_operator("H"):
```

Codage de qubit 2 à qubit 6

```
Qo:=Feynman_evaluate("Kronecker product",Z.H.<1,0>,Z.H.<1,0>,H.<1,0>,
<a1,b1>,H.<1,0>):
Q1:=Feynman_quantum_operator(5,"cn",[5,4]).Qo:
Q2:=Feynman_quantum_operator(5,"cz",[1,4]).Q1:
Q31:=I.Feynman_quantum_operator(5,"cn",[1,4]).Q2:
Q3:=I.Feynman_quantum_operator(5,"cz",[1,5]).Q31:
Q4:=Feynman_quantum_operator(5,"cz",[2,1]).Q3:
Q5:=Feynman_quantum_operator(5,"cz",[2,4]).Q4:
Q6:=I.Feynman_quantum_operator(5,"cn",[2,4]).Q5:
Q7:=Feynman_quantum_operator(5,"cz",[3,2]).Q6:
Q8:=Feynman_quantum_operator(5,"cn",[3,4]).Q7:
```

 # Codage de qubit 7 à qubit 12

```
Q9:=Feynman_evaluate("Kronecker product",Z.H.<1,0>,Z.H.<1,0>,H.<1,0>,
<a2,b2>,H.<1,0>,Z.H.<1,0>):
Q10:=Feynman_quantum_operator(6,"cn",[5,4]).Q9:
Q11:=Feynman_quantum_operator(6,"cz",[6,5]).Q10:
Q12:=Feynman_quantum_operator(6,"cz",[1,4]).Q11:
Q13:=I.Feynman_quantum_operator(6,"cn",[1,4]).Q12:
Q14:=Feynman_quantum_operator(6,"cz",[1,5]).Q13:
Q15:=Feynman_quantum_operator(6,"cz",[2,4]).Q14:
Q16:=I.Feynman_quantum_operator(6,"cn",[2,4]).Q15:
Q17:=Feynman_quantum_operator(6,"cz",[2,5]).Q16:
Q18:=Feynman_quantum_operator(6,"cz",[3,2]).Q17:
Q19:=Feynman_quantum_operator(6,"cn",[3,4]).Q18:
Q20:=Feynman_quantum_operator(6,"cz",[3,5]).Q19:
```

 # Codage de qubit 1 à qubit 12

```
Q21:=Feynman_evaluate("Kronecker product",Q8,Q20):
Q22:=Feynman_quantum_operator(11,"cz",[6,5]).Q21:
Q23:=Feynman_quantum_operator(11,"cz",[2,5]).Q22:
Q24:=Feynman_quantum_operator(11,"cz",[7,6]).Q23:
Q25:=Feynman_quantum_operator(11,"cz",[3,5]).Q24:
```

 # Codage de qubit 13 à qubit 17

```
Q251:=Feynman evaluate("Kronecker product",Z.H.<1,0>,H.<1,0>,<a3,b3>,
H.<1,0>,Z.H.<1,0>):
Q252:=Feynman_quantum_operator(15,"cn",[15,14]).Q251:
```

 # Codage de qubit 2 à qubit 16

```
Q253:=Feynman_evaluate("Kronecker product",Q25,Q252):
Q254:=Feynman_quantum_operator(15,"cz",[11,14]).Q253:
Q255:=I.Feynman_quantum_operator(15,"cn",[11,14]).Q254:
Q256:=Feynman_quantum_operator(15,"cz",[11,15]).Q255:
Q257:=Feynman_quantum_operator(15,"cz",[12,11]).Q256:
Q258:=Feynman_quantum_operator(15,"cz",[12,14]).Q257:
Q259:=I.Feynman_quantum_operator(15,"cn",[12,14]).Q258:
Q260:=Feynman_quantum_operator(15,"cz",[12,15]).Q259:
Q261:=Feynman_quantum_operator(15,"cz",[13,12]).Q260:
Q262:=Feynman_quantum_operator(15,"cn",[13,14]).Q261:
Q26:=Feynman_quantum_operator(15,"cz",[13,15]).Q262:
```

H.2 : Stabilisation de l'état codé $|Q25\rangle$

Avant de procéder au décodage du premier groupe de onze qubits, on doit d'abord vérifier que leur état jΘ25i a été correctement construit. A cette fin, on lui applique les générateurs M_1 à M_8 pour s'assurer que $M|Q25\rangle = |Q25\rangle$ pour $1 \leq i \leq 8$. Le générateur M_1=ZXXZ est appliqué de la manière suivante : la première porte Z est supprimée car le premier qubit n'est pas envoyé, le second qubit (qui devient qubit 1) subit l'opérateur X et l'on obtient l'état S1a. Les qubits 2 et 3 subissent respectivement les opérateurs X et Z, ce qui donne l'état S1. Cette division de la procédure en deux étapes réduit le temps d'exécution. Enfin, on vérifie l'égalité $|S1\rangle = |Q25\rangle$à l'aide d'un message "M1 true". On procède de la même manière pour les autres générateurs qui donnent tous le même message "Mi true", prouvant la justesse du codage simulé. Ici-bas la simulation avec en premier l'explication de quelques instructions utilisées :

H.2.1 : Explications

S1a:=Feynman_quantum_operator(11,"X",[1]).Q25: Application de X sur le premier qubit du système à onze qubits. Notons que cet opérateur X est à la seconde position dans le générateur M1=ZXXZIIIIIIII. Il occupe ici la première position car le premier qubit a été supprimé.
S1:=Feynman_quantum_operator(11,"XZ",[2,3]).S1a : Application de X et Z sur respectivement le premier et second qubit .

H.2.2 : Simulation

```
# Générateur M1
S1a:=Feynman_quantum_operator(11,"X",[1]).Q25:
S1:=Feynman_quantum_operator(11,"XZ",[2,3]).S1a:
if evalb(Equal(S1,Q25))=true then print("M1 true") else print("M1 false";
# Générateur M2
S2a:=Feynman_quantum_operator(11,"ZX",[1,2]).Q25:
S2:=Feynman_quantum_operator(11,"XZ",[3,4]).S2a:
if evalb(Equal(S2,Q25))=true then print("M2 true") else print("M2 false";
# Générateur M3
S3a:=Feynman_quantum_operator(11,"ZX",[2,3]).Q25:
S3:=Feynman_quantum_operator(11,"XZ",[4,5]).S3a:
if evalb(Equal(S3,Q25))=true then print("M3 true") else print("M3 false";
# Générateur M4
S4a:=Feynman_quantum_operator(11,"ZX",[3,4]).Q25:
S4:=Feynman_quantum_operator(11,"XZ",[5,6]).S4a:
if evalb(Equal(S4,Q25))=true then print("M4 true") else print("M4 false";
# Générateur M5
S5a:=Feynman_quantum_operator(11,"ZX",[5,6]).Q25:
S5:=Feynman_quantum_operator(11,"XZ",[7,8]).S5a:
if evalb(Equal(S5,Q25))=true then print("M5 true") else print("M5 false";
# Générateur M6
S6a:=Feynman_quantum_operator(11,"ZX",[6,7]).Q25:
S6:=Feynman_quantum_operator(11,"XZ",[8,9]).S6a:
```

```
if evalb(Equal(S6,Q25))=true then print("M6 true") else print("M6 false";
# Générateur M7
S7a:=Feynman_quantum_operator(11,"ZX",[7,8]).Q25:
S7:=Feynman_quantum_operator(11,"XZ",[9,10]).S7a:
if evalb(Equal(S7,Q25))=true then print("M7 true") else print("M7 false";
# Générateur M8
S8a:=Feynman_quantum_operator(11,"ZX",[8,9]).Q25:
S8:=Feynman_quantum_operator(11,"XZ",[10,11]).S8a:
if evalb(Equal(S8,Q25))=true then print("M8 true") else print("M8 false");
```

Output :

Welcome to Feynman (April 2008)
"M1 true", "M2 true", "M3 true", "M4 true", "M5 true", "M6 true", "M7 true","M8 true"

H.3 : Extraction des syndromes (générateurs M_1 à M_8)

Nous simulons ici la procédure d'extraction des syndromes. En premier, on introduit une erreur sur l'état $|Q25\rangle$, par exemple une erreur X sur le premier qubit ou bien une double erreur X sur qubit 1 et qubit 8. Ensuite, on rajoute un nouveau qubit dans un état superposé (H.<1,0>=$|+\rangle$) en construisant un produit tensoriel $|Q28\rangle$ avec l'état infecté $|Q27\rangle$. Ce qubit jouera le rôle d'une sonde permettant au récepteur de savoir si l'état reçu $|Q27\rangle$ est infecté sans le perturber (voir section VI-4). Le générateur M_1 est conditionnellement appliqué en deux étapes pour obtenir l'état à douze qubits $|Q28b\rangle$ (le symbole 'C' indique une application conditionnelle de X ou XZ sur le second ([1,2]) ou le troisième et quatrième [1,3,4] qubits avec qubit 1 comme contrôleur). L'application de H sur le premier qubit de l'état $|Q281b\rangle$ (12,"H",[1]) va le transformer en un simple état $|0\rangle$ ou $|1\rangle$ dans le nouvel état à douze qubits $|Q281c\rangle$. Enfin, on détermine l'état du qubit rajouté par l'application sur lui de la porte Z : $|Q281\rangle=|0\rangle|Q27\rangle=|Q281c\rangle$ ou $|Q281\rangle=-|0\rangle|Q27\rangle=-|Q281c\rangle$. Nous présentons ici-bas la simulation avec en premier l'explication de quelques instructions utilisées.

H.3.1 : Explications

Q27:=Feynman_quantum_operator(11,"X",[1]).Q25: Production d'une erreur de canal X sur le premier qubit .
Q28:=Feynman_evaluate("Kronecker product",H.<1,0>,Q27): L'état superposé$|+\rangle$= H.<1,0> est rajouté à l'état codé reçu Q27.
Q281a:=Feynman_quantum_operator(12,"c","X",[1,2]).Q28:
Q281b:=Feynman_quantum_operator(12,"c","XZ",[1,3,4]**).Q281a:** Générateur M_1 conditionnellement appliqué sur l'état infecté Q28=$|+\rangle$Q27.
Q281c:=Feynman_quantum_operator(12,"H",[1]).Q281b: Application de H sur le qubit rajouté.
Q281:=Feynman_quantum_operator(12,"Z",[1]).Q281c: Application de Z sur le qubit rajouté.
Q281a:=Feynman_quantum_operator(12,"c","X",[1,2]).Q27: Porte X appliquée conditionnellement ("c") sur qubit 2 (si le premier qubit vaut 1) dans le système à douze qubits.

Q281b:=Feynman_quantum_operator(12,"c","XZ",[1,3,4]**).Q281a :** On applique conditionnellement X et Z sur respectivement le troisième et quatrième qubits. On note que c'est ici l'application conditionnelle du générateur M_1.
Q281c:=Feynman_quantum_operator(12,"H",[1]).Q281b: On applique H sur le premier qubit pour obtenir un état simple $H|+\rangle = |0+\rangle$ ou $H|-\rangle = |1\rangle$:
Q281:=Feynman_quantum_operator(12,"Z",[1]).Q281c: Application de Z sur le premier qubit qui donne $Z|0\rangle = |0\rangle$ ou $Z|1\rangle = -|1\rangle$:

H.3.2 : Simulation

 # Erreur unique entre qubit 2 et qubit 12.
Q27:=Feynman_quantum_operator(11,"X",[1]).Q25:
 # Double erreur entre qubit 2 et qubit 12
Q27:=Feynman_quantum_operator(11,"XX",[1,8]).Q25:
 # Rajout d'un qubit en état superposé.
Q28:=Feynman_evaluate("Kronecker product",H.<1,0>,Q27):
 # Générateur M_1
 # Application conditionnelle de M_1.
Q281a:=Feynman_quantum_operator(12,"c","X",[1,2]).Q28:
Q281b:=Feynman_quantum_operator(12,"c","XZ",[1,3,4]).Q281a:
 # Application de H et Z sur le qubit rajouté.
Q281c:=Feynman_quantum_operator(12,"H",[1]).Q281b:
Q281:=Feynman_quantum_operator(12,"Z",[1]).Q281c:
 # Générateur M_2
Q282a:=Feynman_quantum_operator(12,"c","ZX",[1,2,3]).Q28:
Q282b:=Feynman_quantum_operator(12,"c","XZ",[1,4,5]).Q282a:
Q282c:=Feynman_quantum_operator(12,"H",[1]).Q282b:
Q282:=Feynman_quantum_operator(12,"Z",[1]).Q282c:
 # Générateur M_3
Q283a:=Feynman_quantum_operator(12,"c","ZX",[1,3,4]).Q28:
Q283b:=Feynman_quantum_operator(12,"c","XZ",[1,5,6]).Q283a:
Q283c:=Feynman_quantum_operator(12,"H",[1]).Q283b:
Q283:=Feynman_quantum_operator(12,"Z",[1]).Q283c:
 # Générateur M_4
Q284a:=Feynman_quantum_operator(12,"c","ZX",[1,4,5]).Q28:
Q284b:=Feynman_quantum_operator(12,"c","XZ",[1,6,7]).Q284a:
Q284c:=Feynman_quantum_operator(12,"H",[1]).Q284b:
Q284:=Feynman_quantum_operator(12,"Z",[1]).Q284c:
 # Générateur M_5
Q285a:=Feynman_quantum_operator(12,"c","ZX",[1,6,7]).Q28:
Q285b:=Feynman_quantum_operator(12,"c","XZ",[1,8,9]).Q285a:
Q285c:=Feynman_quantum_operator(12,"H",[1]).Q285b:
Q285:=Feynman_quantum_operator(12,"Z",[1]).Q285c:
 # Générateur M_6
Q286a:=Feynman_quantum_operator(12,"c","ZX",[1,7,8]).Q28:
Q286b:=Feynman_quantum_operator(12,"c","XZ",[1,9,10]).Q286a:

Q286c:=Feynman_quantum_operator(12,"H",[1]).Q286b:
Q286:=Feynman_quantum_operator(12,"Z",[1]).Q286c:
 # Générateur M_7

```
Q287a:=Feynman_quantum_operator(12,"c","ZX",[1,8,9]).Q28:
Q287b:=Feynman_quantum_operator(12,"c","XZ",[1,10,11]).Q287a:
Q287c:=Feynman_quantum_operator(12,"H",[1]).Q287b:
Q287:=Feynman_quantum_operator(12,"Z",[1]).Q287c:
# Générateur M8
Q288a:=Feynman_quantum_operator(12,"c","ZX",[1,9,10]).Q28:
Q288b:=Feynman_quantum_operator(12,"c","XZ",[1,11,12]).Q288a:
Q288c:=Feynman_quantum_operator(12,"H",[1]).Q288b:
Q288:=Feynman_quantum_operator(12,"Z",[1]).Q288c:
# Générateur M9
# Erreur
Q27a:=Feynman_quantum_operator(16,"X",[1]).Q26:
# Rajout d'un qubit en état superposé.
Q28a:=Feynman_evaluate("Kronecker product",H.<1,0>,Q27a):
Q289a:=Feynman_quantum_operator(17,"c","ZX",[1,10,11]).Q28a:
Q289b:=Feynman_quantum_operator(17,"c","XZ",[1,12,13]).Q289a:
Q289c:=Feynman_quantum_operator(17,"H",[1]).Q289b:
Q289:=Feynman_quantum_operator(17,"Z",[1]).Q289c:
# Générateur M10
Q290a:=Feynman_quantum_operator(17,"c","ZX",[1,11,12]).Q28a:
Q290b:=Feynman_quantum_operator(17,"c","XZ",[1,13,14]).Q290a:
Q290c:=Feynman_quantum_operator(17,"H",[1]).Q290b:
Q290:=Feynman_quantum_operator(17,"Z",[1]).Q290c:
```

H.4 : Détection et correction d'erreur de qubit 2 à qubit 12

Les syndromes sont disposés dans les tables 3a, 3b et 3c de manière à accélérer la détection par le récepteur de l'erreur de canal sur l'état codé transmis, afin d'éviter la décohérence. Les erreurs Y_3 et Z_2Z_4 sont mises dans la première ligne car elles contiennent la valeur 1 dans les quatre premières positions de leur syndrome. L'erreur Z_2X_5 est en seconde position car les trois premières valeurs de leur syndrome de même que la cinquième sont égales à 1. Ainsi de suite jusqu'à l'erreur Z_3X_6 qui a la valeur 0 dans la première position de son syndrome. On continue de placer les erreurs telles que les valeurs 1 des syndromes soient décalées de ligne en ligne vers la droite jusqu'à la dernière erreur X_1X_4 qui n'a aucune valeur 1 dans son syndrome. Cette disposition permet d'identifier pour une erreur donnée E, les générateurs à mesurer afin de la détecter en cherchant dans les tables d'autres erreurs ayant des syndromes proches de celui de E. On présente ici-bas la procédure de détection pour les deux premières (table 3a) et deux dernières lignes (table 3c) avec d'abord l'explication de quelques instructions.

H.4.1: Explications

- if evalb(Equal(Q281,-Q281c))=true and evalb(Equal(Q282,-Q282c))=true and evalb(Equal(Q283,-Q283c))=true and evalb(Equal(Q284,-Q284c))= true then print("Y3 or Z2Z4 error detected"):

On mesure ici les valeurs propres de générateurs nécessaires à l'identification de deux erreurs possibles: La plus probable est choisie selon le canal de transmission (une erreur simple est plus probable qu'une erreur double).

- if evalb(Equal(Q281,-Q281c))=true and evalb(Equal(Q282,-Q282c))=true
and evalb(Equal(Q283,-Q283c))=true and evalb(Equal(Q285,-Q285c))=true
then Q29:=Feynman_quantum_operator(11,"ZX",[2,5]).Q27:
if evalb(Equal(Q29,Q25))=true then print("Z2X5 error detected"):
Le syndrome mesuré ici permet une identification parfaite de l'erreur de canal.

H.4.2 : Simulation

 # Détection donnant une liste de deux erreurs (table 3a)
if evalb(Equal(Q281,-Q281c))=true and evalb(Equal(Q282,-Q282c))=true
and evalb(Equal(Q283,-Q283c))=true and evalb(Equal(Q284,-Q284c))=true
then print(" Y3 or Z2Z4 error detected"):
 # Correction d'une erreur parfaitement identifiée (table 3a)
if evalb(Equal(Q281,-Q281c))=true and evalb(Equal(Q282,-Q282c))=true
and evalb(Equal(Q283,-Q283c))=true and evalb(Equal(Q285,-Q285c))=true
then Q29:=Feynman_quantum_operator(11,"ZX",[2,5]).Q27:
if evalb(Equal(Q29,Q25))=true then print("Error Z2X5 corrected") ;
 # Correction d'une erreur parfaitement identifiée (table 3c)
if evalb(Equal(Q285,Q285c))=true and evalb(Equal(Q287,Q287c))=true
and evalb(Equal(Q288,Q288c))=true and evalb(Equal(Q289,Q289c))=true
and evalb(Equal(Q290,-Q290c))=true
then Q29:=Feynman_quantum_operator(11,"ZX",[10,11]).Q27: .:
if evalb(Equal(Q29,Q25))=true then print("Error Z10X11 corrected"):.:
 # Détection d'erreur unique ou d'absence d'erreur (table 3c)
if evalb(Equal(Q281,Q281c))=true and evalb(Equal(Q282,Q282c))=true
and evalb(Equal(Q283,Q283c))=true and evalb(Equal(Q284,Q284c))=true
and evalb(Equal(Q285,Q285c))=true and evalb(Equal(Q286,Q286c))=true
and evalb(Equal(Q287,Q287c))=true and evalb(Equal(Q288,Q288c))=true
and evalb(Equal(Q289,Q289c))=true and evalb(Equal(Q290,Q290c))=true
then print("No error or error X1X4 detected") :

H.5 : Décodage de qubit 2 à qubit 12

La procédure de décodage est simulée en exécutant en sens inverse le circuit de codage de la figure 9 (couche 6 à couche 1). Ici-bas la simulation avec d'abord l'explication de quelques instructions.

H.5.1 : Explications

Q30:=Feynman_quantum_operator(11,"cz",[3,2]).Q29: La porte Z est appliquée sur qubit 2 si qubit 3 a la valeur 1.
Q31:=Feynman_quantum_operator(11,"cn",[3,4]**).Q30:** La porte X est appliquée sur qubit 4 si qubit 3 à la valeur 1.
Q47:=Feynman_quantum_operator(11,"Z",[10]).Q46: Porte Z appliquée sur qubit 10.

Q59:=Feynman_quantum_operator(11,"H",[1]).Q58: La porte H est appliquée sur le premier qubit. Notons qu'il est possible d'appliquer en une seule fois la porte H sur les neuf qubits à l'aide de l'instruction suivante:
Feynman_quantum_operator(11,"HHHHHHHHH",[1,2,3,5,6,7,8,10,11]).
Cette procédure a été évitée car son temps d'exécution est énorme.

H.5.2 : Simulation

 # Couche de portes 6
Q30:=Feynman_quantum_operator(11,"cz",[3,2]).Q29:
Q31:=Feynman_quantum_operator(11,"cn",[3,4]).Q30:
Q32:=Feynman_quantum_operator(11,"cz",[3,5]).Q31:
Q33:=Feynman_quantum_operator(11,"cz",[8,7]).Q32:
Q34:=Feynman_quantum_operator(11,"cn",[8,9]).Q33:
Q35:=Feynman_quantum_operator(11,"cz",[8,10]).Q34:
 # Couche de portes 5
Q36:=Feynman_quantum_operator(11,"cz",[2,1]).Q35:
Q37:=Feynman_quantum_operator(11,"cz",[2,4]).Q36:
Q38:=-I.Feynman_quantum_operator(11,"cn",[2,4]).Q37:
Q39:=Feynman_quantum_operator(11,"cz",[2,5]).Q38:
Q40:=Feynman_quantum_operator(11,"cz",[7,6]).Q39:
Q41:=Feynman_quantum_operator(11,"cz",[7,9]).Q340:
Q42:=-I.Feynman_quantum_operator(11,"cn",[7,9]).Q41:
Q43:=Feynman_quantum_operator(11,"cz",[7,10]).Q42:
 # Couche de portes 4
Q44:=Feynman_quantum_operator(11,"cz",[6,5]).Q43:
Q45:=Feynman_quantum_operator(11,"cz",[6,9]).Q44:
Q46:=-I.Feynman_quantum_operator(11,"cn",[6,9]).Q45:
Q47:=Feynman_quantum_operator(11,"cz",[6,10]).Q46:
Q48:=Feynman_quantum_operator(11,"cz",[1,4]).Q47:
Q49:=-I.Feynman_quantum_operator(11,"cn",[1,4]).Q48:
Q50:=Feynman_quantum_operator(11,"cz",[1,5]).Q49:
Q51:=Feynman_quantum_operator(11,"cz",[11,10]).Q50:
 # Couche de portes 3
Q52:=Feynman_quantum_operator(11,"cn",[5,4]).Q51:
Q53:=Feynman_quantum_operator(11,"cn",[10,9]).Q52:
 # Couche de portes 2
Q54:=Feynman_quantum_operator(11,"Z",[1]).Q53:
Q55:=Feynman_quantum_operator(11,"Z",[2]).Q54:
Q56:=Feynman_quantum_operator(11,"Z",[6]).Q55:
Q57:=Feynman_quantum_operator(11,"Z",[7]).Q56:
Q58:=Feynman_quantum_operator(11,"Z",[11]).Q57:
 # Couche de portes 1
Q59:=Feynman_quantum_operator(11,"H",[1]).Q58:
Q60:=Feynman_quantum_operator(11,"H",[2]).Q59:
Q61:=Feynman_quantum_operator(11,"H",[3]).Q60:
Q62:=Feynman_quantum_operator(11,"H",[5]).Q61:
Q63:=Feynman_quantum_operator(11,"H",[6]).Q62:
Q64:=Feynman_quantum_operator(11,"H",[7]).Q63:

Q65:=Feynman_quantum_operator(11,"H",[8]).Q64:
Q66:=Feynman_quantum_operator(11,"H",[10]).Q65:
Q67:=Feynman_quantum_operator(11,"H",[11]).Q66:

H.6 : Fidélité

#Comparaison entre l'état décodé et celui envoyé du système à onze qubits
 # Etat décodé (la permutation met les qubits utiles 4 et 9 en premier)
Q68:=Feynman_quantum_operator("permute",[4,9,1,2,3,5,6,7,8,10,11]).Q67 ;
 # Etat envoyé
Qo1:=Feynman_evaluate("Kronecker product",<a1,b1>, <a2,b2> , <1,0> , <1,0> , <1,0> , <1,0> , <1,0> , <1,0> , <1,0> , <1,0> , <1,0> ;
Q688:=Feynman_print(Q68) ;Qo11 := Feynman_print(Qo1) ;
 # Comparaison (Fail indique une fidélité <1)
Feynman_equal(-IQ688,Qo11) ;

Output :

$$Q688 := -\mathrm{I}\ a1\ a2\ |00110011000> - \mathrm{I}\ a1\ b2\ |01110011000> + \mathrm{I}\ b1\ a2\ |10110011000> + \mathrm{I}\ b1\ b2\ |11110011000>$$

$$Qo11 := a1\ a2\ |00000000000> + a1\ b2\ |01000000000> + b1\ a2\ |10000000000> + b1\ b2\ |11000000000>$$

FAIL

 # Etat envoyé des deux premiers qubits utiles (déduit de Qo11)
Psit := Feynman_set_register((1/2)*(a1a2*cbs("00 ")+a1b2*cbs("01")
+b1a2*cbs("10"+b1b2*cbs("11")) ;
 # Etat mesuré des deux premiers qubits utiles (déduit de Q688)
Psim := Feynman_set_register((1/2)*(-a1a2*cbs("00 ")-a1b2*cbs("01")
+b1a2*cbs("10")+b1b2*cbs("11")) ;
 # Calcul de la fidélité
F:= Feynman_measures("fidelity",Psit,Psim) ;
Output :

$$Psit := qregister\left(id, 2, \begin{bmatrix} \frac{1}{2}\ a1a2 \\ \frac{1}{2}\ a1b2 \\ \frac{1}{2}\ b1a2 \\ \frac{1}{2}\ b1b2 \end{bmatrix}\right) \qquad Psim := qregister\left(id, 2, \begin{bmatrix} -\frac{1}{2}\ a1a2 \\ -\frac{1}{2}\ a1b2 \\ \frac{1}{2}\ b1a2 \\ \frac{1}{2}\ b1b2 \end{bmatrix}\right)$$

$$F := \left|\frac{1}{4}\ a1a2\ \overline{a1a2} + \frac{1}{4}\ a1b2\ \overline{a1b2} - \frac{1}{4}\ b1a2\ \overline{b1a2} - \frac{1}{4}\ b1b2\ \overline{b1b2}\right|^2$$

Ce qui donne F=| ($|a_1|^2$-$|b_1|^2$) ($|a_2|^2$+$|b_2|^2$) |^2 avec $|a_2|^2$ +$|b_2|^2$=1. Le calcul donne F=|2$(a_1)^2$-1|^2 qui est le résultat mentionné sur la table 4 en dernière ligne.

Annexe I : Partage de secret par un état de graphe à 5 qubits

I.1 : Préparation de l'état de graphe

```
with(Feynman): with(LinearAlgebra): Digits := 20:
G1:=Feynman_evaluate("Kronecker product",<1,0>,<1,0>,<1,0>,<1,0>, <1,0>):
G21:=Feynman_quantum_operator(5,"HHH",[1,2,3].G1:
G2:=Feynman_quantum_operator(5,"HH",[4,5].G21:
G31:=Feynman_quantum_operator(5,"cz",[1,2].G2:
G32:=Feynman_quantum_operator(5,"cz",[2,3].G31:
G33:=Feynman_quantum_operator(5,"cz",[3,4].G32:
G34:=Feynman_quantum_operator(5,"cz",[4,5].G33:
G3:=Feynman_quantum_operator(5,"cz",[5,1].G34:
G411:=Feynman_quantum_operator(5,"ZZZ",[1,2,3].G3:
G41:=Feynman_quantum_operator(5, "ZZ", [4, 5]).G411:
G4 := a*G3+b*G41: G44 := Feynman_print(G4);
```

On obtient en output l'état de graphe à cinq qubits en notation de Dirac :

G44: = (√2/8) { (a+b) [-|11011> + |00000> - |00011> + |00101> + |01001> +|01010> - |11000> - |01100> - |00110> - |11101> - |11110> - |01111> - |10111> - |10001> + |10010> + |10100>] + (a-b) [|00100> + |00001> - |10110>+|01000>-|01011>+|11100> - |01101> + |11001> + |01110> + |00010> + |10000> -|11111> + |10011> - |10101> - |11010> + |00111>]}

I.2 : Codage de l'état de graphe par le code à cinq qubits

```
# Rajout des quatre qubits protecteurs
G5 := Feynman_evaluate("Kronecker product", G4,<1,0>, <1,0>,<1,0>,<1,0>);
# Positionnement des ancillas prés du premier qubit protégé
G6 := Feynman apply(operator("permute", [1, 6, 7, 8, 9, 2, 3, 4, 5]), G5);
# Codage
G711 := Feynman apply(operator(9, "H", [2]), G6);
G71 := Feynman apply(operator(9, "H", [3]), G711);
G72 := Feynman apply(operator(9, "H", [4]), G71);
G7 := Feynman apply(operator(9, "H", [5]), G72);
G8 := Feynman apply(operator(9, "can", [2, 1]), G7);
G9 := Feynman apply(operator(9, "H", [1]), G8);
G10 := Feynman apply(operator(9, "can", [3, 2]), G9);
G11 := Feynman apply(operator(9, "can", [3, 1]), G10);
G12 := Feynman apply(operator(9, "H", [2]), G11);
G13 := Feynman apply(operator(9, "can", [4, 3]), G12);
G14 := Feynman apply(operator(9, "can", [4, 2]), G13);
G151 := Feynman apply(operator(9, "H", [2]), G14);
G15 := Feynman apply(operator(9, "H", [3]), G151);
G16 := Feynman apply(operator(9, "can", [5, 4]), G15);
```

```
G17 := Feynman apply(operator(9, "can", [5, 3]), G16);
G18 := Feynman apply(operator(9, "can", [5, 1]), G17);
G191 := Feynman apply(operator(9, "H", [1]), G18);
G19 := Feynman apply(operator(9, "H", [3]), G191) ;
```

I.3 : Correction d'erreur et décodage

 # Double erreur de canal

```
G20:= Feynman applies(operator(9, "ZZ", [3,4]),G19):
```

 # Correction par l'erreur simple de même syndrome

```
G20a:=Feynman applies(operator(9,"X", [1]),G20):
```

 # Décodage

```
G211:=Feynman apply(operator(9,"H", [1]),G20a);  G21:=Feynman apply(operator(9,"H",
[3]),G211);  G22:=Feynman apply(operator(9, "can", [5,1]),G21);
G23:=Feynman_apply(qoperator(9, "cn", [5,3]),G22); G24:=Feynman_apply(qoperator(9,
"cn", [5,4]),G23);  G251:=Feynman_apply(qoperator(9, "H", [2]),G24);
G25:=Feynman_apply(qoperator(9, "H", [3]),G251);
G26:=Feynman_apply(qoperator(9,"cn", [4,2]),G25);
G27:=Feynman_apply(qoperator(9,"cn", [4,3]),G26); G28:=Feynman_apply(qoperator(9,
"H", [2]),G27); G29:=Feynman_apply(qoperator(9,"cn", [3, 1]),G28);
G30:=Feynman_apply(qoperator(9,"cn", [3, 2]),G29); G31:=Feynman_apply(qoperator(9,
"H", [1]),G30);  G32:=Feynman_apply(qoperator(9, "cn", [2, 1]),G31);
G331:=Feynman_apply(qoperator(9, "H", [4]),G32);  G33:=Feynman_apply(qoperator(9,
"H", [5]),G331);  G341:=Feynman_apply(qoperator(9, "H", [2]),G33);
G34:=Feynman_apply(qoperator(9, "H", [3]),G341);
G35:=Feynman_apply(qoperator("permute", [1,6,7, 8, 9, 2, 3, 4, 5]),G34);
G355:= Feynman_print(G35);
```