Calcul quantique universel sur qubits supraconducteurs

par

Alexandre Blais

mémoire présenté au Département de Physique en vue
de l'obtention du grade de maître ès sciences (M.Sc.)

Faculté des Sciences
Université de Sherbrooke

Sherbrooke, Québec, Canada, septembre 1999

Sommaire

Ce mémoire est consacré à la théorie de l'information quantique et, en particulier, aux ordinateurs quantiques. Les ordinateurs quantiques utilisent le principe de superposition, l'interférence et la non localité pour mener à terme certains calculs beaucoup plus rapidement que leur contrepartie classique.

Les quatres premiers chapitres de ce document sont écrit sous forme d'introduction pédagogique aux principes de base de l'informatique quantique. On y présente d'abord quelques conséquences des postulats de la théorie quantique sur la manipulation de l'information pour ensuite s'intéresser au concept même d'ordinateur quantique. On décrit par la suite le phénomène de décohérence et ses conséquences sur la manipulation de l'information quantique. Cette introduction à l'informatique quantique se termine par une présentation des techniques de correction quantique d'erreurs. On présente en particulier le code $[[1, 9, 1]]$ de Shor et comment celui-ci peut venir à bout de la décohérence et des portes logiques imparfaites.

On s'intéresse ensuite à une architecture d'ordinateur quantique basée sur les jonctions Josephson entre électrodes supraconductrices de type d (i.e. cuprate). Après avoir décrit les éléments de base de cette architecture, on expose une méthode permettant l'initialisation de l'ordinateur et la mesure de l'état des qubits. On montre ensuite comment freiner l'évolution des qubits passifs en utilisant une technique s'approchant de l'écho de spins en RMN. À l'aide de ce résultat, on montre finalement comment réaliser un ensemble complet de portes logiques quantiques sur ce système, prouvant par le fait même que cette architecture correspond à un ordinateur quantique universel.

Remerciements

Je tiens d'abord à exprimer ma gratitude à mes directeurs de recherche Serge Lacelle et André-Marie Tremblay. Merci à Serge pour m'avoir présenté ce projet et soutenu dans les explorations diverses qui en ont découlé. Il est satisfaisant de voir que toutes les avenues explorées au cours de ce projet ont finalement abouti en un tout cohérent. Merci à André-Marie, premièrement pour avoir accepté de superviser un tel projet. Un lien entre informatique quantique et physique du solide aura finalement émergé ! Merci aussi pour son suivi et ses conseils éclairés.

Je tiens de même à remercier Alexandre M. Zagoskin pour m'avoir introduit à la physique des jonctions Josephson (encore beaucoup de travail reste à faire de ma part ...). Merci aussi pour sa confiance.

J'exprime aussi ma reconnaissance à Martin Beaudry pour les discussions, nombreuses et intéressantes, sur différents aspects de l'informatique quantique. Le groupe de discution du vendredi après-midi (Martin, Serge et moi-même) m'aura été très profitable. Qui sait, peut-être sommes nous les premiers membres d'un futur Institut de Recherche en Informatique Quantique de l'Université de Sherbrooke (IRIQUS) !

Je remercie aussi chaleureusement les membres et étudiants du département de physique pour l'atmosphère de travail agréable.

De plus, je remercie Hélène pour sa patience et son écoute. Si vous avez besoin de cours d'introduction à l'informatique quantique, Hélène pourra vous expliquer sans problème, pour en avoir entendu parler des centaines de fois, les concepts de qubit et d'enchevêtrement !

Finalement, je remercie les copains pour leur encouragement et les bons moments passés ensembles : Hélène (encore), Benoit (les deux), Marie-Josée et Étienne, David, Steve, Céline, Marjorie, Marie-Claude et Daniel, ...

Je souligne le support financier du Fonds pour la formation de chercheurs et l'aide à la recherche (Fonds FCAR).

Table des matières

Liste des Figures

Liste des Tableaux

Introduction

C'est en 1965 que G.E. Moore, co-fondateur de la société Intel, nota que chaque nouvelle puce contenait environ deux fois plus de transistors que son prédécesseur, de même chacune était disponible entre 18 et 24 mois après ce dernier. Il réalisa que si cette tendance se maintenait, cela signifiait une augmentation exponentielle de la puissance de calcul. Cette tendance est toujours d'actualité et ce qui était une remarque intéressante en 1965 constitue aujourd'hui une ligne directrice de l'industrie.

Mais cette miniaturisation n'est pas sans limite. En effet, une limite fondamentale est qu'un transistor ne peut être constitué de moins d'un atome. Les transistors actuels étant composés de quelques millions d'atomes, il semble que l'industrie n'aura pas à se préoccuper de cette contrainte avant quelques dizaines d'années. Une contrainte beaucoup plus pressante existe toutefois. Il est bien connu que la technologie des semiconducteurs est présentement basée sur le silicium. Une des raisons principales de ce choix est la grande qualité de l'oxyde natif de ce matériau. Or une étude récente [1, 2] montre qu'une couche de dioxide de silicium doit avoir une épaisseur d'au moins 5 atomes pour fonctionner comme un isolant. Sous la limite des 5 atomes, les effets quantiques deviennent importants et on s'attend à avoir conduction par effet tunnel.

Les transistors commerciaux actuels utilisent une couche d'oxyde d'une vingtaine d'atomes d'épaisseur et il est prévu que la limite critique de 5 atomes sera atteinte en 2012. Lorsque tel sera le cas, la miniaturisation ne sera plus possible sans l'apport d'une nouvelle technologie.

Une solution envisageable à ce problème dû à la miniaturisation est de prendre en considération les effets quantiques dans notre description de l'information et de les utiliser à notre avantage pour mener à bien des calculs. Dans cette situation, on peut alors mettre à profit les phénomènes quantiques tels les superpositions d'états, l'interférence et la non localité (théorème de Bell). Un système capable de mettre à profit ces phénomènes pour mener à terme des calculs est un ordinateur quantique.

Cette notion d'ordinateur quantique a été introduite au début des années 1980 mais n'a vraiment été prise au sérieux qu'en 1994 lorsque Peter Shor, des laboratoires de AT&T, a mis au point un algorithme quantique de factorisation. Depuis, la majorité des questions théoriques concernant le fonctionnement de ces systèmes ont été résolues [3] mais plusieurs aspects de la réalisation pratique de tels systèmes représentent toujours un problème majeur. C'est dans le contexte de la réalisation pratique d'un système quantique de manipulation de l'information que se situe ce mémoire.

Les premiers chapitres de ce document se veulent une introduction aux idées de base de l'informatique quantique. Ainsi, dans le premier chapitre, on s'attardera principalement à présenter quelques conséquences des postulats de la théorie quantique sur le traitement de l'information. Le deuxième chapitre constitue quant à lui un tour d'horizon des notions fondamentales concernant les ordinateurs quantiques. C'est donc dans ce chapitre que seront définies les notions de qubit et de parallélisme quantique. Les opérations logiques quantiques ainsi que la notion d'universalité y seront aussi abordées.

Le troisième chapitre s'intéresse quant à lui à l'une des difficultés majeures pour la réalisation d'un ordinateur quantique : la décohérence. On présentera un modèle de décohérence pour ensuite montrer l'effet de ce phénomène sur un registre quantique. Le chapitre suivant présente l'une des percées les plus importantes du domaine : la correction quantique d'erreurs. On montrera alors comme appliquer une méthode basée sur les techniques classiques de correction d'erreurs pour vaincre la décohérence. On verra aussi comment ces techniques nous permettent d'utiliser des portes logiques imparfaites.

Le cinquième chapitre est le coeur de ce mémoire et contient la plupart des résultats originaux. Dans ce chapitre, on s'intérese à une architecture particulière d'ordinateur quantique due à Alexandre M. Zagoskin de l'Université de la Colombie-Britannique

[4] . Dans la première section, on revoit les principales difficultés techniques liées à la mise en place d'un système quantique de manipulation de l'information pour ensuite décrire les éléments de base de l'architecture suggérée par A.M Zagoskin. On s'intéressera par la suite à la réalisation d'opérations logiques de base sur ce système pour finalement présenter quelques perspectives de recherche.

Chapitre 1

Théorie quantique et information

Tout calcul est exécuté par un système réalisable physiquement et qui obéit aux lois de la physique. De même, toute information est nécessairement encodée à l'aide d'un système physique. On est donc en droit de se questionner sur le rôle des lois de la physique concernant le traitement de l'information.

Dès le début du siècle, la thermodynamique a été exploitée dans ce but s'est révélée très fructueuse [5, 6, 7, 8]. En effet, après la deuxième guerre, Claude Shannon établit les bases de la théorie de l'information en montrant que l'information d'un message X, écrit dans un alphabet $\{x\}$ pour lequel chaque x à une probabilité d'occurence $p(x)$, est quantifiée par l'entropie de Shannon

$$H(X) = -\sum_x p(x) \log_2 p(x). \tag{1.1}$$

Par la suite, Rolf Landauer (1961) montre qu'effacer de l'information est un processus nécessairement dissipatif. Il est alors clair que les calculs non réversibles (qui effacent de l'information en cours d'excution) ont un coût thermodynamique minimal. Charles Bennett montre ensuite (1973) que tout calcul peut être effectué réversiblement et par conséquent sans coût énergétique (l'ordinateur effectue le calcul, copie le résultat final puis renverse le calcul pour compléter le cycle thermodynamique). Utilisant ces derniers résultats et se basant sur les travaux de Szilard

(1929), Bennett parvient (1981) à une solution au paradoxe du démon de Maxwell. Le démon peut apprendre où se trouvent les molécules sans faire de travail et sans augmenter l'entropie de l'environnement. Celui-ci peut alors mettre à profit la différence de température qu'il a créée pour faire un travail utile. Toutefois, selon Bennett, le démon est un système physique et par conséquent a une mémoire finie (si l'univers est fini il est impossible, par manque de ressources, d'avoir une mémoire infinie). Il devra alors régulièrement "réinitialiser" sa mémoire ce qui, selon l'argument de Landauer, est un processus dissipatif et donc irréversible. Il y a alors augmentation de l'entropie tel que prescrit par la deuxième loi.

Les analogies entre thermodynamique et information sont riches mais l'univers semble être fondamentalement quantique. C'est donc vers cette théorie que l'on doit se tourner dans le but de pousser davantage notre questionnement sur les implications des lois de la physique sur le traitement de l'information. Avant d'aborder à proprement parler la manipulation de l'information quantique (i.e. le concept d'ordinateur quantique), examinons quelques conséquences des postulats de la théorie quantique sur le traitement de l'information.

Premièrement, le postulat de réduction nous apprend que, lors d'une mesure, l'état du système mesuré est altéré de façon irréversible. Cet état de fait n'a aucune contrepartie classique et il est possible de lire un texte (comme celui-ci) sans en modifier le contenu. De plus, le résultat d'une telle mesure est stochastique. De ce fait, il est possible de générer des séquences de nombres purement aléatoires[1]. Encore une fois, aucun phénomène classique n'a ce caractère.

De même, deux observables A et B ne commutant pas ne peuvent avoir simultanément des valeurs bien définies. De ce fait, la mesure de l'observable A influence le résultat d'une mesure subséquente de B. Le fait d'acquérir de l'information sur un système perturbe donc l'état de celui-ci, ce qui n'a évidemment aucune contrepartie classique.

Par ailleurs, il est impossible de copier l'information quantique avec une fidélité

[1]On peut par exemple préparer n spins 1/2 selon l'axe z puis les mesurer selon x pour obtenir une séquence aléatoire de n bits.

arbitraire[2]. Le principe de “non clonage” dû à Wootters et Zurek [9] et indépendament Dieks [10] est une conséquence de la linéarité de la mécanique quantique.

Imaginons qu'il existe un opérateur U copiant l'état d'un système quantique avec une fidélité arbitrairement grande

$$\begin{aligned} \mathsf{U}\,|\uparrow\rangle\,|\varnothing\rangle &= |\uparrow\rangle\,|\uparrow\rangle\,; \\ \mathsf{U}\,|\rightarrow\rangle\,|\varnothing\rangle &= |\rightarrow\rangle\,|\rightarrow\rangle\,, \end{aligned} \tag{1.4}$$

où $|\uparrow\rangle$ et $|\rightarrow\rangle$ sont des états orthogonaux représentant par exemple l'état de polarisation d'un photon et $|\varnothing\rangle$, l'état nul, représentant alors l'état vide du champ electromagnétique. Le premier ket est l'état à copier et le second, initialement dans l'état nul, est le clone. Considérons maintenant la copie d'un état arbitraire à l'aide de ce même opérateur

$$\begin{aligned} \mathsf{U}(a\,|\uparrow\rangle + b\,|\rightarrow\rangle)\,|\varnothing\rangle &= a\,\mathsf{U}\,|\uparrow\rangle\,|\varnothing\rangle + b\,\mathsf{U}\,|\rightarrow\rangle\,|\varnothing\rangle \\ &= a\,|\uparrow\rangle\,|\uparrow\rangle + b\,|\rightarrow\rangle\,|\rightarrow\rangle \\ &\neq (a\,|\uparrow\rangle + b\,|\rightarrow\rangle) \otimes (a\,|\uparrow\rangle + b\,|\rightarrow\rangle). \end{aligned} \tag{1.5}$$

L'état final ne correspondant pas à un état produit tensoriel de l'original et de son clone, on en déduit que U ne peut réaliser le clonage parfait d'un état arbitraire[3].

[2]La fidélité F de l'état $|\phi\rangle$ relativement à l'état $|\psi\rangle$ est définie comme la projection de $|\phi\rangle$ sur $|\psi\rangle$

$$F = |\langle\phi|\psi\rangle|^2\,. \tag{1.2}$$

De façon plus générale, la fidélité de la matrice densité ρ par rapport à $|\psi\rangle$ est

$$F = \langle\psi\,|\,\rho\,|\,\psi\rangle\,. \tag{1.3}$$

Dans le cas du clonage quantique, la fidélité est en quelque sorte une mesure de la réussite de l'opération. Ainsi, $|\psi\rangle$ représente l'état initial tandis que $|\phi\rangle$ ou ρ représente l'état cloné. Une fidélité $F = 1$ correspond alors à un clonage parfait.

[3]Selon (1.3), la fidélité du clonage (1.5) est $F = |a|^2\,|a|^2 + |b|^2\,|b|^2$, ce qui est toujours plus petit que 1 si aucun des coefficients a et b n'est nul.

Notons que s'il était possible de copier un état arbitraire avec une grande fidélité, il serait alors possible d'arriver à connaître l'état de ce système sans le perturber en le copiant puis en mesurant les copies.

1.1 Mesure de l'information quantique

Comme dans le cas classique, l'information quantique est quantifiée à l'aide de la notion d'entropie. Dans ce cas, on utilise toutefois l'entropie de von Neumann

$$S(\rho) = -\mathrm{Tr}\left(\rho \log_2 \rho\right), \tag{1.6}$$

pour une matrice densité ρ. Pour un état pur $S(\rho) = 0$, tandis que pour un état mixte, $0 < S(\rho) \leq n$, l'égalité étant atteinte pour un état maximalement mixte (i.e. proportionnel à l'opérateur identité) de n systèmes à deux niveaux.

1.2 Enchevêtrement

L'état final lors de la tentative échouée de clonage (1.5) ne peut être exprimé comme un produit tensoriel des états de ses sous-systèmes. De même, les propriétés du système global ne peuvent être décrites en termes des propriétés individuelles de ces sous-systèmes. On dit alors que ces états sont enchevêtrés (ou non séparables). La notion d'enchevêtrement[4] a été introduite par Schrödinger en 1935 [11, 12, 13] et traduit la présence de corrélations non locales entre les sous-systèmes.

On distinguera ainsi les états enchevêtrés (ou non séparables), des états produits tensoriels (ou non enchevêtrés, séparables). Un état séparable peut toujours être représenté comme un produit tensoriel de l'état de ces sous-systèmes. Par exemple, pour deux systèmes A et B :

$$|\,\Phi\rangle_{AB} = |\,\phi\rangle_A \otimes |\,\psi\rangle_B\,. \tag{1.7}$$

[4]De l'anglais *entanglement*, parfois traduit par intrication.

À l'opposé, un état enchevêtré ne peut être factorisé, par exemple :

$$|\,\Psi\rangle_{AB} = |\,\phi\rangle_A \otimes |\,\chi\rangle_B + |\,\alpha\rangle_A \otimes |\,\xi\rangle_B\,. \tag{1.8}$$

Pour les systèmes composés, l'état de chaque sous-système individuel est décrit à l'aide de la matrice densité réduite obtenue de la trace sur les degrés de liberté des autres sous-systèmes. Ainsi, pour un état séparable, les sous-systèmes seront décrits par des états purs. Par exemple, le sous-système A de $|\,\Phi\rangle_{AB}$ s'exprime comme

$$\begin{aligned} \rho_A &= \mathrm{Tr}_B\,|\,\Phi\rangle_{AB}\,\langle\Phi\,| \\ &= |\,\phi\rangle_A\,\langle\phi\,|\,. \end{aligned} \tag{1.9}$$

Pour les états enchevêtrés, les sous-systèmes seront plutôt décrits par des états mixtes.

Les corrélations non locales entre les sous-systèmes d'un état enchevêtré sont révélées par une série de mesures. Par exemple, lors de mesures sur l'état $|\,\Phi\rangle_{AB}$, les résultats ne présenteront que des corrélations classiques. Ainsi, lors d'une mesure selon l'axe z sur deux spins dans l'état $|\uparrow\uparrow\rangle_z$, les résultats seront corrélés : on obtiendra $|\uparrow\rangle$ pour les deux sous-systèmes. Toutefois, si l'on mesure le premier spin selon z et le second selon x, les résultats ne seront pas corrélés puisque le résultat de la mesure selon x d'un spin orienté selon z est totalement aléatoire.

À l'opposé, lors de mesures de l'état enchevêtré $|\,\psi^+\rangle = (|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)/\sqrt{2}$, les résultats seront opposés peu importent les bases respectives choisies pour la mesure. Connaissant l'état du premier spin, on peut en déduire aussitôt l'état du second. La mesure d'un des sous-systèmes pour un état enchevêtré a ainsi pour conséquence de déterminer l'état des autres sous-systèmes même si ceux-ci sont éloignés et n'interagissent pas au moment de la mesure. C'est ce que l'on entend par corrélations non locales.

Pour l'état $|\,\psi^+\rangle$ de l'exemple précédent, on sait que le premier spin est dans l'état $|\uparrow\rangle$ et le second $|\downarrow\rangle$, ou vice versa, mais on ne peut dire dans lequel des états ils sont avant la mesure. Tout ce qui est préalablement défini est que les spins sont dans des états différents. En ce sens, pour un état non séparable, l'information est distribuée entre les sous-systèmes de sorte qu'aucun des deux ne contient individuellement d'information.

Ainsi, pour $|\,\psi^+\rangle$, l'état du sous-système A est décrit par une matrice densité proportionnelle à l'identité

$$\begin{aligned}\rho_A &= \mathrm{Tr}_B\{|\,\psi^+\rangle\,\langle\psi^+\,|\} \\ &= \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}.\end{aligned} \tag{1.10}$$

Puisque les cohérences (i.e. les éléments hors-diagonaux) sont nulles, cet état ne contient aucune information de phase. Cette information est contenue dans les corrélations non locales entre les sous-systèmes qui ne sont pas accessibles lorsque l'on considère seulement une partie du système global. Notons que la trace partielle d'un état enchevêtré ne donne pas nécessairement un résultat proportionnel à l'identité. Lorsque c'est le cas, on dit qu'il s'agit d'un état d'enchevêtrement maximal.

Ce dernier exemple conduit à la notion de mesure de l'enchevêtrement [5, 14, 15]. Pour les états purs[5], la mesure unique de l'enchevêtrement est

$$E(|\,\psi\rangle_{AB}) \equiv S(\rho_A) = S(\rho_B), \tag{1.11}$$

où $S(\rho)$ est l'entropie de von Neumann et ρ_A (ρ_B) est la matrice densité réduite du sous-système A (B). La quantité E, nommée simplement enchevêtrement, prend des valeurs allant de zéro, pour un état séparable, à $\log_2 N$, pour un état d'enchevêtrement maximal de deux sous-systèmes de dimensions N. Pour l'état $|\,\psi^+\rangle$ d'enchevêtrement maximal, on a $E = 1$.

Notons que l'enchevêtrement est invariant sous l'application d'opérations locales unitaires, i.e. sous toutes transformations U pouvant s'exprimer sous la forme d'un produit d'opérateurs $\mathsf{U} = \mathsf{U}_A \otimes \mathsf{U}_B$. Ainsi, l'enchevêtrement ne peut être créé localement de sorte que deux expérimentateurs, Alice et Bob, n'ayant accès qu'au sous-système A et B respectivement, ne peuvent créer d'enchevêtrement à l'aide d'actions

[5]Dans le cas des états mixtes, la situation est beaucoup plus complexe et il s'agit d'un sujet actif de recherche. À ce jour (été 1999), il n'y a pas de consensus quant à la définition d'une mesure unique d'enchevêtrement pour de tels états.

locales et de communication classique. Pour créer de l'enchevêtrement, ils devront faire interagir leur particule (ou mettre à profit une paire de particules enchevêtrées qu'ils se sont déjà partagées).

Chapitre 2

Ordinateur quantique

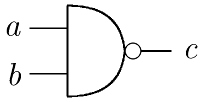
2.1 Ordinateur classique

Avant de s'intéresser aux ordinateurs quantiques, attardons-nous aux concepts de base régissant leur contrepartie classique [16, 17]. L'élément de base de l'informatique classique est le bit (pour **bi**nary digi**t**) et est matérialisé par un système macroscopique à deux niveaux. Un ordinateur classique est un système composé d'un ensemble de bits (un registre) sur lesquels est appliquée une suite d'opérations logiques portant la configuration initiale du registre vers une configuration finale, le résultat.

Ces opérations sont représentées sous forme de portes logiques obéissant à l'algèbre booléenne. Une porte logique agissant sur un seul bit n'a que deux valeurs d'entrées possibles (0 ou 1). De ce fait, il n'existe que $2^1 = 2$ opérations différentes sur un bit : l'inversion (NOT) et l'identité (un simple fil). De même, pour deux bits, quatre valeurs sont possibles (00, 01, 10 et 11) et par conséquent $4^2 = 16$ portes différentes. Mais toutes ces portes ne sont pas nécessaires et on peut montrer que la porte NAND (figure 2.1) est suffisante. On peut donc réaliser toute opération logique voulue à l'aide de cette seule opération. Elle est alors dite universelle pour le calcul classique[1]

[1] Il est important de noter que pour que la porte NAND soit universelle elle doit être accompagnée des portes FANOUT (duplication d'un bit), EXCHANGE (échange de deux bits) et d'un réservoir de bits '0' et de bits '1'. Dans le cas classique, ces éléments sont triviaux et il est coutume de

[16]. Un ordinateur ayant cette porte dans son répertoire et pouvant agir sur un nombre arbitraire de bits est alors qualifié d'universel puisqu'il peut mener à bien toute fonction calculable.



a	b	c
0	0	1
0	1	1
1	0	1
1	1	0

Figure 2.1: Représentation graphique et table de vérité de la porte NAND.

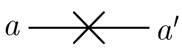
Le NAND est toutefois irréversible : puisque cette porte a moins de bits de sorties que de bits d'entrés, connaissant le bit de sortie il est impossible de dire quelle était la valeur des bits d'entrées. Ainsi, pour chaque utilisation de cette opération, un bit d'information est effacé et, en raison du principe de Landauer, il y a dissipation d'énergie. On peut cependant éviter cette dissipation en copiant les bits d'entrées vers la sortie de façon à en faire une porte réversible.

Pour éviter cette perte d'information, on peut aussi imaginer de nouvelles portes réversibles. Parmi celles-ci mentionnons le Controlled-NOT et la porte de Toffoli [16]. Ces portes, ainsi que leur table de vérité, sont présentées à la figure 2.2. Notons que la porte de Toffoli est universelle pour le calcul classique réversible.

2.2 Qubits

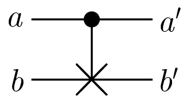
Le bit quantique ou, plus simplement, qubit (*quantum bit*) est l'unité fondamentale de l'information quantique. Un qubit est un système quantique résidant dans un espace d'Hilbert de dimension deux. Un bit quantique peut donc prendre deux valeurs, notées $|0\rangle$ et $|1\rangle$, avec $\langle i|j\rangle = \delta_{ij}$ et $i, j = \{0, 1\}$. En raison du principe de superposition,

les omettre dans la description d'un ensemble complet [16]. On affirmera donc que le NAND est universel en sous entendant que ces derniers éléments sont requis.



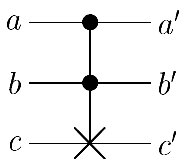
a	a'
0	1
1	0

(a)



a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

(b)



a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	0
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

(c)

Figure 2.2: Représentation graphique et table de vérité de quelques portes réversibles. Toutes les portes réversibles ont autant de bits d'entrées que de sorties. (a) NOT (b) Controlled-NOT. Cette porte inverse le second bit si le premier est 1. (c) Porte de Toffoli. Cette porte agit comme un Controlled-Controlled-NOT : si les premier et second bit sont 1, le troisième est inversé.

un qubit peut aussi exister dans une superposition de ces états

$$|\,\psi\rangle = a\,|\,0\rangle + b\,|\,1\rangle \tag{2.1}$$

avec a et b des coefficients complexes représentant les amplitudes de probabilité d'obtenir $|\,0\rangle$ ou $|\,1\rangle$ respectivement lors de la mesure de $|\,\psi\rangle$. Ces coefficients satisfont la condition de normalisation $|a|^2 + |b|^2 = 1$. Toujours en raison du principe de superposition, un qubit a aussi la possibilité d'être enchevêtré avec d'autres qubits.

Puisque a et b prennent un continum de valeur, il semble qu'un qubit encode une quantité infinie d'information classique. Toutefois, on peut montrer, à l'aide de la limite de Holevo [5], qu'il n'est possible d'extraire qu'un seul bit d'information classique d'un qubit. D'ailleurs, lors de la mesure de l'état $|\,\psi\rangle$ dans la base $\{|\,0\rangle\,, |\,1\rangle\}$, on obtient $|\,0\rangle$ ou $|\,1\rangle$ et non une superposition de ces états. Il s'agit d'un résultat classique et on obtient alors un bit d'information classique de cette mesure.

On définit un registre quantique comme un ensemble de qubits. Ainsi, un registre de n qubits est un espace d'Hilbert de dimensions 2^n. Dans la base $\{|\,0\rangle\,, |\,1\rangle\}^{\otimes\,n}$, on note ces états à n bits quantiques

$$|\,q_{n-1}\rangle \otimes \cdots \otimes |\,q_1\rangle \otimes |\,q_0\rangle \;=\; |\,q_{n-1}\,\cdots\,q_1\,q_0\rangle\,, \tag{2.2}$$

où chacun des q_i prend la valeur 0 ou 1. Pour simplifier la notation, on associe à l'aide de la relation $x = \sum_{l=0}^{n-1} q_l 2^l$, un nombre décimal x à cette chaîne binaire. Par exemple, on a les correspondances suivantes pour des registres ayant respectivement 3, 4 et 8 qubits

$$\begin{aligned} |\,000\rangle &\longleftrightarrow |\,0\rangle\,; \\ |\,0101\rangle &\longleftrightarrow |\,5\rangle\,; \\ |\,10011110\rangle &\longleftrightarrow |\,158\rangle\,. \end{aligned} \tag{2.3}$$

Lorsque la taille (n) du registre est spécifiée, il n'y a pas d'ambiguité possible avec cette notation. Utilisant la représentation décimale, on écrit la superposition linéaire arbitraire d'un registre de n qubits comme :

$$\sum_{x=0}^{2^n-1} a_x \,|\, x\rangle \,, \tag{2.4}$$

où $\sum_{x=0}^{2^n-1} |a_x|^2 = 1$. Lors d'une mesure de cet état où l'on projette chacun des qubits sur la base de calcul $\{|\,0\rangle\,, |\,1\rangle\}$, la probabilité d'obtenir $|\,x\rangle$ est $|a_x|^2$. Le résultat de cette mesure, correspond à n bits d'information classique.

Évidemment, il n'est pas nécessaire de se limiter à des mesures sur tout le registre. Il est possible de mesurer une partie seulement du registre définissant par le fait même la valeur des autres qubits s'ils étaient enchevêtrés avec les qubits mesurés. Ces mesures partielles sont utilisées par la plupart des techniques de correction quantique d'erreurs et par certains algorithmes quantiques. De même, par l'utilisation de qubits auxilliaires, il est possible d'effectuer des mesures ne correspondant pas à une projection orthogonale (on nomme ce type de mesures POVM, de l'anglais *Positive Operator Valued Measures* [18]).

2.3 Opérations logiques

De façon générale, un calcul quantique est réalisé en trois étapes :

1. Préparation de l'état initial : $|\,\mathrm{input}\rangle$;
2. Calcul : $|\,\mathrm{output}\rangle = \mathsf{U}\,|\,\mathrm{input}\rangle$;
3. Mesure : projection sur la base de calcul,

Les états $|\,\mathrm{input}\rangle$ et $|\,\mathrm{output}\rangle$ sont des combinaisons linéaires des états de la base de calcul $\{|\,0\rangle\,, |\,1\rangle\}^{\otimes n}$. La dynamique du système, i.e. l'opérateur d'évolution U, est choisie de façon à correspondre au calcul désiré (U est donc le “programme quantique”). La dernière étape, la mesure, est habituellement réalisée dans la base de calcul. Le résultat est classique et probabiliste.

L'équation de Schrödinger nous apprend que l'évolution d'un vecteur d'état est unitaire et de ce fait, toutes les opérations logiques quantiques sont elles-même unitaires. De même, elles doivent être réversibles puisque l'inverse d'un opérateur unitaire, $\mathsf{U}^{-1} = \mathsf{U}^\dagger$, existe toujours. Le calcul quantique est donc, en quelque sorte, analogue au calcul classique réversible (en fait, ce dernier est un sous ensemble du calcul quantique [19]).

L'opération U, correspondant au 'programme quantique', est généralement réalisée par une séquence d'opérations unitaires agissant chacune sur un petit nombre de qubits. Définissons maintenant ces opérations logiques de base (le "langage de programmation quantique").

On distingue trois types d'opérations logiques quantiques : les opérations sur un qubit, les opérations locales sur $n > 1$ qubits et les opérations non locales sur $n > 1$ qubits. Les opérations sur un qubit sont les matrices de rotations : $\mathsf{R}_{\mathbf{n}}(\theta) = e^{-i\mathbf{n}\cdot\boldsymbol{\sigma}\theta/2}$, où $\mathbf{n}$ est la direction de l'axe de rotation et $\boldsymbol{\sigma}$ le vecteur des matrices de Pauli. Une opération à un qubit largement utilisée en informatique quantique est la transformation d'Hadamard (parfois nommée transformation de Walsh-Hadamard) $\mathsf{H} \equiv \mathsf{R}_{\mathbf{n}=\frac{1}{\sqrt{2}}(\mathbf{x}+\mathbf{z})}(\pi)$. On peut écrire cette transformation sous la forme

$$\begin{aligned} \mathsf{R}_{\mathbf{n}=\frac{1}{\sqrt{2}}(\mathbf{x}+\mathbf{z})}(\pi) &= \mathbb{I}\cos(\pi/2) - i\frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)\sin(\pi/2) \\ &= \frac{-i}{\sqrt{2}}(\sigma_x + \sigma_z), \end{aligned} \tag{2.5}$$

de sorte que, dans la base de calcul et prenant comme convention $|\,0\rangle = (1,0)^T$ et $|\,1\rangle = (0,1)^T$, cette opération s'exprime comme suit sous forme matricielle

$$\mathsf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.6}$$

Ainsi, cette porte a pour effet de créer des superpositions d'états

$$\begin{aligned} \mathsf{H} : |\,0\rangle &\to \frac{1}{\sqrt{2}}\left(|\,0\rangle + |\,1\rangle\right); \\ \mathsf{H} : |\,1\rangle &\to \frac{1}{\sqrt{2}}\left(|\,0\rangle - |\,1\rangle\right). \end{aligned} \tag{2.7}$$

Remarquons que les relations (2.5) et (2.6) diffère par une phase $-i$. Puisqu'il s'agit d'une phase globale ne dépendant pas de l'état du qubit celle-ci est sans conséquence et peut être ignoré.

De façon plus intuitive, on représente les opérations logiques sous forme de circuits quantiques. Dans cette notation, les qubits sont représentés par des lignes horizontales et on place les opérations, successivement de la gauche vers la droite, sur ces lignes. Le circuit effectuant l'opération d'Hadamard est présenté à la figure 2.3.

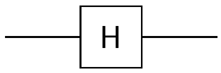


Figure 2.3: Porte d'Hadamard.

Les opérations locales sur $n > 1$ qubits s'expriment sous la forme d'un produit tensoriel d'opérateurs. Une telle transformation agissant sur deux qubits s'exprime comme $\mathsf{U}_{12} = \mathsf{U}_1 \otimes \mathsf{U}_2$, où U_i est une transformation agissant sur le $i^{\text{ième}}$ qubit seulement. De façon générale, la représentation matricielle du produit tensoriel d'une paire d'opérateurs est

$$\mathsf{A} \otimes \mathsf{B} = \begin{pmatrix} a_{11}\,\mathsf{B} & \cdots & a_{1n}\,\mathsf{B} \\ \vdots & \ddots & \vdots \\ a_{n1}\,\mathsf{B} & \cdots & a_{nn}\,\mathsf{B} \end{pmatrix}. \tag{2.8}$$

Le circuit réalisant l'opération U_{12} est présentée à la figure 2.4. Ces transformations locales ne peuvent créer d'enchevêtrement.

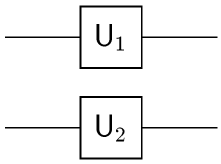
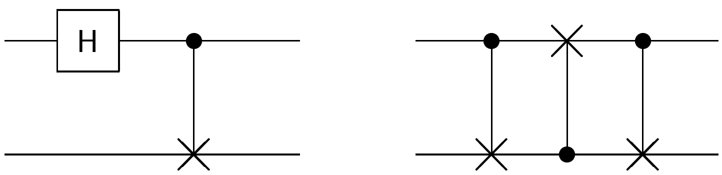


Figure 2.4: Opérations locales sur deux qubits.

Les transformations non locales ne peuvent quant à elle s'exprimer sous forme d'un produit tensoriel d'opérateurs et sont les seules opérations, parmi les trois types définis précédemment, pouvant engendrer de l'enchevêtrement. La plus importante de ces transformations est le Controlled-NOT, déjà introduite à la section §2.1. Cette opération notée CN_{ij} avec i et j les bits de contrôle et cible respectivement, a l'effet suivant : $\mathsf{CN}_{12}\,|\,i,j\rangle = |\,i, i \oplus j\rangle$, où $\oplus$ dénote l'addition modulo[2] 2. Cette opération est similaire à celle introduite dans le cas classique sauf qu'elle est ici habilitée à opérer sur des superpositions d'états. De même, la porte de Toffolli, notée ici $\mathsf{CCN}_{i,j,k}$, est non locale et peut créer de l'enchevêtrement. Cette porte effectue la transformation suivante sur trois qubits : $\mathsf{CNN}_{123}\,|\,i,j,k\rangle = |\,i,j,ij \oplus k\rangle$. Les représentations graphiques de ces portes ont été présentées à la figure 2.2.

On combine les portes logiques pour réaliser des circuits plus complexes. Considérons par exemple les circuits de la figure 2.5.



(a) (b)

Figure 2.5: Concaténation de portes logiques en un circuit plus complexe. (a) Circuit enchevêtrant une paire de qubits. Le premier bit quantique (ligne du haut) définit la phase relative de l'état final et le second (ligne du bas) sa parité. Dans ce contexte, un état $|\,i,j\rangle$ est dit pair si $i \oplus j = 0$ et impair sinon. (b) Circuit échangeant l'état de deux qubits.

Le circuit de la figure 2.5(a) a l'effet suivant sur les états de la base de calcul

$$\begin{aligned}
|\,00\rangle &\xrightarrow{\mathsf{H}_1} \frac{1}{\sqrt{2}}(|\,0\rangle + |\,1\rangle)\,|\,0\rangle \xrightarrow{\mathsf{CN}_{12}} \frac{1}{\sqrt{2}}(|\,00\rangle + |\,11\rangle) = \left|\,\phi^+\right\rangle; \\
|\,01\rangle &\xrightarrow{\mathsf{H}_1} \frac{1}{\sqrt{2}}(|\,0\rangle + |\,1\rangle)\,|\,1\rangle \xrightarrow{\mathsf{CN}_{12}} \frac{1}{\sqrt{2}}(|\,01\rangle + |\,10\rangle) = \left|\,\psi^+\right\rangle; \\
|\,10\rangle &\xrightarrow{\mathsf{H}_1} \frac{1}{\sqrt{2}}(|\,0\rangle - |\,1\rangle)\,|\,0\rangle \xrightarrow{\mathsf{CN}_{12}} \frac{1}{\sqrt{2}}(|\,00\rangle - |\,11\rangle) = \left|\,\phi^-\right\rangle; \\
|\,11\rangle &\xrightarrow{\mathsf{H}_1} \frac{1}{\sqrt{2}}(|\,0\rangle - |\,1\rangle)\,|\,1\rangle \xrightarrow{\mathsf{CN}_{12}} \frac{1}{\sqrt{2}}(|\,01\rangle - |\,10\rangle) = \left|\,\psi^-\right\rangle.
\end{aligned} \tag{2.9}$$

[2]Si $a - b \in n\mathbb{Z}$ alors on dit de a et b qu'ils sont congruents modulo n : $a \equiv b \bmod n$. Dans le cas qui nous intéresse, on a donc $0 \equiv 0 \bmod 2,\ 1 \equiv 1 \bmod 2,\ 2 \equiv 0 \bmod 2, \ldots$

Ainsi, ce circuit a pour action d'enchevêtrer les qubits en faisant la correspondance entre la base de calcul et la base $\{|\,\phi^+\rangle\,,|\,\phi^-\rangle\,,|\,\psi^+\rangle\,,|\,\psi^-\rangle\}$. Cette dernière base, communément appellée "base de Bell", est la base des états à deux bits quantiques d'enchevêtrement maximal.

Le circuit de la figure 2.5(b), quand à lui, échange l'état des deux qubits. On note cette opération Sw (pour *swap*)

$$\begin{aligned}\mathsf{Sw}_{12}\,|\,i,j\rangle &\equiv \mathsf{CN}_{12}\mathsf{CN}_{21}\mathsf{CN}_{12}\,|\,i,j\rangle \\ &= |\,i\oplus i\oplus j, i\oplus j\oplus i\oplus i\oplus j\rangle \\ &= |\,j,i\rangle\,,\end{aligned} \tag{2.10}$$

où on a utilisé le fait que $i\oplus i=0$ et $i\oplus 0=i$, $\forall\, i$.

2.4 Universalité

Comme dans le cas classique, plusieurs portes logiques quantiques sont possibles mais elles ne sont pas toutes nécessaires. À ce sujet, D. Deutsch a montré (1989) qu'une généralisation de la porte de Toffoli est universelle pour le calcul quantique. Cette opération, maintenant connue sous le nom de porte de Deutsch, agit sur trois qubits :

$$\mathsf{D} = \begin{array}{c} \begin{array}{cccccccc} |\,000\rangle & |\,001\rangle & |\,010\rangle & |\,011\rangle & |\,100\rangle & |\,101\rangle & |\,110\rangle & |\,111\rangle \end{array} \\ \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & i\cos\theta & \sin\theta \\ & & & & & & \sin\theta & i\cos\theta \end{pmatrix} \end{array} \tag{2.11}$$

avec θ/π irrationnel [20]. Afin de pouvoir réaliser cette transformation, on doit faire interagir simultanément trois qubits. Il s'avère difficile de réaliser physiquement une telle interaction [21] et il est ainsi grandement avantageux d'avoir une porte universelle à deux qubits. (Puisqu'une porte universelle doit pouvoir créer de l'enchevêtrement, il n'y a pas de portes universelles à 1 qubit seulement.) Heureusement, D. DiVincenzo (1995) a montré qu'un ensemble de portes à un et deux qubits est complet pour le calcul quantique [21]. De même, S. Lloyd (1995) [22] et Deutsch *et. al.* (1995) [23] ont indépendamment montré que presque toutes opérations sur $n \geq 2$ qubits sont universelles.

D'un point de vue classique, ce résultat est surprenant puisqu'il faut au moins 3 bits pour qu'une porte réversible classique soit universelle et il n'existe pas d'ensemble complet de portes réversibles agissant sur seulement deux bits. En informatique quantique, ce plus grand choix de portes universelles est dû à la plus grande richesse du calcul quantique. Dans le cas du calcul classique réversible, l'évolution temporelle des bits est décrite à l'aide de matrices unitaires dont les éléments sont des zéro ou des un. Dans le cas quantique ces éléments sont des nombres complexes arbitraires.

Construisant sur les résultats précédents, A. Barenco *et. al.* (1995) [19] ont montré que l'ensemble formé de toutes les opérations unitaires à un qubit (i.e. $U(2)$, le groupe des matrices unitaire de dimensions 2) et du Controlled-NOT (qui n'est pas par elle-même universelle) est suffisant pour réaliser sur n bits quantiques toutes opérations appartenant à $U(2^n)$ et forment donc un ensemble complet.

Cependant, $U(2^n)$ est isomorphe à $U(1) \times SU(2^n)$, avec $SU(2^n)$ le groupe des matrices unitaires de dimension 2^n et de déterminant unité [24]. Le groupe $U(1)$ est constitué des 'matrices' unitaires $e^{i\delta}$ de tailles 1×1 et les matrices $e^{i\delta}\mathbb{I}_n$, avec $\mathbb{I}_n$ la matrice identité de dimension n, forment une représentation matricielle de dimension n de ce groupe. Ainsi, $U(1)$ correspond à une phase globale n'ayant aucune signification physique sur un vecteur d'état. De ce fait, et des résultats de [19], on en déduit qu'il est suffisant pour pouvoir qualifier un ordinateur quantique d'universel, que celui-ci soit capable de générer $SU(2^n)$ sur n bits quantiques. Il est donc suffisant qu'un tel ordinateur ait dans son répertoire les générateurs de $SU(2)$ et la porte CN.

Notons cependant que l'ensemble complet suggéré ici n'est pas nécessairement optimal. La détermination de l'ensemble complet optimal doit se faire en fonction de l'architecture de l'ordinateur quantique utilisée et du calcul à effectuer.

2.5 Puissance du calcul quantique

Ainsi, les ordinateurs quantiques opèrent selon des lois bien différentes de celles des ordinateurs classiques. On est donc en droit de se demander s'il y a des calculs qu'un ordinateur quantique peut réaliser mais que sa contrepartie classique ne peut effectuer.

Pour répondre à cette question, remarquons qu'un registre de n qubits peut être représenté par un vecteur dans un espace de dimension 2^n. L'application de portes logiques correspond à la rotation et la mesure à la projection de ce vecteur. Toutes ces opérations (description d'un vecteur, rotation et projection) peuvent évidemment être réalisées par un ordinateur classique. On en déduit donc qu'un ordinateur classique peut simuler arbitrairement bien un ordinateur quantique [25]. Par conséquent, tout calcul pouvant être réalisé à l'aide d'un ordinateur quantique peut, *en principe*, être mené à bien par un ordinateur classique.

Considérons les ressources nécessaires à une telle simulation. Prenons par exemple un ordinateur quantique de 100 qubits, un nombre bien modeste comparativement aux nombres de transistors utilisés par les ordinateurs actuels. Dans ce cas, le vecteur d'état du registre réside dans un espace d'Hilbert de dimension $2^{100} \approx 10^{30}$. Pour encoder cette information, un ordinateur classique aura donc besoin de $\sim 10^{30}$ nombres complexes. Aucun ordinateur classique actuel ou envisageable n'a assez de mémoire pour venir à bout de cette tâche. De même, simuler une opération logique signifie calculer la rotation d'un vecteur dans un espace de dimension $\sim 10^{30}$. Encore une fois, aucun ordinateur classique n'a la capacité de réaliser cette opération. Considérons maintenant les ressources en temps nécessaire lors de l'initialisation (i.e. lors de préparation du registre dans un état produit tensoriel des 100 qubits). Dans le cas classique, il est nécessaire de spécifier $2^{100} \approx 10^{30}$ coefficients. Si un milliard de ces coefficients sont entrés à la seconde, cette opération prendra plus de temps que l'âge de l'univers ! Dans le cas quantique, on a évidement besoin d'au plus $n = 100$ opérations.

Comme l'illustre l'exemple précédent, pour une croissance linéaire de la taille de l'ordinateur quantique, la complexité de la simulation classique croît exponentiellement. Ainsi, la simulation d'un ordinateur quantique est *en principe* réalisable mais *en pratique* souvent impossible. Cette constatation a conduit Richard Feynman en 1982 à spéculer qu'un ordinateur quantique pourrait avoir une puissance de calcul au-delà de celle de tout ordinateur classique.

2.6 Parallélisme quantique

Le principe de superposition confère donc aux ordinateurs quantiques une grande puissance de calcul. Pour comprendre davantage l'origine de cette puissance, considérons l'exemple suivant.

Soit une fonction[3] $f : \{0,1\}^n \to \{0,1\}^n$ pour laquelle on dispose d'un circuit quantique, noté U_f :

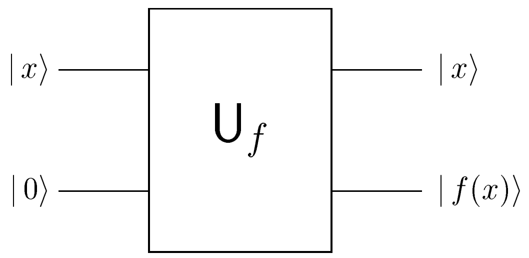


Figure 2.6: Circuit non local pour le parallélisme quantique.

Le circuit effectuant la transformation U_f est réalisé à l'aide des opérations de base décrites aux sections §2.3 et §2.4. On ne s'intéresse pas ici aux détails de cette construction et on considère ce circuit comme un oracle quantique donnant à tout coup la bonne réponse.

La fonction f n'étant pas nécessairement bijective, et par conséquent réversible, ce circuit agit sur deux registres. Le premier contient la valeur d'entrée pour laquelle on cherche à connaître f tandis que le second, initialement dans l'état $|0\rangle$, reçoit

[3]De façon plus générale, on peut prendre une fonction $f : \{0,1\}^n \to \{0,1\}^m$, avec $m \neq n$ en utilisant des qubits auxilliaires.

le résultat du calcul. La transformation U_f est alors réversible puisque le premier registre reste inchangé par le calcul.

Afin de connaître la valeur de $f(x)$ pour un $x \in \{0,1\}^n$ particulier on applique U_f sur $|\,x\rangle\,|\,0\rangle$:

$$\mathsf{U}_f : |\,x\rangle\,|\,0\rangle \to |\,x\rangle\,|\,f(x)\rangle\,. \tag{2.12}$$

Comme l'état initial, le résultat de ce calcul correspond à $2n$ bits classiques (n par registre) et un ordinateur classique aurait put obtenir ce résultat en un temps proportionnel. Considérons maintenant un autre état initial : la superposition uniforme de toutes les valeurs possibles de x : $\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|\,x\rangle$. Lors de l'application de U_f sur cet état, on obtient un état enchevêtré des deux registres

$$\mathsf{U}_f\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|\,x\rangle\,|\,0\rangle = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|\,x\rangle\,|\,f(x)\rangle\,. \tag{2.13}$$

Utilisant les mêmes ressources en temps et en mémoire que (2.12) (en fait, seule la préparation de l'état initial varie; comme souligné à la section §2.5, cette préparation nécessite au plus un nombre d'opérations linéaire en n), $f(x)$ a été calculée pour 2^n valeurs de x.

L'ordinateur quantique a ainsi calculé la valeur de f pour un nombre exponentiel de valeur de x en un seul calcul et donc en un temps proportionnel à celui qu'un ordinateur classique aurait pris pour calculer un seul de ces résultats. En raison de la linéarité de l'équation de Shrödinger, le calcul est effectué simultanément sur tous les "embranchements" de la fonction d'onde. C'est ce que l'on entend par parallélisme quantique.

Si la fonction f est bijective[4], la mesure du premier registre sur l'état final (2.13) donne un résultat $|\,x_0\rangle$ choisi aléatoirement parmi les 2^n valeurs possibles. Le système

[4]Si f n'est pas une bijection, la mesure du premier registre entraîne l'effondrement du second registre vers la superposition de toutes les valeurs de f correspondant au résultat obtenu dans le premier. Par exemple, pour une fonction f de période R, obtenir x_0 lors de la mesure du premier registre résulte en l'état final $|\,x_0\rangle\,(|\,f(x_0)\rangle + |\,f(x_0+R)\rangle + \cdots)$. Cette sélection de l'état du second registre par une mesure du premier est une conséquence de l'enchevêtrement. L'algorithme quantique

est alors projeté vers l'état $|\,x_0\rangle\,|\,f(x_0)\rangle$, un état que l'on peut qualifier de classique au sens où toute superposition et enchevêtrement ont été détruit. Il est alors impossible d'obtenir, par une mesure subséquente, la valeur de f pour un x différent de x_0.

2.7 Exemple d'algorithme quantique : problème de Deutsch

À la vue de l'exemple précédent, il semble que le parallélisme quantique ne soit pas bien utile : il est vrai que 2^n calculs sont effectués simultanément mais, suite à la mesure, seulement $2n$ bits d'information classique sont obtenus. Toutefois, l'ingéniosité des algorithmes quantiques est de mettre à profit ce parallélisme tout en utilisant judicieusement le phénomène d'interférence et l'enchevêtrement.

L'algorithme de Deutsch est l'un des premiers algorithmes quantiques à avoir été développé. Celui-ci résout un problème académique mais est suffisamment simple pour mettre clairement en évidence les phénomènes de parallélisme et d'interférence [26].

Considérons à nouveau une fonction f n'agissant ici que sur un qubit $f : \{0,1\} \to \{0,1\}$. Le problème de Deutsch consiste à déterminer si cette fonction est 'constante' ($f(0) = f(1)$) ou 'balancée' ($f(0) \neq f(1)$). Pour répondre à cette question, on a accès à un oracle quantique effectuant la transformation U_f suivante :

$$\mathsf{U}_f : |\,x\rangle\,|\,y\rangle \to |\,x\rangle\,|\,y \oplus f(x)\rangle\,. \tag{2.14}$$

Afin de comprendre le fonctionnement de cet algorithme, appliquons U_f sur une paire de registres initialement dans l'état $|\,x\rangle\,(|\,0\rangle - |\,1\rangle)/\sqrt{2}$, avec $x \in \{0,1\}$:

de factorisation de Shor utilise ce caractère non local de l'information quantique.

$$
\begin{aligned}
\mathsf{U}_f \,|\, x\rangle \frac{|\,0\rangle - |\,1\rangle}{\sqrt{2}} &= |\,x\rangle \frac{|\,0 \oplus f(x)\rangle - |\,1 \oplus f(x)\rangle}{\sqrt{2}} \\
&= \begin{cases} |\,x\rangle \frac{|\,0\rangle - |\,1\rangle}{\sqrt{2}} & \text{si } f(x) = 0 \\ |\,x\rangle \frac{|\,1\rangle - |\,0\rangle}{\sqrt{2}} & \text{si } f(x) = 1 \end{cases} \\
&= (-1)^{f(x)} \,|\, x\rangle \frac{|\,0\rangle - |\,1\rangle}{\sqrt{2}}.
\end{aligned} \tag{2.15}
$$

Selon la valeur de $f(x)$, cette transformation ajoute une phase globale -1 laissant inchangé l'état physique de la paire de qubits. Fort de ce résultat, on applique U_f sur l'état $(|\,0\rangle + |\,1\rangle)(|\,0\rangle - |\,1\rangle)/2$:

$$
\begin{aligned}
\mathsf{U}_f \frac{|\,0\rangle + |\,1\rangle}{\sqrt{2}} \frac{|\,0\rangle - |\,1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \Bigg(&|\,0\rangle \frac{|\,0 \oplus f(0)\rangle - |\,1 \oplus f(0)\rangle}{\sqrt{2}} \\
&+ |\,1\rangle \frac{|\,0 \oplus f(1)\rangle - |\,1 \oplus f(1)\rangle}{\sqrt{2}} \Bigg)
\end{aligned} \tag{2.16}
$$

$$
= \frac{(-1)^{f(0)} \,|\,0\rangle + (-1)^{f(1)} \,|\,1\rangle}{\sqrt{2}} \frac{|\,0\rangle - |\,1\rangle}{\sqrt{2}} \tag{2.17}
$$

$$
= (-1)^{f(0)} \frac{|\,0\rangle + (-1)^{f(0) \oplus f(1)} \,|\,1\rangle}{\sqrt{2}} \frac{|\,0\rangle - |\,1\rangle}{\sqrt{2}}, \tag{2.18}
$$

où, de (2.16) à (2.17), on a utilisé (2.15). Puisque $f(0) \oplus f(1)$ vaut 0 si f est constante et 1 si f est balancée, la réponse au problème se trouve encodée par la phase relative du premier qubit. Afin d'extraire cette information, on applique une transformation d'Hadamard sur le premier qubit pour obtenir

$$
\frac{(1 + (-1)^{f(0) \oplus f(1)}) \,|\,0\rangle + (1 - (-1)^{f(0) \oplus f(1)}) \,|\,1\rangle}{\sqrt{2}}. \tag{2.19}
$$

On vérifie facilement que la mesure de cet état donne, avec certitude, $|\,1\rangle$ si f est balancée et $|\,0\rangle$ dans le cas contraire. Ainsi, par une seule utilisation de notre oracle quantique, il aura été possible d'obtenir la réponse au problème de Deutsch. Classiquement, la résolution de ce problème nécessite deux utilisations de l'oracle. Comme annoncé en début de section, cet algorithme utilise le parallélisme quantique (éq. (2.16)), l'interférence (éq. (2.19)) mais n'utilise pas l'enchevêtrement.

Cet exemple est peu naturel et ne justifie pas les efforts considérables qui sont présentement investis dans la construction d'un ordinateur quantique. Des algorithmes quantiques efficaces et ayant un potentiel d'application important existent toutefois. On pense principalement à l'algorithme de Shor (1994) et à celui de Grover (1996). Le premier résout le problème important de la factorisation d'un nombre n en ses facteurs premiers p et q. L'importance de cet algorithme vient du fait que la majeure partie des méthodes d'encryption sont fondées sur la difficulté de la factorisation. L'algorithme quantique de Shor résout ce problème en un temps exponentiellement plus court que l'algorithme classique connu (publiquement) le plus efficace. Cet algorithme quantique utilise massivement le parallélisme quantique, l'enchevêtrement et l'interférence. Quant à l'algorithme de Grover, celui-ci est utile pour la recherche dans une base de données désordonnées. Classiquement, trouver, avec une probabilité $\frac{1}{2}$, un item parmi n items demande $\frac{n}{2}$ accès à la base de données. L'algorithme quantique de Grover résout ce probleme, avec une grande probabilité de succès, en $\mathcal{O}(\sqrt{n})$ (i.e. ordre de $\sqrt{n}$) essais. Cet algorithme utilise aussi le parallélisme quantique, l'enchevêtement et l'interférence.

Puisque les algorithmes quantiques efficaces utilisent l'enchevêtrement, il semble que ce soit l'une des ressources essentielles d'où un ordinateur quantique tire sa puissance. Certains vont même jusqu'à affirmer que le principe de superposition n'est pas, en lui même, l'aspect essentiel qu'un ordinateur quantique utilise pour réussir une accélération exponentielle des temps de calcul mais que la ressource essentielle est plutôt l'enchevêtrement. Cette dernière hypothèse ne fait pas l'unanimité et fait présentement l'objet d'un débat [27, 28, 29, 30].

Chapitre 3

Décohérence

3.1 Transition du quantique au classique

L'évolution d'un système quantique est décrite par l'équation de Schrödinger

$$i\hbar\frac{d}{dt}\,|\,\psi(t)\rangle = \mathsf{H}(t)\,|\,\psi(t)\rangle\,. \tag{3.1}$$

L'Hamiltonien H étant un opérateur unitaire, cette relation est unitaire et par conséquent décrit une évolution réversible. De même, l'équation (3.1) est linéaire de sorte qu'un vecteur d'état peut évoluer dans le temps vers une superposition d'états. Pour les systèmes microscopiques, ces prédictions jouissent de vérifications expérimentales quotidiennes.

Toutefois, nos perceptions nous présentent un monde n'étant certainement pas réversible : une flèche du temps existe. De plus, nous ne percevons jamais d'objets macroscopiques existant dans une superposition d'états (ou les conséquences d'une telle superposition). Il semble donc que la relation (3.1) ne soit pas applicable au monde macroscopique.

L'interprétation de Copenhague n'indique toutefois pas de limite claire entre "monde quantique" et "monde classique", limite à partir de laquelle l'équation (3.1) n'est plus valide. Ce désaccord entre perception et prédiction est à l'origine d'un inconfort chez de nombreux physiciens et plusieurs ont cherché à résoudre cette situation en proposant de nouvelles interprétations à la théorie quantique.

Il semble cependant qu'il soit possible de venir à bout de cet inconfort à l'intérieur du cadre conceptuel fourni par l'interprétation traditionnelle de la théorie quantique, l'interprétation de Copenhague. En effet, le postulat concernant l'évolution des systèmes quantiques nous apprend que l'évolution d'un vecteur d'état est régi par l'équation (3.1), où $\mathsf{H}(t)$ est l'observable associée à l'énergie totale du système [31]. Or, un système n'est *jamais* complètement isolé de son environnement de sorte que l'équation (3.1) n'est qu'approximative si H n'est pas l'Hamiltonien complet du système étudié (poussant ce raisonnement à l'extrême, H doit être l'Hamiltonien de l'univers). De ce fait, lorsque l'on considère un système, sans tenir en compte des interactions de celui-ci avec son environnement, l'évolution n'est plus unitaire et il y a perte de cohérence vers les degrés de liberté inaccessibles de l'environnement. C'est le phénomène de décohérence [32].

Cette perte de cohérence est due à l'enchevêtrement du système étudié avec son environnement ainsi qu'à notre incapacité de tenir compte de tous les degrés de liberté de l'environnement. Pour fixer les idées, considérons par exemple un qubit (q) interagissant avec un environnement (E) initialement dans l'état $|\,0\rangle_E$, de façon à ce que l'évolution sous l'Hamiltonien total H_{qE} soit [5] :

$$\begin{aligned} \mathsf{U}_{qE} : |\,0\rangle_q\,|\,0\rangle_E &\longrightarrow \sqrt{1-p}\,|\,0\rangle_q\,|\,0\rangle_E + \sqrt{p}\,|\,0\rangle_q\,|\,1\rangle_E\,; \\ \mathsf{U}_{qE} : |\,1\rangle_q\,|\,0\rangle_E &\longrightarrow \sqrt{1-p}\,|\,1\rangle_q\,|\,0\rangle_E + \sqrt{p}\,|\,1\rangle_q\,|\,2\rangle_E\,. \end{aligned} \tag{3.2}$$

On peut considérer le système E comme étant, par exemple, l'environnement électromagnétique du qubit. Ainsi, le champ électromagnétique est initialement dans l'état vide $|\,0\rangle_E$ et, avec une probabilité $1-p$, il reste inchangé par l'interaction avec le qubit. Avec probabilité p il y a cependant création de photons, le nombre étant régi par l'état du qubit. Notons que cette interaction choisi une base préférentielle : la base de calcul $\{|\,0\rangle_q\,, |\,1\rangle_q\}$. Il s'agit de la seule base dans laquelle le qubit ne change pas de valeur lors de l'interaction.

Sur un qubit initialement dans une superposition d'états, cette interaction produit un état enchevêtré du qubit et du champ électromagnétique[1] :

$$|\psi\rangle_{qE} = \sqrt{1-p}\left(|0\rangle_q + |1\rangle_q\right)|0\rangle_E + \sqrt{p}\left(|0\rangle_q|1\rangle_E + |1\rangle_q|2\rangle_E\right). \tag{3.3}$$

Les degrés de liberté de l'environnement nous étant inaccessibles (i.e. on ne peut mesurer et manipuler individuellement les photons comme on le fait pour les qubits), on ne peut inclure l'état de celui-ci dans notre description du système. L'état final du qubit est alors donné par la matrice densité réduite obtenue de la trace sur les degrés de liberté de l'environnement

$$\begin{aligned}\rho_q &= \mathrm{Tr}_E\,|\psi\rangle_{qE}\langle\psi| \\ &= \frac{1}{2}\begin{pmatrix} 1 & 1-p \\ 1-p & 1\end{pmatrix}.\end{aligned} \tag{3.4}$$

où Tr_E signifie la trace sur la base $\{|0\rangle_E, |1\rangle_E, |2\rangle_E\}$. Ainsi, les termes diagonaux (les populations) restent invariants tandis que les termes hors-diagonaux (les cohérences) décroissent d'autant plus que la probabilité de transition est importante.

Si l'environnement a une probabilité de transition Γ par unité de temps, la propabilité p après un laps de temps Δt est $p = \Gamma\Delta t$. L'état du qubit, après un temps $t = n\Delta t$, est alors

$$\rho_q(n\Delta t) = \frac{1}{2}\begin{pmatrix} 1 & (1-p)^n \\ (1-p)^n & 1\end{pmatrix}. \tag{3.5}$$

Ce résultat est obtenu de la trace sur la matrice densité $\mathsf{U}_{qE}\left(\rho_q \otimes |0\rangle_E\langle 0|\right)\mathsf{U}^\dagger_{qE}$ dans la base $\{|0\rangle_E, |1\rangle_E, |2\rangle_E\}$. En répétant cette procédure n fois, on obtient (3.5). Pour $\Delta t \to 0$, on a $(1-p)^n = (1-\Gamma\Delta t)^{t/\Delta t} \to e^{-\Gamma t}$ et par conséquent une atténuation exponentielle des cohérences. En somme, si le qubit était initialement préparé dans l'état $a|0\rangle + b|1\rangle$, il sera, en raison de l'interaction avec son environnement, après

[1] Cet exemple précise l'idée de base préférentielle. En effet, si l'on choisit de représenter initialement le qubit dans la base $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, la relation (3.3) nous apprend que, suite à l'interaction, il n'est plus possible d'utiliser cette base pour décrire l'état du qubit. Il est toutefois toujours possible d'utiliser $\{|0\rangle, |1\rangle\}$, qui forme donc une base préférentielle.

un temps $t \gg \Gamma^{-1}$ dans la superposition incohérente $\rho_q = |a|^2 \,|\, 0\rangle \langle 0 \,| + |b|^2 \,|\, 1\rangle \langle 1 \,|$. Toute l'information de phase étant contenue dans les cohérences, on dit qu'il y a eu "écoulement" d'informations vers les degrés de liberté inaccessibles de l'environnement. Notons que la décohérence se produit dans la base préférentielle $\{|\, 0\rangle \,, |\, 1\rangle\}$.

Pour les objets macroscopiques, l'interaction avec l'environnement est importante et la décohérence est très rapide. On comprend alors pourquoi on n'observe pas de superposition d'états dans le monde macroscopique. Ainsi, à l'intérieur de l'interprétation de Copenhague, il est possible de rallier perception et prédiction[2].

Mentionnons finalement la distinction importante entre décohérence et dissipation. Par exemple, pour un grain de poussière initialement préparé dans la superposition d'états de position $|\, -x\rangle + |\, x\rangle$, la décohérence se fera sentir dès qu'un photon aura diffusé sur la poussière. Toutefois, le grain de poussière étant massif, son mouvement n'est que très peu perturbé par les photons diffusés. Il y a donc deux échelles de temps caractéristiques dans ce problème : le temps de décohérence $t_{déc}$ et le temps de dissipation t_{dis} (le temps pour qu'une proportion significative de l'impulsion du grain soit transférée aux photons). Évidemment, on peut s'attendre, pour les objets macroscopiques, à ce que $t_{déc} \ll t_{dis}$. En effet, dans un modèle particulier de décohérence [32], on a $t_{déc}/t_{dis} = 10^{-40}$ pour une particule d'un kilogramme à la température de la pièce et dans une superposition d'états de positions tel que $\Delta x = 1\ cm$. Ainsi, pour cet exemple particulier, même si le temps de dissipation était de l'ordre de l'âge de l'univers $t_{dis} \sim 10^{17} s$, les cohérences seraient détruites dans un temps $t_{déc} \sim 10^{-23} s$.

[2]On voit ici encore toute l'importance de l'information : c'est en raison d'une perte d'information que la réduction du paquet d'ondes se produit. En fait, l'information n'est pas réellement perdue mais elle se trouve encodée dans les corrélations non locales entre le système étudié et son environnment. Ainsi, il est *en principe* possible d'extraire l'information de phase ayant "coulé" vers l'environnement et ainsi reconstruire la superposition d'états. Toutefois, *en pratique* une telle mesure apparaît impossible.

3.2 Décohérence en tant que source d'erreurs

Pour profiter de la puissance de calcul d'un ordinateur quantique, celui-ci doit être capable de supporter des superpositions et de l'enchevêtrement pendant tout le temps du calcul et ce sur un grand nombre de qubits. Malheureusement, d'après la discussion précédente, il est clair que les qubits ne sont jamais complètement isolés de leur environnment. Ainsi, un ordinateur initialement découplé de l'environnement

$$|\,\psi(0)\rangle = \underbrace{\sum\nolimits_x a_x\,|\,x\rangle}_{\text{Ordinateur}} \quad \otimes \quad \underbrace{|\,e_0\rangle}_{\text{Environnement}}\,, \tag{3.6}$$

se retrouve rapidement enchevêtré avec celui-ci

$$|\,\psi(t)\rangle = \sum_x a_x\,|\,x\rangle \otimes |\,e_x(t)\rangle\,. \tag{3.7}$$

En raison de cette interaction, il y a décohérence et la perte d'information résultante peut être considérée comme la création d'erreurs. Pour fixer les idées, considérons le modèle suivant de décohérence : l'interaction générale d'un qubit avec son environnement conduisant à l'évolution

$$\begin{aligned} |\,e\rangle\,|\,0\rangle &\to |\,e_0\rangle\,|\,0\rangle + \left|\,e_0^B\right\rangle|\,1\rangle\,; \\ |\,e\rangle\,|\,1\rangle &\to |\,e_1\rangle\,|\,1\rangle + \left|\,e_1^B\right\rangle|\,0\rangle\,, \end{aligned} \tag{3.8}$$

avec $|\,e_{0,1}\rangle$ et $\left|\,e_{0,1}^B\right\rangle$ l'état de l'environnement après l'interaction (ces états ne sont généralement pas normalisés ou orthogonaux) [33, 34]. Cette interaction peut être réécrite sous la forme suivante

$$
\begin{aligned}
\frac{1}{\sqrt{2}} \,|\, e \rangle \, (|\, 0\rangle \pm |\, 1\rangle) \rightarrow \frac{1}{\sqrt{2}} \Big\{ \,|\, e_0\rangle \,|\, 0\rangle + \left|\, e_0^B \right\rangle |\, 1\rangle \pm |\, e_1\rangle \,|\, 1\rangle \pm \left|\, e_1^B \right\rangle |\, 0\rangle \Big\} \\
= \frac{1}{2\sqrt{2}} \Big\{ (|\, e_0\rangle + |\, e_1\rangle) \, (|\, 0\rangle \pm |\, 1\rangle) \\
+ (|\, e_0\rangle - |\, e_1\rangle) \, (|\, 0\rangle \mp |\, 1\rangle) \\
+ \left(\left|\, e_0^B \right\rangle + \left|\, e_1^B \right\rangle \right) (|\, 1\rangle \pm |\, 0\rangle) \\
+ \left(\left|\, e_0^B \right\rangle - \left|\, e_1^B \right\rangle \right) (|\, 1\rangle \mp |\, 0\rangle) \Big\} \\
= \frac{1}{\sqrt{2}} \Big\{ \,|\, e_+\rangle \, \mathbb{I} + |\, e_-\rangle \, \sigma_z + \left|\, e_+^B \right\rangle \sigma_x - \left|\, e_-^B \right\rangle i\sigma_y \Big\} \, (|\, 0\rangle \pm |\, 1\rangle) \, ,
\end{aligned}
\tag{3.9}
$$

avec $|\, e_\pm\rangle = (|\, e_0\rangle \pm |\, e_1\rangle)/2$ et $\left|\, e_\pm^B \right\rangle = (\left|\, e_0^B \right\rangle \pm \left|\, e_1^B \right\rangle)/2$, σ_α une matrice de Pauli et $\mathbb{I}$ l'opérateur identité. En raison de la linéarité, l'état d'un registre de n qubits pour lequel le $j^{\text{ième}}$ qubit subit une interaction du type (3.8) peut alors s'écrire

$$
|\, e\rangle \sum_x a_x \,|\, x\rangle \rightarrow \Big\{ \,|\, e_+\rangle \, \mathbb{I} + |\, e_-\rangle \, \sigma_z^j + \left|\, e_+^B \right\rangle \sigma_x^j - \left|\, e_-^B \right\rangle i\sigma_y^j \Big\} \sum_x a_x \,|\, x\rangle \, , \tag{3.10}
$$

avec σ_α^j n'agissant que sur le $j^{\text{ième}}$ qubit. Ainsi, l'interaction avec l'environnement se réduit à quatre types d'erreurs sur un qubit. Premièrement le qubit reste inchangé (correspondant à l'opérateur identité) et devient corrélé à $|\, e_+\rangle$. Ensuite, le qubit subit une erreur de phase (correspondant à σ_z) et devient corrélé à $|\, e_-\rangle$. Troisièmement, la valeur du qubit bascule (correspondant à σ_x), cette possibilité est reliée à $\left|\, e_+^B \right\rangle$. Et, finalement, le qubit subit les deux erreurs précédentes : changement de phase et bascule (correspondant à $-i\sigma_y$) pour être corrélé avec $\left|\, e_-^B \right\rangle$.

Puisque les matrices de Pauli forment une base pour les matrices 2 par 2 [31], toute erreur sur un qubit peut être réduite à une combinaison linéaire des quatre erreurs précédentes. Ces quatre erreurs décrivent ainsi toutes les possibilités.

Chapitre 4

Correction quantique d'erreurs

Une machinerie très sophistiquée a été développée pour la correction classique d'erreurs [35]. Ces techniques sont utilisées dans le but de protéger d'erreurs éventuelles la mémoire des ordinateurs conventionnels et les communications. Le principe à la base de ces techniques est la redondance.

L'exemple suivant présente le code correcteur classique probablement le plus simple (et le moins efficace) : on remplace un bit par trois copies de celui-ci

$$0 \to (000); \qquad\qquad 1 \to (111). \tag{4.1}$$

Une erreur peut faire basculer la valeur d'un bit, du premier par exemple

$$(000) \to (100); \qquad\qquad (111) \to (011), \tag{4.2}$$

mais il est toujours possible de récupérer la valeur initiale par vote majoritaire. Ce simple code peut corriger une erreur mais est mis en défaut par deux erreurs.

De façon plus formelle, les "mots logiques" de k bits (dans l'exemple précédent 0 et 1) sont encodées en "mots de code" de $n > k$ bits (000 ou 111). Ces derniers sont choisis parmi les 2^n séquences de n bits de façon à ce que, suite à l'altération d'au plus t bits, les mots logiques puissent être récupérés. On dit alors qu'il s'agit d'un code de classe $[[k, n, t]]$ encodant k bits en n bits et pouvant corriger jusqu'à t

erreurs[1]. L'exemple précédent est donc un code $[[1, 3, 1]]$.

Ainsi, on protège l'information classique en utilisant le fait qu'il est possible de la copier et qu'elle est numérique : une erreur sur un bit ne peut qu'inverser la valeur de ce bit et non le changer d'une petite quantité. Toutefois, ces deux propriétés font défaut à l'information quantique : il n'est pas possible de copier l'information quantique et celle-ci est analogique, i.e. un qubit $a\,|\,0\rangle + b\,|\,1\rangle$ peut prendre un continuum de valeurs données par les coefficients a et b. Ainsi, comme présenté au chapitre précédent, on doit faire face en informatique quantique non pas à un, mais plutôt quatre types d'erreurs.

De plus, la mesure perturbe inévitablement l'état du système. La mesure qui précède le vote majoritaire dans le cas du code classique $[[1, 3, 1]]$ correspond ainsi à une étape destructrice et irréversible dans le cas quantique. Il est donc impossible d'utiliser directement les techniques classiques pour protéger l'information quantique.

De même, en plus des erreurs dues à la décohérence, il est aussi nécessaire de corriger les erreurs occasionnées par les portes logiques imparfaites. En effet, il est fort probable que les rotations engendrées par les portes quantiques ne soit pas tout à fait exactes. Ainsi, si l'on cherche à appliquer l'opération U, l'opération effectivement réalisée sera en fait

$$\mathsf{U}' = \mathsf{U}(1 + \mathcal{O}(\varepsilon)). \tag{4.3}$$

L'opération effectuée diffère alors d'une quantité de l'ordre de ε, une petite constante, de la transformation voulue. Après environ $1/\varepsilon$ opérations, ces erreurs deviennent assez importantes et faussent les résultats.

[1]Dans la littérature, on note généralement par $[k, n, t]$ ($[[k, n, t]]$) les codes classiques (quantiques). Dans ce texte, on ne suivra pas cette convention : $[[k, n, t]]$ sera utilisé pour désigner les codes classiques et quantiques.

4.1 Code quantique $[[1,9,1]]$ de Shor

Malgré ces difficultés apparentes, Peter Shor [33] et indépendamment Andrew Steane [36] ont découvert en 1995 comment encoder l'information quantique pour la protéger. Ceux-ci ont montré qu'il est possible d'utiliser l'enchevêtrement afin de distribuer l'information de k qubits de façon non locale sur $n > k$ qubits. Ainsi, les codes correcteurs quantiques combattent l'enchevêtrement (avec l'environnement qui est cause de la décohérence) à l'aide de l'enchevêtrement !

Afin de comprendre comment fonctionnent ces codes, étudions plus en détail le code proposé par Shor [5, 33]. Considérons d'abord l'erreur correspondant à la matrice de Pauli σ_x : le renversement de l'état d'un qubit ("bit flip"). Il s'agit du même type d'erreur que rencontrée dans le cas classique, ce qui suggère d'utiliser un code basé sur l'exemple de la section précédente :

$$|\,0\rangle \to |\,0_L\rangle \equiv |\,000\rangle\,; \qquad\qquad |\,1\rangle \to |\,1_L\rangle \equiv |\,111\rangle\,, \tag{4.4}$$

avec $|\,0_L\rangle$ et $|\,1_L\rangle$ les nouveaux états logiques. Une superposition d'états devient alors

$$a\,|\,0\rangle + b\,|\,1\rangle \to a\,|\,0_L\rangle + b\,|\,1_L\rangle \equiv a\,|\,000\rangle + b\,|\,111\rangle\,. \tag{4.5}$$

Ce code ne viole pas le principe de "non clonage" puisque l'état final n'est pas un produit tensoriel de l'état du qubit logique avec ses copies mais correspond plutôt à un état enchevêtré. Cet état est bien connu dans le milieu de l'information quantique et porte le nom d'état GHZ (pour Greenberger-Horne-Zeilinger). Il s'agit, dans le cas $a = b$, de l'état d'enchevêtrement maximal pour trois qubits [37].

Après transmission de l'état encodé (transmission dans le temps (mémoire) ou dans l'espace (communication)) un des qubits voit sa valeur être inversée

$$a\,|\,000\rangle + b\,|\,111\rangle \to a\,|\,100\rangle + b\,|\,011\rangle \tag{4.6}$$

Dans le cas classique, l'étape suivante est la mesure de chaque bit individuellement afin de procéder au vote majoritaire. Cependant, si l'on mesure ici le premier qubit et que l'on obtient $|\,1\rangle$, l'état du système est projeté vers $|\,100\rangle$ et l'information contenue dans les coefficients a et b est perdue.

On cherche donc ici à connaître, s'il y a lieu, la position du qubit erroné sans perturber l'état encodé. Pour ce faire, on utilise le circuit de la figure 4.1. Dans ce circuit, les trois lignes du haut représentent les qubits du code : $a|\underset{q_2}{\underset{\uparrow}{0}}\,\underset{q_1}{\underset{\uparrow}{0}}\,\underset{q_0}{\underset{\uparrow}{0}}\rangle + b|\underset{q_2}{\underset{\uparrow}{1}}\,\underset{q_1}{\underset{\uparrow}{1}}\,\underset{q_0}{\underset{\uparrow}{1}}\rangle$, tandis que celles du bas sont des qubits auxiliaires initialisés à $|\,0\rangle$.

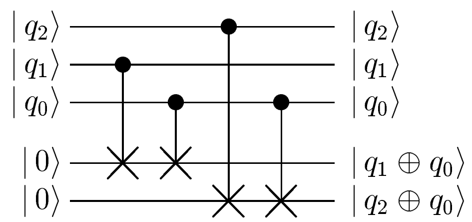


Figure 4.1: Circuit de détection pour les erreurs σ_x pour le code (4.5).

Après avoir appliqué ce circuit, les qubits auxiliaires prennent les valeurs $|\,q_1 \oplus q_0\rangle$ et $|\,q_2 \oplus q_0\rangle$. Ainsi, si q_1 est différent de q_0, le premier qubit auxiliaire prend la valeur $|\,1\rangle$ et de même pour le second dans le cas où q_2 est différent de q_0. Appliqué sur l'état (4.6), on obtient

$$\Big(a\,|\,100\rangle + b\,|\,011\rangle\Big)\,|\,01\rangle\,. \tag{4.7}$$

On mesure ensuite les auxiliaires dans la base de calcul. Il s'agit d'une mesure partielle qui n'affecte pas l'information encodée par le mot de code. Comme le montre le tableau 4.1, la valeur des qubits auxiliaires, lue comme un nombre binaire, donne la position du qubit erroné. Connaissant, s'il y a lieu, le position de l'erreur, il ne reste plus qu'à appliquer $\mathsf{R}_x(\pi) = \sigma_x$ sur le qubit erroné afin de retrouver l'état original.

Cette technique de détection et correction peut aussi venir à bout des erreurs dues aux opérations logiques imparfaites. Considérons l'erreur suivante (on omet ici les facteurs de normalisation)

$(q_1 \oplus q_0, q_2 \oplus q_0)$	qubit erroné
(0,0)	aucun
(0,1)	q_2
(1,0)	q_1
(1,1)	q_0

Tableau 4.1: Relation entre la valeur des auxiliaires et la position du qubit erronée pour le code de l'équation (4.5).

$$|\,000\rangle + |\,111\rangle \to \sqrt{1-\varepsilon}\,(|\,000\rangle + |\,111\rangle) + \sqrt{\varepsilon}\,(|\,100\rangle + |\,011\rangle)\,, \tag{4.8}$$

où ε est une petite constante. L'application du circuit de détection sur le membre de droite de l'expression précédente produit

$$\begin{aligned} &\left\{\sqrt{1-\varepsilon}\,(|\,000\rangle + |\,111\rangle) + \sqrt{\varepsilon}\,(|\,100\rangle + |\,011\rangle)\right\}|\,00\rangle \\ &\qquad \to \sqrt{1-\varepsilon}\,\{|\,000\rangle + |\,111\rangle\}\,|\,00\rangle + \sqrt{\varepsilon}\,\{|\,100\rangle + |\,011\rangle\}\,|\,01\rangle\,. \end{aligned} \tag{4.9}$$

On mesure ensuite les auxiliaires pour obtenir $|\,00\rangle$ ($|\,01\rangle$) avec une probabilité $|1-\varepsilon|^2$ ($|\varepsilon|^2$). Ainsi, avec une grande probabilité on obtient $|\,00\rangle$ et l'état du système est projeté vers $|\,000\rangle + |\,111\rangle$; aucune correction n'est alors nécessaire. Dans le cas où $|\,01\rangle$ est obtenu, le système est projeté vers $|\,100\rangle + |\,011\rangle$ et on corrige en renversant la valeur du premier qubit. Cette technique de correction peut donc corriger les erreurs continues (i.e. analogiques) en projetant l'état encodé dans un sous-espace où l'erreur peut être corrigée. Cette méthode numérise donc en quelque sorte les erreurs analogiques.

En plus des renversement de qubits, il est nécessaire de prendre en considération les erreurs de phase (σ_z)

$$a\,|\,0_L\rangle + b\,|\,1_L\rangle \to a\,|\,0_L\rangle - b\,|\,1_L\rangle\,. \tag{4.10}$$

Ce type d'erreur peut être détecté puis corrigé en utilisant à nouveau la redondance propre aux techniques de correction d'erreurs mais, dans ce cas, pour l'information de phase

$$\begin{aligned}
|\,0\rangle \to |\,0_L\rangle &\equiv (|\,000\rangle + |\,111\rangle)\,(|\,000\rangle + |\,111\rangle)\,(|\,000\rangle + |\,111\rangle)\,; \\
|\,1\rangle \to |\,1_L\rangle &\equiv \underbrace{(|\,000\rangle - |\,111\rangle)}_{\text{Bloc\#1}}\,\underbrace{(|\,000\rangle - |\,111\rangle)}_{\text{Bloc\#2}}\,\underbrace{(|\,000\rangle - |\,111\rangle)}_{\text{Bloc\#3}}.
\end{aligned} \tag{4.11}$$

Un qubit est donc encodé en trois blocs de trois qubits. On obtient (4.11) à l'aide du circuit de la figure 4.2[2].

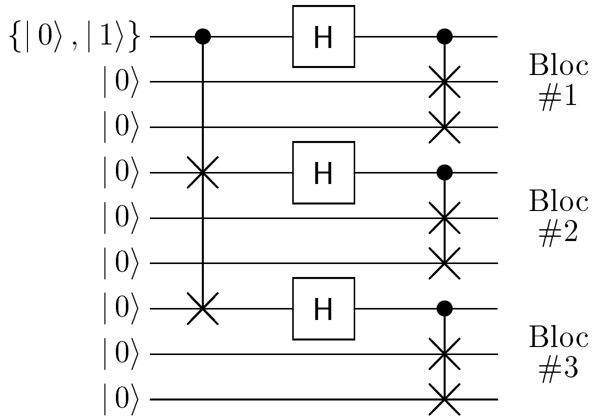
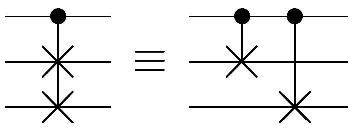


Figure 4.2: Circuit encodeur pour le code $[[1,9,1]]$ de Shor. La première ligne horizontale représente le qubit logique et les 8 dernières des auxiliaires.

La détection d'erreur de phase est réalisée à l'aide du circuit de la figure 4.3. Les neufs premières lignes sont les qubits du code et les autres des auxiliaires. Les opérations d'Hadamard sur les qubits du codes ont pour effet d'encoder l'information de phase de chacun des blocs dans les qubits du bloc correspondant. Par exemple, pour un bloc dans l'état $|\,000\rangle + |\,111\rangle$ on a

$$\frac{1}{\sqrt{2}}\,(|\,000\rangle + |\,111\rangle) \xrightarrow{\mathsf{H}_1,\mathsf{H}_2,\mathsf{H}_3} \frac{1}{2}\,(|\,000\rangle + |\,011\rangle + |\,101\rangle + |\,110\rangle)\,. \tag{4.12}$$

[2]On utilise dans ce circuit la notation abrégée suivante :



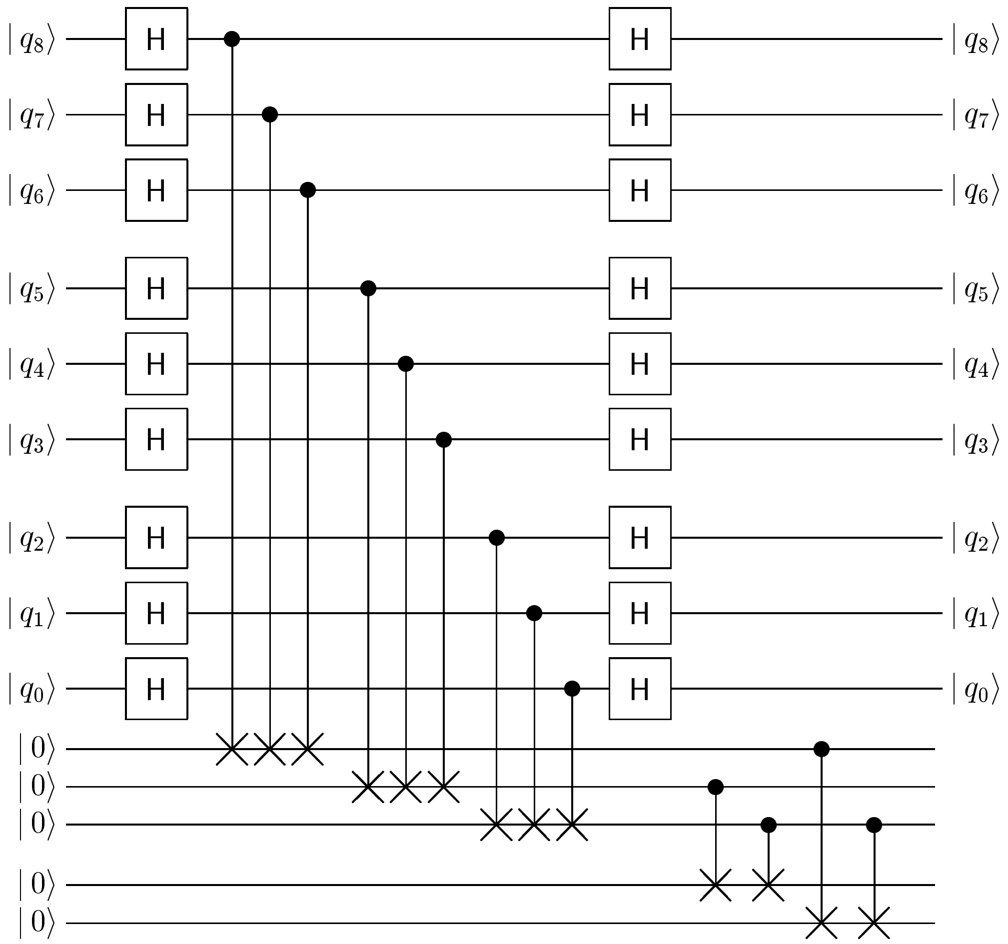


Figure 4.3: Circuit de détection servant à la détection d'erreur de phase pour le code $[[1,9,1]]$ de Shor.

Tous les états de cette superposition ont la même parité et c'est celle-ci qui contient l'information de phase. On applique ensuite un CN sur chacun des qubits encodeurs de façon à écrire cette information de phase sur les auxiliaires. Pour l'état (4.12), cette opération laisse inchangé l'auxiliaire correspondant (dans le cas $|000\rangle - |111\rangle$, on vérifie que l'auxiliaire prend alors la valeur $|1\rangle$). Notons que ces opérations n'enchevêtrent pas les blocs et leur auxiliaire. Puisque $\mathsf{HH} = \mathbb{I}$, la seconde application des portes d'Hadamard ne fait que retourner les blocs vers leur état initial. On trouvera en annexe A une vérification de ce circuit par un code développé à l'aide du langage de manipulation symbolique *Mathematica*.

La seconde étape de détection d'erreur est similaire au cas de la figure 4.1 et indique, s'il y a lieu, la position du bloc ayant une phase différente par rapport aux autres. Suite à l'opération de ce circuit, il ne reste plus qu'à mesurer les deux derniers auxiliaires et à corriger l'erreur de phase en appliquant $\mathsf{R}_z(\pi) = \sigma_z$ sur le qubit erroné. Pour corriger une erreur correspondant à $-i\sigma_y$ sur un qubit, on applique successivement les techniques de correction d'erreurs de renversement et de phase.

L'équation 4.11 correspond au code $[[1,9,1]]$ de Shor et, à l'aide des circuits de détection d'erreurs de renversement (figure 4.1) et de phase (figure 4.3), protège un qubit de l'une des quatre erreurs possibles[3] : $\mathbb{I}$,σ_z, σ_x et $-i\sigma_y$.

On adapte facilement cette technique à la correction de deux erreurs. En effet, pour l'exemple classique (4.1), la généralisation à deux erreurs est

$$0 \rightarrow (00000); \qquad\qquad 1 \rightarrow (11111). \tag{4.13}$$

Par vote majoritaire, on peut alors détecter puis corriger jusqu'à 2 erreurs. Par analogie, on obtient alors pour le cas quantique

$$\begin{aligned} |\,0\rangle \rightarrow |\,0_L\rangle \equiv\, & (|\,00000\rangle + |\,11111\rangle)\,(|\,00000\rangle + |\,11111\rangle)\,(|\,00000\rangle + |\,11111\rangle) \\ & (|\,00000\rangle + |\,11111\rangle)\,(|\,00000\rangle + |\,11111\rangle)\,; \end{aligned} \tag{4.14}$$

$$\begin{aligned} |\,1\rangle \rightarrow |\,1_L\rangle \equiv\, & (|\,00000\rangle - |\,11111\rangle)\,(|\,00000\rangle - |\,11111\rangle)\,(|\,00000\rangle - |\,11111\rangle) \\ & (|\,00000\rangle - |\,11111\rangle)\,(|\,00000\rangle - |\,11111\rangle)\,; \end{aligned} \tag{4.15}$$

Il s'agit d'un code $[[1,25,2]]$. En poussant davantage l'analogie, pour la correction d'un nombre arbitraire t d'erreurs, on obtient un code $[[1,2t+1,t]]$ dans le cas classique et $[[1,(2t+1)^2,t]]$ dans le cas quantique. On peut donc corriger un nombre arbitraire

[3] En fait, ce code peut détecter et corriger un reversement *par* bloc de 3 qubits et un reversement de phase parmi les 3 blocs. Toutefois, si dans un même bloc plus d'un qubit est inversé ou si plus d'un bloc à subit une erreur de phase, ce code ne corrigera pas vers le bon état. On place donc ce code dans la classe $[[1,9,1]]$ puisqu'il ne peut corriger qu'une erreur générale sur un des 9 qubits encodeurs.

d'erreurs à l'aide de ce type de code. Toutefois, la taille des mots de code croît rapidement et, de ce fait, la probabilité que des erreurs surviennent aussi.

Notons qu'avant une nouvelle utilisation, les qubits auxiliaires doivent être réinitialisés. Cette opération n'est pas réversible et la correction d'erreurs est par conséquent un processus dissipatif.

Notons finalement que le succès des codes correcteurs quantiques est dû au fait que l'information est distribuée non localement sur les qubits du mot de code. De ce fait, mesurer un seul qubit ne donne aucune information : on ne peut déterminer par une mesure sur un seul qubit si l'état encodé est $|0\rangle$ ou $|1\rangle$. L'environnement peut ainsi perturber un qubit mais il n'y a pas d'information perdue parce qu'un seul qubit n'en contient pas. En d'autres mots, l'information non locale des mots de code est invulnérable face aux perturbations locales.

4.2 Calcul quantique tolérant aux imperfections

L'extension naïve du code $[[1, 9, 1]]$ de Shor en un code corrigeant un nombre arbitraire d'erreurs est très inefficace puisqu'elle utilise un grand nombre de qubits. Des codes correcteurs plus efficaces existent toutefois pour la correction d'une [34] et de plusieurs erreurs [5]. Cependant, ces techniques exigent que les opérations d'encodage et de correction soient effectuées sans erreurs. Dans le cas contraire, l'utilisation de ces techniques ne fait qu'entraîner des erreurs supplémentaires et le calcul en cours déraille rapidement.

Pour venir à bout de ce problème, des techniques de calcul quantique tolérants aux imperfections (*fault-tolerant quantum computing*) ont été mises au point [38, 39, 40]. Ces méthodes utilisent un encodage répété des qubits : un qubit est encodé (généralement à l'aide du code Calderbank-Shor-Steane (CCS) $[[1, 7, 1]]$, voir par exemple [39]) puis chacun des qubits encodeurs sont à leur tour encodés de la même façon. On répète ce processus jusqu'à avoir L niveaux d'encodage. On applique ensuite, de façon répétée, les techniques de correction d'erreurs simultanément avec le calcul de sorte qu'il est possible de corriger les erreurs dues à la décohérence et aux portes logiques imparfaites au fur et à mesure qu'elles surviennent.

En utilisant cet enchaînement de plusieurs niveaux d'encodage, on peut vérifier que si le taux d'erreur (sur les qubits encodeurs) par porte et par unité de temps est plus petit qu'un certain seuil, il est possible de réaliser des calculs quantiques arbitrairement longs avec un taux d'erreur sur les qubits logiques arbitrairement petit. Ce taux dépend du modèle de décohérence étudié et varie entre 10^{-4} et $1/700$ [41].

Ces techniques de calcul quantique tolérant aux imperfections exigent que les erreurs sur chaque qubit soient indépendantes. Ce critère n'est cependant pas toujours justifié physiquement [42, 43].

Chapitre 5

Qubits supraconducteurs

5.1 Défis techniques

Les années quatre-vingt ont connu, avec les travaux de Benioff [44], Feynman [45] et Deutsch [46], les premiers balbutiements de l'informatique quantique. Ces premières investigations s'intéressaient avant tout à des preuves de principe basées sur des modèles abstraits de systèmes quantiques dont la dynamique pouvait être contrôlée de façon à exécuter un calcul. Ces explorations théoriques ont toutefois fait l'objet de critiques importantes, principalement parce qu'elles étaient totalement déconnectées de la réalité expérimentale [47].

Ce n'est qu'avec la présentation par Shor (1994) d'un algorithme quantique de factorisation [48] que la question de réaliser concrètement un ordinateur quantique a réellement été abordée.

Afin de pouvoir manipuler l'information quantique en préservant la cohérence de phase, un système physique doit répondre à plusieurs critères [49] :

1. L'espace d'Hilbert doit être connu précisément.

2. On doit pouvoir initialiser le système dans un état connu (par exemple $|0\rangle\,|0\rangle \cdots |0\rangle$).

3. Les qubits doivent être isolés de leur environnement de façon à ce que le temps de décohérence soit suffisamment long pour pouvoir mener à terme les calculs.

4. On doit être capable d'appliquer, avec une grande précision, un ensemble complet de portes logiques.

5. On doit disposer d'une méthode très efficace de mesure des qubits.

Ces contraintes sont très exigeantes et, jusqu'à un certain point, contradictoires : les qubits doivent être très bien isolés mais on doit y avoir accès pour les manipuler et les mesurer.

Plusieurs architectures satisfaisant plus ou moins ces contraintes ont néanmoins été proposées dans la deuxième moitié de cette décénnie. Parmi celles-ci, on pense en particulier aux pièges à ions linéaires (Cirac et Zoller, 1995 [50]), aux cavités optiques (Turchette *et. al.*, 1995 [51]) et plus récemment à l'utilisation des techniques de résonance magnétique nucléaire (Cory *et. al.*, 1997 [52] et indépendamment Gershenfeld et Chang, 1997 [53]).

Appliquer ces suggestions à la réalisation d'un ordinateur quantique ayant un petit nombre de qubits (1 ou 2) ne pose pas de problème majeur. Toutefois, l'extension de ces idées à un plus grand nombre de qubits s'avère un problème de taille. Ainsi, à ce jour, à l'aide des techniques de RMN, qui mènent le peloton, seulement 7 qubits ont pu être contrôlés de façon cohérente [54] et ce malgré le travail de nombreux groupes de recherche depuis maintenant plus de deux ans.

Dans le but de construire un ordinateur quantique utile ($n > 1000$), la capacité d'intégrer un grand nombre de qubits est cruciale et plusieurs s'accordent maintenant pour dire qu'à long terme, les techniques plus traditionnelles de micro fabrication seront la meilleure façon de relever ce défi [55, 56]. En effet, par l'utilisation de ces techniques, la recherche sur les ordinateurs quantiques bénéficierait directement de la grande expertise déjà acquise et des développements futurs dans le domaine de la micro fabrication et de la physique des systèmes mésoscopiques. C'est ainsi que beaucoup d'efforts ont été investis dans la recherche de systèmes mésoscopiques répondant aux 5 critères précédents et plusieurs architectures ont déjà été proposées :

points quantiques [57], transistors à résonance paraélectronique [58, 59], jonctions Josephson [60, 61, 4], ...

Dans ce chapitre on s'intéresse à l'une de ces dernières suggestions basée sur l'effet Josephson et due à Alexandre M. Zagoskin de l'Université de la Colombie-Britannique [4]. On commencera par une présentation de quelques effets quantiques macroscopiques observés dans les supraconducteurs. Par la suite on s'attardera au concept de niveaux d'Andréev puis à un cas particulier de jonction Josephson : les jonctions DND triangulaires. Ce dernier exemple nous conduira naturellement aux qubits supraconducteurs qui nous intéressent ici. Par la suite, on décrira comment réaliser un ensemble complet de portes logiques sur ce système [62], pour finalement aborder quelques perspectives d'avenir. Rappelons que ce chapitre, et plus particulièrement la section §5.7, contient la plupart des résultats originaux de ce mémoire.

5.2 Effets quantiques macroscopiques

Dans la recherche d'un système répondant aux critères précédents, les supraconducteurs semblent être un choix naturel. En effet, la supraconductivité et ses conséquences indiquent que la cohérence quantique de phase peut être maintenue sur des longueurs macroscopiques dans les supraconducteurs. Dans cette section, nous nous attarderons à quelques-unes de ces conséquences.

5.2.1 Effet Josephson

Premièrement, il est bien connu qu'en l'absence de champ électrique et magnétique une jonction formée de deux supraconducteurs de type s séparés d'une mince couche isolante (jonction SIS) est traversée par un courant continu spontané

$$I_s = I_c \sin\phi. \tag{5.1}$$

Dans cette expression, ϕ est la différence de phase entre les supraconducteurs et I_c le courant critique, i.e. le supercourant maximal supporté par la jonction. De même, en présence d'une différence de potentiel V entre les supraconducteurs, la différence de phase évolue dans le temps selon la relation

$$\frac{d\phi}{dt} = \frac{2eV}{\hbar}, \tag{5.2}$$

de sorte que le courant traversant la jonction est un courant alternatif d'amplitude I_c et de fréquence $2eV/\hbar$. Utilisant les relations (5.1) et (5.2), on obtient l'énergie libre emmagasinée dans la jonction par intégration du travail électrique

$$\begin{aligned} F &= \int I_s V \, dt \\ &= \frac{\hbar}{2e} \int I_s \, d\phi \\ &= a - E_J \cos\phi, \end{aligned} \tag{5.3}$$

avec $E_J \equiv \hbar I_c/2e$ et a une constante d'intégration.

Les relations (5.1) et (5.2) correspondent à l'effet Josephson CC et CA, respectivement. Celles-ci s'obtiennent facilement en considérant le transport de paires de Cooper par effet tunnel cohérent entre les électrodes supraconductrices [63].

5.2.2 Fluctuations de phase

Dans la discussion précédente, la différence de phase supraconductrice ϕ a été considérée comme une variable semi-classique ayant une valeur bien définie. Toutefois, il existe une relation d'incertitude

$$\Delta N \Delta\phi \gtrsim 1 \tag{5.4}$$

limitant la précision avec laquelle N et ϕ peuvent être déterminés simultanément[1] (N est ici le nombre de paires de Cooper transférées d'une électrode à l'autre),[65, 64].

[1]Notons que cette relation n'est pas juste si ΔN est très petit. En effet, si $\Delta N \to 0$ alors, selon (5.4), $\Delta\phi \to \infty$ ce qui n'a aucun sens puisque la phase est définie modulo 2π. La relation d'incertitude (5.4) n'est donc raisonnable que pour ΔN grand et $\Delta\phi$ petit. Voir la section §1.4.3 de la référence [64] pour plus de détails à ce sujet.

Dans le cas d'un système macroscopique, N est très grand et il est alors possible de connaître N et ϕ avec peu d'incertitude relative.

Toutefois, pour un système mésoscopique, ce n'est plus le cas et la phase n'est plus une quantité bien définie. Pour s'en convaincre, considérons maintenant une jonction isolée de capacité C et à température nulle. Utilisant la relation 5.3 et incluant le terme capacitif, l'énergie de la jonction s'écrit, à une constante près,

$$E = -E_J \cos\phi + \frac{Q^2}{2C}, \tag{5.5}$$

où $Q = 2Ne$. En représentation de phase [64], on obtient l'Hamiltonien correspondant à l'aide de la transformation $N \rightarrow i\frac{\partial}{\partial\phi}$:

$$H = -E_J \cos\phi - 4E_c \partial_\phi^2, \tag{5.6}$$

avec $E_c = e^2/2C$. Le premier terme de cette relation peut être assimilé à une énergie potentielle et le second à une énergie cinétique. Lorsque $E_J \gg E_c$, le système tend a maximiser le premier terme, $\cos\phi$, de (5.6) de façon à minimiser l'énergie. De ce fait, la phase est localisée autour de $\phi = 0$ et l'incertitude sur cette quantité est petite. À l'opposé, si $E_c \gg E_J$, le système maximise plutôt le second terme et la phase est complètement délocalisée. L'incertitude sur cette quantité est alors grande. Ainsi, pour une faible capacité, et par conséquent une jonction de petite taille, la phase n'est pas une quantité bien définie et il y a fluctuation de phase car E_c domine.

5.2.3 Observations expérimentales

Les effets quantiques macroscopiques dans les supraconducteurs ont reçu beaucoup d'attention et ce principalement depuis les travaux de A.J. Leggett au début des années 1980. Celui-ci s'intéressait à la validité de la théorie quantique au niveau macroscopique et, en particulier, à déterminer quels systèmes physiques pourraient présenter des phénomènes quantiques macroscopiques : effet tunnel macroscopique (effet tunnel entre deux états ayant des propriétés macroscopiques différentes) et effet tunnel cohérent macroscopique (oscillations cohérentes entre ces deux états macroscopiques). Leggett arrive alors à la conclusion que les systèmes supraconducteurs, et en particulier les jonctions Josephson, sont parmi les meilleurs candidats [66].

Par la suite, Caldeira et Leggett [67] et Leggett *et. al.* [68] se sont intéressés aux effets de la dissipation (du couplage à l'environnement) sur ces phénomènes quantiques macroscopiques. La conclusion principale de ces études est que l'environnement tend à supprimer les effets quantiques (voir section §3.1). En particulier, l'effet tunnel cohérent macroscopique est atténué beaucoup plus rapidement que l'effet tunnel macroscopique [66].

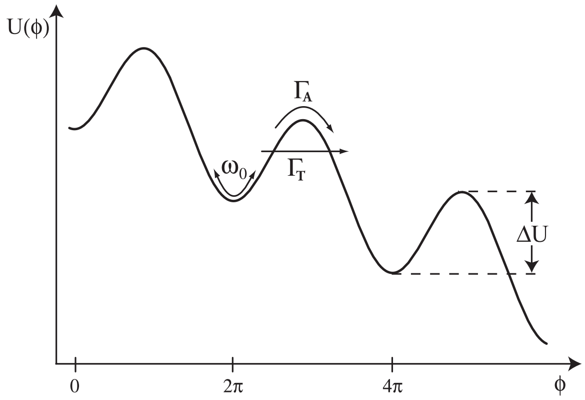


Figure 5.1: Potentiel effectif pour l'analogue mécanique d'une jonction Josephson SIS traversée par un courant I. Les taux d'activation thermique et tunnel sont respectivement Γ_A et Γ_T. ω_0 est la fréquence des petites oscillations dans un puits et ΔU la hauteur de la barrière de potentiel. Cette hauteur est fonction du courant appliqué.

Depuis ces travaux, beaucoup d'efforts ont été investis dans le but d'observer expérimentalement ces phénomènes dans les systèmes supraconducteurs. En particulier, Martinis *et. al.* [69] ont pu observer les conséquences de l'effet tunnel macroscopique du degré de liberté de phase dans une jonction Josephson SIS. Pour observer cet effet, ceux-ci ont appliqué un courant continu I sur une jonction SIS. On peut montrer que dans cette situation, la dynamique de la jonction est équivalente à celle d'une particule de masse $M = (\hbar/2e)^2 C$ se déplaçant dans le potentiel

$$U(\phi) = -E_J \cos\phi - \frac{\hbar I}{2e}\phi, \tag{5.7}$$

de la figure 5.1, où ϕ joue le rôle de coordonnée. Lorsque le courant I est faible, la phase reste piégée dans un des minima de ce potentiel et, tel qu'indiqué par la relation (5.2), on ne mesure pas de différence de potentiel aux bornes de la jonction.

Deux mécanismes permettent à la phase de s'échapper d'un minimum local : l'activation thermique (la particule passe par dessus la barrière de potentiel) et l'effet tunnel (celle-ci passe au travers de la barrière), voir figure 5.1. Le taux d'activation thermique est donné par $\Gamma_A \sim \omega_0 e^{-\Delta U/k_B T}$, où ω_0 est la fréquence des petites oscillations dans un puits et ΔU la hauteur de la barrière de potentiel. Pour de faible températures ce processus est gelé et il n'y a plus que l'effet tunnel, dont le taux est donné par la relation $\Gamma_T \sim \omega_0 e^{-\Delta U/\hbar\omega_0}$, qui permet à la phase de quitter un minimum local. Notons que lorsque la particule quitte un minimum par l'un de ces processus, celle-ci a suffisamment d'énergie et se met à dévaler le potentiel de la figure 5.1. La phase varie alors dans le temps et de ce fait une différence de potentiel s'établit aux bornes de la jonction.

Expérimentalement, on varie le courant appliqué I, et donc la hauteur de la barrière de potentiel, jusqu'à mesurer une différence de potentiel aux bornes de la jonction. En répétant à plusieurs reprises cette procédure, on obtient une distribution de probabilité de transition en fonction de ΔU. Les résultats ainsi obtenus sont en très bon accord avec la théorie et en particulier avec le modèle de Leggett. Notons que ce même groupe a aussi pu mettre en évidence la quantification des niveaux d'énergie dans ces puits [69].

Plus récemment, Rouse *et. al.* ont pu observer l'effet tunnel résonnant macroscopique entre les états à zéro et un quantum de flux d'un SQUID [70]. Ceux-ci ont observé que le taux de transition présente une série de maxima correspondant à la situation où le fondamental du premier puits (0 quantum de flux) coïncide avec un état excité du second puits (1 quantum de flux). Encore une fois, l'accord entre théorie et expérience est excellent [70, 71].

Ainsi, plusieurs effets quantiques macroscopiques ont pu être observés dans les supraconducteurs et en particulier à l'aide de jonctions Josephson. Toutefois, l'effet tunnel cohérent n'a pas encore été observé dans ces systèmes mais beaucoup d'efforts sont maintenant investis en ce sens [72].

5.3 Niveaux d'Andréev

L'effet Josephson n'est pas limité aux jonctions SIS et à une dépendance en $\sin\phi$ du courant : cet effet apparaît dans toutes situations où un supercourant circule en raison d'un transport cohérent de paires de Cooper à travers un lien faible (*weak link*). Par lien faible on entend une région de la jonction où les corrélations supraconductrices ne sont pas supportées, par exemple : conducteur normal (jonction SNS), constriction dont le diamètre est petit par rapport à la longueur de cohérence ξ_0 (jonction ScS), barrière de grain (jonction SgS), etc. De façon générale, on note ces jonctions SXS, où X représente le lien faible. Évidemment, l'effet Josephson n'est pas limité aux électrodes supraconductrices de type s et s'observe également pour les supraconducteurs de type d (cuprate par exemple). On a alors des jonctions SXD et DXD.

Une description détaillée de ces structures dépasse le cadre de ce texte traitant d'informatique quantique et n'est pas nécessaire à la compréhension des sections suivantes. On se contentera donc de présenter une image intuitive de la physique de ces systèmes[2].

Pour décrire un système supraconducteur ayant des variations spatiales du paramètre d'ordre, on utilise l'équation de Bogoliubov-de Gennes (BdG) [64, 73]. L'équation de BdG,

$$\begin{pmatrix} -\frac{\hbar^2}{2m}\nabla^2 - \mu & \Delta(\mathbf{r}) \\ \Delta^*(\mathbf{r}) & \frac{\hbar^2}{2m}\nabla^2 + \mu \end{pmatrix} \begin{pmatrix} u_n \\ v_n \end{pmatrix} = E_n \begin{pmatrix} u_n \\ v_n \end{pmatrix}, \tag{5.8}$$

est une équation de Schrödinger à deux composantes, u_n et v_n, décrivant respectivement des quasiparticules de type électrons et de type trous. Dans l'équation (5.8), μ est le potentiel chimique et $\Delta(\mathbf{r})$ le paramètre d'ordre. Celui-ci doit, en principe, être déterminé de façon auto-cohérente à l'aide de la relation $\Delta(\mathbf{r}) = \lambda \sum_n v_n^* u_n (1 - 2f_n)$, où f_n est la fonction de distribution de Fermi et λ (> 0) une constante.

Pour une jonction SNS, on peut montrer que l'équation (5.8) a des solutions décrois-

[2] Le lecteur intéressé trouvera une introduction à la physique de ces structures mésoscopiques à la section §4.5 de la référence [64].

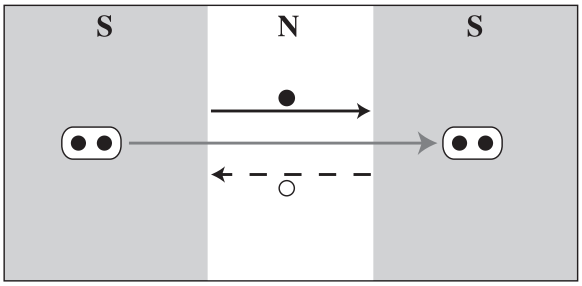


Figure 5.2: État lié transportant le courant dans une jonction SNS. Un tel état lié est une manifestation des réflexions d'Andréev multiples aux interfaces NS et SN. Un cercle plein (vide) représente un électron (trou). Les ovales contenant deux cercles représentent une paire de Cooper.

sant exponentiellement dans les électrodes supraconductrices et des solutions liées dans la partie normale (pour des énergies inférieures au gap des régions supraconductrices). Ces états liés sont les niveaux d'Andréev et jouent un rôle central dans le transport du supercourant à travers la jonction. L'image physique qui ressort de ces états est la suivante : un quasiélectron se dirigeant vers l'interface NS avec une vitesse de groupe $\mathbf{v}_g$ est transformé à l'interface en un quasitrou de vitesse $-\mathbf{v}_g$, figure 5.2. Par la suite, ce quasitrou incidant sur l'interface SN est réfléchit en un quasiélectron et le processus recommence. Ces réflexions multiples forment un niveau d'Andréev. (Le processus inverse est évidemment possible : un quasitrou se déplaçant vers la droite est réfléchit en un quasiélectron se propageant vers la gauche).

Ainsi, suite à la réflexion d'Andréev à l'interface NS, un électron initialement audessus de la surface de Fermi dans le conducteur normal quitte la partie normale pour l'électrode supraconductrice en formant une paire de Cooper avec un électron, initialement dans la mer de Fermi. Le trou "réfléchi" dans le processus est celui laissé dans la mer de Fermi par le second électron. L'électron et le trou transportant le courant dans la même direction, ce mécanisme est responsable du transfert d'une paire de Cooper d'une électrode supraconductrice à l'autre.

Dans le cas d'une jonction SXD, deux familles distinctes de niveaux d'Andréev existent. En effet, dans un supraconducteur de type d, le paramètre d'ordre a un signe différent selon la direction de la trajectoire dans l'espace des vecteurs d'onde, figure 5.3 [74]. En écrivant le paramètre d'ordre sous la forme $|\Delta|e^{i\tilde{\phi}}$ (donc en l'approximant par

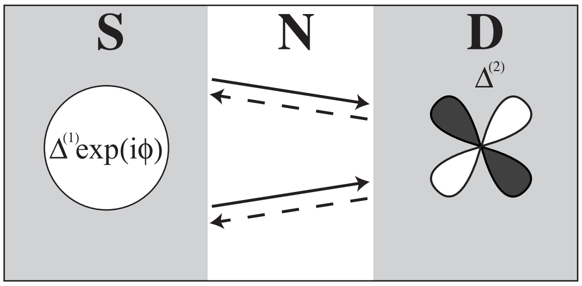


Figure 5.3: Jonction SND. Les lobes positifs du paramètre d'ordre du supraconducteur de type d sont grisés. (Figure adaptée de [64].)

une fonction changeant de signe de façon discontinue), cette différence de signe peut être traitée comme une différence de phase π intrinsèque entre les électrodes supraconductrices : $\tilde{\phi} = \phi$ (niveau connectant l'électrode S au lobe positif du paramètre d'ordre de la jonction D) et $\tilde{\phi} = \phi + \pi$ (lobe négatif)[3]. On distingue donc deux types de trajectoire entre les électrodes S et D et par conséquent deux familles de niveaux d'Andréev distinctes. Dans ces jonctions, le courant Josephson est dû à ces deux contributions dont l'importance relative dépend de l'orientation du paramètre d'ordre de l'électrode de type d par rapport à l'interface ND.

Dans le cas d'une jonction DXD, cette multiplicité des niveaux d'Andréev existe aussi et la différence de phase effective entre les électrodes dépend de l'orientation de chacun des paramètres d'ordre par rapport aux interfaces.

5.4 Jonctions DND triangulaires

Considérons maintenant la jonction Josephson de la figure 5.4. Celle-ci est formée d'une région normale de forme triangulaire séparant deux électrodes supraconductrices de type d. Pour cette configuration, A. Zagoskin a montré [4] que le courant total, transporté par les niveaux d'Andréev et traversant l'électrode A de la jonction, est donné par

[3]En réalité, comme le suggère la représentation imagée de la figure 5.3 et contrairement à l'approximation utilisée ici, le paramètre d'ordre d'un supraconducteur de type d varie de façon continue et s'annule dans certaines directions.

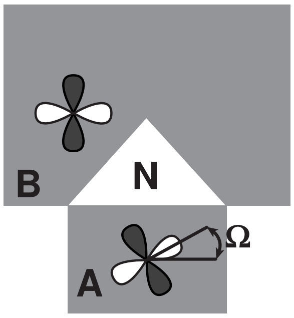


Figure 5.4: Jonction DND triangulaire. Les lobes positifs du paramètre d'ordre du supraconducteur de type d sont grisés. Ω est l'angle de désalignement entre les paramètres d'ordre des deux terminaux.

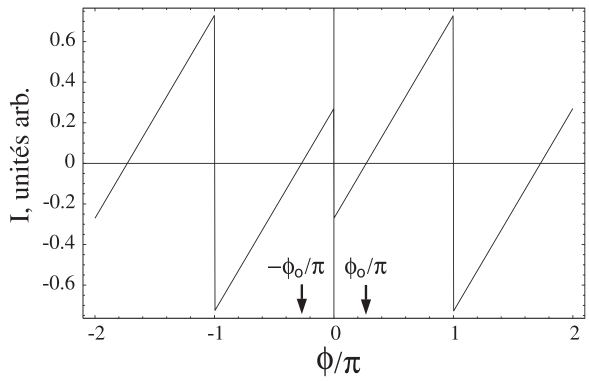
$$I(\phi) = \frac{2j_c W}{\pi}\left[\frac{1+Z(\Omega)}{2}F(\phi) + \frac{1-Z(\Omega)}{2}F(\phi+\pi)\right]. \tag{5.9}$$

Dans cette relation, j_c est la densité de courant critique de la jonction, W la taille transversale de la région normale, $F(\phi)$ est la fonction créneau de période 2π et d'amplitude unité et $Z(\Omega)$ une fonction qui dépend de l'orientation du paramètre d'ordre des électrodes supraconductrices à travers l'angle de désalignement Ω. Dans le cas de la jonction présentée à la figure 5.4, on a la relation suivante entre ϕ_0, la phase à l'équilibre, et $Z(\Omega)$:

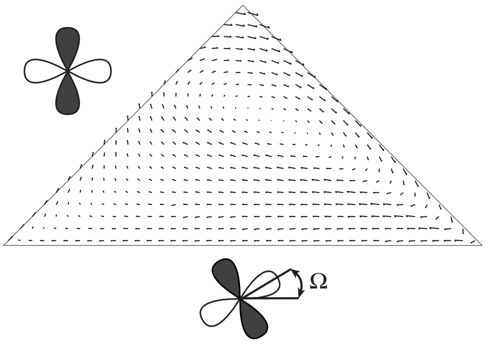
$$|\phi_0(\Omega)| = \pm\left|\frac{1-Z(\Omega)}{2}\right|\pi = \pm\frac{\sin|\Omega|}{\sqrt{2}}\pi. \tag{5.10}$$

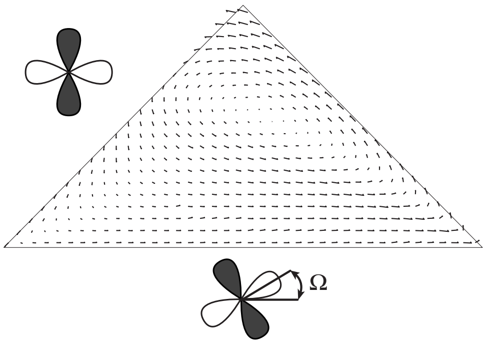
La relation (5.9) ainsi que la distribution de courant à l'intérieur de la partie normale de la jonction sont représentées à la figure 5.5. Des figures 5.5 b) et c), on remarque clairement un courant spontané circulaire dans la région normale de ces jonctions triangulaires. Le sens de circulation de ce courant dépend de la phase $\pm\phi_0$. Notons qu'aucun courant net ne s'écoule entre les électrodes lorsque $\phi = \phi_0$ (figure 5.5 a); voir aussi la référence [75] à ce sujet).

L'énergie Josephson correspondant à ce courant est obtenue des relations (5.3) et (5.9) et est présentée à la figure 5.6. La dynamique de cette jonction est équivalente à celle d'une particule de masse proportionnelle à la capacité du terminal A et se déplaçant dans le potentiel de la figure 5.6.



(a)





(b) (c)

Figure 5.5: a) Relation courant-phase pour une jonction DND triangulaire. L'angle de désalignement est $\Omega = \pi/8$. b) Distribution de courant dans la région normale de la jonction. Cas $\phi = -\phi_0 \approx -0.27\pi$ c) Version de b) avec $\phi = \phi_0 \approx 0.27\pi$. (Figures adaptées de [4].)

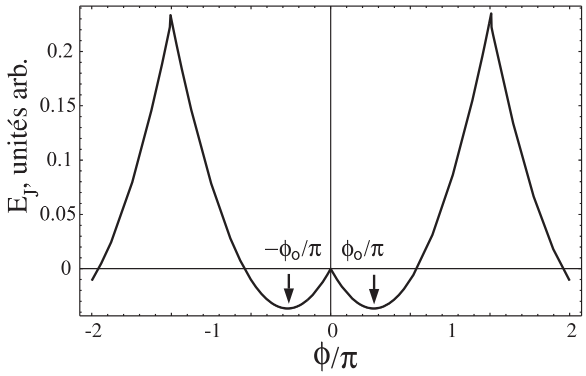


Figure 5.6: Potentiel effectif du système. Le désalignement est fixé à $\Omega = \pi/8$. (Figure adaptée de [4].)

Le potentiel dans lequel se déplace cette masse est une série de double puits de potentiel. Puisque la hauteur de la barrière de potentiel d'un double puits à l'autre est grande (et par conséquent la probabilité tunnel très faible), on se limite au double puits central de la figure 5.6. De même, lorsque la condition

$$\Delta U \gg \hbar\omega_0 \gg k_B T \tag{5.11}$$

est respectée, il est possible de se limiter au deux premiers niveaux de chaque double puits seulement [68]. On se limite donc à un espace d'Hilbert de dimension 2. Dans cette dernière relation, ΔU est la hauteur de la barrière de potentiel entre les états $-\phi_0/\pi$ et ϕ_0/π, $\hbar\omega_0$ l'énergie associée aux oscillations dans un puits et k_BT l'énergie thermique.

Finalement, on choisit la taille du terminal A de la jonction petite de sorte que la capacité associée soit petite. Dans ce cas, l'incertitude sur la phase est grande (voir section §5.2.2) et elle n'est plus une quantité semi-classique bien définie[4]. Par conséquent, la particule associée est délocalisée dans le double puits de potentiel et il y a possibilité d'effet tunnel cohérent. Notons finalement que puisque le flux associé au courant spontané circulaire dans la région normale est plus petit que le quantum de flux (voir section §5.8), le couplage à l'environnement est plus faible que dans le cas d'un simple SQUID et, de ce fait, les chances d'observer l'effet tunnel cohérent sont meilleures dans ce système.

[4]À l'opposé, la taille du terminal B est grande de sorte que la phase y soit bien définie.

5.5 Qubits supraconducteurs

Ayant limité l'espace d'Hilbert de la jonction DND triangulaire à un espace de dimension 2, celle-ci peut jouer le rôle de qubit. Aux minima en $\pm\phi_0$ du puits de la figure 5.6 on associe les états de base d'un qubit : $|-\phi_0\rangle \equiv |0\rangle$ et $|\phi_0\rangle \equiv |1\rangle$. Ainsi, c'est la différence de phase entre les électrodes supraconductrices qui joue ici le rôle de qubit. Rappelons qu'à ces états de base sont associés des courants spontanés circulant dans le sens horaire ou anti-horaire respectivement.

Afin de pourvoir manipuler et lire l'état des qubits, on ajoute aux jonctions DND triangulaires une pointe de microscope à force magnétique [76] (que l'on peut approcher et éloigner à volonté de la jonction) et une clé de parité connectant le terminal A à un réservoir d'électrons. (Une clé de parité laisse passer seulement des paires de Cooper et seulement à certains voltages, voir section §5.6.) La figure 5.7 présente un qubit supraconducteur tel que suggéré par A.M. Zagoskin et utilisant ces concepts.

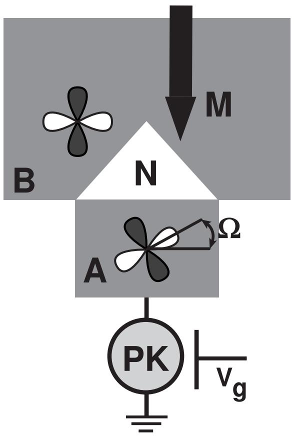


Figure 5.7: Qubit supraconducteur formé par une jonction DND. Les terminaux A et B sont des supraconducteurs de type d (cuprate par exemple), N un conducteur normal, PK une clé de parité, M pointe de microscope à force magnétique et Ω l'angle de désalignement entre les réseaux cristallins de A et B. Le terminal B est clivé dans les directions (110) et $(1\bar{1}0)$. Les lobes positifs du paramètre d'ordre sont grisés.

En raison des fluctuations quantiques de phase, le qubit peut être préparé dans une superposition d'états de phase lorsque le terminal A est isolé de la masse. La réduction de la fonction d'onde est réalisée en connectant ce terminal à une source extérieure d'électrons (la masse) à l'aide de la clé de parité. En raison de la relation d'incertitude entre phase et nombre de particules, les fluctuations de phase sont alors bloquées car N peut fluctuer [65].

Pour un système à plusieurs qubits, le terminal B forme un "bus" commun (figure 5.8). Dans ce cas, des clés de parité (ayant des caractéristiques différentes de celle reliant les terminaux A à la masse) relient les qubits adjacents.

5.6 Clé de parité

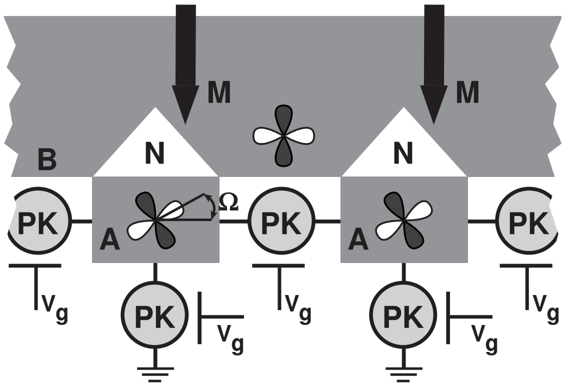
Considérons un grain non supraconducteur entouré par trois électrodes non supraconductrices de capacités mutuelles respectives C_1, C_2 et C_g, figure 5.9. La distance entre les électrodes 1 et 2 et le grain est petite de sorte que lorsqu'un voltage suffisamment élevé est appliqué, la probabilité qu'un électron passe par effet tunnel d'une électrode au grain (ou du grain vers une électrode) est grande. À l'opposé, l'électrode g est placée loin du grain de façon à ce que la probabilité tunnel soit petite. Ainsi, aucun courant ne circule entre cette électrode et le grain. De même, les électrodes sont suffisamment éloignées les unes de autres pour que l'on néglige tout couplage entre celles-ci. On verra que, dans le cas supraconducteur, ce système laisse passer des paires de Cooper et ce seulement pour certains voltages de grille V_g. Il s'agit donc d'un 'transistor à paires de Cooper'.

Lorsque les capacités sont suffisamment petites[5], l'énergie électrostatique correspondant à l'ajout d'un électron sur le grain

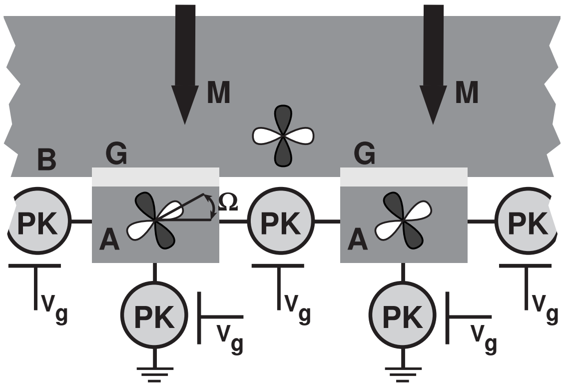
$$E_c = \frac{e^2}{2C_\Sigma}, \tag{5.12}$$

où $C_\Sigma = C_1 + C_2 + C_g$, est suffisamment grande pour jouer un rôle important sur la caractéristique $I - V$ du système [65, 64].

[5]On doit avoir C suffisamment petit de sorte que $E_c \gg k_B T$. De même, la résistance entre le grain et les électrodes doit excéder $R_Q = h/4e^2$, la résistance quantique, de façon à ce que les fluctuations quantiques du nombre de particules ne masquent les effets qui nous intéressent ici.



(a)



(b)

Figure 5.8: a) Registre de qubits. Les terminaux A sont connectés par des clés de parité. Deux qubits sont représentés. b) Version de a) utilisant une barrière de grain (G). Les résultats pour la jonction DND s'appliquent sans changement à ce cas. Pour simplifier la discussion, on ne traitera que le cas DND dans le texte.

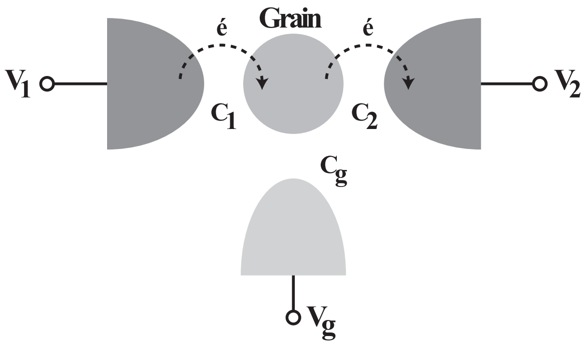


Figure 5.9: Transistor à un électron. Dans le cas d'un système supraconducteur, la parité du nombre d'électrons sur le grain est importante. Il s'agit alors d'une clé de parité.

En effet, l'énergie électrostatique d'un condensateur isolé C est donnée par $Q^2/2C = CV^2/2$, où Q (≥ 0) et $-Q$ sont les charges sur les électrodes et $V = Q/C$. Si un électron est transféré par effet tunnel de l'électrode négative vers sa voisine positive, la charge du système devient $(Q - |e|)$ et son énergie $(Q - |e|)^2/2C$. (On prend ici comme convention $e = -|e|$, la charge de l'électron incluant son signe.) Ce transfert d'un électron correspond à une augmentation de l'énergie du système si $Q < |e|/2$ ou, de façon équivalente, si $V < |e|/2C$. Ainsi, le transfert d'électrons d'une électrode à l'autre est énergétiquement défavorable et est bloqué pour des voltages inférieurs à $|e|/2C$. Il s'agit de la barrière de Coulomb. En raison de cette barrière, aucun courant ne circulera à travers le dispositif de la figure 5.9 tant que le voltage des électrodes 1 et 2 n'aura pas atteint $|e|/2C_1$ et $|e|/2C_2$ respectivement.

Considérons maintenant l'énergie totale du dispositif de la figure 5.9 ayant n électrons en excès sur le grain et fixant $V_1 = V_2 = 0$. La charge effective induite par l'électrode g sur le grain est $q_g = C_g V_g$ de sorte que la charge totale est $q_T = ne + C_g V_g$. L'énergie électrostatique du grain[6] est alors donnée par la relation (5.12) qui devient dans ce cas

[6]Une analyse plus détaillée prenant en compte de l'énergie électrostatique du grain ainsi que le travail effectué par les sources de voltage V_1, V_2 et V_g lorsqu'un électron passe d'une électrode au grain (ou l'inverse) par effet tunnel est présentée à la section §7.5 de la référence [65] et conduit à un résultat similaire.

$$\begin{aligned} E(n) =& \frac{q_T^2}{2C_\Sigma} \\ =& \frac{1}{2C_\Sigma}\left(C_g V_g + ne\right)^2 . \end{aligned} \tag{5.13}$$

Bien qu'aucune charge ne soit transférée par l'électrode g, le voltage appliqué sur celle-ci affecte le transport à travers le grain. Ainsi, lorsque $V_1 = V_2 = 0$, comme dans le cas de l'équation (5.13), seul V_g affecte la dynamique du dispositif. Dans ce cas, l'équation (5.13) décrit une famille de paraboles, chacune définie par n, le nombre d'électrons sur le grain, figure 5.10 a). Lorsque $C_g V_g/e = (n \pm \frac{1}{2})$, l'énergie du système avec n et $n \pm 1$ électrons est classiquement dégénérée. Un électron peut alors sortir ou entrer du grain par effet tunnel. Le dispositif de la figure 5.9 agit ainsi comme un transistor à un électron, laissant passer un électron à la fois et seulement à certains voltages V_g.

Dans le cas d'un grain supraconducteur, on doit tenir compte de l'appariement électronique. Ainsi, si le nombre d'électrons sur le grain est pair, ceux-ci sont tous appariés en paires de Cooper. Toutefois, si n est impair, un électron occupera un état excité d'énergie au moins Δ, où Δ est le gap supraconducteur. La relation (5.13) prend alors la forme [64]

$$E(n) = \frac{1}{2C_\Sigma}\left(C_g V_g + ne\right)^2 + n_q \Delta, \tag{5.14}$$

avec $n = 2n_c + n_q$ et où n_c est le nombre de paires de Cooper et $n_q = 0$ ou 1, le nombre d'électrons non appariés. Dans la description de ce système, on distingue deux cas : $\Delta < E_c$ et $\Delta > E_c$. Ces deux situations sont représentées aux figures 5.9 b) et c). Dans le premier cas, il y a toujours résonance entre les états à n et $n+1$ électrons mais les voltages auxquels se produisent ces résonance sont déplacés par rapport au cas non supraconducteur. Dans le second cas, les énergies $E(n)$ et $E(n+2)$ sont classiquement dégénérées pour les valeurs de $C_g V_g/e$ impaires.

Pour un système entièrement supraconducteur, le grain agit comme lien faible entre les électrodes 1 et 2 et un courant Josephson apparaît s'il y a une différence de phase entre ces électrodes. La dégénérescence entre $E(n)$ et $E(n\pm 2)$ permet alors le transfert

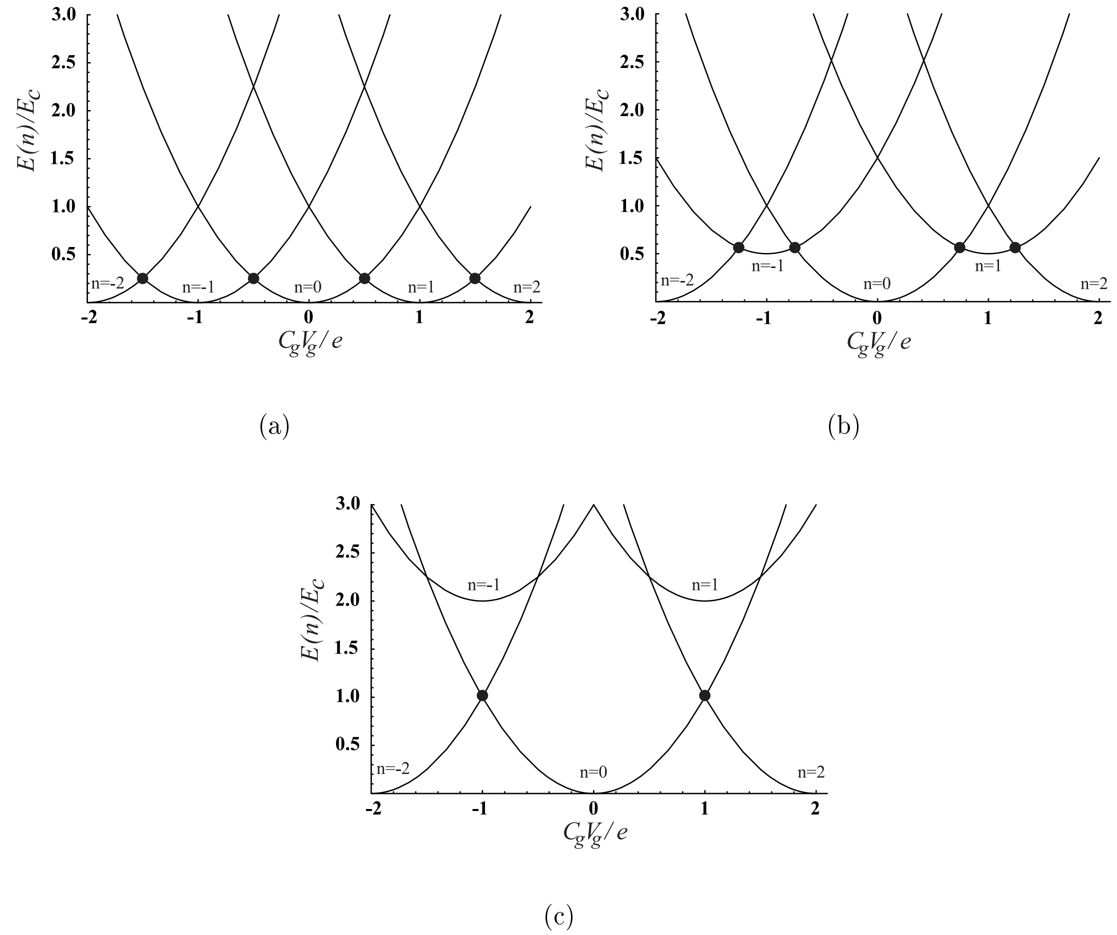


Figure 5.10: a) Grain normal. b) Grain supraconducteur avec $\Delta < E_c$. c) Grain supraconducteur avec $\Delta > E_c$. Les points noirs indiquent les régions où la valeur de n dans l'état fondamental change. En ces points, le transport se fait sans barrière énergétique. (Figures adaptées de [65].)

cohérent de paires de Cooper. Ainsi, lorsque le dipositif de la figure 5.9 est entièrement supraconducteur et si $\Delta > E_c$, il agit comme transistor laissant passer des paires de Cooper et ce seulement à certains voltages V_g, tel qu'annoncé en début de section. Ces transistors "à paires de Cooper" sont les clés de parité du dispositif de la figure 5.8.

5.7 Mesure, initialisation et opérations logiques

Décrivons maintenant comment le dispositif de la figure 5.8 répond aux critères #1, #2, #4 et #5 de la section §5.1, [62]. On sait que l'état fondamental de l'une de ces jonctions triangulaires est doublement dégénéré. Sans perturbations extérieures, ce système est alors limité à un espace d'Hilbert $\mathcal{H}_1(2)$ de dimension deux. Un arrangement de n de ces jonctions a donc comme espace d'état le produit tensoriel de n espaces d'Hilbert à deux dimension, $\mathcal{H}_t = \mathcal{H}_1(2) \otimes \mathcal{H}_1(2) \otimes \cdots \otimes \mathcal{H}_1(2)$, pour un espace de dimension totale 2^n. L'espace d'Hilbert de ce système est bien caractérisé et le premier critère est de ce fait satisfait. Les deuxième, quatrième et dernier critères portent sur les opérations de base : l'initialisation, les opérations logiques et la mesure.

La mesure (critère #5) est réalisée sur ce système en deux étapes et peut être effectuée sur un seul qubit ou simultanément sur un groupe de qubits. La première étape, l'effondrement de la fonction d'onde, est réalisée en bloquant les fluctuations de phase dans le terminal A du qubit à mesurer. En pratique, on effectue cette opération en appliquant un potentiel V_g sur la clé de parité reliant le terminal A du qubit à mesurer à la masse de façon à permettre le transfert d'électrons. En raison de la relation d'incertitude entre phase et nombre de particules, les fluctuations quantiques de phase sont alors bloquées. Un qubit se trouvant initialement dans une superposition d'états se trouve alors dans un de ses états de base. Celui-ci a alors un état de phase bien défini, correspondant à une circulation du courant spontané dans le sens horaire ou anti-horaire. La lecture de ce courant, et par conséquent de l'état du qubit, est réalisée à l'aide d'une pointe de microscope à force magnétique. (De façon à éviter tout couplage, cette pointe est reculée lors des calculs.) Le flux associé au courant spontané est suffisant pour permettre la lecture efficace de l'état des qubits mais trop petit ($\ll \Phi_0$) pour conduire à un couplage inductif entre ceux-ci.

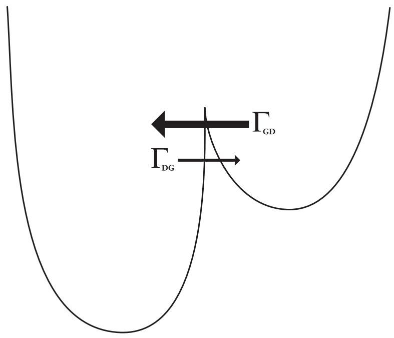


Figure 5.11: Effet d'un champ magnétique sur un qubit. La barrière de potentiel est beaucoup plus élevée pour passer du puits de droite au puits de gauche que l'inverse. Après un certain temps, le qubit se retrouvera, avec une très grande probabilité, dans le puits de gauche.

L'initialisation (critère #2) est réalisée, par exemple, en appliquant un champ magnétique extérieur à l'aide de la pointe M. À ce champ extérieur est associé un flux induisant un courant dans la 'boucle de courant spontané' présente dans la région normale de la jonction. À ce courant est associé une énergie qui a pour effet de lever la dégénérescence favorisant ainsi un des états de base, figure 5.11. À l'aide de cette technique, il est possible d'initialiser les qubits individuellement ou globalement. De plus, il est possible d'initialiser simultanément tous les qubits en faisant circuler un courant spontané dans le terminal B.

Décrivons maintenant comment réaliser les opérations logiques de base (critère #4). Afin de maintenir la cohérence, les électrodes A sont isolées de la masse lors des calculs. Les opérations de base à un qubit définies sur ce système sont les rotations autour des axes x et z

$$\mathsf{R}_x(\theta) = e^{-i\sigma_x\theta/2}; \tag{5.15}$$

$$\mathsf{R}_z(\varphi) = e^{-i\sigma_z\varphi/2}. \tag{5.16}$$

L'opération $R_x(\theta)$ est possible grâce aux oscillations naturelles du système entre les états de base $|0\rangle$ et $|1\rangle$. En effet, en négligeant tout couplage à l'environnement on peut modéliser la dynamique d'un qubit par l'Hamiltonien effectif

$$\mathsf{H} = E \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + \Delta \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \tag{5.17}$$

dans la base de calcul. Le coefficient E correspond à l'energie du fondamental et le second membre de droite de (5.17) représente phénoménologiquement le couplage entre les puits dû au fait que la hauteur de potentiel $U(0)$ n'est pas infinie.

En raison de ce couplage, les états propres du système ne sont plus les états de la base de calcul mais plutôt des combinaisons linéaires de ceux-ci

$$|\pm\rangle = \frac{1}{2}\left(|0\rangle \pm |1\rangle\right), \tag{5.18}$$

avec comme énergies propres associées $E_{\pm} = E \pm \Delta$. Ces nouveaux états propres correspondent à des états complètement délocalisés entre les deux puits et la probabilité de trouver le qubit dans l'un de ces puits varie alors dans le temps selon la formule de Rabi [31]. Il y a donc oscillations entre les états de base. En fixant le zéro d'énergie à E et en utilisant une notation plus compacte, on réécrit l'Hamiltonien (5.17) comme

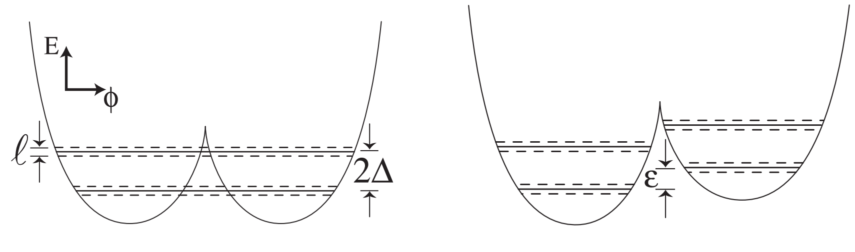
$$\mathsf{H} = \Delta\, \sigma_x. \tag{5.19}$$

Ainsi, sans perturbation extérieure, les qubits sont en rotation par rapport à un axe x effectif :

$$\begin{aligned} |\psi(t)\rangle &= e^{-i\mathsf{H}t/\hbar}\,|\psi(0)\rangle \\ &= e^{-i\sigma_x \Delta t/\hbar}\,|\psi(0)\rangle \\ &= \mathsf{R}_x(\theta)\,|\psi(0)\rangle\,, \end{aligned} \tag{5.20}$$

où $|\psi(0)\rangle$ décrit l'état initial des qubits et $\theta = 2t\Delta/\hbar$. (La renormalisation de l'énergie, effectuée entre les relations (5.17) et (5.19), ne correspond qu'à une phase globale sans conséquence physique dans l'application des opérations logiques.)

L'opération $R_z(\phi)$ est quant à elle réalisée en levant la dégénérescence entre les états de bases $|0\rangle$ et $|1\rangle$, figure 5.12. En effet, en appliquant par exemple un champ



(a) (b)

Figure 5.12: a) Sans perturbation extérieure les états propres sont complètement délocalisés. l représente la largeur des niveaux. b) Levé de la dégénérescence par une énergie ε.

magnétique local près de la région normale d'un qubit ou un supercourant local dans le terminal B, l'Hamiltonien (5.17) devient

$$\mathsf{H} = \frac{1}{2}\,\varepsilon\,\sigma_z + \Delta\,\sigma_x, \tag{5.21}$$

où ε représente la différence d'énergie entre les fondamentaux de chaque puits, figure 5.12 b). Lorsque ε est supérieure à la largeur des niveaux, l'effet tunnel résonnant est bloqué et on peut considérer que $\Delta \to 0$ [77] dans l'Hamiltonien effectif (5.21). Celui-ci génère alors une rotation autour d'un axe z effectif

$$\begin{aligned} |\,\psi(t)\rangle &= e^{-i\mathsf{H}t/\hbar}\,|\,\psi(0)\rangle \\ &\simeq e^{-i\varepsilon\sigma_z t/2\hbar}\,|\,\psi(0)\rangle \\ &= \mathsf{R}_z(\phi)\,|\,\psi(0)\rangle\,, \end{aligned} \tag{5.22}$$

avec $\phi = \varepsilon t/\hbar$. On sait donc comment appliquer les opérations logiques R_x et R_z sur un qubit.

Toutefois, comme le suggère l'Hamiltonien (5.19), l'état au repos de ce système correspond à l'application de l'opération logique $\mathsf{R}_x(\theta)$. Pour un 'ordinateur quantique' à un qubit cette situation ne pose pas de problème puisque les opérations logiques sont appliquées séquentiellement, sans temps d'attente. De même, si un temps d'attente (période où aucune opération logique n'est appliquée) est nécessaire, il suffit de le choisir de façon à ce qu'il soit un multiple de la période d'oscillations naturelles du système. En d'autres termes, pour un qubit, une période d'attente doit correspondre à un multiple de 2π : $\mathsf{R}_x(2\pi n) = \pm\mathbb{I}$ avec n est un entier.

Pour plusieurs qubits, la situation est plus délicate. Dans ce cas, les qubits passifs (sur lesquel n'est appliquée aucune opération logique) doivent être "gelés" pendant le temps d'application des opérations sur les qubits actifs (sur lesquels sont appliquées les opérations logiques). Par exemple, si $\mathsf{R}_z(\varphi)$ est appliquée sur le premier qubit, les autres doivent rester inchangés par cette opération. Puisque le temps d'application des opérations logiques sera typiquement incommensurable avec le temps requis pour que $\mathsf{R}_x(\theta)$ soit égale à l'identité, une technique pour geler l'état des qubits passifs s'avère nécessaire.

Pour venir à bout de ce problème, il est avantageux d'avoir un état au repos pour lequel l'effet tunnel est bloqué de façon cohérente tout en conservant l'énergie des états $|0\rangle$ et $|1\rangle$ dégénérée. On réalise cela en introduisant une capacité extérieure C_{ext} reliée au terminal A, comme proposé dans [61]. En effet, le taux tunnel est donné par $\Gamma_T \sim \omega_0 e^{-U(0)/\hbar\omega_0}$, où $\omega_0 \propto 1/\sqrt{C}$ est la fréquence des petites oscillations dans un des puits de la figure 5.6 et $U(0)$ la hauteur de la barrière de potentiel, [4]. En raison de la dépendance en $\sqrt{C}$ de l'exposant, Γ_T est exponentiellement atténué par une augmentation de C. Ainsi, pour C_{ext} suffisamment grand, l'effet tunnel est bloqué tout en conservant la dégénérescence entre les états logiques. Toutefois, une telle capacité extérieure peut être source de décohérence en raison des processus inélastiques qui auront lieu si le circuit est normal. De même, choisir une capacité et un circuit la reliant avec le terminal A supraconducteur introduira une évolution non voulue des états de base en raison du couplage Josephson entre le circuit externe et le terminal A[7].

Une solution alternative à ce problème est d'utiliser une technique s'approchant de la refocalisation utilisée en RMN [78, 79]. Cette méthode consiste en des perturbations périodiques abruptes et d'amplitude δE légèrement supérieure à la largeur des niveaux

[7]Toutefois, si la capacité extérieure est suffisamment grande, le courant traversant le circuit extérieur sera petit et l'énergie Josephson associée sera elle-même petite. L'utilisation d'une capacité extérieure pourrait donc, selon les paramètres du système, être possible mais compliquerait la fabrication de ces qubits.

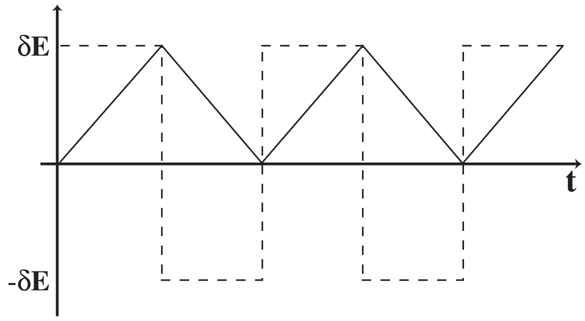


Figure 5.13: Dépendance temporelle de l'angle de rotation $\varphi'(t)$ (trait plein) et de l'énergie (traits pontillés).

d'énergie du potentiel de la figure 5.6. La différence d'énergie entre les états de base est alors variée, avec une période 2τ, abruptement de δE à $-\delta E$. Explicitement, ceci correspond à la séquence d'impulsions

$$\cdots \to \mathsf{R}_z(+\delta E\tau/\hbar) \to \mathsf{R}_z(-\delta E\tau/\hbar) \to \mathsf{R}_z(+\delta E\tau/\hbar) \to \cdots . \tag{5.23}$$

Avec l'application de cette séquence, l'angle de rotation autour de l'axe z acquiert une dépendence temporelle $\varphi'(t)$ et est donné, dans le cas idéal, par une fonction triangulaire de période 2τ (figure 5.13). De même, l'effet tunnel cohérent est bloqué puisqu'il n'y a plus résonance (voir figure 5.12).

En effet, sous l'action de la refocalisation, l'opérateur d'évolution d'un qubit est donné par

$$\begin{aligned} \mathsf{U}(t) &= \mathsf{T}\, e^{-i\sigma_z \int_0^t dt'\; \varphi'(t')/2} \\ &= e^{-i\sigma_z \delta E F(t,2\tau)/2\hbar}, \end{aligned} \tag{5.24}$$

où $F(t, 2\tau)$ est une fonction triangulaire de période 2τ et d'amplitude unité. En se limitant à des observations stroboscopiques de période τ, l'effet de cette refocalisation sur un qubit s'écrit

$$\mathsf{U}(t) = e^{-i\sigma_z(\delta E\tau - \delta E\tau + \delta E\tau - \cdots)/2\hbar}, \tag{5.25}$$

de sorte que, dans le pire des cas, $\mathsf{U}(t) = \exp\left[i\sigma_z \delta E\tau/2\hbar\right]$. Pour τ suffisamment petit,

$U(t) \approx \mathbb{I}$. Ainsi, à l'aide de cette méthode on obtient un état au repos pour lequel les qubits ne sont pas perturbés par l'effet tunnel ou par l'accumulation de phase relative.

Les portes logiques peuvent être appliquées simultanément à cette refocalisation. En effet, puisque $\mathsf{R}_z(\varphi)$ commute avec la séquence (5.23), cette opération peut être appliquée sur un qubit ou en parallèle sur un groupe de qubits tout en réalisant la refocalisation sur tous les qubits (actifs et passifs). Dans ce cas, l'évolution d'un qubit actif est donnée par $\exp\left[-i\sigma_z\left(\int_0^t dt'\,\varphi'(t') + \varphi\right)/2\right] \approx \mathsf{R}_z(\varphi)$. Ainsi, l'application de $\mathsf{R}_z(\varphi)$ sur le premier qubit, combinée à l'application d'une refocalisation global sur tous les qubits, conduit au résultat voulu : $\mathsf{R}_z(\varphi) \otimes \mathbb{I} \otimes \cdots \otimes \mathbb{I}$. L'application de $\mathsf{R}_x(\theta)$ se réduit à arrêter la refocalisation sur les qubits actifs pour la période voulue d'application de $\mathsf{R}_x(\theta)$. Cette opération, combiné à la refocalisation sur les qubits passifs, conduit aussi au résultat global désiré.

Notons que la période de perturbation 2τ ne doit pas correspondre à une fréquence propre du système de façon à ne pas introduire de transition à l'intérieur d'un même puits. Une telle transition aurait pour effet d'introduire un déphasage. De même, on doit s'assurer que le fondamental d'un puits n'entre pas en résonance avec un état excité du second puits lorsque l'on applique une impulsion de refocalisation. Dans ce cas, il y aurait effet tunnel entre ces niveaux ce qui rendrait la technique de refocalisation inutile. De plus, dans le cas non idéal, on doit s'assurer que la transition entre δE et $-\delta E$ soit plus rapide que le temps caractéristique de l'effet tunnel de façon à ne pas permettre de transition entre les puits lorsque ceux-ci sont près de ou à la résonnance. Notons aussi que la technique de refocalisation n'est pas nécessaire pendant l'application de $\mathsf{R}_z(\varphi)$ si la fréquence associée à cette rotation est beaucoup plus grande que celle correspondant à l'effet tunnel.

Pour de petits τ, la méthode proposée ici s'approche de la technique de réduction dynamique de décohérence proposée récemment par L. Viola *et. al.* [80, 81] et pourrait, en principe, servir à cette fin. Cette technique, dite de 'contrôle "bang-bang" quantique', est basée sur l'application répétée de impulsions inversant l'état des qubits et conduit à l'inhibition de la décohérence si le délais entre ces impulsions est plus petit ou de l'ordre du temps de corrélation de l'environnement. Ce temps de corrélation est donné par l'inverse d'une fréquence de coupure naturelle $\tau_c \sim \omega_c^{-1}$ (fréquence de coupure ultraviolette) et détermine l'échelle de temps la plus rapide de l'environnement. Dans ce contexte, on montre facilement, à l'aide de la théorie de l'hamiltonien moyen [79, 82] (voir en particulier la relation (38) de la référence [82]), que la séquence (5.23) avec $\phi = \pi$ conduit à une supression des couplages en σ_x et σ_y avec l'environnement.

Notons que dans le cas de semiconducteurs, où la décohérence est causée par les phonons, τ_c est donné par l'inverse de la fréquence de Debye $\omega_c \approx 10^{13}\mathrm{s}^{-1}$ [81]. Dans le cas des qubits supraconducteurs considérés ici, τ très petit signifie $\tau \ll t_b$, où $t_b \sim l/v_f$ est le temps ballistique (le temps requis pour la formation des niveaux d'Andréev dans la partie normale du système), l la taille du système et v_f la vitesse de Fermi. Des estimations de la référence [4], on a $l \sim 10^3 \mathring{A}$, $v_f \sim 10^7 cm/s$ et donc $t_b \sim 10^{-12}s$, un estimation similaire à celui de la référence [81][8]. Toutefois, l'application de la refocalisation dans le contexte de la réduction de décohérence peut s'avérer difficile en pratique. Cela est dû, en particulier, aux très petites échelles de temps en jeux.

En plus des opérations logiques sur un qubit, des opérations non locales à plusieurs qubits sont nécessaires. Dans ce système, une telle opération est réalisée en ouvrant la clé de parité connectant les terminaux A de qubits adjacents (figure 5.8). Avec cette clé ouverte, un courant Josephson circule entre les états de phases opposées (le courant Josephson dépendant de la différence de phase entre les électrodes supraconductrices). Ainsi, un courant ne circule pas pour les combinaisons $|\,00\rangle$ et $|\,11\rangle$, tandis qu'un courant Josephson circule pour $|\,01\rangle$ et $|\,10\rangle$ qui correspondent à des états de phases opposées. À ce courant est associé une énergie Josephson $E_J \sim [1 - \cos(2\phi_0)]$ et les états de phases opposées accumulent en conséquence une phase $E_J t/\hbar$ avec le temps :

$$|\,00\rangle + |\,01\rangle + |\,10\rangle + |\,11\rangle \xrightarrow{t} |\,00\rangle + e^{-iE_J t/\hbar}\,|\,01\rangle + e^{-iE_J t/\hbar}\,|\,10\rangle + |\,11\rangle\,. \tag{5.26}$$

Cette évolution correspond à l'application d'une phase relative conditionnelle ($\mathsf{CP}(\gamma)$,

[8]Il est important de comprendre que les temps données ici ne sont pas les temps de décohérence mais bien les temps de corrélation. Ceux-ci sont en général beaucoup plus petit que les temps de décohérence.

pour *Conditionnal Phase shift*) et peut être représentée dans la base de calcul, à une phase globale près, par l'opérateur

$$\mathsf{CP}(\gamma) = \begin{pmatrix} e^{i\gamma/2} & & & \\ & e^{-i\gamma/2} & & \\ & & e^{-i\gamma/2} & \\ & & & e^{i\gamma/2} \end{pmatrix}, \tag{5.27}$$

où $\gamma = E_J t/\hbar$. Remarquons que l'état initial de la relation (5.26) est séparable tandis que l'état final ne l'est pas. L'opération $\mathsf{CP}(\gamma)$ correspond donc bien à une opération non locale.

Puisque cet opérateur est diagonal dans la base de calcul, il commute avec la séquence de refocalisation. Ainsi, si l'énergie Josephson E_J correspondante ne perturbe que légérement les niveaux d'énergie des qubits individuels, cette dernière opération peut être réalisée simultanément avec la séquence de refocalisation. Cette condition peut toujours être réalisée par un choix approprié du voltage V_g de la clé de parité, de ce fait choisissant la transparence (i.e. la probabilité tunnel) et l'énergie Josephson correspondante. L'évolution d'une paire de qubits subissant l'opération logique $\mathsf{CP}(\gamma)$ et la séquence de refocussing s'écrit alors

$$\begin{pmatrix} e^{i\gamma/2+i\int dt\,\varphi'(t)} & & & \\ & e^{-i\gamma/2} & & \\ & & e^{-i\gamma/2} & \\ & & & e^{i\gamma/2-i\int dt\,\varphi'(t)} \end{pmatrix} \approx \mathsf{CP}(\gamma), \tag{5.28}$$

où on a utilisé (2.8) pour écrire de façon matricielle l'effet de la refocalisation sur une paires de qubit. Ainsi, l'opération CP n'est pas perturbée par R_x.

À l'aide de ces opérations sur un et deux qubits, il est possible de réaliser l'opération logique Controlled-NOT sur une paire de qubits. En effet, CN_{12} est réalisée sur ce système, à une phase globale près, par la séquence de transformations

$$\begin{aligned}\mathsf{CN}_{12} = e^{i5\pi/4}&\mathsf{R}_{x2}(\pi/2)\mathsf{R}_{z2}(\pi/2)\mathsf{R}_{x2}(\pi/2)\mathsf{R}_{z2}(\pi)\mathsf{R}_{z1}(\pi/2)\\ &\times \mathsf{CP}(\pi/2)\mathsf{R}_{x2}(\pi/2)\mathsf{R}_{z2}(3\pi/2)\mathsf{R}_{x2}(\pi/2),\end{aligned} \tag{5.29}$$

où $\mathsf{R}_{\alpha j}$ applique R_{α} sur le $j^{\text{ième}}$ qubit tout en laissant les autres inchangés, par exemple : $\mathsf{R}_{z1} = \mathsf{R}_z \otimes \mathbb{I} \otimes \cdots \otimes \mathbb{I}$.

De plus, dans l'architecture proposée à la figure 5.8 il n'est possible d'appliquer des portes non locales que sur des qubits (physiquement) adjacents. Afin de réaliser un calcul quantique utile, il est nécessaire d'interagir avec plusieurs qubits. On doit alors introduire un opérateur qui échange l'état de deux qubits. Un tel opérateur, noté Sw_{ij}, a déjà été introduit (section §2.3) et est obtenu par l'application de trois Controlled-NOT. Puisque le Controlled-Not est dans notre répertoire, le *Swap* l'est aussi.

L'utilisation répétée de cet opérateur permet de juxtaposer toutes paires de qubits et, de ce fait, d'appliquer un Controlled-NOT sur toutes paires de qubits. Considérons par exemple le cas d'un registre de trois bits quantiques $|\,a,b,c\rangle$. Afin d'appliquer CN_{13} sur ce registre les opérations suivantes sont nécessaires

$$\begin{aligned}\mathsf{CN}_{13}\,|\,a,b,c\rangle &\equiv \mathsf{Sw}_{23}\mathsf{CN}_{12}\mathsf{Sw}_{23}\,|\,a,b,c\rangle\\ &= \mathsf{Sw}_{23}\mathsf{CN}_{12}\,|\,a,c,b\rangle\\ &= \mathsf{Sw}_{23}\,|\,a,a\oplus c,b\rangle\\ &= |\,a,b,a\oplus c\rangle\,.\end{aligned} \tag{5.30}$$

La généralisation à un nombre arbitraire de qubits s'ensuit facilement.

En somme, on a montré comment appliquer les opérations logiques $\mathsf{R}_x(\theta)$ et $\mathsf{R}_z(\varphi)$ sur un bit quantique et l'opération non locale $\mathsf{CP}(\gamma)$ sur deux bits quantiques. On a ensuite montré comment obtenir un CNOT de ces opérations de base. En raison des relations de commutation entre les matrices de Pauli, ces deux rotations sur un qubit sont suffisantes pour générer $SU(2)$. Par des combinaisons appropriées de R_x et R_z, il est donc possible de réaliser toutes les opérations logiques à un qubit sur ce système.

Puisque l'on peut réaliser la porte Controlled-Not à l'aide de ces rotations et de la transformation CP, on en déduit, des résultats de [19] et de la section §2.4, que

$\{\mathsf{R}_x, \mathsf{R}_z, \mathsf{CP}\}$ forment un ensemble complet pour le calcul quantique. Il est ainsi possible de générer $SU(2^n)$ sur un tel ordinateur quantique supraconducteur de n qubits à l'aide de séquences appropriées d'opérations choisies dans l'ensemble $\{\mathsf{R}_x, \mathsf{R}_z, \mathsf{CP}\}$. L'architecture proposée à la figure 5.8 correspond donc à un ordinateur quantique universel.

5.8 Estimations et ordres de grandeur

Présentons maintenant quelques estimations et ordres de grandeur pour un qubit basé sur les jonctions D-(barrière de grain)-D, figure 5.8b). Premièrement, le flux magnétique associé au courant spontané circulant dans la barrière de grain, figure 5.5, est donné par $\Phi_s = cLI_s$. En approximation, on considère une boucle de courant circulaire de rayon R de sorte que l'inductance est $\sim R/c^2$ [83]. La densité de courant dans la barrière de grain est estimée à [4, 75]

$$j_c \sim \frac{ev_f R}{\lambda_f A}, \tag{5.31}$$

où v_f est la vitesse de Fermi, λ_f la longueur d'onde de Fermi et A l'aire de la jonction (notons que que j_c est une densité de courant de surface : $[j_c] = [\mathrm{A/cm}]$). Dans notre cas, on prend $R \sim 1000\text{Å}$, $v_f \sim 10^7\mathrm{cm/s}$ et $\lambda_f = h/m^* v_f \sim h/10 m_e v_f \sim 5\text{Å}$ où $m^* \sim 10 m_e$ est la masse effective dans le YBCO [83]. On peut donc écrire pour le flux spontané

$$\Phi_s \sim \frac{j_c R^2}{c} \sim \frac{1}{c} N_\perp e v_f. \tag{5.32}$$

où $N_\perp \sim R/\lambda_f$ est le nombre de modes de transport dans le système [64]. En unité de quantum de flux magnétique, $\Phi_0 = hc/2e$, on peut réécrire cette expression sous la forme

$$\Phi_s \sim \frac{N_\perp e v_f}{c}\frac{2e}{hc}\,\Phi_0 \sim \frac{e^2}{\hbar c}\frac{N_\perp}{\pi}\frac{v_f}{c}\,\Phi_0 \sim \frac{1}{137}\frac{N_\perp}{\pi}\frac{v_f}{c}\,\Phi_0. \tag{5.33}$$

À l'aide des ordres de grandeur annoncés, on trouve $\Phi_s \sim 10^{-4}\Phi_0$. Déterminons maintenant le moment magnétique m_s associé à ce courant spontané. On sait que le module du moment magnétique est $I/c \times$ Aire. On obtient donc dans notre cas

$$m_s \sim \frac{j_c R}{c} A \sim \frac{N_\perp e R v_f}{c}. \tag{5.34}$$

En fonction du magnéton de Bohr, $\mu_B = e\hbar/2m_e$, on réécrit m_s comme

$$m_s \sim \frac{4\pi m_e N_\perp R v_f}{h} \mu_B \tag{5.35}$$

pour obtenir $m_s \sim 10^4 \mu_B$.

Dans la région normale de la jonction, les modes de transport sont formés par les niveaux d'Andréev. Ces niveaux sont quantifiés et l'énergie moyenne $\bar{\epsilon}$ entre deux de ces niveaux est [4, 64, 75]

$$\bar{\epsilon} \sim \frac{\hbar v_f}{2R} \sim 10^{-16}\, erg. \tag{5.36}$$

En raison de cette quantification, il n'y pas d'excitation élémentaire dans la région normale de la jonction ayant une énergie inférieure à $\bar{\epsilon}$. De ce fait, si la température du système est inférieure à $\bar{T} \sim \bar{\epsilon}/k_B \sim 4K$ les excitations thermiques sont gelées. Le transport à travers la région normale se fait alors de façon cohérente et donc sans dissipation. Toutefois, les fluctuations de phase dans le terminal A génèrent un voltage CA (éq. (5.2)) et ce voltage peut provoquer des transitions interniveaux. Dans ce cas, le transport n'est plus cohérent et il y dissipation. Pour éviter cette situation, on doit avoir

$$2e\langle V_J \rangle \sim \hbar\sqrt{\langle \dot{\varphi}^2 \rangle} \sim \hbar\omega_0 < \bar{\epsilon}, \tag{5.37}$$

où $\omega_0 \sim \sqrt{N_\perp \bar{\epsilon} \varepsilon_Q}/\hbar$ [75] est la fréquence des oscillations autour des minimas du potentiel de la figure 5.6 et ε_Q est l'énergie électrostatique due à la capacité classique C du terminal A : $\varepsilon_Q = e^2/2C$. En utilisant l'expression approximative pour ω_0 on peut réécrire l'inégalité (5.37) sous la forme

$$\varepsilon_Q < \frac{\bar{\epsilon}}{N_\perp}, \tag{5.38}$$

ou encore, en utilisant la relation pour $\bar{\epsilon}$

$$\omega_0 < \frac{v_F}{2R}. \tag{5.39}$$

Puisque $\sim 2R/v_f$ est le temps que prend un électron et le trou "réfléchi" dans le processus d'Andréev pour traverser la région normale, cette dernière inégalité signifie que les oscillations de phase doivent être suffisamment lentes pour laisser au système le temps de réajuster les niveaux d'Andréev. Dans le cas contraire, le transport cohérent n'a pas le temps de s'établir et un courant dissipatif circule alors. Pour que cette contrainte soit respectée, on déduit de (5.38) que la capacité du terminal A doit être supérieure ou égale à

$$C_{min} = \frac{e^2 N_\perp}{2\bar{\epsilon}} \sim 10^{-13} F. \tag{5.40}$$

De même, de (5.39) on obtient la fréquence d'oscillations ω_0 maximale :

$$\omega_{max} \sim \frac{v_F}{2R} \sim 10^{11} s^{-1}. \tag{5.41}$$

À l'aide de cette relation pour ω_{max} on peut maintenant estimer le taux de transition entre les deux états de phase $\pm\varphi_0$. Des travaux de Leggett *et. al.* [68], on sait que ce taux est donné par la somme du taux de transitions activées thermiquement $\Gamma_A \sim \omega_0 e^{-U(0)/k_B T}$ (au-dessus de la barrière de potentiel $U(0)$, figure 5.6) et du taux de transitions tunnels $\Gamma_T \sim \omega_0 e^{-U(0)/\hbar\omega_0}$ (sous la barrière). Le potentiel $U(\varphi)$ est donné par la relation [64]

$$U(\phi) = \frac{N_\perp \bar{\epsilon}}{4\pi^2} \left(|\phi| - \phi_0\right)^2, \tag{5.42}$$

de sorte que $U(0) = N_\perp \bar{\epsilon} \phi_0^2 / 4\pi^2$. À la température $\bar{T}$, l'activation thermique est négligeable de sorte que seul Γ_T contribue. Pour ω_{max} $(= \bar{\epsilon}/\hbar$, éq. (5.37)), on obtient le taux tunnel maximal

$$\Gamma_{T\,max} \sim \omega_{max}\; e^{-\frac{U(0)}{\hbar\omega_{max}}} \sim \omega_{max}\; e^{-N_\perp\left(\frac{\phi_0}{2\pi}\right)^2}. \tag{5.43}$$

Pour $\varphi_0 \sim 0.2\pi$ (et donc $\Omega \sim 0.3$), on obtient Γ_T de l'ordre du GHz. La fréquence obtenue ici est une estimation de la fréquence caractéristique de l'opération $\mathsf{R}_x(\theta)$. La largeur des niveaux d'énergie est de l'ordre de $\Delta E \sim \hbar/\Delta t \sim \hbar\Gamma_T \sim 10^{-17} erg$. Cette dernière estimation correspond à l'ordre de grandeur de l'énergie ε minimale associée à l'opération $\mathsf{R}_z(\varphi)$.

5.9 Perspectives

Considérons maintenant quelques avantages et inconvénients de cette architecture particulière d'ordinateur quantique pour ensuite aborder quelques aspects qui restent à étudier.

Les jonctions présentées à la figure 5.8 ont l'avantage d'avoir un flux magnétique spontané Φ_s beaucoup plus petit que le quantum de flux Φ_0. Le couplage inductif entre qubits et le couplage à l'environnement (dû à ce flux) est alors beaucoup plus faible que dans le cas d'un SQUID, augmentant de ce fait les chances d'observer l'effet tunnel cohérent dans ce système. De même, on remarque que la hauteur de la barrière de potentiel $U(0) = N_\perp \bar{\epsilon}\phi_0^2/4\pi^2$ varie avec ϕ_0 et donc avec l'angle de désalignement Ω. Ainsi, contrairement au cas de l'architecture suggérée par Ioffe *et. al.* [61], la probabilité tunnel (5.43) peut être choisie parmi une grande plage de valeurs, de façon à obtenir des conditions optimales. De même, et toujours contrairement à [61], la hauteur de la barrière de potentiel séparant un double puits d'un autre (figure 5.6) est très grande dans ce système et la probabilité tunnel alors presque nulle.

Mentionnons aussi que, par opposition à l'architecture suggérée par Mooij *et. al.* [84], les jonctions présentées à la figure 5.8 ont l'avantage d'être relativement facilement intégrables à une structure à plusieurs qubits.

Citons maintenant quelques problèmes et difficultés potentiels. Premièrement, la mesure, l'initialisation et l'opération R_z, telles que présentées ici, nécessitent une pointe de microscope à force magnétique. Pour plus d'efficacité, on utilisera une pointe par qubit (ou par groupe de qubits). De plus, afin de minimiser le couplage à l'environnement, ces pointes devront être reculées lors des calculs. En pratique, il semble qu'il puisse être difficile d'utiliser de telles pointes de microscope. D'autres techniques pour réaliser ces opérations sont toutefois possibles. De plus, en pratique, la différence de conductivité entre l'état ouvert et l'état fermé des clés de parité (laissant circuler ou non un courant) n'est d'environ que d'un facteur cent [85]. Ainsi, ces éléments causeront un couplage non voulu à la masse et aux qubits voisins. Évidemment, les conséquences d'un tel couplage peuvent être désastreuses du point de vue de la manipulation de l'information quantique. On peut toutefois s'attendre à obtenir des clés de parité de plus en plus efficaces avec l'amélioration des techniques de fabrication.

Au niveau de la fabrication, il n'y a pas que les clés de parité qui causent problème. En effet, la fabrication des jonctions DND qui sont au coeur de cette architecture n'est elle-même pas chose facile. En particulier, dans le cas des jonctions triangulaires, contrôler l'angle de désalignement et par conséquent la phase à l'équilibre ϕ_0 n'est pas une mince tâche. Notons aussi que les jonctions fabriquées ne seront pas toutes identiques. Ainsi, on doit s'attendre à des variations dans les propriétés (phase à l'équilibre, barrière tunnel, ...) des qubits. Ce problème peut, en partie, être résolu en mesurant préalablement toutes les propriétés nécessaires des qubits puis en corrigeant classiquement pour ces différences lors de l'application des portes logiques.

Notons par ailleurs que, contrairement à l'architecture de Mooij *et. al.* [84] qui n'utilise que des supraconducteurs conventionnels, on devra porter attention aux quasiparticules nodales dans les qubits formés de supraconducteurs de type d qui nous intéressent ici [86]. Ainsi, avant de passer au laboratoire pour la réalisation expérimentale d'un ordinateur quantique utile ($n > 1000$) utilisant ces jonctions, beaucoup de travail théorique reste à faire.

En particulier, des estimations des dimensions et fréquences caractéristiques de ces jonctions ont été présentées à la section §5.8 mais une analyse plus précise est requise. En particulier, les énergies caractéristiques correspondant aux rotations par rapport aux axes z ainsi que E_J pour l'opération CP doivent être déterminées.

De plus, une analyse plus détaillée de la technique de refocalisation est nécessaire.

On doit entre autres s'assurer que la perturbation périodique n'entraîne pas de transitions dans un même puit et entre les puits. L'utilisation potentielle de cette technique de refocalisation global dans le cadre de la réduction de décohérence devra aussi être étudiée.

Beaucoup de travail reste à faire sur la caractérisation des sources de décohérence et du temps de décohérence, t_d, de ce système (critère #3 de la section §5.1). Ce temps de décohérence doit être comparé aux fréquences caractéristiques des opérations logiques afin d'obtenir une estimation du nombre de portes qu'il sera possible d'appliquer sur ce système.

Deux séries de résultats expérimentaux récents sur des systèmes supraconducteurs mésoscopiques permettent toutefois d'être optimiste quant au temps de décohérence du système considéré ici. En effet, une expérience récente par un groupe français [87] montre qu'il est possible de préparer une 'boîte supraconductrice' dans une superposition cohérente d'états de charges. Cette étude montre aussi que la source de décohérence principale pour un tel système est la dissipation induite par l'environnement électromagnétique du circuit. Le temps de décohérence estimé est supérieur à $10\mu s$. Un second groupe a récemment poussé plus loin cette réalisation expérimentale [88]. En plus de préparer une superposition cohérente d'états de charges (i.e. un qubit), ceux-ci ont réussi à contrôler l'état de ce qubit de façon cohérente à l'aide de courtes impulsions électriques. La figure 5.14 présente la 'boîte supraconductrice' utilisée par cette équipe.

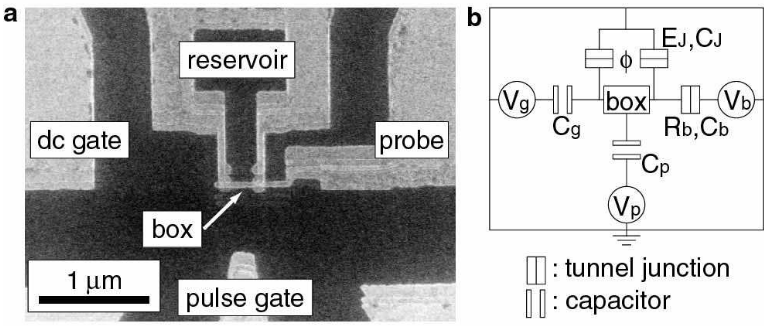


Figure 5.14: a) Image par microscope à effet tunnel de l'échantillon. b) Circuit équivalent. (Tirée de [88].)

La 'boîte', faite d'aluminium et de dimensions $700 \times 50 \times 15nm$, contient $\sim 10^8$ électrons de conduction. Les énergies caractéristiques du systèmes sont : l'énergie électrostatique correspondant à l'ajout d'un électron sur la boîte $E_c = e^2/C_\Sigma \approx 117\mu eV$, où C_Σ est la capacité totale de la boîte, l'énergie Josephson $E_J(\phi = 0) \approx 84\mu eV$ et le gap supraconducteur $\Delta \approx 230\mu eV$. Les expériences sont conduites dans un réfrigérateur à dilution à la température d'environ $30mK$ $(k_BT \approx 3\mu eV)$[9]. (Notons que $E_J < E_c < \Delta$ et que toutes ces énergies sont beaucoup plus grandes que k_BT, ceci correspond au régime pour lequel les effets de parité sont importants [65].) Pour ce système, le temps de décohérence mesuré est d'environ $2ns$. Ce résultat est beaucoup plus petit que les $10\mu s$ du groupe français et est dû à l'effet de la jonction sonde (*probe*) qui 'mesure' constamment l'état du système. Malgré le cours temps de décohérence obtenu, cette dernière expérience montre la validité du concept de qubits 'mésoscopiques' qui nous intéresse ici.

Il sera aussi essentiel de calculer en détail l'évolution d'un qubit lorsque celui-ci est relié à la masse à l'aide de la clé de parité et ainsi s'assurer que cette opération correspond bien à une mesure à la von Neumann (i.e. projection orthogonale sur la base de calcul). Il sera aussi nécessaire de déterminer l'effet de cette mesure sur les qubits adjacents. Un point de départ pour ces calculs sont les travaux récents de A. Shnirman et G. Schön [89].

Il sera de même profitable de chercher des réalisations plus efficaces des portes importantes CN et Sw et d'optimiser l'utilisation des 'Swaps'. En effet, l'équation (5.30) montre qu'il est très coûteux, en terme de nombre d'opérations, de ne pouvoir

[9] L'expérience consiste à préparer le système de façon à ce que la boîte soit électriquement neutre. On note cet état $|0\rangle$ signifiant qu'il y a aucun (0) électron en excès sur la boîte. On applique ensuite une impulsion électrique pendant un temps Δt (les impulsions utilisées sont extrêmement courts et varient entre 80 et $450ps$). Cette impulsion est choisie de façon à ce que l'état initial, $|0\rangle$, entre en résonance avec l'état ayant deux électrons en excès, $|2\rangle$. Il y a alors oscillations cohérentes entre ces états. Après l'impulsion, la 'boîte' se trouve dans une superposition cohérente de ces deux états, leur poids respectif ne dépendant que de la durée Δt. Suite à l'impulsion, l'état $|2\rangle$ relaxe vers $|0\rangle$ par tunneling séquentiel de deux quasiparticules à travers la jonction sonde (*probe*). On mesure ce courant à travers cette jonction, courant qui est proportionnel à l'amplitude de probabilité que le système se trouve dans l'état $|2\rangle$. L'effet des oscillations cohérentes et donc du contrôle cohérent est mesuré à l'aide de ce courant.

appliquer les portes non locales que sur des qubits adjacents. Pour réaliser une telle opération sur des qubits occupant initialement les positions k et l (avec $l > k$), $2[(l-k)-1]$ applications de Sw sont nécessaires. Cependant, il est possible d'appliquer simultanément plusieurs portes sur des qubits ou des groupes de qubits différents. On peut ainsi, selon le calcul effectué, réaliser ces Sw 'en tâche de fond' simultanément avec les opérations logiques sur les qubits actifs. De cette façon, on peut faire en sorte que les qubits impliqués dans une opération non locale soient juxtaposés au moment où cette opération doit être effectuée et ce, sans avoir à utiliser de cycles d'horloge supplémentaires. Suite à cette opération, on déplace ensuite l'état logique de ces qubits vers la prochaine destination où ils subiront une opération logique non locale et ce, tout en continuant les opérations logiques sur les qubits actifs. Il peut aussi être avantageux de déplacer simultanément l'état logique de deux qubits devant interagir (et non seulement un de ces qubits vers l'autre). Ces façons de procéder doivent être optimisées en fonction du calcul à effectuer.

De façon alternative, on peut utiliser la téléportation quantique [38, 90] pour déplacer rapidement l'état logique des qubits. Cette technique nécessite toutefois, pour chaque qubit à téléporter, la présence d'une paire EPR (i.e. un état de la base de Bell) distribuée entre le lieu source et cible. Puisque l'on ne peut créer d'enchevêtrement à distance, ces paires doivent avoir été distribuées à l'aide de Sw. Utilisant ces paires comme canaux quantiques on peut rapidement déplacer les qubits à l'intérieur du registre. Évidemment, toutes ces variantes utilisent le même nombre d'opérations Sw, mais tentent de faire un meilleur usage de la ressource importance qu'est le temps.

Finalement, puisqu'il est possible d'appliquer des opérations logiques en parallèle, il semble qu'il sera possible d'effectuer du calcul quantique tolérant aux imperfections (§4.2) sur ce système. Puisqu'il s'agit d'un aspect important, il peut être profitable de s'attarder aux limitations imposées par le fait qu'il ne soit pas possible d'appliquer un CN avec un qubit source et plusieurs qubits cibles simultanément [40] et qu'il ne soit possible d'appliquer les portes non locales que sur des qubits adjacents [41].

Conclusion

Nous avons vu que les lois de la théorie quantique donnent accès à une grande puissance de calcul. Les ressources principales d'où un ordinateur quantique tire cette puissance sont le principe de superposition, l'interférence et l'enchevêtrement. En raison du principe de superposition, un ordinateur quantique explore lors des calculs un espace de dimension exponentielle. Par l'utilisation de cet espace exponentiel (i.e. du parallélisme quantique), celui-ci peut venir à bout de certains problèmes plus rapidement que sa contrepartie classique.

Toutefois, l'information quantique est très fragile et subit rapidement la décohérence : l'information de phase se retrouve alors encodée dans l'environnement et les effets quantiques sont perdus. Pour les systèmes de taille importante la décohérence est rapide. Heureusement, les techniques de correction quantique d'erreurs peuvent venir à bout de ce problème. En particulier, les techniques de calcul quantique tolérant aux imperfections nous apprennent, *qu'en principe*, un ordinateur quantique ayant un taux d'erreurs suffisamment bas peut réaliser des calculs arbitrairement longs.

Pour dépasser le titre de problème intéressant en mathématique appliquée, un ordinateur quantique doit être réalisé expérimentalement. En pratique plusieurs contraintes se posent. En particulier, on doit être capable de contrôler de l'extérieur l'état des qubits tout en les isolant de l'environnment de façon à limiter la décohérence. Malgré ces difficultés, à ce jour plusieurs architectures ont été présentées et, à l'aide des techniques de RMN, jusqu'à 7 qubits ont pu être manipulés de façon cohérente.

Dans le but de réaliser un ordinateur quantique utile (i.e. ayant plusieurs qubits), il semble que les techniques plus traditionnelles de micro-fabrication présentent une solution favorable. Nous nous sommes donc intéressés à une architecture basée sur l'utilisation de jonctions Josephson entre supraconducteurs de type d. Dans ce système, la phase entre les électrodes supraconductrices joue le rôle de qubit. De même, l'interaction entre les qubits est réalisée à l'aide de clés de parité. Nous avons montré comment réaliser sur ce système l'initialisation et la mesure. Nous avons également montré comment réaliser un ensemble complet de portes logiques sur ce système, prouvant par le fait qu'il s'agit d'un ordinateur quantique universel. Pour arriver à ce résultat, nous avons utilisé une technique de refocusing global pour inhiber l'évolution des qubits passifs. Cette technique peut être utilisée simultanément avec les opérations logiques et peut, en principe, conduire à une réduction de la décohérence. Plusieurs aspects de cette suggestion de réalisation expérimentale restent toutefois à étudier. En particulier, une analyse détaillée des sources de décohérence est nécessaire.

Un ordinateur quantique capable de manipuler plusieurs qubits et ayant un long temps de décohérence aurait une puissance de calcul à ce jour inégalée. Les applications principales d'un tel calculateur quantique seraient la factorisation de grands nombres et la recherche dans des bases de données désordonnées. Une autre application potentielle des ordinateurs quantiques est la simulation de systèmes quantiques.

Toutefois, avant la réalisation d'un système de traitement de l'information quantique universel ($> 10^6$ qubits), beaucoup de travail (et possiblement de temps) reste. Le chemin menant vers un tel système est parsemé d'embûches mais aussi de physique et de réalisations passionnantes : ingénierie d'états quantiques, contrôle cohérent de système quantique, cryptographie quantique, communication quantique, non localité, téléportation quantique ... Études qui mènent, en bout de ligne, à une meilleure compréhension du monde quantique et par conséquent du monde dans lequel nous vivons.

Annexe A

Manipulation symbolique de qubits à l'aide de Mathematica

Dans cette annexe, on décrit un ensemble de fonctions (écrites à l'aide du langage de manipulation symbolique Mathematica, version 3.0) permettant de simuler l'application d'opérations logiques sur un registre quantique. Ces procédures facilitent les calculs associés à l'évolution d'un ensemble de qubits, calculs souvent simples mais lourds. Elles seront donc appréciées, par exemple, dans le développement de nouveaux circuits quantiques.

A.1 Représentation des kets

On définit un ket par deux tableaux. Le premier décrit les états présents dans la superposition et le second leur coefficient respectif. Par exemple, la superposition $\frac{1}{\sqrt{2}}|00\rangle + |11\rangle$ s'écrit

{{{0, 0}, {1, 1}}, {1/Sqrt[2], 1/Sqrt[2]}}

On peut aussi utiliser la représentation décimale pour décrire le même état :

{{0, 3}, {1/Sqrt[2], 1/Sqrt[2]}}

On utilise la fonction **ketDec** pour décrire la superposition arbitraire de n qubits en représentation décimale

```
ketDec[n_,x_]:=Join[{Range[0,2^n-1]},{Table[x[i],{i,0,2^n-1}]}]
```

Le premier paramètre définit le nombre de qubits dans la superposition et le second, l'index des coefficients. Par exemple, une superposition arbitraire de 5 qubits est

ketDec[5,a]

{{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31}, {a[0], a[1], a[2], a[3], a[4], a[5], a[6], a[7], a[8], a[9], a[10], a[11], a[12], a[13], a[14], a[15], a[16], a[17], a[18], a[19], a[20], a[21], a[22], a[23], a[24], a[25], a[26], a[27], a[28], a[29], a[30], a[31]}}

Les coefficients $a[x]$ doivent être définis pour spécifier complètement l'état du système. La fonction **ketBin** est l'équivalent de **ketDec** pour la représentation binaire

```
ketBin[n_,x_]:= Join[{IntegerDigits[Range[0,2^n-1],2,n]},
  {Table[x[i],{i,0,2^n-1}]}]
```

Pour trois qubits on a par exemple

ketBin[3,a]

{{{0, 0, 0}, {0, 0, 1}, {0, 1, 0}, {0, 1, 1}, {1, 0, 0}, {1, 0, 1}, {1, 1, 0}, {1, 1, 1}}, {a[0], a[1], a[2], a[3], a[4], a[5], a[6], a[7]}}

On utilisera principalement la notation binaire. Celle-ci est moins compacte mais simplifie l'application des portes logiques.

A.2 Opérations Logiques

Décrivons d'abord l'application des opérateurs de Pauli. On applique la matrice de Pauli σ_x sur un ket arbitraire à l'aide de la fonction suivante (le premier paramètre est le nom du ket cible et le deuxième, la position du qubit sur laquelle l'opérateur agit) :

```
sx[y_,z_]:= (A2temp[x_]:=Mod[x+1,2];
   MapAt[A2temp,y,Table[{1,i,z},{i,1,Length[Part[y,1]]}]])
```

Par exemple sur la superposition arbitraire de 3 qubits on obtient lors de l'application de **sx** sur le troisième qubit :

sx[ketBin[3,a],3]

{{{0, 0, 1}, {0, 0, 0}, {0, 1, 1}, {0, 1, 0}, {1, 0, 1}, {1, 0, 0}, {1, 1, 1}, {1, 1, 0}}, {a[0], a[1], a[2], a[3], a[4], a[5], a[6], a[7]}}

On applique l'opérateur σ_z à l'aide de la fonction **sz**:

```
sz[y_,z_]:=
  ReplacePart[y,Table[y[[2,i]]*(-1)^y[[1,i,z]],
  {i,1,Length[Part[y,1]]}],2]
```

Finalement on applique σ_y (on applique σ_z puis σ_x) à l'aide de **sy**:

```
sy[y_,z_]:= (sytemp=sz[y,z];sx[sytemp,z])
```

Décrivons maintenant comment appliquer un controlled-NOT, une phase conditionnelle et la porte d'Hadamard. La fonction **CN1** applique la porte logique Controled-NOT sur un ket général y (le premier argument) avec comme bit source x (deuxième argument) et comme cible le qubit z (troisième argument):

```
CN1[y_,x_,z_]:=
Module[{temp,CN1temp},
(
Clear[temp,CN1temp];
CN1temp=Length[Part[y,1]];
```

```
temp[0]=y;
For[i=1,i<=CN1temp,i++,
temp[i]=ReplacePart[temp[i-1],Mod[y[[1,i,x]]+y[[1,i,z]],2],{1,i,z}]];
      Return[temp[CN1temp]])]
```

Par exemple pour l'état

ketBin[3,a]

{{{0, 0, 0}, {0, 0, 1}, {0, 1, 0}, {0, 1, 1}, {1, 0, 0}, {1, 0, 1}, {1, 1, 0}, {1, 1, 1}} , {a[0], a[1], a[2], a[3], a[4], a[5], a[6], a[7]}}

on a

CN1[ketBin[3,a],1,2]

{{{0, 0, 0}, {0, 0, 1}, {0, 1, 0}, {0, 1, 1}, {1, 1, 0}, {1, 1, 1}, {1, 0, 0}, {1, 0, 1}}, {a[0], a[1], a[2], a[3], a[4], a[5], a[6], a[7]}}

Ainsi, après application de cette opération, le qubit z prend comme valeur $x \oplus z$ (et x reste inchangé). La fonction **CN** généralise cette dernière opération:

```
CN[y_,a_,a1_,d_]:=
Module[{temp,CNtemp2},
(
Clear[temp,CNtemp2];
CNtemp2=Length[Part[y,1]];
CNtemp3[x_]:=Mod[x+1,2];
temp[0]=y;
For[i=1,i<=CNtemp2,i++,
If[y[[1,i,a]]==a1,temp[i]=MapAt[CNtemp3,temp[i-1],{1,i,d}],
          temp[i]=temp[i-1]]
];
Return[temp[CNtemp2]]
)]
```

Cette fonction prend comme argument un nombre arbitraire de qubits sources. Ainsi, **CN**[**y,a,a1,d**] applique l'opération NOT sur le d ième qubit du ket y si les qubits spécifiés par la liste a ont chacun la valeur spécifiée par la liste $a1$. Par exemple, pour l'état

ketBin[4,a]

{{{0, 0, 0, 0}, {0, 0, 0, 1}, {0, 0, 1, 0}, {0, 0, 1, 1}, {0, 1, 0, 0}, {0, 1, 0, 1}, {0,1, 1, 0}, {0, 1, 1, 1}, {1, 0, 0, 0}, {1, 0, 0, 1}, {1, 0, 1, 0}, {1, 0, 1, 1}, {1, 1, 0, 0}, {1, 1, 0, 1}, {1, 1, 1, 0}, {1, 1, 1, 1}}, {a[0], a[1], a[2], a[3], a[4], a[5], a[6], a[7], a[8], a[9], a[10], a[11], a[12], a[13], a[14], a[15]}}

l'opération suivante change la valeur du quatrième qubit, si le premier qubit prend la valeur 1, le second 0 et le troisième 1:

CN[**ketBin**[4,a],**{1,2,3}**,**{1,0,1}**,4]

{{{0, 0, 0, 0}, {0, 0, 0, 1}, {0, 0, 1, 0}, {0, 0, 1, 1}, {0, 1, 0, 0}, {0, 1, 0, 1}, {0, 1, 1, 0}, {0, 1, 1, 1}, {1, 0, 0, 0}, {1, 0, 0, 1}, {1, 0, 1, 1}, {1, 0, 1, 0}, {1, 1, 0, 0}, {1, 1, 0, 1}, {1, 1, 1, 0}, {1, 1, 1, 1}}, {a[0], a[1], a[2], a[3], a[4], a[5], a[6], a[7], a[8], a[9], a[10], a[11], a[12], a[13], a[14], a[15]}}

L'opération **Cpi**, applique une phase $e^{i\pi}$ sur chacun des états de la superposition dont les qubits spécifiés par la liste a ont la valeur spécifiée par la liste $a1$:

```
Cpi[y_,a_,a1_]:=
Module[{temp,Cpitemp2},
(
Clear[temp,Cpitemp2];
Cpitemp2=Length[Part[y,1]];
temp[0]=y;
For[i=1,i<=Cpitemp2,i++,

If[y[[1,i,a]]==a1,
temp[i]=ReplacePart[temp[i-1],-y[[2,i]],{2,i}],
```

```
temp[i]=temp[i-1]
]];
Return[temp[Cpitemp2]]
)]
```

Par exemple:

Cpi[ketBin[4,a],{1,2,3},{1,0,1}]

{{{0, 0, 0, 0}, {0, 0, 0, 1}, {0, 0, 1, 0}, {0, 0, 1, 1}, {0, 1, 0, 0}, {0, 1, 0, 1}, {0, 1, 1, 0}, {0, 1, 1, 1}, {1, 0, 0, 0}, {1, 0, 0, 1}, {1, 0, 1, 0}, {1, 0, 1, 1}, {1, 1, 0, 0}, {1, 1, 0, 1}, {1, 1, 1, 0}, {1, 1, 1, 1}}, {a[0], a[1], a[2], a[3], a[4], a[5], a[6], a[7], a[8], a[9], -a[10], -a[11], a[12], a[13], a[14], a[15]}}

L'opération **H** applique la matrice d'Hadamard sur le qubit x du ket y. Rappelons que la matrice d'Hadamard 2×2 agit comme suit sur les états de la base $\{|\,0\rangle\,, |\,1\rangle\}$:

$$\mathsf{H} : \begin{cases} |\,0\rangle \\ |\,1\rangle \end{cases} \longrightarrow \quad \frac{1}{\sqrt{2}} \begin{cases} |\,0\rangle + |\,1\rangle \\ |\,0\rangle - |\,1\rangle \end{cases} \tag{A.1}$$

```
H[y_,x_]:=
Module[{temp,Htemp1,Htemp2,n},
(
Clear[temp,Htemp1,Htemp2,n];
temp[0]=y;

For[i=1,i<=Length[Part[y,1]],i++,

  If[y[[1,i,x]]==0,z[i]=1,z[i]=-1];
  n=i-1;

  Htemp1[i]=ReplacePart[temp[i-1],0,{1,i+n,x}];
  Htemp2[i]=Insert[Htemp1[i],
      ReplacePart[Part[temp[i-1],1,i+n],1,x],{1,i+n+1}];
```

```
  temp[i]=Insert[Htemp2[i],z[i]*y[[2,i]],{2,i+n+1}];
];

Join[{Part[temp[Length[Part[y,1]]],1]},
    {1/Sqrt[2]*Part[temp[Length[Part[y,1]]],2]}]
)]
```

Par exemple, appliquée sur le premier qubit de l'état

ketBin[2,a]

{{{0,0},{0,1},{1,0},{1,1}},{a[0],a[1],a[2],a[3]}}

on obtient:

H[ketBin[2,a],1]

{{{0, 0}, {1, 0}, {0, 1}, {1, 1}, {0, 0}, {1, 0}, {0, 1}, {1, 1}}, { a[0]/Sqrt[2], a[0]/Sqrt[2], a[1]/Sqrt[2], a[1]/Sqrt[2], a[2]/Sqrt[2], -a[2]/Sqrt[2], a[3]/Sqrt[2], -a[3]/Sqrt[2]}}

A.3 Exemple d'application : correction quantique d'erreurs

En guise d'exemple d'application, on appliquera les portes définies précédemment au code correcteur $[[1, 5, 1]]$ (Laflamme *et. al.* [34]). Pour ce code, l'état initial est $|\,0\rangle\,|\,0\rangle\,(a\,|\,0\rangle + b\,|\,1\rangle)\,|\,0\rangle\,|\,0\rangle$, où le troisième bit est celui à protéger et les autres des auxiliaires. La séquence d'opérations logiques de la fonction **encodeur** correspond au circuit encodeur décrit par Laflamme *et. al.* :

```
encodeur[a_,b_]:=
Module[{ini,ini1,ini2,ini3,ini4,ini5,ini6,ini7,ini8,ini9,ini10,ini11},
(
```

```
ini = {{{0,0,0,0,0},{0,0,1,0,0}},{a,b}};
ini1=H[ini,1];
ini2=H[ini1,2];
ini3=H[ini2,4];
ini4=Cpi[ini3,{2,3,4},{1,1,1}];
ini5=Cpi[ini4,{2,3,4},{0,1,0}];
ini6=CN[ini5,3,1,5];
ini7=CN[ini6,1,1,3];
ini8=CN[ini7,1,1,5];
ini9=CN[ini8,4,1,3];
ini10=CN[ini9,2,1,5];
ini11=Cpi[ini10,{4,5},{1,1}])
]
```

On vérifie (voir [34]) que ce circuit donne bien le résultat attendu :

encodeur[a,b]

{{{0, 0, 0, 0, 0}, {0, 0, 1, 1, 0}, {0, 1, 0, 0, 1}, {0, 1, 1, 1, 1}, {1, 0, 1, 0, 1}, {1, 0, 0, 1, 1}, {1, 1, 1, 0, 0}, {1, 1, 0, 1, 0}, {0, 0, 1, 0, 1}, {0, 0, 0, 1, 1}, {0, 1, 1, 0, 0}, {0, 1, 0, 1, 0}, {1, 0, 0, 0, 0}, {1, 0, 1, 1, 0}, {1, 1, 0, 0, 1}, {1, 1, 1, 1, 1}}, {a/(2*Sqrt[2]), a/(2*Sqrt[2]), a/(2*Sqrt[2]), -(a/(2*Sqrt[2])), a/(2*Sqrt[2]), -(a/(2*Sqrt[2])), a/(2*Sqrt[2]), a/(2*Sqrt[2]), -(b/(2*Sqrt[2])), -(b/(2*Sqrt[2])), b/(2*Sqrt[2]), -(b/(2*Sqrt[2])), -(b/(2*Sqrt[2])), b/(2*Sqrt[2]), b/(2*Sqrt[2]), b/(2*Sqrt[2])}}

La fonction **decodeur** correspond quant à elle au circuit de détection d'erreurs de ce même code :

```
decodeur[y_]:=
Module[{deco1,deco2,deco3,deco4,deco5,deco6,deco7,deco8,deco9,deco10,
deco11,deco12},
(
deco1=Cpi[y,{4,5},{1,1}];
```

```
deco2=CN[deco1,2,1,5];
deco3=CN[deco2,4,1,3];
deco4=CN[deco3,1,1,3];
deco5=CN[deco4,1,1,5];
deco6=CN[deco5,3,1,5];
deco7=Cpi[deco6,{2,3,4},{0,1,0}];
deco8=Cpi[deco7,{2,3,4},{1,1,1}];
deco9=H[deco8,1];
deco10=H[deco9,2];
deco11=H[deco10,4];
deco12=ketreduce[deco11];
deco13= nonnul[deco12])]
```

Cette dernière fonction utilise la fonction **ketreduce** qui simplifie la description des superpositions d'états en additionnant les coefficient des états équivalents :

```
ketreduce[y_]:=
Module[{temp,dumy,dum1,dum2,boucle2,limite,nbr,posi},
(Clear[temp,dumy,dum1,dum2,boucle2,limite,dum1,dum2,nbr,posi];
temp[0]=y;
limite=Length[Part[y,1]];

For[i=1,i<=limite,i++,(

nbr[i]=Count[Part[temp[i-1],1],Part[temp[i-1],1,i]];

 If[nbr[i]!=1,(

  Clear[posi,boucle2,dum1,dum2,dumy];
  dumy[1]=temp[i-1];
  boucle2=0;
```

```
  For[j=2,j<=nbr[i],j++,(
    posi[j]=Extract[Extract[
           Position[Part[temp[i-1],1],Part[temp[i-1],1,i]],j],1];
    dum1=ReplacePart[dumy[j-1],
              dumy[j-1][[2,i]]+temp[i-1][[2,posi[j]]],{2,i}];
    dum2=Delete[dum1,{1,posi[j]-boucle2}];
    dumy[j]=Delete[dum2,{2,posi[j]-boucle2}];
    boucle2=boucle2+1;)
   ]
   temp[i]=dumy[j-1];

),
  (temp[i]=temp[i-1];
   boucle2=0;)   (*le Else du If*)

  ];  (*fin du If*)

  limite=limite-boucle2;
  )]; (*fin du For i*)
  temp[i-1]
)]
```

Le "circuit" **decodeur** utilise aussi la fonction **nonnul** qui ne conserve que les états dont les coefficients sont non nuls :

```
nonnul[y_]:=
Module[{temp,boucle},
(
 Clear[temp,boucle];
 boucle=0;
 temp[0]=y;
 For[i=1,i<=Length[y[[2]]],i++,
```

```
   If[ToString[y[[2,i]]]==ToString[0],
    (temp[i]=Delete[temp[i-1],{{1,1+boucle},{2,1+boucle}}];),
    (temp[i]=temp[i-1];
    boucle=boucle+1;)
   ] (*EndIf*)
 ]; (*EndFor*)
temp[Length[y[[2]]]]
)]
```

Appliqué a l'état encodé, on retrouve l'état initial à l'aide du circuit **decodeur** :

decodeur[**encodeur**[**a,b**]]

{{{0, 0, 0, 0, 0}, {0, 0, 1, 0, 0}}, {a, b}}

Simulons maintenant une erreur de phase sur le troisième qubit de l'état encodé en appliqant la matrice de Pauli σ_z sur ce qubit :

sz[**encodeur**[**a,b**],**3**]

{{{0, 0, 0, 0, 0}, {0, 0, 1, 1, 0}, {0, 1, 0, 0, 1}, {0, 1, 1, 1, 1}, {1, 0, 1, 0, 1}, {1, 0, 0, 1, 1}, {1, 1, 1, 0, 0}, {1, 1, 0, 1, 0}, {0, 0, 1, 0, 1}, {0, 0, 0, 1, 1}, {0, 1, 1, 0, 0}, {0, 1, 0, 1, 0}, {1, 0, 0, 0, 0}, {1, 0, 1, 1, 0}, {1, 1, 0, 0, 1}, {1, 1, 1, 1, 1}}, {a/(2*Sqrt[2]), -(a/(2*Sqrt[2])), a/(2*Sqrt[2]), a/(2*Sqrt[2]), -(a/(2*Sqrt[2])), -(a/(2*Sqrt[2])), -(a/(2*Sqrt[2])), a/(2*Sqrt[2]), b/(2*Sqrt[2]), -(b/(2*Sqrt[2])), -(b/(2*Sqrt[2])), -(b/(2*Sqrt[2])), -(b/(2*Sqrt[2])), -(b/(2*Sqrt[2])), b/(2*Sqrt[2]), -(b/(2*Sqrt[2]))}}

On décode maintenant cet état à l'aide du circuit décodeur :

decodeur[**sz**[**encodeur**[**a,b**],**3**]]

{{{1, 0, 0, 1, 0}, {1, 0, 1, 1, 0}}, {a, -b}}

On obtient donc pour le qubit logique (le troisième qubit) l'état $a\,|\,0\rangle - b\,|\,1\rangle$ et le syndrome $|\,1\rangle\,|\,0\rangle\,|\,1\rangle\,|\,0\rangle$ ce qui correspond au résultat attendu (voir [34] pour plus de détails sur ce code correcteur et en particulier pour la correspondance entre erreurs et syndromes).

A.4 Exemple d'application : Circuit de la figure 4.3

Comme dernier exemple, voici le code correspondant au circuit de la figure 4.3 (ce code ne décrit que la première étape de ce circuit; voir section §4.1) servant à la détection d'erreur de phase pour le code $[[1, 9, 1]]$ de Shor :

```
circuitphase[y_]:=
Module[{temp,temp1,temp2,temp3,temp4,temp5,temp6,temp7,temp8,temp9,
temp10,temp11,temp12,temp13,temp14,temp15,temp16,temp17,temp18,temp19,
temp20,temp21,temp22,temp23,temp24,temp25,temp26,temp27,temp28,temp29,
temp30,temp31},
(
temp=H[y,1];
temp1=H[temp,2];
temp2=H[temp1,3];
temp3=H[temp2,4];
temp4=H[temp3,5];
temp5=H[temp4,6];
temp6=H[temp5,7];
temp7=H[temp6,8];
temp8=H[temp7,9];
temp9=CN1[temp8,1,10];
temp10=CN1[temp9,2,10];
temp11=CN1[temp10,3,10];
temp12=CN1[temp11,4,11];
temp13=CN1[temp12,5,11];
temp14=CN1[temp13,6,11];
```

```
temp15=CN1[temp14,7,12];
temp16=CN1[temp15,8,12];
temp17=CN1[temp16,9,12];
temp18=H[temp17,1];
temp19=nonnul[ketreduce[temp18]];
temp20=H[temp19,2];
temp21=nonnul[ketreduce[temp20]];
temp22=H[temp21,3];
temp23=H[temp22,4];
temp24=nonnul[ketreduce[temp23]];
temp25=H[temp24,5];
temp26=H[temp25,6];
temp27=H[temp26,7];
temp28=nonnul[ketreduce[temp27]];
temp29=H[temp28,8];
temp30=H[temp29,9];
temp31=nonnul[ketreduce[temp30]])]
```

On utilise les fonctions **ketreduce** et **nonnul** pour diminuer l'espace mémoire requis. Appliqué sur l'état encodé $|\,0\rangle_L$, on s'attend à obtenir du circuit 4.3 le syndrome $|\,000\rangle$ et c'est effectivement le résultat obtenu à l'aide de la fonction **circuitphase**. Ainsi, appliqué sur l'état $|\,0\rangle_L$ on obtient

{{{0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}, {0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0}, {0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0}, {0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0}, {1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0}, {1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0}, {1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0}, {1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0}}, {1/(2*Sqrt[2]), 1/(2*Sqrt[2]), 1/(2*Sqrt[2]), 1/(2*Sqrt[2]), 1/(2*Sqrt[2]), 1/(2*Sqrt[2]), 1/(2*Sqrt[2]), 1/(2*Sqrt[2])}}

En notation habituelle, ce dernier résultat s'écrit :

$$\frac{1}{2\sqrt{2}}\left(|\,000\rangle+|\,111\rangle\right)\left(|\,000\rangle+|\,111\rangle\right)\left(|\,000\rangle+|\,111\rangle\right)\otimes|\,000\rangle\equiv|\,0\rangle_L\,|\,000\rangle \tag{A.2}$$

et correspond au résultat attendu.

Ainsi, le code décrit dans cette annexe peut être utilisé pour calculer l'effet de circuits quantiques sur les états de la base de calcul. Cependant, les ressources en mémoire et temps nécessaires pour un tel calcul augmentent rapidement avec le nombre de qubits. On ne doit toutefois pas s'en étonner puisqu'il s'agit d'une simulation classique d'un système quantique (voir à ce sujet la section §2.5). Notons que dans le code présenté ici peu d'effort ont été investi dans l'optimisation de ces ressources. Finalement, l'utilisation du langage de programmation C, plutôt que de Mathematica, permettrait possiblement d'obtenir un gain en rapidité considérable.

Bibliographie

[1] D.A. Muller *et. al.* The electronic structure at the atomic scale of ultrathin gate oxides. *Nature (London)*, 399:758, 1999.

[2] M. Schulz. The end of the road for silicon? *Nature (London)*, 399:729, 1999.

[3] C.H. Bennett et P.W. Shor. Quantum information theory. *EEE Transactions on Information Theory*, 44:2724, 1998.

[4] A.M. Zagoskin. A scalable, tunable qubit, based on a clean DND or grain boundary D-D junction. LANL cond-mat/9903170.

[5] J. Preskill. Quantum computing. Notes de cours, disponible sur le web http://www.theory.caltech.edu/people/preskill/ph229/, 1997.

[6] C. Bennett. Notes on the history of reversible computation. *IBM J. Res. Dev.*, 32:16, 1998.

[7] R. Landauer. Information is physical. *Physics Today*, page 23, Mai 1991.

[8] F.S. Leff et A.F. Rex, editor. *Maxwell's demon, entropy, information, computing.* Princeton University Press, 1990.

[9] W.K. Wootters et W.H. Zurek. A single quantum cannot be cloned. *Naure (London)*, 299:802, 1982.

[10] D. Dieks. Communication by EPR devices. *Phys. Lett.*, 92A:271, 1982.

[11] J.D. Trimmer. The present situation in quantum mechanics: a translation of Schrodinger's cat paradox paper. *Proc. Amer. Phil. Soc.*, 124:323, 1980.

[12] E. Schrodinger. Discussion of probability relation between separated systems. *Cambridge Phil. Soc.*, 31:555, 1935.

[13] E. Schrodinger. Probability relations between separated systems. *Cambridge Phil. Soc.*, 32:446, 1936.

[14] C. Bennett *et. al.* Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824, 1996.

[15] S. Popescu et D. Rohrlich. Thermodynamics and the measure of entanglement. *Phys. Rev. A*, 56:R3319, 1997.

[16] R.P. Feynman. *Feynman lectures on computation.* Addison-Wesley, 1996.

[17] V. Vedral et M.B. Plenio. Basics of quantum computation. *Prog. in Quantum Elec.*, 22:1, 1998.

[18] A. Peres. *Quantum Theory: Concepts and Methods.* Kluwer Academic Publishers, 1995.

[19] A. Barenco *et. al.* Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457, 1995.

[20] D. Deutsch. Quantum computational networks. *Proc. R. Soc. Lond. A*, 425:73, 1989.

[21] D.P. DiVincenzo. Two-bit gates are universal for quantum computation. *Phys. Rev. A*, 51, 1995.

[22] S. Lloyd. Almost any quantum logic gate is universal. *Phys. Rev. Lett.*, 75:346, 1995.

[23] D. Deutsch *et. al.* Universality in quantum computation. *Proc. R. Soc. Lond. A*, 449:669, 1995.

[24] L.I. Schiff. *Quantum Mechanics.* McGraw-Hill, 3 edition, 1968.

[25] D. Beckman *et. al.* Efficient networks for quantum factoring. *Phys. Rev. A*, 54:1034, 1996.

[26] J.A. Jones et M. Mosca. Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer. *J. Chem. Phys.*, 109:1648, 1998.

[27] R. Jozsa. Entanglement and quantum computation. LANL quant-ph/9707034.

[28] E. Knill et R. Laflamme. Power of one bit of quantum information. *Phys. Rev. Lett.*, 81:5672, 1998.

[29] S. Lloyd. Quantum search without entanglement. LANL quant-ph/9903057.

[30] N. Linden et S. Popescu. Good dynamics versus bad kinematics. Is entanglement needed for quantum computation? LANL quant-ph/9906008.

[31] F. Laloë C. Cohen-Tannoudji et B. Diu. *Mécanique Quantique*, volume I et II. Hermann, Paris, 1973.

[32] W.H. Zurek. Decoherence and the transition from quantum to classical. *Physics Today*, page 36, Octobre 1991.

[33] P.W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493, 1995.

[34] R. Laflamme *et. al.* Perfect quantum error correcting code. *Phys. Rev. Lett.*, 77:198, 1996.

[35] F.J. MacWilliams et N.J.A. Sloane. *The theory of error-correcting codes*. North-Holland Publishing, 1978.

[36] A.M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77:793, 1996.

[37] N.D. Mermin. What's wrong with these elements of reality? *Physics Today*, page 9, juin 1990.

[38] D. Gottesman. Theory of fault-tolerant quantum computation. *Phys. Rev. A*, 57:127, 1998.

[39] J. Preskill. Reliable quantum computers. *Proc. R. Soc. Lond. A*, 454:385, 1998.

[40] A.M. Steane. Efficeint fault-tolerant quantum computing. *Nature (London)*, 399:124, 1999.

[41] D. Gottesman. Fault-tolerant quantum computation with local gates. LANL quant-ph/9903099.

[42] J. Gea-Banacloche. Qubit-qubit interaction in quantum computers. *Phys. Rev. A*, 57:R1, 1998.

[43] S. Lacelle. Time-reversal in NMR of solids. *Can. J. Chem.*, 1999. Sous presse.

[44] P. Benioff. Quantum mechanical Hamiltonian models of Turing machines. *J. Stat. Phys.*, 29:515, 1982.

[45] R. Feynman. Quantum-mechanical computers. *Found. Phys.*, 16:507, 1986.

[46] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400:97, 1985.

[47] R. Landauer. Is quantum mechanics useful? *Phil. Trans. R. Soc. Lond. A*, 353:367, 1995.

[48] P.W. Shor. Polynomial-time algorithms for prime factorisation and discrete logarithms on a quantum computer. *SIAM J. Comp.*, 26:1484, 1997.

[49] D.P. DiVincenzo. Topics in quantum computers. LANL cond-mat/9612126.

[50] J.I. Cirac et P. Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, 74:4091, 1995.

[51] Q. A. Turchette. Measurement of conditional phase shifts for quantum logic. *Phys. Rev. Lett.*, 75:4710, 1995.

[52] D.G. Cory *et. al.* Ensemble quantum computing by NMR spectroscopy. *Proc. Natl. Acad. Sci.*, 94:1634, 1997.

[53] N.A. Gershenfeld et I.L. Chuang. Bulk spin-resonance quantum computation. *Science*, 275:351, 1997.

[54] E.Knill *et. al.* A cat-state benchmark on a seven bit quantum computer. LANL quant-ph/9908051.

[55] D.P. DiVincenzo. Quantum information is physical. LANL quant-ph/9710259.

[56] J. Preskill. Quantum computing: pro and con. LANL quant-ph/9705032.

[57] D. Loss et D. P. DiVincenzo. Quantum computation with quantum dots. *Phys. Rev. A*, 57:120, 1998.

[58] B.E. Kane. A silicon-based nuclear spin quantum computer. *Nature (London)*, 393:133, 1998.

[59] R. Vrijen *et. al.* Electron spin resonance transistors for quantum computing in Silicon-Germanium heterostructures. LANL quant-ph/9905096.

[60] Y. Makhlin *et. al.* Josephson-junction qubits with controlled couplings. *Nature (London)*, 398:305, 1999.

[61] L.B. Ioffe *et. al.* Quiet SDS Josephson junctions for quantum computing. *Nature (London)*, 398:679, 1999.

[62] A. Blais et A.M. Zagoskin. Operation of universal gates in a DXD superconducting solid state quantum computer. LANL quant-ph/9905043.

[63] C. Kittel. *Introduction to solid state physics.* John Wiley & Sons, New York, 7 edition, 1996.

[64] A.M. Zagoskin. *Quantum theory of many-body systems.* Spinger, 1998.

[65] M. Tinkham. *Introduction to superconductivity.* McGraw Hill, New York, 2 edition, 1996.

[66] A.J. Leggett. Macroscopic quantum systems and the quantum theory of measurement. *Supp. Prog. Theo. Phys.*, (69), 1980.

[67] A.O. Caldeira et A.J. Leggett. Quantum tunneling in a dissipative system. *Annals of Physics.*, 149:374, 1983.

[68] A.J. Leggett *et. al.* Dynamics of the dissipative two-state system. *Rev. Mod. Phys.*, 59:1, 1987.

[69] J.M. Martinis *et. al.* Experimental tests for the quantum behavior of a macroscopic degree of freedom : The phase difference across a Josephson junction. *Phys. Rev. B*, 35:4682, 1987.

[70] R. Rouse *et. al.* Observation of resonant tunneling between macroscopically distinct quantum levels. *Phys. Rev. Lett.*, 75:1614, 1995.

[71] P. Silvestrini *et. al.* Resonant macroscopic quantum tunneling in SQUID systems. *Phys. Rev. B*, 54:1246, 1996.

[72] M.G. Castellano *et. al.* Switching dynamics of Nb/AlOx/Nb Josephson junctions: Measurements for an experiment of macroscopic quantum coherence. *J. Appl. Phys.*, 80:2922, 1996.

[73] A. Furusaki. Josephson current carried by Andreev levels in superconducting quantum point contacts. LANL cond-mat/9811026.

[74] A.M. Zagoskin. The half-periodic Josephson effect in an s-wave superconductor–normal-metal–d-wave superconductor junction. *J. Phys.: Cond. Matter*, 9:L419, 1997.

[75] A.M. Zagoskin et M. Oshikawa. Spontaneous magnetic flux and quantum noise in an annular mesoscopic SND junction. *J. Phys.: Condens. Matter*, 10:L105, 1998.

[76] J.A. Sidles *et. al.* Magnetic resonance force microscopy. *Rev. Mod. Phys.*, 67:249, 1995.

[77] N. Hatakenaka *et. al.* Anomalous current-voltage characteristics due to macroscopic resonant tunneling in a small Josephson jontion. *Phys. Rev. B*, 42:3987, 1990.

[78] C.P. Slichter. *Principles of Magnetic Resonance.* Springer-Verlag, 3 edition, 1990.

[79] G. Bodenhausen et A. Wokaun R.R. Ernst. *Principles of Nuclear Magnetic Resonance in One and Two Dimensions.* Clarendon Press, Oxford, 1987.

[80] L. Viola et S. Lloyd. Dynamical suppression of decoherence in two-state quantum system. *Phys. Rev. A*, 58:2733, 1998.

[81] E. Knill et S. Lloyd L. Viola. Dynamical decoupling of open quantum systems. *Phys. Rev. Lett.*, 82:2417, 1999.

[82] L. Viola et S. Lloyd. Decoherence control in quantum information processing : simple models. LANL quant-ph/9809058.

[83] H.A Farach et R.J. Creswick C.P. Poole. *Superconductivity.* Academic Press, 1995.

[84] J.E. Mooij *et. al.* Josphson persistent-current qubit. *Science*, 285:1039, 1999.

[85] M. Devoret. Communication personelle.

[86] P.A. Lee. Localized states in a d-wave superconductor. *Phys. Rev. Lett.*, 71:1887, 1993.

[87] V. Bouchiat *et. al.* Quantum coherence with a single Cooper pair. *Physica Scripta*, T76:165, 1998.

[88] Y. Nakamura *et. al.* Coherent control of macroscopic quantum states in a single-Cooper-pair box. *Nature (London)*, 398:786, 1999.

[89] A. Shnirman et G. Schön. Quantum measurements performed with a single-electron transistor. *Phys. Rev. B*, 57:15400, 1998.

[90] C. Bennett *et. al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895, 1993.