9.
Les codes correcteurs quantiques: contrôle de la décohérence due à un environnement arbitraire

Récapitulation des méthodes de contrôle de la décohérence basées sur l'observation et la manipulation de l'environnement. Insuffisance de ces méthodes pour résoudre le problème de la décohérence de l'ordinateur quantique. Une approche différente: les codes correcteurs quantiques. Leur principe et lien avec la correction d'erreur classique. Correction du basculement de phase: codage redondant d'un qubit logique dans trois qubits intriqués, détection des erreurs par mesure d'un ensemble de deux opérateurs, correction restituant le qubit initial. Amélioration de la fidélité attendue. Nombre minimum de qubits pour protéger un qubit logique de toutes les erreurs possibles à un bit. Codes obtenus par *concaténation*. Conclusion sur le caractère pratique de ces méthodes.

Caractéristiques des méthodes de contrôle de la décohérence décrites précédemment

Il est possible de ralentir les processus de décohérence d'un système quantique si on connaît son environnement et sait le mesurer ou le manipuler. Dans le cas de la gomme ou de l'asservissement quantique, on mesure l'environnement et exploite le résultat de cette mesure soit pour le corréler aux résultat de la mesure effectuée sur le système, soit pour agir de façon conditionnelle sur celui-ci. Les méthodes de modification du spectre de l'environnement ou celles du codage sans bruit impliquent la modification des caractéristiques d'un environnement connu en jouant soit sur la distribution de ses niveaux d'énergie, soit sur la symétrie de son coupage avec le système. Les méthodes de type effet Zénon ou «bang bang» assument que le temps de corrélation de l'environnement est assez long pour que l'on puisse altérer son couplage effectif au système en lui appliquant une suite rapide d'impulsions. Les méthodes d'environnements artificiels pour des ions piégés supposent enfin que l'on cherche à protéger un type d'état précis.

Aucune de ces méthodes n'apporte de réponse universelle au problème de la décohérence: comment protéger un système de qubits des effets perturbateurs d'un environnement arbitraire?

Le principe des codes correcteurs d'erreurs

L'idée est radicalement différente: on ne s'intéresse pas à l'environnement mais on observe uniquement le système. On code l'information de chaque qubit de façon redondante dans un ensemble de qubits intriqués. La décohérence modifie l'état de cet ensemble. Une mesure adéquate permet de reconnaître le type d'erreur survenue (syndrome) puis de la corriger pour restituer l'information quantique contenue dans l'état initial.

Contrairement aux méthodes précédentes, la nature de l'environnement n'importe pas. La mesure d'opérateurs du *système seul* permet de détecter les erreurs dues à des sauts quantiques décrits par un petit nombre d'opérateurs, puis de les corriger en appliquant des transformations simples.

La méthode s'apparente aux codes correcteurs de la théorie de l'information classique: coder un bit 0 ou 1 de façon redondante dans un ensemble (bit logique) 000 ou 111. Si une erreur se produit, on peut par décision «□*à la majorité*□», reconnaître la valeur du bit initial. Il n'est pas *a priori* évident que la méthode puisse se généraliser à des qubits, dont la fonction d'onde ne peut en général ni être clonée ni mesurée sans être perturbée. Nous allons montrer qu'une correction quantique est possible en utilisant les propriétés de l'intrication.

Exemple: erreur due au basculement de phase

Elle correspond au saut quantique défini par l'opérateur $_z$:

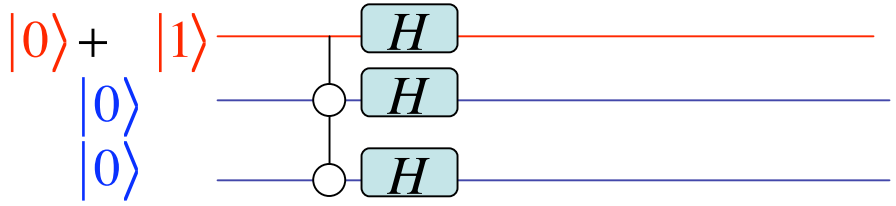
$$|0\rangle + |1\rangle \quad _z \quad |0\rangle + |1\rangle = |0\rangle \quad |1\rangle \quad (9 \quad 1)$$

Après rotation sur la sphère de Bloch (décrite par une transformation de Hadamard) cette erreur apparaît comme un basculement de la composante transversale du spin fictif associé au qubit:

$$H \quad |0\rangle + |1\rangle = |0_x\rangle + |1_x\rangle \quad _z \quad |0_x\rangle + |1_x\rangle = |1_x\rangle + |0_x\rangle \quad (9 \quad 2)$$

Le codage consiste à construire, à partir du qubit dans l'état initial et de deux ancillae initialement dans l'état 0, 3 qubits intriqués superposition de $|0_x 0_x 0_x>$ et $|1_x 1_x 1_x>$ suivant la transformation réalisée par 2 portes CNOT et 3 Hadamard:

$$|0\rangle + |1\rangle \; |00\rangle \quad |0_x 0_x 0_x\rangle + |1_x 1_x 1_x\rangle \quad (9 \quad 3)$$



Si 0 ou 1 erreur se produit sur ce qubit logique, on le trouve dans l'un des états:

$$|\ \rangle_0 = |0_x 0_x 0_x\rangle + |1_x 1_x 1_x\rangle \quad (pas\ d'erreur); \quad |\ \rangle_1 = |1_x 0_x 0_x\rangle + |0_x 1_x 1_x\rangle \quad (erreur\ sur\ bit\ 1)$$

$$|\ \rangle_2 = |0_x 1_x 0_x\rangle + |1_x 0_x 1_x\rangle \quad (erreur\ sur\ bit\ 2); |\ \rangle_3 = |0_x 0_x 1_x\rangle + |1_x 1_x 0_x\rangle \quad (erreur\ sur\ bit\ 3)$$

$$(9 \quad 4)$$

Une mesure permet alors d'identifier l'erreur sans détruire l'information initiale.

Lecture du syndrome

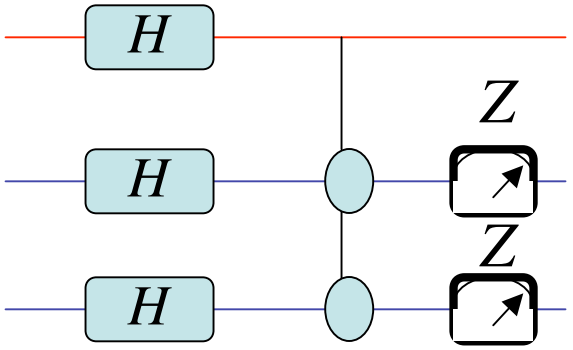
Soient les observables $X_1X_2 = {}_{x1}\ {}_{x2}$ et $X_1X_3 = {}_{x1}\ {}_{x3}$. Elles admettent pour états propres les $|\ \rangle_i\ (i=0,1,2,3)$ définis par l'équation (9-4):

$$X_1X_2|\ \rangle_0 = +|\ \rangle_0 \ ;\ X_1X_3|\ \rangle_0 = +|\ \rangle_0 \ ;\ X_1X_2|\ \rangle_1 = -|\ \rangle_1 \ ;\ X_1X_3|\ \rangle_1 = -|\ \rangle_1$$
$$X_1X_2|\ \rangle_2 = -|\ \rangle_2 \ ;\ X_1X_3|\ \rangle_2 = +|\ \rangle_2 \ ;\ X_1X_2|\ \rangle_3 = +|\ \rangle_3 \ ;\ X_1X_3|\ \rangle_3 = -|\ \rangle_3 \quad (9\text{-}5)$$

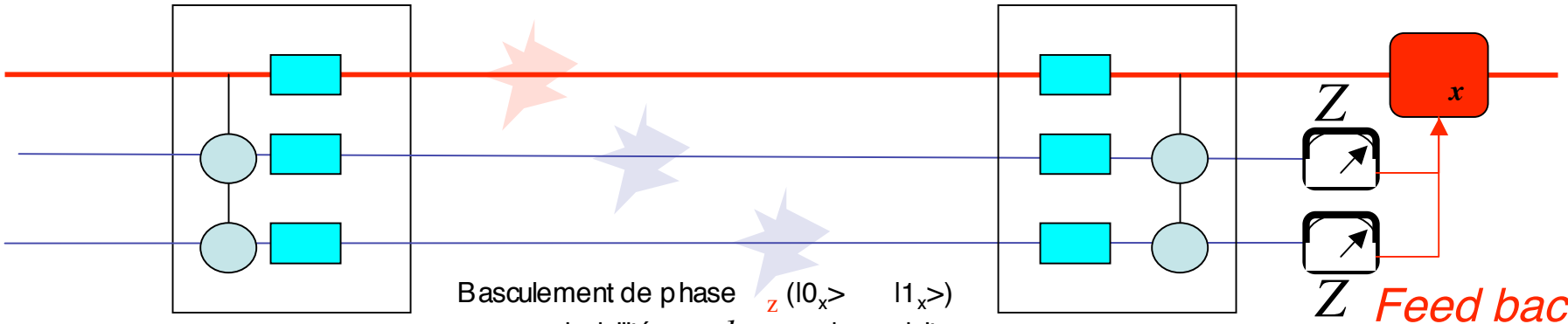
La mesure des deux observables X_1X_2 et X_1X_3 correspond donc à l'acquisition de 2 bits classique d'information indiquant la nature de l'erreur:

$$X_1X_2 = 1,\ X_1X_3 = 1 \quad pas\ d'erreur\ ; \quad X_1X_2 = -1,\ X_1X_3 = -1 \quad erreur\ sur\ bit\ 1$$
$$X_1X_2 = -1,\ X_1X_3 = 1 \quad erreur\ sur\ bit\ 2\ ; \quad X_1X_2 = 1,\ X_1X_3 = -1 \quad erreur\ sur\ bit\ 3$$
$$(9\text{-}6)$$

La mesure des observables collectives doit se faire sans mesurer individuellement les qubits, se qui conduirait à la destruction de l'information que l'on cherche à préserver. On vérifie que l'on mesure X_1X_2 et X_1X_3 à l'aide du circuit quantique ci-contre (*qubit 1: contrôle*, *qubits 2 et 3: cibles*). La mesure finale de Z sur le qubit 2 (3) donne la valeur de X_1X_2 (X_1X_3).



Récapitulation: correction du basculement de phase



Basculement de phase $_z$ (|0$_x$> |1$_x$>)
avec probabilité $p<<1$ sur un des qubits

Feed back ssi /11> (Z= -1 pour les 2 ancillae)

Préparation:

$|0\rangle + |1\rangle \; |00\rangle$ *portes* $|000\rangle + |111\rangle$

Hadamard $|0_x 0_x 0_x\rangle + |1_x 1_x 1_x\rangle$ (9 7)

1 qubit codant +2 qubits auxiliaires (ancillae)

Pas d'erreur:

$|0_x 0_x 0_x\rangle + |1_x 1_x 1_x\rangle$ *propagation sans erreur* $|0_x 0_x 0_x\rangle + |1_x 1_x 1_x\rangle$ *Hadamard+portes* $|0\rangle + |1\rangle \; |00\rangle$ (9 8)

Erreurs de phase:

$|0_x 0_x 0_x\rangle + |1_x 1_x 1_x\rangle$ *erreur de phase sur qubit 1* $|1_x 0_x 0_x\rangle + |0_x 1_x 1_x\rangle$ *Hadamard+portes* $|1\rangle + |0\rangle \; |11\rangle$

$|0_x 0_x 0_x\rangle + |1_x 1_x 1_x\rangle$ *erreur de phase sur qubit 2* $|0_x 1_x 0_x\rangle + |1_x 0_x 1_x\rangle$ *Hadamard+portes* $|0\rangle + |1\rangle \; |10\rangle$

$|0_x 0_x 0_x\rangle + |1_x 1_x 1_x\rangle$ *erreur de phase sur qubit 3* $|0_x 0_x 1_x\rangle + |1_x 1_x 0_x\rangle$ *Hadamard+portes* $|0\rangle + |1\rangle \; |01\rangle$ (9 9)

Augmentation de la fidélité par correction d'erreur

Sans correction, un qubit dans l'état | > subissant un basculement de phase avec une probabilité p est décrit par l' opérateur densité = $(1\text{-}p)$| >< | + $p\,Z$ | >< | Z. La fidélité du processus est F_0 :

$$F_0 = \min\left\{\sqrt{\langle \quad | \quad | \quad \rangle}\right\} = \min\left\{\sqrt{(1 \quad p) + p\langle \quad |Z| \quad \rangle\langle \quad |Z| \quad \rangle}\right\} = \sqrt{1 \quad p} \quad 1 \quad p/2 \quad (9 \quad 10)$$

Après correction du basculement de phase, l'opérateur densité du 1er bit devient:

$$_C = \ (1 \quad p)^3 + 3p(1 \quad p)^2 \ | \ \rangle\langle \ | + \ ' \quad (9 \quad 11)$$

Le facteur entre [ ] est la probabilité cumulée pour qu'il n'y ait eu aucune erreur (terme $(1\text{-}p)^3$) ou une erreur sur l'un des 3 qubits (terme $3p(1\text{-}p)^2$). Dans ces cas, le 1er qubit se propage sans erreur après correction. Le terme ' est la matrice densité du 1er qubit au cas ou deux erreurs ou plus se sont produites. Compte tenu du caractère positif de ' on obtient la fidélité après correction:

$$F_C = \min\left\{\sqrt{\langle \quad | \quad _C | \quad \rangle}\right\} = \sqrt{(1 \quad p)^3 + 3p(1 \quad p)^2} = (1 \quad p)\sqrt{1 + 2p} \quad 1 \quad 3p^2/2 \quad (9 \quad 12)$$

La fidélité, qui diffère de 1 par un terme linéaire en p en l'absence de correction, n'en diffère que par un terme quadratique après correction. Si on effectue la correction en un temps assez court pour que $p \sim 0{,}01$, on passe de $F_0 = 0{,}995$ à $F_c = 0{,}99985$.

Correction d'erreur arbitraire sur un qubit: nombre minimal de qubits intriqués codant un qubit logique

Nous n'avons considéré qu'un type d'erreur (basculement de phase Z). La dépolarisation la plus générale d'un qubit correspond à une transformation construite à l'aide des 4 opérateurs de Kraus I, X, Y *et* Z (voir cours 2003-2004):

$$|\ \rangle\langle\ |\quad (1\quad p_x\quad p_y\quad p_z)|\ \rangle\langle\ |+p_xX|\ \rangle\langle\ |X+p_yY|\ \rangle\langle\ |Y+p_zZ|\ \rangle\langle\ |Z \qquad (9\quad 13)$$

Généralisant l'analyse précédente, on protègera un qubit logique en le codant dans n qubits intriqués de façon que la mesure d'observables appropriées sur les $n-1$ ancillae fournisse l'information nécessaire à la détection des 3 erreurs à un bit possibles. Le nombre de situations à distinguer est égal à $1+3n$ (soit pas d'erreur, soit basculement X,Y ou Z sur l'un des n bits). Pour que ces $1+3n$ cas correspondent sans ambiguïté à des états mesurés indépendants dans l'espace de $n-1$ qubits, n doit satisfaire:

$$2^{n\ 1}\quad 3n+1\quad soit\quad n\quad 5\qquad (9\quad 14)$$

La valeur minimale est $n=5$, satisfaisant l'égalité dans (9-14). La limite établie ici pour un type particulier d'erreurs et de code, est générale. Il faut au moins 5 qubits pour protéger un qubit logique de toute erreur affectant au plus un des bits et on sait construire explicitement de tels codes. Nous ne les décrirons pas explicitement ici.

Conclusion sur les codes correcteurs

Nous avons donné le principe des codes correcteurs et montré que la propagation d'un qubit dans un environnement bruyant s'effectue avec une probabilité $1\text{-}p$ en absence de correction, en $1\text{-}cp^2$ après correction (c est une constante). La méthode repose sur le caractère *discret* des erreurs (et des syndromes). La propagation d'un qubit en présence d'un bruit arbitraire est décrite par un petit nombre d'opérateurs de Kraus, décomposables en somme d'opérateurs de Pauli. Il suffit d'associer à chacun d'eux un ensemble d'observables dont la mesure constitue le syndrome de l'erreur et de combiner cette mesure à l'exécution d'une correction. Lorsque les bits sont manipulés dans un circuit logique, il faut également tenir compte des erreurs dues aux portes. On peut, de façon équivalente, considérer que celles-ci sont parfaites, mais suivies d'erreurs sur les qubits après action des portes. Ces erreurs se corrigent suivant les mêmes principes.

En itérant le procédé, on code les bits en cascade (*concaténation*), 1 qubit logique étant d'abord protégé dans n bits intriqués, chacun de ces bits étant à son tour codé dans n bits (soit n^2 bits en tout, etc..). La probabilité d'erreur devient $1\text{-}\ cp^2$, puis $1\text{-}c'p^4$... Si p est inférieur à un seuil $\sim 10^{-5}\text{-}10^{-6}$ on peut en «concaténant» jusqu'à un niveau approprié effectuer un calcul arbitrairement long avec une probabilité finale d'erreur aussi faible que l'on veut. C'est le théorème du «*calcul tolérant aux fautes*», dont la preuve ne sera pas donnée.

Conclusion générale du cours 2004-2005

Le cours de cette année nous a appris qu'il est possible, par des méthodes variées, de contrôler et de diminuer les effets de la décohérence sur un système quantique. De nombreuses méthodes sont associées à l'observation et à la manipulation de l'environnement du système. Si elles nous apprennent beaucoup sur la nature des processus de décohérence, ces méthodes ne sont pas pratiquement applicables à la correction systématique des erreurs dans la réalisation d'un algorithme de calcul quantique comprenant un grand nombre de bits et d'opérations, en présence d'un environnement a priori inconnu.

Les codes correcteurs d'erreur quantique, inspirés par les codes classiques des ordinateurs usuels, sont d'une autre nature et répondent, en principe, aux exigences du fonctionnement d'un ordinateur quantique. Ils sont applicables à des processus généraux de décohérence, avec environnement arbitraire. Il existe un seuil fini de fidélité des opérations élémentaires au delà duquel les erreurs ne s'accumulent pas de façon critique. C'est l'existence du théorème de «*calcul tolérant aux fautes*» qui a déclenché la recherche active sur l'ordinateur quantique. Le seuil critique $(p < 10^{-5}\text{-}10^{-6})$ est cependant très faible et pose un défi considérable aux expérimentateurs. Il est loin d'être sur que ce seuil soit atteignable avec des qubits réalistes.Le codage par *concaténation* demande d'autre part des ressources énormes, exigeant que l'on sache contrôler un très grand nombre de qubits. C'est encore loin d'être le cas.