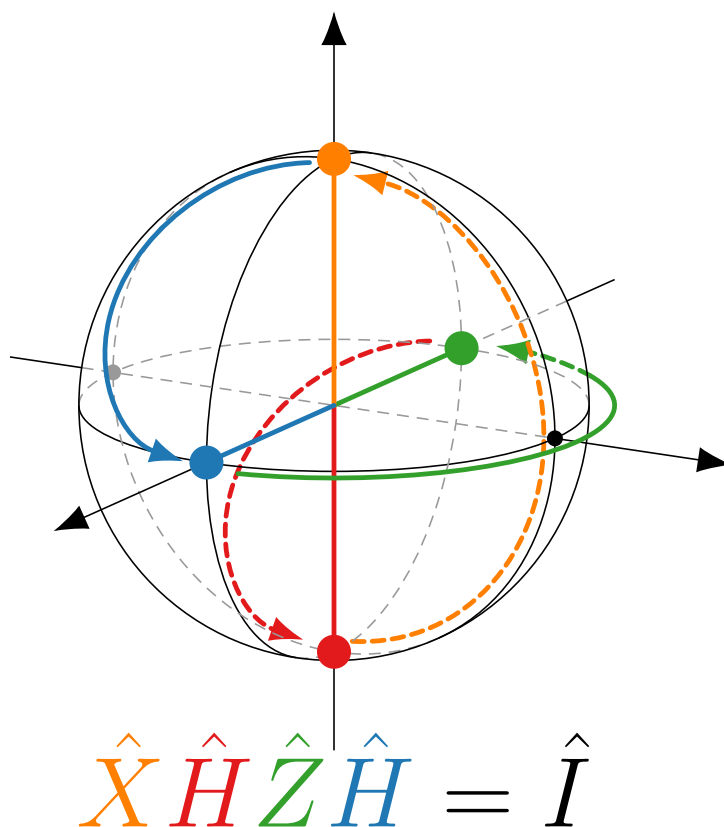


Introduction au calcul quantique

Sciences de l'information quantique

par
Maxime Dion



Compilé le 31 janvier 2023
Version numérique régulièrement mise à jour.
Pensez-y avant d'imprimer.

Table des matières

1	Le qubit	5
A	État d'un qubit	5
A.1	Superposition d'états	6
A.2	Vecteur d'état	6
A.3	Produit scalaire entre deux états	7
A.4	Normalisation d'un vecteur d'état	9
A.5	Notion de base	9
A.6	Probabilités de mesure	10
A.7	Effet de la mesure	12
A.8	Phase globale	12
A.9	Phase relative	13
A.10	Sphère de Bloch	14
A.11	États quantiques notables	16
A.12	Arrière-scène quantique	17
B	Portes quantiques à un qubit	18
B.1	Application d'une porte quantique	18
B.2	Diagramme	18
B.3	Représentation matricielle	18
B.4	Effet d'une porte quantique	19
B.5	Composition de portes quantiques	20
B.6	Transformation d'un $\langle \cdot $	21
B.7	Transformation d'états quantiques normalisés	21
B.8	Propriétés des portes quantiques	22
B.9	Quelques portes quantiques à un qubit	23
B.10	Portes quantiques paramétrées	26
B.11	Formulation dyadique d'une porte quantique	28
B.12	Discussion sur la superposition et l'interférence	29
S	Solutions aux exercices	31
2	Deux qubits	33
A	État à deux qubits	33
A.1	Vecteur d'état	34
A.2	Produit tensoriel	34
A.3	États produits	35
A.4	Intrication	36
A.5	Mesure d'états à deux qubits	36
A.6	États quantiques notables	38
B	Portes quantiques à deux qubits	39
B.1	Diagramme	39

B.2	Portes contrôlées	39
B.3	Quelques portes quantiques à deux qubits	41
B.4	Portes à un qubit pour un système de deux qubits	42
B.5	Composition de portes quantiques	45
C	Circuits quantiques	46
C.1	Effet d'un circuit quantique	46
C.2	Représentation matricielle	47
C.3	Quelques circuits quantiques à deux qubits	47
S	Solutions aux exercices	49
3	Plus de deux qubits	51
A	État à n qubits	51
A.1	Pour $n = 3$	51
A.2	Forme générale	52
A.3	États quantiques notables	53
B	Portes quantiques à plus de deux qubits	55
C	Circuits quantiques et calcul quantique	55
C.1	Transformation unitaire	56
C.2	Mesure	56
S	Solutions aux exercices	58
4	Mesures et observables	59
A	Observables à un qubit	59
A.1	Déterminer le vecteur d'état	59
A.2	Coordonnée en z	60
A.3	Observable \hat{Z}	61
A.4	Observable \hat{X}	62
A.5	Observable \hat{Y}	62
A.6	Observable \hat{I}	62
A.7	Estimation sur un ordinateur quantique	62
A.8	Reconstruire le vecteur d'état	64
A.9	Autres observables à un qubit	64
B	Observables à plusieurs qubits	65
B.1	Les chaines de Pauli	66
B.2	Observables à n qubits	67
B.3	Estimation de la valeur moyenne d'une chaîne de Pauli	67
C	Observables en général	70
C.1	Mesures projectives	70
C.2	Équation aux valeurs propres	71
C.3	Dégénérescence	72
C.4	Forme spectrale	73
C.5	Opérateur Hermitien	74
C.6	Probabilités de mesure	75
C.7	Valeur moyenne	75
D	Précision de l'estimation	76
5	Algorithmes quantiques jouets	77
A	Algorithme de Deutsch	77
A.1	Problème	77
A.2	Solution classique	78

	A.3	Solution quantique	78
B		Algorithme de Deutsch-Jozsa	82
	B.1	Problème	82
	B.2	Solution classique	82
	B.3	Solution quantique	83
C		Algorithme de Bernstein-Vazirani	85
	C.1	Problème	85
	C.2	Solution classique	86
	C.3	Solution quantique	86
S		Solutions aux exercices	88
A	Démonstrations		89
1		Transformation Hadamard à plusieurs qubits	89
	1.1	Transformation du premier état de base	89
	1.2	Relations utiles	90
	1.3	Transformation générale d'un état de base	91
B	Nombres complexes		93
1		Représentation géométrique des nombres réels	93
2		Représentation géométrique des nombres complexes	94
3		Représentation des nombres complexes	95
4		Relation d'Euler	96
5		Complexe conjugué	97
C	Notation indicielle		99
1		Matrices et vecteurs comme tenseurs	99
2		Produit matricielle en notation indicielle	100
3		Tenseurs d'ordre supérieur à 2	100
4		Analogie avec la programmation	101
5		Notation d'Einstein	101
6		Tenseurs importants	102
	6.1	Symbole de Kronecker	102
	6.2	Levi-Civita	102
7		Quelques astuces et mises en garde	103
	7.1	Cohérence dans les indices	103
	7.2	Commutation des éléments de tenseurs	103
	7.3	Matrice transposée	104
	7.4	Choix des indices	104
	7.5	Piège : redondance accidentelle d'indices muets	105
	7.6	Mélanger les notations	105
8		Les dérivées	105
	8.1	Gradient	106
	8.2	Différentielle d'une fonction à n variables	106
D	Variables aléatoires		109
1		Espérance	109
2		Variance	109
3		Covariance	110
4		Estimation de l'espérance	111
	4.1	Espérance	112
	4.2	Variance	113

4.3	Covariance	113
5	Estimation de la variance	114
6	Estimation de la covariance	114

Chapitre 1

Le qubit

Là où le bit est l'unité fondamentale d'information classique, le bit quantique, communément appelé le qubit, est l'unité fondamentale d'information quantique. C'est donc le point de départ pour quiconque s'intéressant à l'informatique quantique et à la programmation quantique.

Dans ce chapitre, nous allons d'abord voir comment décrire mathématiquement l'état d'un qubit. Cela nous permettra ensuite de nous intéresser aux outils à notre disposition pour modifier et observer cet état. Nous ferons cela en utilisant un outil mathématique parfaitement adapté : l'algèbre linéaire. Nous répondrons ainsi à une des questions les plus fondamentales de l'existence humaine : À quoi ça sert, l'algèbre linéaire ?

Le qubit est aussi ce qu'on appelle en mécanique quantique un système à deux niveaux ; c'est le système quantique le plus simple qu'on puisse imaginer. L'étude et la compréhension d'un qubit est donc une excellente manière d'introduire les concepts fondamentaux de la mécanique quantique et de se familiariser avec cette science parfois contre-intuitive.

A État d'un qubit

L'état d'un bit d'information classique est décrit sur la base de deux états possibles : l'état 0 et l'état 1. Le bit d'information est dans l'un de ces deux états. On dit également que le bit peut prendre les valeurs 0 ou 1.

Par analogie, l'état d'un bit d'information quantique est décrit à l'aide de deux états de base

$$|0\rangle \text{ et } |1\rangle.$$

Ces deux états sont les deux seuls auxquels le qubit a accès. Cependant, le qubit peut être dans une infinité d'états différents¹. Cela est possible, car le qubit peut occuper les états $|0\rangle$ et $|1\rangle$ *en même temps* !

Info notation A.1 : Le ket

L'écriture $|\cdot\rangle$ avec une barre verticale et un angle à droite est appelée un *ket*. On s'en sert pour représenter un état quantique. Cela fait partie d'un ensemble de notations nommé la notation de Dirac qui est universellement utilisée dans le contexte de la mécanique quantique.

Notez que l'intérieur du *ket*, par exemple le 0 dans $|0\rangle$, n'est qu'une étiquette. Généralement, on tentera d'utiliser des étiquettes qui caractérisent bien l'état quantique identifié par celle-ci.

De manière générale, l'état d'un qubit est représenté comme une combinaison linéaire (somme pondérée) de ces deux états de base

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{1.1}$$

1. Ces deux dernières phrases vous semblent peut-être contradictoires. Revenez-y une fois cette section complétée pour réévaluer leur cohérence.

où α et β sont généralement des nombres complexes et sont appelés *amplitudes de probabilité* ou encore simplement *composantes* pour des raisons qui deviendront bientôt évidentes.

A.1 Superposition d'états

Lorsque le qubit est dans un état de base, une des composantes est égale à 1 et l'autre à zéro. Par exemple,

$$\begin{aligned} |\psi\rangle &= |0\rangle & (\alpha = 1, \beta = 0) \\ |\psi\rangle &= |1\rangle & (\alpha = 0, \beta = 1). \end{aligned}$$

Dans tous les autres cas, le qubit est, en quelques sortes, dans un état qui *combine* ou qui *mélange* les états $|0\rangle$ et $|1\rangle$. On dit alors que le qubit est en *superposition* d'états. La superposition est le premier phénomène quantique à la base du calcul quantique.

A.2 Vecteur d'état

Comme l'état d'un qubit a toujours la forme de l'équation 1.1, on est tenté (par pure paresse) de seulement fournir les valeurs de α et β pour définir $|\psi\rangle$, la première étant toujours associée à l'état de base $|0\rangle$ et la seconde à l'état de base $|1\rangle$. On peut fournir ces deux valeurs comme étant les composantes d'un vecteur d'un espace à deux dimensions

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \quad (1.2)$$

C'est ce qu'on appelle le vecteur d'état d'un qubit.

Remarque

En informatique quantique, la base $\{|0\rangle, |1\rangle\}$ est également appelée la base computationnelle.

Remarque

Dans les présentes notes, on appelle *vecteur d'état* le tableau de composantes qui représente un état quantique dans une base donnée. C'est une interprétation *informatique* de ce qu'est un vecteur, en opposition à une définition plus *mathématique* où un vecteur existe indépendamment de la base dans laquelle il est exprimé.

Info notation A.2 : Vecteur d'état et état quantique

On utilisera souvent (presque tout le temps) l'abus de notation

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad (1.3)$$

pour définir un état quantique $|\psi\rangle$, même si ce n'est pas rigoureusement vrai : l'état n'est pas égal à son vecteur d'état. Ce que cette dernière égalité signifie vraiment est que l'état $|\psi\rangle$ est un état caractérisé par les composantes α et β dans la base formée par les états $|0\rangle$ et $|1\rangle$.

Ce qui distingue l'état quantique du vecteur d'état est que le second est toujours exprimé dans une base donnée. Dans la plupart des cas, la base dite *computationnelle* ($\{|0\rangle, |1\rangle\}$) est sous-entendue, mais il existe d'autres bases possibles. Les composantes des vecteurs d'état représentant un même état quantique, mais dans deux bases différentes, ne seront pas égales. L'état quantique, lui, est cependant toujours pareil et ne dépend pas d'une base. Ces notions de changement de base sont plus avancées et nous y reviendrons plus tard.

À moins d'avis contraire, une égalité telle que celle de l'équation 1.3 suppose que le vecteur d'état est exprimé dans la base computationnelle.

Il est extrêmement utile de représenter l'état d'un qubit sous la forme d'un vecteur. Cela nous permet d'utiliser la force de l'algèbre linéaire pour représenter l'état d'un qubit, mais surtout pour décrire les opérations qui permettront de modifier son état.

Pour que tout cela soit cohérent, on associe les deux états de base d'un qubit aux deux vecteurs de base d'un espace à deux dimensions

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ et } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Ceux-ci sont orthogonaux et normés (orthonormés pour faire court). Par analogie avec un vecteur général dans un espace à deux dimensions,

$$\mathbf{r} = x \hat{\mathbf{x}} + y \hat{\mathbf{y}} = x \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

l'état général d'un qubit est bien

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

L'état général d'un qubit peut donc être représenté par un vecteur à deux composantes (α et β) qui sont, on le rappelle, des nombres complexes.

Exercice A.1 : Vecteurs d'état

Écrivez les vecteurs d'état des états quantiques suivants dans la base $\{|0\rangle, |1\rangle\}$:

a) $|\phi\rangle = \gamma |0\rangle + \delta |1\rangle$

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

b) $|\psi\rangle = a |1\rangle + b |0\rangle$

e) $|\eta\rangle = e^{i\varphi_0}(a |0\rangle + b |1\rangle)$

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

f) $|\theta\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$

Comme on peut associer un état quantique à un vecteur d'état, certaines opérations qui sont valides pour des vecteurs le sont aussi pour des états quantiques. Par exemple, on peut multiplier un état quantique par un scalaire ou encore additionner des états quantiques, choses que l'on faisait déjà en écrivant, par exemple, l'état général d'un qubit (équation 1.1).

Info notation A.3 : Différentes notations pour les composantes

À l'équation 1.2, les composantes utilisées pour le vecteur d'état sont α et β . Lorsqu'on manipule plusieurs états quantiques à la fois, il est pratique de pouvoir identifier les composantes associées aux différents états. On utilisera alors des notations différentes. Par exemple,

$$|a\rangle = a_0 |0\rangle + a_1 |1\rangle \quad \text{et} \quad |b\rangle = b_0 |0\rangle + b_1 |1\rangle$$

où les lettres a et b permettent d'identifier les états à un qubit, alors que les composantes avec des indices a_0 et a_1 (b_0 et b_1) peuvent facilement être associées aux bons états de base. Dans ce cas, les vecteurs d'état sont

$$|a\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \quad \text{et} \quad |b\rangle = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}.$$

A.3 Produit scalaire entre deux états

Maintenant que nous pouvons représenter des états quantiques par des vecteurs, nous pouvons les multiplier ensemble en utilisant le produit scalaire. Pourquoi voudrions-nous multiplier des états ensemble ? Le produit entre deux états nous permet, en quelque sorte, de comparer des états. Cela nous sera très utile par la suite.

En algèbre linéaire, on écrit le produit scalaire entre deux vecteurs \mathbf{a} et \mathbf{b} comme le produit entre le vecteur ligne \mathbf{a} et le vecteur colonne \mathbf{b}

$$\mathbf{a} \cdot \mathbf{b} = (a_1 \quad a_2) \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = a_1 b_1 + a_2 b_2.$$

Ce produit porte bien son nom car il retourne un nombre, un scalaire. Dans le cas général où on a les deux états quantiques à 1 qubit

$$|a\rangle = a_0 |0\rangle + a_1 |1\rangle \quad \text{et} \quad |b\rangle = b_0 |0\rangle + b_1 |1\rangle ,$$

le produit entre ces deux états s'écrit

$$\langle a|b\rangle = \begin{pmatrix} a_0^* & a_1^* \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} = a_0^* b_0 + a_1^* b_1. \quad (1.4)$$

Info notation A.4 : Le bra

L'écriture $\langle \cdot |$ est appelée *bra*, l'alter ego du *ket*, et fait également partie de la notation de Dirac. On s'en sert également pour représenter un état quantique, mais son vecteur d'état prend alors la forme d'un vecteur ligne dont les composantes sont les complexes conjugués des composantes originales. Cette transformation s'appelle également le conjugué hermitien.

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \rightarrow \langle \psi| = (\alpha^* \quad \beta^*)$$

Le produit entre deux états quantiques $\langle \cdot | \cdot \rangle$ est donc un *braket* !

Exemple A.1 : Produits scalaires entre les états de base

Illustrons le calcul de produits scalaires à partir des états de base. D'abord, le produit entre les vecteurs d'état des deux états de base donne

$$\langle 0|1\rangle = \begin{pmatrix} 1^* & 0^* \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$$

ce qui signifie que ces deux vecteurs d'état sont orthogonaux. On dit aussi que ces états quantiques sont orthogonaux. Ensuite, les produits de ces vecteurs d'état avec eux-mêmes donnent respectivement

$$\langle 0|0\rangle = \begin{pmatrix} 1^* & 0^* \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1 \quad \text{et} \quad \langle 1|1\rangle = \begin{pmatrix} 0^* & 1^* \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 1$$

nous informant que les vecteurs de base sont normalisés. On dit aussi que les états quantiques sont normalisés. En fait, pour qu'un état quantique en général soit valide, il doit être normalisé, comme on va le voir à la section A.4.

En particulier, le produit entre un état général et un état de base permet d'obtenir la composante devant cet état de base. Par exemple, avec $|0\rangle$

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

ou avec $|1\rangle$ en notation vectorielle

$$\langle 1|\psi\rangle = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = 0 \times \alpha + 1 \times \beta = \beta.$$

Exercice A.2 : Ordre du produit scalaire

Est-ce que les produits scalaires suivants

$$\langle a|b\rangle \quad \text{et} \quad \langle b|a\rangle$$

sont égaux ? Sinon, comment se comparent-ils ?

A.4 Normalisation d'un vecteur d'état

Les composantes d'un vecteur d'état d'un qubit ne sont pas complètement indépendantes. En effet, pour des raisons qui vont devenir plus claires à la section A.6, on exige qu'elles respectent la condition de *normalisation*

$$|\alpha|^2 + |\beta|^2 = 1. \quad (1.5)$$

Par construction, les états de base sont des états normalisés. En effet,

$$\begin{array}{lll} |\psi\rangle = |0\rangle & (\alpha = 1, \beta = 0) & |1|^2 + |0|^2 = 1 \\ |\psi\rangle = |1\rangle & (\alpha = 0, \beta = 1) & |0|^2 + |1|^2 = 1. \end{array}$$

Exercice A.3 : Normalisation

Est-ce que ces états sont normalisés ?

- | | |
|---|--|
| a) $ \psi_a\rangle = \frac{1}{\sqrt{2}} 0\rangle + \frac{1}{\sqrt{2}} 1\rangle$ | d) $ \psi_d\rangle = \sqrt{\frac{3}{4}} 0\rangle + \frac{1}{2} 1\rangle$ |
| b) $ \psi_b\rangle = \frac{1}{\sqrt{2}} 0\rangle - \frac{1}{\sqrt{2}} 1\rangle$ | e) $ \psi_e\rangle = 0.9 1\rangle$ |
| c) $ \psi_c\rangle = \frac{1}{3} 0\rangle + \frac{2}{3} 1\rangle$ | f) $ \psi_f\rangle = - 0\rangle$ |

On peut vérifier qu'un état est normalisé en calculant son produit scalaire avec lui-même. En effet pour un état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ le produit scalaire est

$$\langle\psi|\psi\rangle = \alpha^*\alpha + \beta^*\beta = |\alpha|^2 + |\beta|^2.$$

Ainsi pour vérifier si un état quantique $|\psi\rangle$ est normalisé, on doit simplement vérifier que $\langle\psi|\psi\rangle = 1$. Si ce n'est pas le cas, on peut créer une version normalisée du même état en renormalisant ses composantes

$$|\psi'\rangle \equiv \frac{1}{\sqrt{\langle\psi|\psi\rangle}} |\psi\rangle. \quad (1.6)$$

Exercice A.4 : Renormalisation

Démontrer que l'état de l'équation 1.6 est toujours normalisé, en autant que $\langle\psi|\psi\rangle \neq 0$.

A.5 Notion de base

Bien qu'on fera un usage limité de bases différentes de la base computationnelle dans ce texte, il est pertinent de donner une définition de ce qu'est une base et de fournir au moins un exemple supplémentaire. Pour un système à un qubit, une base est un ensemble de deux états $\{|u\rangle, |v\rangle\}$ qui sont mutuellement orthogonaux, c'est-à-dire que

$$\langle u|v\rangle = 0.$$

Ensuite ces vecteurs doivent être normés, c'est-à-dire que

$$\langle u|u\rangle = 1 \quad \text{et} \quad \langle v|v\rangle = 1.$$

On dit alors que $|u\rangle$ et $|v\rangle$ forment une base canonique.

Exemple A.2 : La base $|\pm\rangle$

Vérifions que les états

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

forment bien une base. D'abord, on peut écrire les vecteurs d'état dans la base computationnelle

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{et} \quad |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Ensuite, on vérifie facilement que ces vecteurs sont normés

$$\begin{aligned} \langle + | + \rangle &= \frac{1}{\sqrt{2}^*} (1^* \quad 1^*) \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2}(1+1) = 1 \\ \langle - | - \rangle &= \frac{1}{\sqrt{2}^*} (1^* \quad -1^*) \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{2}(1+1) = 1 \end{aligned}$$

et orthogonaux

$$\langle - | + \rangle = \frac{1}{\sqrt{2}^*} (1^* \quad -1^*) \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2}(1-1) = 0.$$

Exemple A.3 : Changement de base

Soit un état quelconque exprimé dans la base computationnelle

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

quelles sont ses composantes lorsqu'exprimé dans la base $|\pm\rangle$? Pour répondre à cette question, on peut d'abord exprimer les états $|0\rangle$ et $|1\rangle$ à l'aide des états $|+\rangle$ et $|-\rangle$. On peut facilement obtenir que

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \quad \text{et} \quad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle).$$

Et donc,

$$\begin{aligned} |\psi\rangle &= \frac{\alpha}{\sqrt{2}}(|+\rangle + |-\rangle) + \frac{\beta}{\sqrt{2}}(|+\rangle - |-\rangle) \\ &= \frac{\alpha + \beta}{\sqrt{2}}|+\rangle + \frac{\alpha - \beta}{\sqrt{2}}|-\rangle. \end{aligned}$$

Exercice A.5 : Vérification de base

- Vérifiez que la base computationnelle $\{|0\rangle, |1\rangle\}$ est bien une base.
- Vérifiez que les états

$$|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \quad \text{et} \quad |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle).$$

forment bien une base.

- Exprimez l'état quelconque $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ dans la base $\{|+i\rangle, |-i\rangle\}$.

A.6 Probabilités de mesure

Bien que l'état d'un qubit puisse être décrit grâce à son vecteur d'état, en pratique, cette information n'est pas vraiment accessible. La seule manière d'obtenir de l'information sur l'état d'un qubit est de le

mesurer. On ne peut pas assez insister sur l'importance de ce concept en mécanique quantique. La mesure est notre seule fenêtre sur l'étrange monde quantique.

Remarque

Dans le cadre de cette introduction au calcul quantique, on va considérer la mesure comme une opération ponctuelle dont le résultat dépend de l'état du qubit avant la mesure. En réalité, le processus de la mesure en mécanique quantique comprend son lot de complexités qui dépasse largement les objectifs de cette introduction.

Lorsqu'on mesure un qubit, seulement deux résultats sont possibles : 0 ou 1. Ces valeurs sont associées aux deux états de base $|0\rangle$ et $|1\rangle$. Un aspect important de la mesure d'un état quantique est que le résultat est aléatoire et impossible à prévoir. Cependant, la théorie de la mécanique quantique nous permet de déterminer très précisément les probabilités d'obtenir chacun des résultats possibles. Ces probabilités dépendent directement de l'état du qubit juste avant que la mesure soit prise.

On note les probabilités d'obtenir les résultats 0 et 1 respectivement p_0 et p_1 . Pour un qubit dans un état général $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ ces probabilités sont respectivement données par les modules au carré des amplitudes de probabilité α et β , c'est-à-dire

$$p_0 = |\alpha|^2 \quad \text{et} \quad p_1 = |\beta|^2.$$

C'est ce qu'on appelle, en mécanique quantique, la règle de Born, attribuée au physicien Max Born.

Comme ces probabilités sont égales à des modules au carré, elles sont garanties d'être réelles et positives. La somme des probabilités de tous les résultats possibles doit toujours être égale à 1. En d'autres mots, la probabilité d'obtenir un résultat (n'importe lequel) est toujours de 100%. Ainsi, les probabilités d'obtenir les résultats 0 et 1 doivent respecter l'égalité

$$p_0 + p_1 = 1$$

qui n'est rien d'autre que la condition de normalisation de l'équation 1.5 ! C'est ici que cette condition prend tout son sens. En effet, la condition de normalisation d'un état quantique s'assure que ses amplitudes de probabilité permettent bien de calculer les probabilités d'obtenir les différents résultats possibles.

Exemple A.4 : Probabilités de mesure pour l'état $|+\rangle$

Illustrons le calcul des probabilités d'obtenir les résultats 0 et 1 lors de la mesure d'un qubit dans l'état

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

La probabilité d'obtenir le résultat 0 est le module au carré de l'amplitude de probabilité devant l'état $|0\rangle$, c'est-à-dire

$$p_0 = \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2}.$$

La mesure d'un qubit dans l'état $|+\rangle$ retournera le résultat 0 50% des fois. Similairement, la probabilité d'obtenir le résultat 1 est

$$p_1 = \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2}$$

et on a également 50% des chances d'obtenir 1. On vérifie du même coup que l'état $|+\rangle$ est bien un état normalisé.

Pour vérifier cela expérimentalement, on pourrait préparer 100 qubits, tous dans l'état $|+\rangle$, et les mesurer un à un. On pourrait aussi refaire la même expérience 100 fois avec le même qubit. Dans ces deux cas, on devrait alors obtenir le résultat 0 environ 50 des fois et le résultat 1 les autres fois.

Comme chaque résultat est aléatoire, il se peut que le nombre total de 0 obtenus ne soit pas exactement 50. Cependant, si on augmente le nombre de fois que l'on répète l'expérience, on augmentera nos chances d'obtenir un nombre de 0 proche du 50% théorique.

Exercice A.6 : Probabilités de mesure

- a) Écrivez un état d'un qubit qui, lorsque mesuré, retourne le résultat 0 dans $\frac{1}{3}$ des cas et le résultat 1 dans $\frac{2}{3}$ des cas.
- b) Écrivez un état d'un qubit qui, lorsque mesuré, retourne la valeur 0 avec une probabilité p et la valeur 1 avec une probabilité $1 - p$.
- c) Écrivez un autre état quantique, différent du précédent qui a les mêmes probabilités de retourner les valeurs 0 et 1 lorsqu'on le mesure.

À la section A.3, on a vu que le produit entre un état quantique et un des différents états de base permet d'extraire l'amplitude de probabilité associée à cet état de base. Cela nous permet donc d'utiliser le produit d'états quantiques pour calculer des probabilités de mesure. Par exemple, les probabilités d'obtenir 0 ou 1 lors de la mesure d'un qubit dans l'état $|\psi\rangle$ peuvent être écrites comme

$$p_0 = |\alpha|^2 = |\langle 0|\psi\rangle|^2 \quad \text{et} \quad p_1 = |\beta|^2 = |\langle 1|\psi\rangle|^2.$$

La forme générale d'une probabilité de mesure est donc la suivante : la probabilité d'obtenir un résultat de mesure associé à un état de base $|u\rangle$ alors que le qubit est dans l'état $|\psi\rangle$ est

$$p_u = |\langle u|\psi\rangle|^2 \quad (1.7)$$

qui peut également être exprimé comme

$$p_u = \langle u|\psi\rangle^* \langle u|\psi\rangle = \langle \psi|u\rangle \langle u|\psi\rangle.$$

A.7 Effet de la mesure

La mesure d'un système quantique comme un qubit est décidément assez différente de la notion de mesure qu'on entend habituellement (appelons-la mesure classique). D'abord, la mesure classique n'est pas un processus aléatoire : la mesure de plusieurs objets identiques résultera en des résultats similaires. Ensuite, la mesure classique n'influence pas l'état de l'objet mesuré. L'état d'un objet classique sera le même qu'on le mesure ou non.

Comme on vient de le voir, la mesure d'un système quantique retourne d'abord un résultat aléatoire. Seules les probabilités des différents résultats peuvent être calculées. Ensuite, le simple fait de mesurer un qubit modifiera irrémédiablement son état quantique : tout le contraire de la mesure classique ! En effet, l'état d'un qubit après sa mesure est l'état de base associé au résultat obtenu. On dit aussi que le qubit a été projeté dans l'état de base par la mesure.

Par exemple, si la mesure d'un qubit a retourné le résultat 0, le qubit est alors dans l'état $|0\rangle$. Toutes autres mesures subséquentes du même qubit retourneront encore l'état 0, à moins qu'on effectue d'autres opérations sur celui-ci entre temps.

Remarque

Parce que la mesure laisse le qubit dans l'état de base associé au résultat de mesure obtenu, on utilisera parfois la formulation suivante : « le qubit a été mesuré dans l'état $|u\rangle$ ». Cela signifie que le résultat de la mesure est celui associé à l'état de base $|u\rangle$ et que le qubit a été projeté dans cet état.

A.8 Phase globale

Considérons un état à un qubit quelconque $|\psi\rangle$ et une version légèrement différente

$$|\psi'\rangle = e^{i\theta} |\psi\rangle$$

à laquelle on a appliqué une phase θ . On peut d'abord s'assurer que $|\psi'\rangle$ est un état normalisé

$$\langle \psi'|\psi'\rangle = \langle \psi|e^{-i\theta}e^{i\theta}|\psi\rangle = \langle \psi|\psi\rangle$$

si l'état $|\psi\rangle$ est normalisé. Ensuite, comme notre seule manière d'observer ces états est de les mesurer, on peut se demander comment les résultats diffèrent pour ces deux états. On peut utiliser l'équation 1.7 pour exprimer de manière générale la probabilité de mesurer les états $|\psi\rangle$ et $|\psi'\rangle$ dans l'état de base $|u\rangle$. On obtient,

$$p'_u = |\langle u|\psi'\rangle|^2 = e^{-i\theta} \langle \psi|u\rangle e^{i\theta} \langle u|\psi\rangle = p_u.$$

Les probabilités de mesure sont donc identiques pour les deux états, peu importe la phase θ . Autrement dit, il est impossible de distinguer les états $|\psi\rangle$ et $|\psi'\rangle$. La phase θ est appelée la phase globale et $e^{i\theta}$, le facteur de phase globale. La phase globale n'a aucune conséquence physique et peut donc toujours être ignorée sans que cela ne change les prédictions physiques.

A.9 Phase relative

En revanche, une phase relative peut avoir des conséquences physiques et ne peut généralement pas être ignorée. Une phase relative est une phase entre différentes composantes d'un état quantique. Considérons les deux états suivants

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad \text{et} \quad |\psi'\rangle = a|0\rangle + e^{i\varphi}b|1\rangle$$

qui diffèrent par une phase relative φ et supposons que a et b sont réels par soucis de simplicité. La probabilité de mesurer le premier état dans l'état $|u\rangle$ est

$$p_u = a^2|\langle u|0\rangle|^2 + b^2|\langle u|1\rangle|^2 + ab(\langle 0|u\rangle\langle u|1\rangle + \langle 1|u\rangle\langle u|0\rangle) \quad (1.8)$$

alors que pour le second

$$p'_u = a^2|\langle u|0\rangle|^2 + b^2|\langle u|1\rangle|^2 + ab(e^{i\varphi}\langle 0|u\rangle\langle u|1\rangle + e^{-i\varphi}\langle 1|u\rangle\langle u|0\rangle). \quad (1.9)$$

On voit que dans ce second cas, le résultat dépend directement de la phase φ . Deux états quantiques qui diffèrent uniquement par une phase relative peuvent donc produire des résultats de mesure différents et il est possible de les distinguer. Une phase relative a donc des conséquences physiques et ne peut pas simplement être ignorée.

Exemple A.5 : Phase globale et phase relative

Illustrons les concepts de phase globale et de phase relative grâce à un exemple. Considérons l'état quantique suivant

$$|\psi\rangle = e^{i\theta}(a_0e^{i\varphi_0}|0\rangle + a_1e^{i\varphi_1}|1\rangle)$$

où a_0 , a_1 , φ_0 , φ_1 et θ sont réels. Si on distribue la phase globale θ on peut écrire le même état comme

$$|\psi\rangle = a_0e^{i(\theta+\varphi_0)}|0\rangle + a_1e^{i(\theta+\varphi_1)}|1\rangle.$$

Dans tous les cas, la phase relative peut être calculée en effectuant le ratio des amplitudes complexes devant les états $|1\rangle$ et $|0\rangle$. La phase relative est alors la phase du nombre complexe obtenu. Dans le cas présent, la phase relative est obtenue grâce à

$$\frac{a_1e^{i(\theta+\varphi_1)}}{a_0e^{i(\theta+\varphi_0)}} = \frac{a_1}{a_0}e^{i((\theta+\varphi_1)-(\theta+\varphi_0))} = \frac{a_1}{a_0}e^{i(\varphi_1-\varphi_0)}.$$

La phase relative peut donc être identifiée comme étant $\varphi_1 - \varphi_0$. Remarquez qu'on aurait obtenu le même résultat pour les états quantiques suivants

$$|\psi'\rangle = a_0e^{i\varphi_0}|0\rangle + a_1e^{i\varphi_1}|1\rangle \quad \text{et} \quad |\psi''\rangle = a_0|0\rangle + a_1e^{i(\varphi_1-\varphi_0)}|1\rangle$$

qui ne diffèrent les uns des autres que par des phases globales.

Exercice A.7 : Phase relative

- a) Obtenez d'abord les expressions des équations 1.8 et 1.9.
 b) Ensuite, en utilisant une forme polaire pour

$$\langle 0|u\rangle\langle u|1\rangle = e^{i\delta}|\langle 0|u\rangle\langle u|1\rangle|$$

montrez que

$$p_u = a^2|\langle u|0\rangle|^2 + b^2|\langle u|1\rangle|^2 + 2ab\cos(\delta)|\langle 0|u\rangle\langle u|1\rangle|$$

et

$$p'_u = a^2|\langle u|0\rangle|^2 + b^2|\langle u|1\rangle|^2 + 2ab\cos(\varphi + \delta)|\langle 0|u\rangle\langle u|1\rangle|.$$

- c) Pouvez-vous identifier au moins un cas où la phase relative φ n'aura pas de conséquence physique.

A.10 Sphère de Bloch

La sphère de Bloch est un outil de visualisation d'un état à un qubit. Dans la plupart des ouvrages sur la mécanique quantique, elle est simplement décrite. Nous allons plutôt tenter de construire la sphère de Bloch à partir de ce que l'on sait des états quantiques à un qubit en espérant que cela nous ouvre une compréhension plus profonde de son utilisation.

La construction de la sphère de Bloch s'appuie sur le fait que l'état d'un qubit peut être écrit comme une combinaison linéaire de deux états de base

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

où les états $|0\rangle$ et $|1\rangle$ forment une base, c'est-à-dire qu'ils sont normés et mutuellement orthogonaux

$$\langle 0|0\rangle = 1$$

$$\langle 1|1\rangle = 1$$

$$\langle 0|1\rangle = 0.$$

Le cercle de Bloch

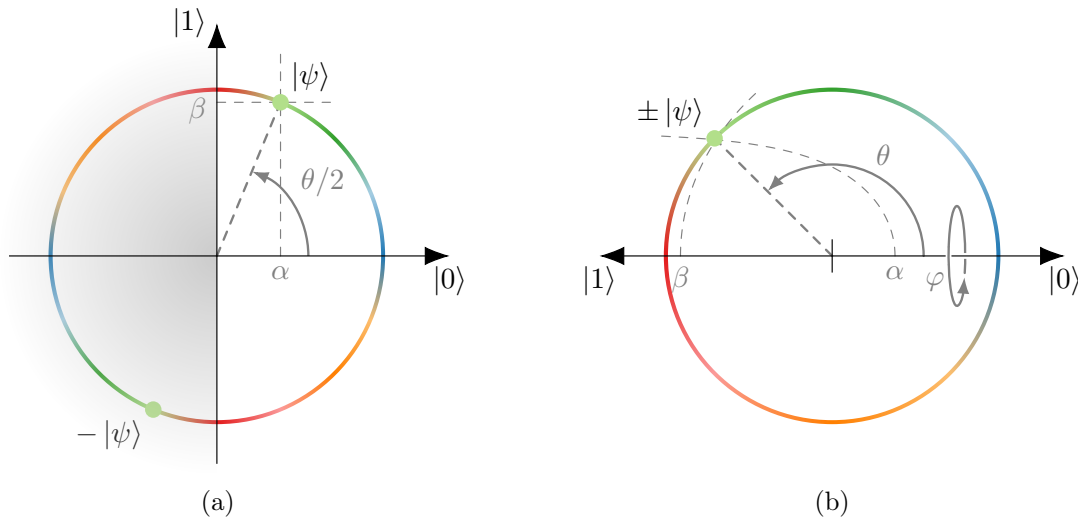
Considérons d'abord uniquement les états quantiques avec des composantes réelles, et ce, jusqu'à la fin de cette section. Ceux-ci vivent dans un espace à deux dimensions qu'on pourra facilement illustrer. La première direction de l'espace (l'axe horizontal) sera attribuée à $|0\rangle$ avec la composante α . La seconde direction (l'axe vertical) sera attribuée à $|1\rangle$ avec la composante β .

Comme ces composantes doivent respecter la condition de normalisation (équation 1.5), les états quantiques valides doivent se retrouver sur un cercle de rayon unité comme cela est illustré à la figure 1.1a. Les états de base $|0\rangle$ et $|1\rangle$ se situent alors aux intersections entre ce cercle et les axes.

Un état quelconque $|\psi\rangle$ se retrouve donc quelque part sur ce cercle, alors qu'un état $-|\psi\rangle$ se retrouve du côté diamétralement opposé du même cercle. Or, comme on a vu à la section A.8 un facteur de phase (ici $e^{i\pi} = -1$) n'a pas de conséquence physique observable. Utilisons un code de couleurs pour illustrer que les états $|\psi\rangle$ et $-|\psi\rangle$ sont physiquement indistinguables : deux états identifiés par la même couleur sur le cercle mèneront aux mêmes observations expérimentales.

L'espace illustré à la figure 1.1a est en quelque sorte deux fois trop grand ; on pourrait se débarrasser de la moitié cet espace sans perte de généralité. Imaginons donc que l'on coupe ce cercle à deux endroits (en $\pm|1\rangle$) ; que l'on se débarrasse de sa moitié gauche de la figure 1.1a ; et que l'on rejoigne les deux bouts de l'arc restant. On obtiendrait alors une construction telle qu'illustrée à la figure 1.1b que l'on appellera temporairement le *cercle* de Bloch.

Remarquez comment, sur la figure 1.1b, chaque couleur n'apparaît alors qu'une seule fois et comment les états de base $|0\rangle$ et $|1\rangle$ sont maintenant opposés l'un à l'autre. Le code de couleur nous permet également d'identifier la position de l'état $|\psi\rangle$. Notez qu'on aurait pu faire la même construction en gardant la moitié

FIGURE 1.1 – Construction du *cercle* de Bloch.

gauche de la figure 1.1a. Pour cette raison, on voit que les états $|\psi\rangle$ et $-|\psi\rangle$ tombent exactement l'un sur l'autre sur la figure 1.1b. Nous avons donc éliminé la redondance dans cet espace et il est alors possible d'identifier un état quantique physique $|\psi\rangle$ à l'aide d'une seule coordonnée : l'angle θ entre celui-ci et l'état $|0\rangle$. Remarquez que l'angle entre les états $|\psi\rangle$ et $|0\rangle$ sur la figure 1.1a est notée $\theta/2$.

La sphère de Bloch

Constatons maintenant que les états quantiques dont les composantes α et β sont du même signe (les deux positifs ou les deux négatifs) se retrouvent dans la partie supérieure de la figure 1.1b, et que les états avec des composantes de signes opposés, dans la partie inférieure. Ce qui distingue ces deux groupes d'états quantiques est donc la phase relative φ entre α et β .

Lorsqu'on se limite à des composantes réelles, la phase relative ne peut prendre que les valeurs 0 et π pour des facteurs de phase de $e^{i0} = 1$ ou $e^{i\pi} = -1$. Lorsqu'on permet des composantes complexes, ce facteur de phase peut prendre toutes les valeurs $e^{i\varphi}$ avec φ compris entre 0 et 2π . L'angle φ nous permet donc de faire le tour de l'axe qui relie les états $|0\rangle$ et $|1\rangle$ en sortant du plan de la figure. La révolution du *cercle* de Bloch autour de cet axe produit une sphère appelée la sphère de Bloch.

La figure 1.2 illustre une représentation typique de la sphère de Bloch. L'axe des z étant l'axe qui passe par les états de base $|0\rangle$ (au pôle Nord) et $|1\rangle$ (au pôle Sud). De manière analogue au système de coordonnées géographiques, l'angle θ permet de changer de latitude et l'angle ϕ de longitude. Le tableau 1.1 dresse également la liste des correspondances entre le cercle et la sphère de Bloch.

Remarque

Un fait intéressant à noter, et qui est parfois source de confusion, est que bien que les états $|0\rangle$ et $|1\rangle$ apparaissent comme *colinéaires* sur la sphère de Bloch, ils sont bien orthogonaux ! En effet, on doit se reporter à la figure 1.1a pour se convaincre qu'ils sont orthogonaux, même si la représentation en sphère de Bloch semble illustrer le contraire.

État quantique général d'un qubit

On voit donc que tous les états quantiques physiques possibles d'un qubit se retrouvent à la surface de la sphère de Bloch. Chacun d'eux peut être entièrement décrit par seulement deux paramètres θ et φ . Terminons cette section en écrivant l'état quantique à l'aide de ces deux paramètres.

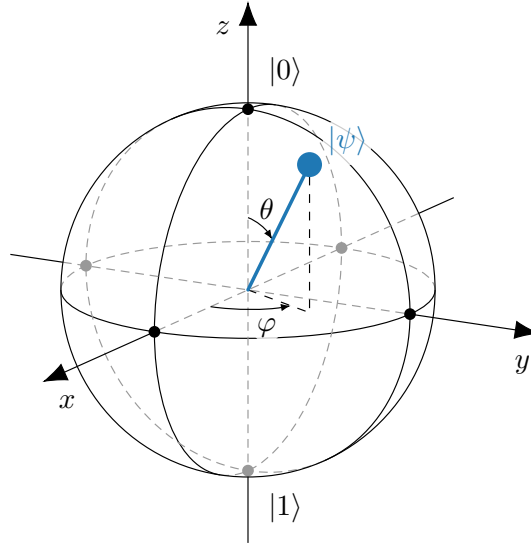
FIGURE 1.2 – La sphère de Bloch et la position d'un état $|\psi\rangle$ à sa surface en fonction des angles θ et φ .

Figure 1.1b	Figure 1.2
Axe horizontal	Axe des z
Axe vertical	Axe des x
Hors du plan	Axe des y

TABLE 1.1 – Liste de correspondances entre le cercle et la sphère de Bloch.

Si on revient à la figure 1.1a, il est clair que pour un état quantique aux composantes réelles on peut écrire l'état quantique

$$|\psi\rangle = \cos(\theta/2) |0\rangle + \sin(\theta/2) |1\rangle \quad (\text{Composantes réelles})$$

avec θ compris entre 0 et 2π . Les états pour $\theta \in [0, \pi]$ correspondent aux états avec un facteur de phase relatif +1 et, les états pour $\theta \in [\pi, 2\pi]$, un facteur de phase relatif -1 .

Pour obtenir la forme d'un état quantique aux composantes complexes, il ne reste qu'à inclure un facteur de phase relative complexe en écrivant

$$|\psi\rangle = \cos(\theta/2) |0\rangle + e^{i\varphi} \sin(\theta/2) |1\rangle \quad (1.10)$$

où θ est alors limité entre 0 et π car la phase relative permet déjà de visiter l'autre côté de la sphère.

A.11 États quantiques notables (à un qubit)

Il est parfois pratique d'établir une liste d'états quantiques qui reviennent souvent dans le cadre du calcul et de la programmation quantique. Dans le cas des états à un qubit, on identifie les états sur la sphère de Bloch qui croisent les axes dans les trois directions. La figure 1.3 permet d'illustrer les positions de ces états sur la sphère de Bloch.

Ainsi, les états qui se trouvent sur l'axe des z sont les états de base $|0\rangle$ et $|1\rangle$ que nous connaissons déjà. Les états qui se trouvent sur l'axe des x sont notés $|+\rangle$ et $|-\rangle$. On peut exprimer ceux-ci en fonction des états de base comme étant

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{et} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

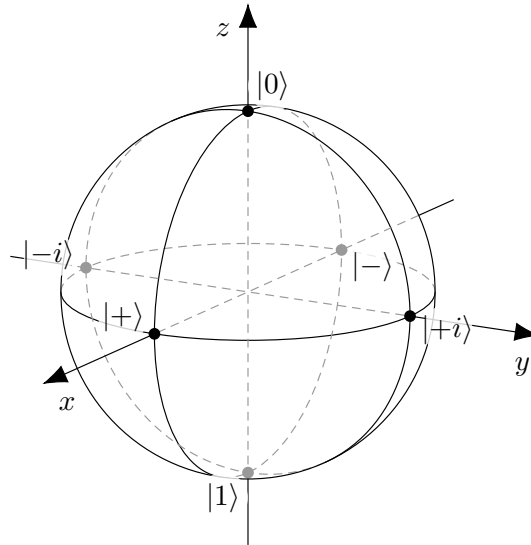


FIGURE 1.3 – Positions d'états quantiques notables sur la sphère de Bloch.

Finalement, les états qui se trouvent sur l'axe des y sont notés $|+i\rangle$ et $|-i\rangle$ (également parfois notés $|R\rangle$ et $|L\rangle$ ou encore $|\odot\rangle$ et $|\ominus\rangle$). Leurs expressions en fonction des états de base sont quant à elles

$$|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \quad \text{et} \quad |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle).$$

Exercice A.8 : États spéciaux sur la sphère de Bloch

Vérifiez que les états $|0\rangle$, $|1\rangle$, $|\pm\rangle$ et $|\pm i\rangle$ se trouvent bien aux endroits identifiés sur la figure 1.3 en utilisant l'équation 1.10 et en déterminant les angles θ et φ pour chacun d'eux.

Remarque

Notez que comme la paire d'états $\{|0\rangle, |1\rangle\}$, les paires $\{|+\rangle, |-\rangle\}$ et $\{|+i\rangle, |-i\rangle\}$ peuvent également être utilisées comme bases des états à un qubit. En d'autres mots, n'importe quel état à un qubit peut être exprimé comme une combinaison linéaire des états $|+\rangle$ et $|-\rangle$, ou comme une combinaison linéaire des états $|+i\rangle$ et $|-i\rangle$. C'est-à-dire

$$|\psi\rangle = \alpha' |+\rangle + \beta' |-\rangle \quad \text{ou} \quad |\psi\rangle = \alpha'' |+i\rangle + \beta'' |-i\rangle.$$

Cela est possible car les états de $\{|+\rangle, |-\rangle\}$ et $\{|+i\rangle, |-i\rangle\}$ sont normalisés et mutuellement orthogonaux.

A.12 Arrière-scène quantique

Nous avons maintenant en main tous les outils pour décrire l'état quantique d'un qubit. Nous avons également vu aux sections A.6 et A.7 comment on acquiert de l'information sur cet état à l'aide de la mesure. Prenons un pas de recul pour décrire comment ces deux aspects vont entrer en interaction.

Comme nous allons le voir, la théorie de la mécanique quantique va permettre de décrire de manière déterministe comment l'état d'un qubit évolue en fonction des différentes opérations qu'on va lui appliquer. Par déterministe, on entend que pour un état quantique de départ donné et une série d'opérations données (excluant la mesure), l'état quantique final sera parfaitement déterminé. Cependant, le résultat de la mesure sur cet état final lui n'est pas déterministe, mais probabiliste et impossible à prévoir.

C'est comme s'il y avait une avant-scène et une arrière-scène à la réalité. L'arrière-scène est régie par la mécanique quantique. Les phénomènes étranges de la mécanique quantique telle que la superposition, l'intrication (que l'on va voir au chapitre 2) et l'interférence sont possibles dans l'arrière-scène. Tout ce qui s'y passe évolue de manière déterministe et prévisible, mais reste inaccessible à un observateur.

En contre partie, l'avant-scène est une manifestation, par l'intermédiaire de la mesure, de ce qui se passe en arrière-scène. Ainsi, aussitôt qu'on mesure un système dans un état quantique quelconque, il apparaît à l'avant-scène. L'état dans lequel il apparaît est aléatoire et les différents résultats possibles ont des probabilités de survenir qui dépendent de l'état qu'avait le système dans l'arrière-scène. L'avant-scène correspond donc plutôt à notre monde habituel classique où les choses se comportent de manière « normale », c'est-à-dire que les phénomènes de superposition, d'intrication et d'interférence ne peuvent pas survivre à l'avant-scène.

Pour un qubit, par exemple, toute la sphère de Bloch est accessible tant qu'il reste à l'arrière-scène. Cependant quand il est à l'avant-scène, il ne peut être que dans les états $|0\rangle$ ou $|1\rangle$.

Exercice A.9 : Retour à l'arrière scène

Lorsqu'on mesure un qubit, son état est projeté dans un des deux états de base. Que se passe-t-il si on tente de modifier l'état du qubit après cette mesure ? Vous pouvez utiliser l'analogie de l'avant et de l'arrière scène pour illustrer votre propos.

B Portes quantiques à un qubit

La première section de ce chapitre nous a permis d'introduire les outils mathématiques pour décrire l'état d'un qubit. Dans la présente section, on s'intéresse aux outils qui nous permettront de modifier l'état d'un qubit pour ainsi commencer à effectuer des calculs quantiques. Dans le cadre du calcul quantique, les opérations qui modifient l'état d'un ou de plusieurs qubits sont appelées des portes quantiques. Cette section introduit donc les portes quantiques qui s'appliquent à un seul qubit.

B.1 Application d'une porte quantique

Pour modifier l'état d'un qubit, on lui applique une porte quantique. L'application d'une porte \hat{P} sur un état $|\psi\rangle$ produit un nouvel état $|\psi'\rangle$. On exprime cette opération ainsi

$$|\psi'\rangle = \hat{P}|\psi\rangle.$$

Info notation B.1 : Des chapeaux

On utilise le chapeau $\hat{}$ pour distinguer les portes quantiques des simples scalaires. En fait, on va vite voir que cette notation sera utilisée pour les portes, les opérateurs et les observables. Dans les présentes notes et par souci esthétique, on omet le chapeau lorsqu'on identifie une porte dans un circuit quantique, comme à la figure 1.4a.

B.2 Diagramme

On va éventuellement vouloir illustrer l'application de plusieurs portes quantiques sur un ensemble de plusieurs qubits. On appelle un circuit quantique une représentation diagrammatique de cette série d'opérations. En particulier, on représente une porte quantique à un qubit par un diagramme comme celui illustré à la figure 1.4a où la porte est représentée par une boîte qui recouvre une ligne horizontale associée au qubit sur lequel elle agit. La ligne horizontale permet de suivre l'évolution de l'état d'un qubit où l'état initial se trouve du côté gauche de la porte et l'état final du côté droit. Par convention, certaines portes quantiques sont représentées par des diagrammes différents.

La mesure d'un qubit est représentée par le diagramme illustré à la figure 1.4d. Notez que la mesure n'est pas une opération quantique car elle n'est pas réversible. C'est pour cette raison, qu'en règle générale, la mesure est la dernière opération effectuée sur un qubit.

B.3 Représentation matricielle

On a vu, à la section A.2, que l'état quantique d'un qubit peut être décrit grâce à un vecteur à deux composantes complexes. Que pourrait-on utiliser pour décrire l'effet d'une porte quantique ? En d'autres

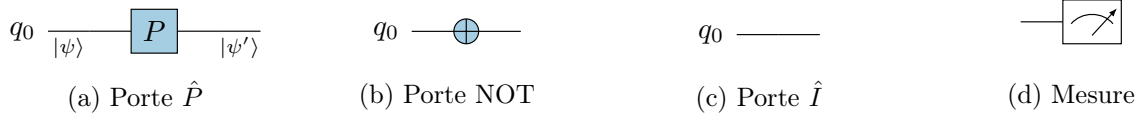


FIGURE 1.4 – Diagrammes représentant différentes portes quantiques à un qubit (a-c) ainsi que la mesure (d). Ces représentations seront utilisées pour construire des circuits quantiques.

termes, que peut-on utiliser pour transformer un vecteur à deux composantes en un autre vecteur à deux composantes ? Une matrice !

Alors qu'on peut écrire l'état d'un qubit comme un vecteur à deux composantes, on peut également écrire l'effet d'une porte sous la forme d'une matrice 2×2 . Écrivons la forme générale d'une telle matrice

$$\hat{P} = \begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix}$$

où les éléments de matrice P_{ij} peuvent également être des nombres complexes.

Info notation B.2 : Les indices

Puisqu'on fera une utilisation intensive des vecteurs, des matrices et des tenseurs, nous serons amenés tôt ou tard à utiliser la notation indicielle. Cette notation permet de faire référence de manière abstraite à un élément d'un vecteur (composante), d'une matrice ou d'un tenseur. Par exemple, lorsqu'on écrit P_{ij} on fait référence à l'élément de la matrice P qui se situe à la ligne i et à la colonne j .

Info notation B.3 : Numérotation à partir de 0

Dans de nombreux cas, nous allons numéroter les indices à partir de 0 et non à partir de 1. Cela permet, entre autre, d'être cohérent avec la plupart des langage de programmation ainsi qu'avec la représentation binaire des entiers.

Info notation B.4 : Portes quantiques et matrices

Comme pour les états quantiques et les vecteurs d'état (voir équation 1.3), l'égalité entre une porte quantique et une matrice

$$\hat{P} = \begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix} \quad (1.11)$$

est un abus de notation. La raison pour laquelle cela n'est pas rigoureusement vrai est encore une question de base : une porte quantique pourrait être décrite par une autre matrice si on l'exprimait dans une base différente.

Encore une fois, à moins d'avis contraire, une égalité telle que celle de l'équation 1.11 suppose que la porte quantique est exprimée dans la base computationnelle $\{|0\rangle, |1\rangle\}$.

B.4 Effet d'une porte quantique

L'état quantique résultant de l'application d'une porte quantique sur un état quantique initial s'obtient en effectuant le produit de la matrice représentant la porte avec le vecteur d'état représentant l'état quantique. Le résultat de ce produit est un nouveau vecteur qui représente l'état quantique du qubit après l'application de la porte

$$|\psi'\rangle = \hat{P} |\psi\rangle = \begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} P_{00}\alpha + P_{01}\beta \\ P_{10}\alpha + P_{11}\beta \end{pmatrix}. \quad (1.12)$$

Exemple B.1 : La porte \hat{X}

Une porte très utile en calcul quantique est la porte \hat{X} aussi appelé porte NOT (non). Elle a l'effet de transformer l'un des états de base ($|0\rangle$ ou $|1\rangle$) en son état opposé, c'est-à-dire

$$|1\rangle = \hat{X} |0\rangle \quad \text{et} \quad |0\rangle = \hat{X} |1\rangle.$$

Tentons de déduire la représentation matricielle de la porte \hat{X} : quels sont ses éléments de matrice ? D'abord, la première équation nous permet de déterminer la première colonne de \hat{X} . En effet,

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} X_{00} & X_{01} \\ X_{10} & X_{11} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} X_{00} \\ X_{10} \end{pmatrix}.$$

De la même manière, la seconde équation permet de déduire la seconde colonne de \hat{X} ,

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & X_{01} \\ 1 & X_{11} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} X_{01} \\ X_{11} \end{pmatrix}$$

et donc la matrice qui représente la porte \hat{X} est

$$\hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Exercice B.1 : Deux portes \hat{X}

Montrez que l'application de deux portes \hat{X} successives permet de revenir à l'état initial peu importe cet état initial.

B.5 Composition de portes quantiques

L'application de plusieurs portes successives (ou composition) peut être résumée par le produit des matrices représentant les différentes portes. Par exemple, les applications successive des portes \hat{P}_1 et \hat{P}_2 à la figure 1.5a peuvent être remplacées par l'application d'une seule porte \hat{P}_3 à la figure 1.5b.

Illustrons cela mathématiquement en appliquant d'abord une porte \hat{P}_1 sur un état initial $|\psi\rangle$. On obtient ainsi un nouvel état quantique intermédiaire

$$|\psi'\rangle = \hat{P}_1 |\psi\rangle.$$

Appliquons ensuite une seconde porte \hat{P}_2 sur cet état pour obtenir l'état final

$$|\psi''\rangle = \hat{P}_2 |\psi'\rangle.$$

En combinant ces applications successives, on constate que l'état final peut être obtenu directement à partir de l'état initial

$$|\psi''\rangle = \hat{P}_2 \hat{P}_1 |\psi\rangle.$$

en appliquant la porte combinée $\hat{P}_2 \hat{P}_1$. Notez que la porte \hat{P}_1 s'applique en premier et se trouve donc à droite du produit, plus proche de l'état initial. Comme \hat{P}_1 et \hat{P}_2 sont des matrices, on peut construire une nouvelle porte \hat{P}_3 en effectuant le produit matriciel de celles-ci

$$\hat{P}_3 = \hat{P}_2 \hat{P}_1$$

de sorte que

$$|\psi''\rangle = \hat{P}_3 |\psi\rangle.$$

L'effet de plusieurs portes quantiques successives peut donc toujours être résumé à l'application d'une seule porte quantique.

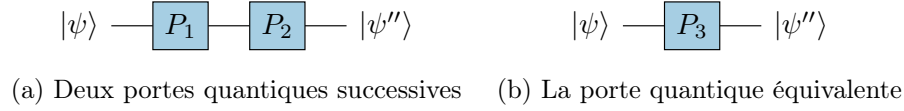


FIGURE 1.5 – L'application successive de deux portes quantiques (a) est équivalente à l'application d'une seule porte quantique (b).

B.6 Transformation d'un $\langle \cdot |$

Nous avons vu à la section B.4 comment une porte transforme un état écrit sous la forme d'un $|\cdot\rangle$. Nous avons également vu, à la section A.3, qu'un état peut être représenté sous la forme d'un $\langle \cdot |$. On peut donc se demander comment écrire l'application d'une porte quantique sur un $\langle \cdot |$.

On sait que $\langle \cdot |$ est le conjugué hermitien (transposé et conjugué complexe) de $|\cdot\rangle$. Écrivons donc une version conjuguée hermitienne de l'équation 1.12 en se rappelant que la transposée d'un produit inverse l'ordre des facteurs

$$\langle \psi' | = (\alpha^* \quad \beta) \begin{pmatrix} P_{00}^* & P_{10}^* \\ P_{01}^* & P_{11}^* \end{pmatrix} = \langle \psi | \hat{P}^\dagger \quad (1.13)$$

où

$$\hat{P}^\dagger = (\hat{P}^\top)^* = (\hat{P}^*)^\top \quad (1.14)$$

est la matrice conjuguée hermitienne de \hat{P} . On voit que l'application d'une porte quantique sur un $\langle \cdot |$ s'effectue par la droite et en utilisant la conjuguée hermitienne de la matrice qui représente la porte quantique.

Donc pour une transformation \hat{P} d'un $|\cdot\rangle$, le $\langle \cdot |$ se transforme grâce à \hat{P}^\dagger

$$|\psi'\rangle = \hat{P} |\psi\rangle \quad \langle \psi' | = \langle \psi | \hat{P}^\dagger.$$

Exercice B.2 : Conjuguée hermitien

Exprimez les matrices conjuguées hermitiennes pour les trois matrices suivantes

$$\hat{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \hat{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad \hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

B.7 Transformation d'états quantiques normalisés

Si l'état $|\psi\rangle$ est normalisé, on doit également exiger que l'état résultant d'une transformation $|\psi'\rangle = \hat{P} |\psi\rangle$ le soit aussi. C'est-à-dire que

$$\langle \psi | \psi \rangle = 1 \quad \text{et} \quad \langle \psi' | \psi' \rangle = 1.$$

Explicitement, on exige l'égalité suivante,

$$\langle \psi' | \psi' \rangle = \langle \psi | \hat{P}^\dagger \hat{P} | \psi \rangle = \langle \psi | \psi \rangle = 1.$$

ce qui est vérifié si $\hat{P}^\dagger \hat{P} |\psi\rangle = |\psi\rangle$. Cela implique que le produit $\hat{P}^\dagger \hat{P} = \hat{I}$ où \hat{I} est la matrice identité. Cela implique également que l'inverse de \hat{P} est donnée par sa conjuguée hermitienne

$$\hat{P}^{-1} = \hat{P}^\dagger \quad (1.15)$$

Finalement, on voit que la matrice \hat{P} respecte l'identité suivante

$$\hat{P}^\dagger \hat{P} = \hat{P} \hat{P}^\dagger = \hat{I} \quad (1.16)$$

qui n'est rien d'autre que la définition d'une matrice unitaire. Notons que le déterminant d'une matrice unitaire est un nombre complexe de module 1. La matrice qui représente une porte quantique respecte toujours

$$|\det(\hat{P})| = 1. \quad (1.17)$$

Soulignons cependant que cette propriété n'est pas suffisante pour qu'une matrice soit unitaire.

Exemple B.2 : Matrice unitaire

Montrons que la matrice qui représente la porte

$$\hat{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

est bien unitaire. On effectue donc le produit de cette matrice avec sa conjuguée hermitienne

$$\hat{Y}^\dagger \hat{Y} = \begin{pmatrix} 0 & (i)^* \\ (-i)^* & 0 \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

On obtient donc bien la matrice identité. La matrice \hat{Y} est donc unitaire et peut être utilisée comme une porte quantique.

Exemple B.3 : Matrice non-unitaire

En contre partie, la matrice

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

n'est pas unitaire. En effet,

$$\hat{M}^\dagger \hat{M} = \begin{pmatrix} 1^* & 1^* \\ 1^* & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \hat{I}.$$

La matrice \hat{M} n'est donc pas unitaire malgré que son déterminant respecte

$$|\det(\hat{M})| = 1.$$

B.8 Propriétés des portes quantiques

Comme les portes quantiques peuvent être représentées par des matrices unitaires, elles partagent les mêmes propriétés que ces matrices. Tentons d'en dresser une liste utile.

Non abélienne

Comme pour le produit de matrices, l'ordre d'application des portes quantiques est important : elles sont non abéliennes ou non commutatives. À priori, l'application de deux portes quantiques dans un ordre et dans l'autre ne produira pas le même résultat

$$\hat{P}_2 \hat{P}_1 \neq \hat{P}_1 \hat{P}_2.$$

Bien qu'il existe des exceptions où des portes quantiques commutent, en général ce n'est pas le cas.

Unitaire

Une matrice unitaire est toujours inversible. Les portes quantiques sont également inversibles. Dans un calcul quantique, il existe toujours une opération qui nous permet de revenir en arrière, tant qu'on n'a pas effectué de mesure évidemment.

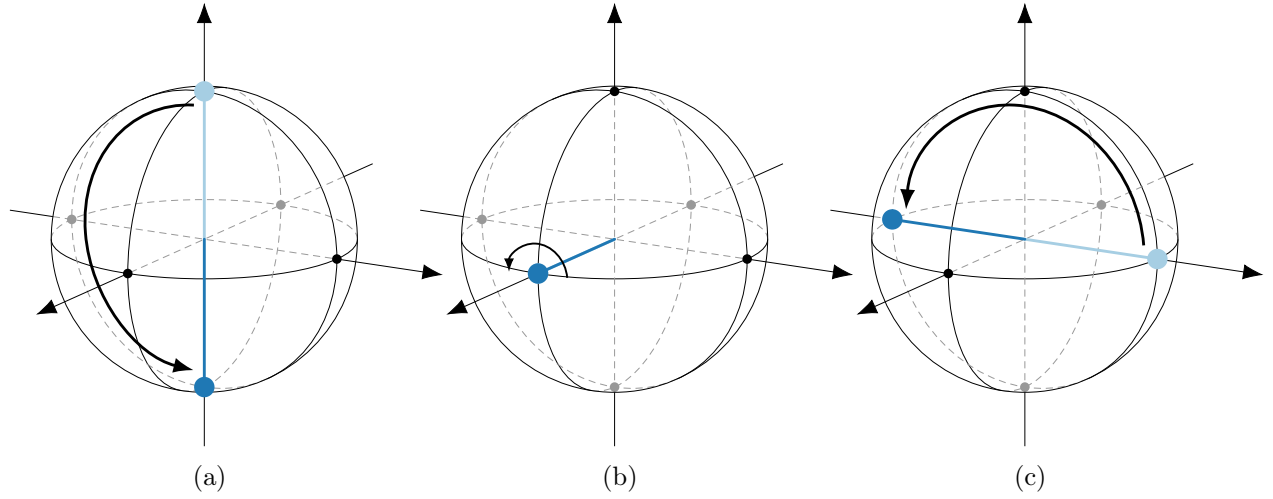


FIGURE 1.6 – Exemples des trajectoires pour les transformations de différents états initiaux avec la porte \hat{X} . Ces trajectoires sont générées par une rotation de 180° autour de l'axe x . Par exemple, la porte \hat{X} transforme (a) l'état $|0\rangle$ en $|1\rangle$, (b) laisse l'état $|+\rangle$ inchangé et (c) l'état $|+i\rangle$ en $|-i\rangle$

De plus, la matrice inverse (porte inverse) d'une matrice unitaire (porte quantique) est très facile à obtenir : on doit simplement prendre le conjugué hermitien (voir les équations 1.14 et 1.15) c'est-à-dire prendre la transposée et le conjugué complexe. Dans le cas d'une suite de portes quantiques, on ne doit pas oublier d'inverser l'ordre des opérations lorsqu'on prend la matrice transposée.

B.9 Quelques portes quantiques à un qubit

Bien qu'on puisse construire une infinité de portes quantiques à un qubit différentes, certaines portes sont utilisées plus souvent que d'autres. Ces portes peuvent également servir de base afin de définir d'autres portes. Dans cette section, on dresse la liste de quelques portes quantiques importantes. On verra aussi que chacune des portes quantiques peut être vue comme une rotation sur la sphère de Bloch (section A.10). On donnera donc quelques exemples de trajectoires pour illustrer la transformation de quelques états quantiques par ces portes.

Porte \hat{X}

Nous avons déjà introduit la porte \hat{X} (aussi appelée porte NOT) à l'exemple B.1. Cette porte a pour effet de transformer un état de base à un qubit ($|0\rangle$ ou $|1\rangle$) en l'état de base opposé. L'effet de la porte \hat{X} est équivalent à une rotation d'un demi-tour (π rad) autour de l'axe des x . La matrice qui représente cette transformation est

$$\hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

La figure 1.6 illustre comment la porte \hat{X} transforme les états $|0\rangle$, $|+\rangle$ et $|+i\rangle$. Cette porte est sa propre inverse

$$\hat{X}^\dagger = \hat{X}$$

c'est-à-dire que si on l'applique deux fois de suite, on retrouve l'état initial du qubit.

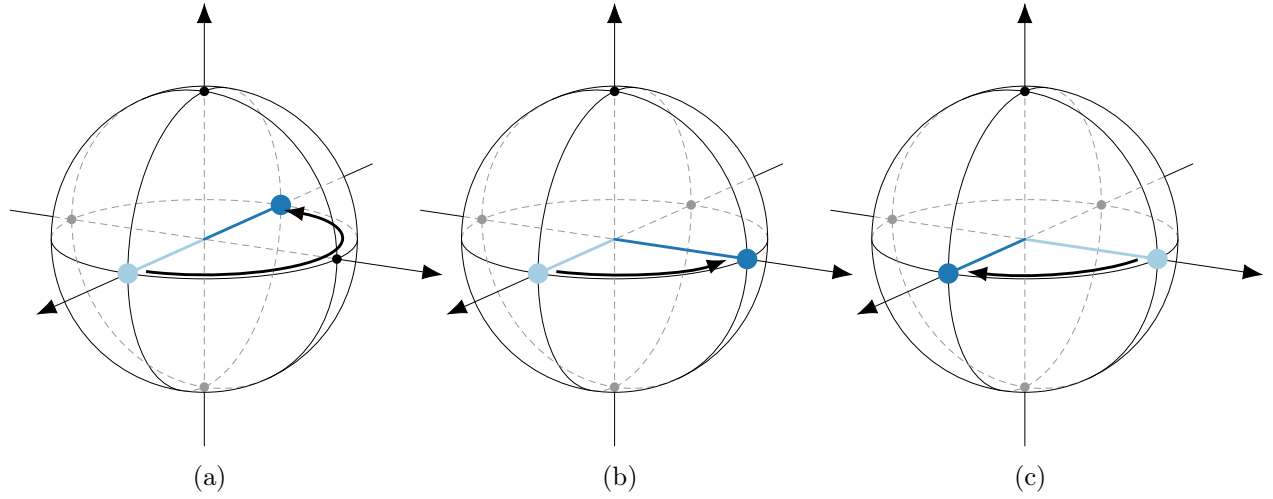


FIGURE 1.7 – Exemples des trajectoires pour les transformations de différents états initiaux avec les portes de phase (a) \hat{Z} , (b) \hat{S} et (c) \hat{S}^\dagger .

Exercice B.3 : La porte \hat{X}

a) Quel est l'effet de la porte \hat{X} sur un état général ?

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

b) Identifiez les composantes α et β d'un état qui reste inchangé sous l'effet de cette porte. Assurez-vous que cet état soit normalisé.

$$\hat{X} |\psi\rangle = |\psi\rangle$$

c) Identifiez les composantes α et β d'un état qui change de signe sous l'effet de cette porte.

$$\hat{X} |\psi\rangle = -|\psi\rangle$$

d) Démontrez que la porte \hat{X} est sa propre inverse.

Porte \hat{Z}

Analogue à la porte \hat{X} , la porte \hat{Z} effectue une rotation d'un demi-tour, mais cette fois, autour de l'axe des z comme illustré à la figure 1.7a. La rotation autour de l'axe des z se résume à un changement de la phase φ (voir la figure 1.2). Une rotation de π rad autour de l'axe des z engendre un facteur de phase relatif de $e^{i\pi} = -1$. La matrice qui représente cette transformation est donc

$$\hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

La porte \hat{Z} prend aussi le nom de porte d'inversion de phase. Cette porte est également sa propre inverse.

Porte \hat{Y}

La porte \hat{Y} agit également de manière analogue aux portes \hat{X} et \hat{Z} mais, cette fois-ci, autour de l'axe des y . La matrice qui représente cette porte quantique est

$$\hat{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

Comme les portes \hat{X} et \hat{Z} , cette porte est également sa propre inverse.

Remarque : Matrices de Pauli

Les matrices qui représentent les portes \hat{X} , \hat{Z} et \hat{Y} correspondent aussi aux trois matrices de Pauli.

Exercice B.4 : Les portes de Pauli

Les portes \hat{X} , \hat{Y} et \hat{Z} sont représentées par les trois matrices de Pauli.

- Montrez que ces trois portes quantiques sont bien unitaires.
- Vérifiez, avec un exemple, que le produit de deux matrices de Pauli différentes retourne la troisième matrice de Pauli.
- Comment ce résultat change si vous changez l'ordre du produit ?

Porte \hat{S}

La porte \hat{S} effectue une rotation d'un quart de tour dans le sens anti-horaire ($\pi/2$ rad) autour de l'axe des z , comme cela est illustré à la figure 1.7b. Une succession de deux de ces portes effectue donc une rotation d'un demi-tour résultant en une porte \hat{Z} . Autrement dit

$$\hat{S}\hat{S} = \hat{S}^2 = \hat{Z}. \quad (1.18)$$

Pour cette raison, cette porte quantique porte également le nom de racine carrée de \hat{Z} (*square root of \hat{Z}* en anglais). La matrice représentant cette transformation est

$$\hat{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

L'équation 1.18 montre également que la porte \hat{S} n'est pas sa propre inverse. Par définition, l'inverse de \hat{S} est \hat{S}^\dagger et correspond une rotation d'un quart de tour dans le sens horaire ($-\pi/2$ rad) autour de l'axe des z (voir figure 1.7c).

Exercice B.5 : Une version alternative pour \hat{S}

Montrez que la matrice

$$\hat{S}' = \frac{1}{\sqrt{2}} \begin{pmatrix} 1-i & 0 \\ 0 & 1+i \end{pmatrix}.$$

est égale à la matrice \hat{S} à un facteur de phase global près. Expliquez ensuite les conséquences d'utiliser la matrice \hat{S}' plutôt que la matrice \hat{S} pour représenter la porte \hat{S} .

Porte Hadamard (\hat{H})

La porte Hadamard permet de préparer un état quantique en superposition d'états à partir d'un état de base. La porte Hadamard est équivalente à une rotation de π rad autour d'un axe qui se situe à $\pi/4$ entre les axes x et z comme cela est illustré à la figure 1.8. Ses effets sur les deux états de base sont

$$\hat{H} |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \quad \text{et} \quad \hat{H} |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle.$$

La matrice qui permet d'appliquer une porte Hadamard est donc

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

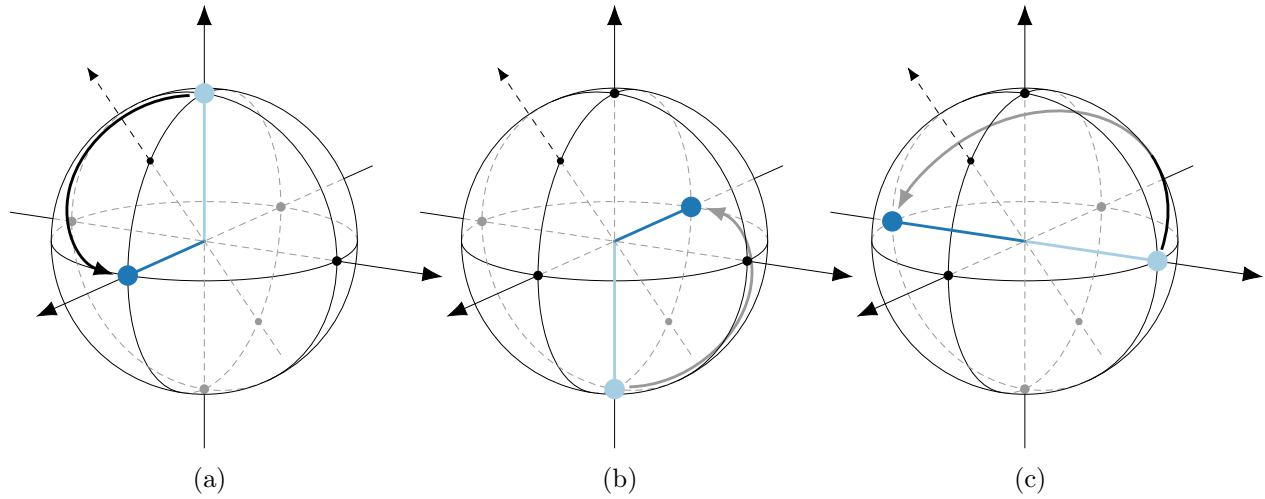
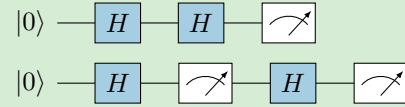


FIGURE 1.8 – Exemples des trajectoires pour les transformations de différents états initiaux avec la porte Hadamard. Ces trajectoires sont générées par une rotation de π rad (180°) autour d'un axe situé à $\pi/4$ rad (45°) entre les axes x et z . La porte Hadamard transforme (a) l'état $|0\rangle$ en $|+\rangle$, (b) l'état $|1\rangle$ en $|-\rangle$ et (c) l'état $|+i\rangle$ en $|-i\rangle$

La porte Hadamard est sa propre inverse.

Exercice B.6 : Porte Hadamard et mesure intermédiaire

Considérez les deux circuits ci-contre. Pour chacun d'eux, quelles sont les probabilités d'obtenir les résultats 0 et 1 lors de la mesure finale ?



Porte identité (\hat{I})

Terminons cette section avec la porte la plus triviale qui soit : la porte-identité qui laisse un état quantique inchangé. La matrice qui la représente est simplement la matrice identité

$$\hat{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

En général, cette porte n'apparaît pas explicitement dans les circuits quantiques.

B.10 Portes quantiques paramétrées

Les portes quantiques vues à la section précédente ont toutes des effets fixes ; c'est-à-dire des rotations autour d'axes donnés pour des angles de π ou $\pi/2$ (sauf l'identité qui laisse l'état inchangé). On peut cependant construire des portes dont l'effet dépend d'un ou plusieurs paramètres : ce sont des portes quantiques paramétrées. En particulier, les rotations autour des axes x , y et z pour des angles arbitraires sont des portes paramétrées.

Rotation autour de y

Voyons d'abord la rotation d'un angle θ autour de l'axe y , notée $\hat{R}_y(\theta)$. La matrice qui représente cette rotation est la suivante

$$\hat{R}_y(\theta) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}.$$

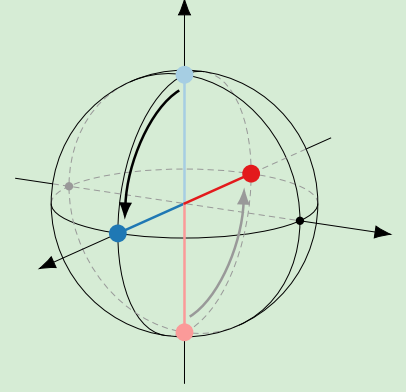
En particulier, une rotation \hat{R}_y d'un angle π n'est rien d'autre qu'une porte \hat{Y} .

On remarque que les éléments de matrice de \hat{R}_y sont réels. Par conséquent, la transformation d'un état quantique aux coefficients réels avec cette porte produit un nouvel état quantique aux coefficients réels. En effet, un état dans le plan xz sur la sphère de Bloch restera dans ce plan après une rotation autour de l'axe y .

Exercice B.7 : La porte Hadamard vs R_y

La figure ci-contre illustre une rotation de $\pi/4$ autour de l'axe des y (aussi notée $\hat{R}_y(\pi/4)$) appliquée aux deux états de base. En comparant cet effet à l'effet de la porte Hadamard aux figures 1.8a et b, on pourrait croire que ces deux rotations ont le même effet. Trouver un argument qui montre hors de tout doute que ces deux rotations sont différentes

$$\hat{H} \neq \hat{R}_y(\pi/4).$$



Rotation autour de z

La matrice qui permet d'effectuer une rotation d'un angle θ autour de l'axe des z est

$$\hat{R}_z(\theta) = \begin{pmatrix} \exp(-i\theta/2) & 0 \\ 0 & \exp(i\theta/2) \end{pmatrix}$$

La porte \hat{R}_z modifie la phase relative d'un état quantique à un qubit en appliquant une phase de $-\theta/2$ à la composante de l'état $|0\rangle$ et une phase $\theta/2$ à celle de l'état $|1\rangle$. La porte de phase

$$\hat{P}(\theta) = \exp(i\theta/2)\hat{R}_z(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\theta) \end{pmatrix}$$

a le même effet en appliquant uniquement une phase θ à l'état $|1\rangle$.

Rotation autour de x

La porte quantique \hat{R}_x permet d'effectuer une rotation autour de l'axe des x

$$\hat{R}_x(\theta) = \begin{pmatrix} \cos(\theta/2) & -i \sin(\theta/2) \\ -i \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}.$$

Exercice B.8 : Le retour des portes \hat{X} , \hat{Y} et \hat{Z}

Montrez que les rotations $\hat{R}_x(\theta)$, $\hat{R}_y(\theta)$ et $\hat{R}_z(\theta)$ pour le même angle $\theta = \pi$ ont respectivement les mêmes effets que les portes \hat{X} , \hat{Y} et \hat{Z} .

Exercice B.9 : Identités pour des portes à un qubit

Démontrez les identités suivantes :

a) $\hat{Z} = \hat{H}\hat{X}\hat{H}$

c) $\hat{Z}\hat{H} = \hat{H}\hat{X}$

b) $\hat{Y} = \hat{S}\hat{X}\hat{S}^\dagger$

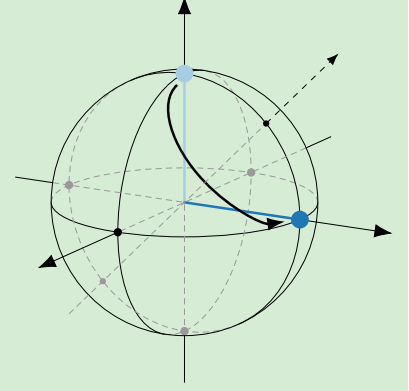
d) $\hat{Z}\hat{X} = -\hat{X}\hat{Z}$

Exercice B.10 : Inventons une nouvelle porte quantique

On aimerait construire une nouvelle porte quantique \hat{G} ayant un effet similaire à la porte Hadamard, mais qui effectue une rotation d'un angle π autour d'un axe située à $\pi/4$ entre les axes y et z , comme c'est illustré à la figure ci-contre.

- Combinez un certain nombre des portes quantiques déjà vues, dont la porte Hadamard, pour obtenir une porte quantique \hat{G} qui applique la rotation désirée.
- Obtenez la matrice qui représente cette transformation dans la base computationnelle et vérifiez que l'application de \hat{G} transforme les états quantiques suivants de la manière attendue

$$\hat{G}|0\rangle = |+\rangle, \quad \hat{G}|1\rangle = |-i\rangle, \quad \hat{G}|+\rangle = |-\rangle.$$

**B.11 Formulation dyadique d'une porte quantique**

Il existe une notation très intuitive pour les portes quantiques qui fait usage de la notation *ket-bra*, c'est-à-dire,

$$|u\rangle\langle v|.$$

Ce *ket-bra*, lorsqu'appliqué à l'état $|v\rangle$, produit l'état

$$|u\rangle\langle v| |v\rangle = |u\rangle$$

et agit donc comme une matrice. En effet, pour des états définis comme

$$|u\rangle = \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} \quad \text{et} \quad |v\rangle = \begin{pmatrix} v_0 \\ v_1 \end{pmatrix}$$

on utilise le produit dyadique pour construire la matrice

$$|u\rangle\langle v| = \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} \begin{pmatrix} v_0^* & v_1^* \end{pmatrix} = \begin{pmatrix} u_0 v_0^* & u_0 v_1^* \\ u_1 v_0^* & u_1 v_1^* \end{pmatrix}.$$

En général, une porte quantique pourra s'écrire comme une combinaison linéaire de produits dyadiques.

Exemple B.4 : Formulation dyadique d'une porte quantique

Calculons les produits dyadiques entre les états de base pour un qubit

$$\begin{aligned} |0\rangle\langle 0| &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & |0\rangle\langle 1| &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ |1\rangle\langle 0| &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} & |1\rangle\langle 1| &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Cela nous permet d'écrire, par exemple, les formulations dyadiques pour les portes \hat{I} , \hat{Z} et \hat{X}

$$\begin{aligned} \hat{I} &= |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \hat{Z} &= |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ \hat{X} &= |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \end{aligned}$$

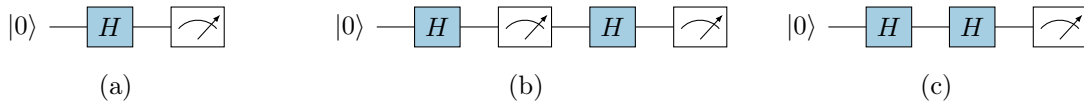


FIGURE 1.9 – Circuits quantiques utilisant la porte Hadamard pour illustrer l’effet d’interférence quantique.

Exercice B.11 : Formulation dyadique de la porte Hadamard

La formulation dyadique de la porte Hadamard à l’aide des états de base est

$$\hat{H} = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|).$$

Trouvez une formulation dyadique plus compacte pour cette porte.

B.12 Discussion sur la superposition et l’interférence

Lors de notre premier contact avec la mesure aux sections A.6 et A.7, nous avons affirmé qu’un qubit placé dans un état quantique

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

qui est ensuite mesuré, a une probabilité $|\alpha|^2$ de retourner la valeur 0 et une probabilité $|\beta|^2$ de retourner la valeur 1. Face à l’étrangeté de la mécanique quantique, on pourrait être tenté de questionner cette interprétation. Est-il possible que le qubit était déjà dans l’état $|0\rangle$ ou déjà dans l’état $|1\rangle$ avec des probabilités $|\alpha|^2$ et $|\beta|^2$, mais que nous ignorions simplement cette information ? En d’autres mots, est-ce qu’un qubit peut être en superposition d’états et la mesure projette celui-ci dans un état donné, ou est-ce que tout cela n’est qu’une manifestation de notre ignorance sur l’état du système ?

Pour lever ce doute, considérons l’utilisation de la porte Hadamard pour préparer un état de superposition

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

et considérons les deux scénarios possibles : 1. un classique où la superposition n’existe pas et l’application d’une porte Hadamard ne fait que *mélanger* le qubit 2. un quantique où la porte Hadamard permet vraiment de préparer une superposition d’états.

Scénario classique

Avec nos nouveaux outils de programmation quantique, ce scénario peut être reproduit par une porte Hadamard suivie d’une mesure, comme illustré à la figure 1.9a. Ainsi, à chaque fois qu’on applique une porte Hadamard, on *mélange* le qubit un peu comme si on lançait une pièce de monnaie, mais qu’on ne regardait pas le résultat.

Si on effectue deux fois cette opération, on agit comme le circuit à la figure 1.9b. Le résultat final sera alors 0 une fois sur deux et 1 l’autre fois².

Scénario quantique

En revanche, si on admet que la porte Hadamard appliquée à l’état $|0\rangle$ permet de préparer une superposition d’états, l’application d’une seconde porte Hadamard (comme illustré à la figure 1.9c) devrait

2. Voir l’exercice B.6 pour plus de détails.

ramener le système dans son état initial, c'est-à-dire $|0\rangle$. Le résultat final sera alors 0 dans tous les cas. Bien que l'état du qubit soit en superposition d'états après la première porte Hadamard, l'interférence quantique fait que l'application de la seconde réduit à zéro les probabilités d'obtenir le résultat 1.

En pratique, c'est le deuxième scénario qui est observé d'où l'importance et la pertinence de la théorie de la mécanique quantique.

S Solutions aux exercices

Exercice A.1 : Vecteurs d'état

Les vecteurs pour ces états sont

$$\text{a) } |\phi\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$$

$$\text{b) } |\psi\rangle = \begin{pmatrix} b \\ a \end{pmatrix}$$

$$\text{c) } |+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$\text{d) } |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\text{e) } |\eta\rangle = e^{i\varphi_0} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} ae^{i\varphi_0} \\ be^{i\varphi_0} \end{pmatrix}$$

$$\text{f) } |\theta\rangle = \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Exercice A.2 : Ordre du produit scalaire

En utilisant les états quantiques

$$|\psi_a\rangle = a_0 |0\rangle + a_1 |1\rangle$$

et

$$|\psi_b\rangle = b_0 |0\rangle + b_1 |1\rangle,$$

ces produits scalaire sont

$$\langle\psi_a|\psi_b\rangle = a_0^* b_0 + a_1^* b_1$$

et

$$\begin{aligned} \langle\psi_b|\psi_a\rangle &= b_0^* a_0 + b_1^* a_1 \\ &= a_0 b_0^* + a_1 b_1^*. \end{aligned}$$

On remarque que les deux produits scalaires sont égaux à un complexe conjugué près

$$\langle\psi_a|\psi_b\rangle = \langle\psi_b|\psi_a\rangle^*.$$

Exercice A.3 : Normalisation

Les états $|\psi_a\rangle$, $|\psi_b\rangle$, $|\psi_d\rangle$ et $|\psi_f\rangle$ sont normalisés. Voici les preuves,

$$\text{(a) } \left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 = 1$$

$$\text{(d) } \left(\sqrt{\frac{3}{4}}\right)^2 + \left(\frac{1}{2}\right)^2 = 1$$

$$\text{(b) } \left(\frac{1}{\sqrt{2}}\right)^2 + \left(-\frac{1}{\sqrt{2}}\right)^2 = 1$$

$$\text{(e) } (0.9)^2 \neq 1$$

$$\text{(c) } \left(\frac{1}{3}\right)^2 + \left(\frac{2}{3}\right)^2 = \frac{5}{9} \neq 1$$

$$\text{(f) } (-1)^2 = 1.$$

Exercice A.4 : Renormalisation

Pour le démontrer, on doit simplement effectuer le produit scalaire de $|\psi'\rangle$ avec lui-même

$$\langle\psi'|\psi'\rangle = \left(\frac{1}{\langle\psi|\psi\rangle^{1/2}} \langle\psi| \right) \left(\frac{1}{\langle\psi|\psi\rangle^{1/2}} |\psi\rangle \right) = \frac{\langle\psi|\psi\rangle}{\langle\psi|\psi\rangle} = 1.$$

Exercice A.6 : Probabilités de mesure

a) Les deux réponses suivantes sont bonnes

$$|\psi\rangle = \frac{1}{\sqrt{3}} |0\rangle + \sqrt{\frac{2}{3}} |1\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{3}} |0\rangle - \sqrt{\frac{2}{3}} |1\rangle$$

b) L'état suivant respecte ces probabilités

$$|\psi\rangle = \sqrt{p} |0\rangle + \sqrt{1-p} |1\rangle$$

Exercice B.3 : La porte \hat{X}

- (a) On applique la porte \hat{X} sur l'état général

$$\hat{X} |\psi\rangle = \alpha \hat{X} |0\rangle + \beta \hat{X} |1\rangle = \alpha |1\rangle + \beta |0\rangle = \beta |0\rangle + \alpha |1\rangle$$

- (b) Pour que l'état précédent soit égal à l'état initial, on doit avoir $\alpha = \beta$. La condition de normalisation nous permet d'identifier un état (aux composantes réelles)

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

ou tout autre état à une phase globale près.

- (c) La condition est $\alpha = -\beta$, ce qui nous permet d'identifier un autre état

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

ou tout autre état à une phase globale près.

Chapitre 2

Deux qubits

Un système d'un seul qubit est intéressant pour étudier des propriétés fondamentales de la mécanique quantique, mais son utilité est limitée. Il est nécessaire d'utiliser plusieurs qubits si on veut arriver à faire un calcul quantique. Dans ce chapitre, nous allons considérer un système de deux qubits. Nous allons d'abord voir comment décrire l'état d'un tel système et ensuite comment il est possible de le modifier en utilisant des portes quantiques à deux qubits.

Une fois que nous aurons bien compris et décrit un système de deux qubits, nous aurons tous les outils en main afin d'en ajouter davantage. Nous serons également mieux équipés pour appréhender l'immense potentiel du calcul quantique.

A État à deux qubits

Pour décrire un état à deux qubits, considérons deux qubits (un qubit **rouge** et un qubit **bleu**) dans des états quelconques. Si on mesure le premier qubit, il retournera la valeur **0** ou la valeur **1** (2 possibilités). C'est la même chose pour l'autre qubit (**0** ou **1**). Dans son ensemble, le groupe de deux qubits retournera l'un des quatre (2×2 possibilités) résultats suivants¹

$$\mathbf{00}, \quad \mathbf{01}, \quad \mathbf{10} \quad \text{ou} \quad \mathbf{11}$$

chacun avec une probabilité donnée. Un état quantique à deux qubits s'exprime donc sur quatre états de base que l'on note

$$|00\rangle, \quad |01\rangle, \quad |10\rangle \quad \text{et} \quad |11\rangle.$$

On peut déjà anticiper que l'état quantique d'un système de deux qubits prend la forme d'une combinaison linéaire de ces quatre états de base

$$|\psi\rangle = \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle \quad (2.1)$$

où α , β , γ et δ sont des amplitudes de probabilités².

Lors de la mesure d'un tel état, les probabilités d'obtenir chacun des quatre résultats possibles sont également données par le module au carré de ces amplitudes de probabilités. Ces amplitudes de probabilité sont donc également soumises à une condition de normalisation

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1 \quad (2.2)$$

afin que la somme des probabilités soit 100%.

Le système de deux qubits est donc, en apparence, très similaire à celui d'un seul qubit à la seule différence qu'il y a quatre résultats possibles à la mesure au lieu de seulement deux.

1. Notez que l'on place le premier qubit (**rouge**) le plus à droite pour suivre la convention de petit-boutisme (*little-endian*).

2. Nous arriverons à la même forme de manière plus rigoureuse un peu plus loin.

A.1 Vecteur d'état

L'état quantique à deux qubits à l'équation 2.1 fait intervenir quatre états de base. Le vecteur d'état pour un système de deux qubits est donc un vecteur à quatre composantes

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} \quad (2.3)$$

qui respectent la condition de normalisation à l'équation 2.2. Ce vecteur est écrit dans la base des états à deux qubits

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{et} \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \quad (2.4)$$

Exercice A.1 : Construction d'un état à deux qubits

Remplacez les vecteurs d'état pour les états de base dans l'équation 2.1 pour vérifier que le vecteur d'état est bien celui donné à l'équation 2.3.

Remarque

Lorsqu'on écrit un état quantique grâce à son vecteur d'état, il est important de garder en tête dans quelle base celui-ci est exprimé. Par exemple, les deux vecteurs d'état suivants

$$\begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} \alpha \\ \gamma \\ \beta \\ \delta \end{pmatrix}$$

pourraient représenter le même état, en fonction de quelle base est utilisée soit

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} \quad \text{ou} \quad \{|00\rangle, |10\rangle, |01\rangle, |11\rangle\}$$

Pour éviter toute confusion, on peut soit utiliser une notation explicite, mais généralement plus lourde, ou bien adhérer à une convention et la suivre à la lettre. Dans notre cas, nous utiliserons la convention où les états de base sont ordonnés en fonction des entiers qu'ils représentent (revoir la section ?? pour plus de précisions).

A.2 Produit tensoriel

Les vecteurs pour la base des états à deux qubits (équation 2.4) ont simplement été posés comme tels. On peut cependant les construire à partir des états de base à un qubit grâce à une opération : le produit tensoriel.

On note le produit tensoriel grâce au symbole \otimes . Par exemple, la définition de l'état de base à deux qubits où les deux qubits sont dans l'état $|0\rangle$ s'écrit

$$|00\rangle = |0\rangle \otimes |0\rangle.$$

En termes de vecteurs d'état le produit tensoriel de deux états s'effectue en multipliant le deuxième vecteur par chacune des composantes du premier et en assemblant un vecteur de plus grande dimension. Par exemple, le produit tensoriel précédent s'effectue de la manière suivante

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \times \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \times \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \times 1 \\ 1 \times 0 \\ 0 \times 1 \\ 0 \times 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \quad (2.5)$$

Le produit tensoriel permet donc de combiner les espaces de deux systèmes en un espace plus grand.

Exercice A.2 : Produit tensoriel et états de base à deux qubits

Combinez les deux états de base à un qubit en utilisant le produit tensoriel pour construire les quatre vecteurs d'état de base à deux qubits de l'équation 2.4.

Info notation A.1 : Produit tensoriel

Les trois expressions suivantes sont parfois utilisées pour le produit tensoriel de deux états quantiques (pour des qubits a et b) et sont jugées équivalentes

$$|0\rangle_b \otimes |1\rangle_a = |0\rangle_b |1\rangle_a = |01\rangle.$$

Aussi, il est parfois nécessaire d'annoter les états de base avec un indice afin de pouvoir identifier à quel qubit ils sont associés (par exemple : $|0\rangle_b$ ou $|1\rangle_a$). Dans bien des cas, il est cependant suffisant de conserver toujours le même ordre dans l'écriture pour arriver au même résultat. Ainsi, les notations suivantes sont également équivalentes

$$|0\rangle \otimes |1\rangle = |0\rangle |1\rangle = |01\rangle.$$

A.3 États produits (à deux qubits)

Le produit tensoriel s'applique à tous les états quantiques en général. Par exemple, considérons les états quantiques de deux qubits a et b respectivement

$$|a\rangle = a_0 |0\rangle_a + a_1 |1\rangle_a \quad \text{et} \quad |b\rangle = b_0 |0\rangle_b + b_1 |1\rangle_b \quad (2.6)$$

où les indices aux kets $|\cdot\rangle_a$ et $|\cdot\rangle_b$ permettent d'identifier les états de base pour chacun des qubits. Le produit tensoriel de ces deux états à un qubit génère l'état à deux qubits

$$|\psi\rangle = |b\rangle \otimes |a\rangle.$$

Si on remplace les expressions des états de l'équation 2.6 et que l'on distribue le produit tensoriel on obtient

$$\begin{aligned} |\psi\rangle &= (b_0 |0\rangle_b + b_1 |1\rangle_b) \otimes (a_0 |0\rangle_a + a_1 |1\rangle_a) \\ &= b_0 a_0 |0\rangle_b \otimes |0\rangle_a + b_0 a_1 |0\rangle_b \otimes |1\rangle_a + b_1 a_0 |1\rangle_b \otimes |0\rangle_a + b_1 a_1 |1\rangle_b \otimes |1\rangle_a \\ &= b_0 a_0 |00\rangle + b_0 a_1 |01\rangle + b_1 a_0 |10\rangle + b_1 a_1 |11\rangle \end{aligned} \quad (2.7)$$

ou encore en notation vectorielle

$$|\psi\rangle = |b\rangle \otimes |a\rangle = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \otimes \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} b_0 \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \\ b_1 \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} b_0 a_0 \\ b_0 a_1 \\ b_1 a_0 \\ b_1 a_1 \end{pmatrix}. \quad (2.8)$$

Un tel état construit comme le produit tensoriel des états de deux sous-systèmes est appelé un état produit.

Lorsque les états quantiques de deux systèmes quantiques (par exemple deux qubits) sont indépendants (par exemple s'ils sont isolés l'un de l'autre) l'état quantique qui décrit l'ensemble du système s'appelle un état produit. On dit aussi que l'état du système est factorisable. Les états produits ne constituent qu'un sous-ensemble de tous les états quantiques possibles. Un état quantique qui ne peut pas être écrit comme le produit de deux états est appelé un état intriqué.

Exercice A.3 : Probabilités pour un état produit

Montrez que la probabilité de mesurer le qubit a dans l'état $|0\rangle$ et le qubit b dans l'état $|1\rangle$ (à l'équation 2.6) est la même que de mesurer le système de deux qubits (à l'équation 2.7) dans l'état $|10\rangle$. Refaites le même exercice pour les trois autres résultats possibles.

Exercice A.4 : Normalisation d'un état produit

Montrez que si les états à un qubits à l'équation 2.6 sont normalisés, l'état produit à deux qubits à l'équation 2.7 l'est aussi.

A.4 Intrication

L'expression à l'équation 2.3 est plus générale que celle à l'équation 2.8. En effet, l'équation 2.3 permet de décrire des états quantiques à deux qubits que l'équation 2.8 ne peut pas décrire. Par exemple l'état

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \quad (2.9)$$

ne peut pas être construit à partir de deux états à un qubit. En d'autres mots, les états produits sont un sous-ensemble de tous les états quantiques possibles.

Exercice A.5 : Factorisation impossible

Essayez de factoriser l'état de l'équation 2.9. C'est-à-dire essayez de le décomposer sous la forme $|\phi^+\rangle = |b\rangle|a\rangle$ avec

$$|a\rangle = a_0|0\rangle + a_1|1\rangle \text{ et } |b\rangle = b_0|0\rangle + b_1|1\rangle$$

et montrez mathématiquement que cela est impossible.

Les états qui ne peuvent pas être factorisés (comme celui à l'équation 2.9) sont dits *intriqués*. L'intrication quantique apparaît lorsqu'au moins deux objets quantiques (comme des qubits) formant un système quantique ne peuvent pas être décrits indépendamment. On peut voir l'intrication comme le fait que c'est le système quantique dans son ensemble qui est en superposition d'états et pas seulement les éléments qui le composent !

Après la superposition (section A.1), l'intrication est le deuxième phénomène quantique à la base du calcul quantique que nous rencontrons.

On parle aussi de corrélations quantiques, car lorsque les qubits participants à un état intriqué seront mesurés, les résultats sur chacun d'eux seront corrélés. Cela veut dire que le résultat de mesure sur le premier qubit détermine le résultat de mesure du second et vice versa. Autrement dit, si on acquiert de l'information sur l'état d'un des qubits qui participent à un état intriqué, on acquiert également de l'information sur le reste du système. Voir l'exemple A.2 pour plus de détails.

A.5 Mesure d'états à deux qubits

Pour un état quantique à deux qubits quelconque écrit sous la forme

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

la probabilité d'obtenir 0 et 0 après la mesure des deux qubits est donnée par $|\alpha|^2$, la probabilité d'obtenir 0 et 1 (dans cet ordre) est $|\beta|^2$, et ainsi de suite. On peut donc résumer ces probabilités par

$$p_{00} = |\alpha|^2 \quad p_{01} = |\beta|^2 \quad p_{10} = |\gamma|^2 \quad p_{11} = |\delta|^2.$$

La mesure partielle

Il est cependant possible de mesurer un seul des deux qubits. On parle alors d'une mesure partielle du système quantique. Cela permet de répondre à la question : quelle est la probabilité d'obtenir le résultat 0 si on mesure seulement le qubit de droite ? Notons cette probabilité $p_{\bullet 0}$ pour insister sur le fait qu'on ne mesure pas le qubit de gauche. Dans ce cas, on doit considérer tous les états de base où le qubit de droite

dans l'état $|0\rangle$. La probabilité est la somme des probabilités associée à chacun de ces états. La probabilité de mesurer le qubit de droite dans l'état 0 est donc

$$p_{\bullet 0} = |\alpha|^2 + |\gamma|^2$$

et celle de le mesurer dans l'état 1 est

$$p_{\bullet 1} = |\beta|^2 + |\delta|^2.$$

La mesure d'un système quantique projette le système dans l'état quantique associé au résultat obtenu. La mesure partielle projette uniquement le sous-système qui a été mesuré, ici le qubit de droite. Par exemple, si le résultat obtenu précédemment est 0, le système est projeté dans un état quantique proportionnel à

$$|\psi^{(0)}\rangle \propto \alpha |00\rangle + \gamma |10\rangle$$

où on ne conserve que les états quantiques qui correspondent au résultat obtenu. Le symbole de proportionnalité est nécessaire, car les composantes α et γ ne définissent pas un état normalisé. On peut cependant effectuer une normalisation pour écrire

$$|\psi^{(0)}\rangle = \frac{\alpha |00\rangle + \gamma |10\rangle}{(|\alpha|^2 + |\gamma|^2)^{1/2}}$$

Similairement, si le résultat de la mesure est 1, l'état du système est alors projeté dans

$$|\psi^{(1)}\rangle = \frac{\beta |01\rangle + \delta |11\rangle}{(|\beta|^2 + |\delta|^2)^{1/2}}$$

Exemple A.1 : La mesure partiel d'un état produit

Pour un état produit, les deux qubits peuvent être considérés comme étant des systèmes indépendants. Vérifions que la mesure partielle est cohérente avec cela. Considérons donc l'état produit $|b\rangle \otimes |a\rangle$ écrit à l'équation 2.8

$$|\psi\rangle = b_0 a_0 |00\rangle + b_0 a_1 |01\rangle + b_1 a_0 |10\rangle + b_1 a_1 |11\rangle.$$

La probabilité d'obtenir 0 lors d'une mesure partielle du qubit de droite est donnée par

$$p_{\bullet 0} = |b_0 a_0|^2 + |b_1 a_0|^2 = (|b_0|^2 + |b_1|^2) |a_0|^2$$

où on a pu mettre $|a_0|^2$ en évidence. Comme l'état du qubit $|b\rangle$ est normalisé, on retrouve donc

$$p_{\bullet 0} = |a_0|^2$$

qui n'est rien d'autre que la probabilité d'obtenir 0 lors de la mesure du qubit $|a\rangle$ si on l'avait considéré indépendamment. L'état quantique résultant de cette mesure est alors

$$|\psi^{(0)}\rangle = \frac{b_0 a_0 |00\rangle + b_1 a_0 |10\rangle}{(|b_0 a_0|^2 + |b_1 a_0|^2)^{1/2}}.$$

En procédant à diverses simplifications on peut réécrire cet état simplement comme,

$$|\psi^{(0)}\rangle = (b_0 |0\rangle + b_1 |1\rangle) \otimes |0\rangle.$$

qui n'est rien d'autre que l'état produit où l'état du qubit $|b\rangle$ est inchangé et où l'état du qubit $|a\rangle$ a été projeté dans l'état 0.

Exemple A.2 : La mesure d'un état intriqué

Supposons qu'on prépare un système de deux qubits dans l'état $|\Phi^+\rangle$ de l'équation 2.9 et qu'on procède à la mesure du qubit de droite. Les probabilités d'obtenir 0 et 1 sont données par

$$p_{\bullet 0} = \frac{1}{2} \quad \text{et} \quad p_{\bullet 1} = \frac{1}{2}.$$

Les états quantiques résultants (renormalisés) dans ces deux cas sont

$$|\psi^{(0)}\rangle = |00\rangle \quad \text{et} \quad |\psi^{(1)}\rangle = |11\rangle$$

Ainsi, après la mesure, le système sera soit dans l'état $|00\rangle$ si on a mesuré 0, soit dans l'état $|11\rangle$ si on a mesuré 1. Le résultat de la mesure du second qubit est alors déjà déterminé. Si on le mesure, on constatera que les résultats des deux mesures sont toujours identiques.

Insistons sur le fait que le résultat de la première mesure est aléatoire, mais détermine ici complètement le résultat de la seconde.

A.6 États quantiques notables (à deux qubits)

Décrivons quelques états quantiques à deux qubits qui reviennent régulièrement en calcul quantique.

Superposition uniforme

L'état en superposition uniforme pour deux qubits est un état où toutes les amplitudes de probabilités sont égales. Cet état est donc,

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

où chaque état de base a une chance sur 4 (25%) d'être observé.

Exercice A.6 : États de superposition uniforme à deux qubits

Montrez que l'état de superposition uniforme à deux qubits est un état produit

$$|q_1\rangle \otimes |q_0\rangle$$

et déterminez les états à un qubit $|q_0\rangle$ et $|q_1\rangle$ qui le constituent.

Les paires de Bell

L'état 2.9 qu'on a utilisé pour illustrer l'intrication est aussi appelé *la première paire de Bell*. On peut identifier quatre paires de Bell, aussi appelées états de Bell,

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle & |\Phi^-\rangle &= \frac{1}{\sqrt{2}} |00\rangle - \frac{1}{\sqrt{2}} |11\rangle \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}} |01\rangle + \frac{1}{\sqrt{2}} |10\rangle & |\Psi^-\rangle &= \frac{1}{\sqrt{2}} |01\rangle - \frac{1}{\sqrt{2}} |10\rangle. \end{aligned} \tag{2.10}$$

Tous ces états sont des états intriqués. En fait, il s'agit des états à deux qubits maximalement intriqués. Chaque état de Bell est orthogonal aux autres états de Bell.

Exercice A.7 : Paires de Bell orthogonales

Montrez que l'état de Bell $|\Phi^+\rangle$ est orthogonal aux trois autres états de Bell.

Remarque

Notez que comme les quatre états de base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, les quatre états de Bell peuvent également être utilisés comme une base canonique pour les états à deux qubits. En d'autres mots, n'importe quel état à deux qubits peut être exprimé comme une combinaison linéaire

$$|\psi\rangle = \alpha' |\Phi^+\rangle + \beta' |\Phi^-\rangle + \gamma' |\Psi^+\rangle + \delta' |\Psi^-\rangle$$

où les composantes α' , β' , γ' et δ' respectent une condition de normalisation. Cela est possible, car les états de Bell sont normalisés et mutuellement orthogonaux.

B Portes quantiques à deux qubits

Pour préparer des états quantiques à deux qubits qui ne sont pas de simples états produits, nous aurons besoin d'outils qui font interagir les qubits : des portes à deux qubits.

Une porte à 2 qubits permet de modifier un système de 2 qubits. Comme un tel système comporte 4 vecteurs de base (équation 2.4), une porte à deux qubits est représentée par une matrice 4×4

$$\hat{P} = \begin{pmatrix} P_{00} & P_{01} & P_{02} & P_{03} \\ P_{10} & P_{11} & P_{12} & P_{13} \\ P_{20} & P_{21} & P_{22} & P_{23} \\ P_{30} & P_{31} & P_{32} & P_{33} \end{pmatrix}.$$

Ce qui distingue les portes quantiques à deux qubits de celles à un qubit est simplement le nombre de dimensions de l'espace dans lequel elles agissent. Ainsi, l'application d'une porte quantique à deux qubits s'effectue comme pour une porte quantique à un qubit

$$|\psi'\rangle = \hat{P} |\psi\rangle$$

où $|\psi\rangle$ est l'état initial du système de deux qubits et $|\psi'\rangle$, son état final. De plus, comme les portes à un qubit et toutes les autres portes quantiques, les portes à deux qubits doivent également être unitaires afin de préserver la normalisation des états quantiques qu'elles transforment.

B.1 Diagramme

En représentation diagrammatique, la porte quantique à deux qubits apparaît comme une boîte qui agit sur deux qubits et qui recouvre les deux lignes horizontales associées à ces deux qubits, comme illustrés à la figure 2.1a. Chaque ligne horizontale représente l'évolution de chaque qubit et elles sont généralement numérotées à partir de 0 pour la ligne du haut de sorte que la porte à deux qubits agit sur les états de base $|q_1 q_0\rangle$.

Certaines portes quantiques à deux qubits utilisent des diagrammes différents (figures 2.1b à 2.1e). Cependant, dans tous les cas, ces diagrammes impliquent toujours deux qubits.

B.2 Portes contrôlées

De nombreuses portes à deux qubits sont en fait des versions dites *contrôlées* de portes à un qubit. Pour ce type de porte à deux qubits, un des qubits est le *qubit de contrôle* et l'autre est le *qubit cible*. Le principe d'une porte contrôlée s'exprime ainsi : une porte à un qubit est appliquée au qubit cible si le qubit de contrôle est dans l'état $|1\rangle$, et ne fait rien si le qubit de contrôle est dans l'état $|0\rangle$.

Malgré cette description, insistons sur le fait que le qubit de contrôle n'a pas besoin d'être mesuré afin de déterminer si la porte à un qubit est appliquée sur le qubit cible. La porte contrôlée ne mesure pas le qubit de contrôle, mais va plutôt appliquer *et* ne pas appliquer la porte à un qubit *en même temps*, et ce, en fonction de l'état de superposition du qubit de contrôle.

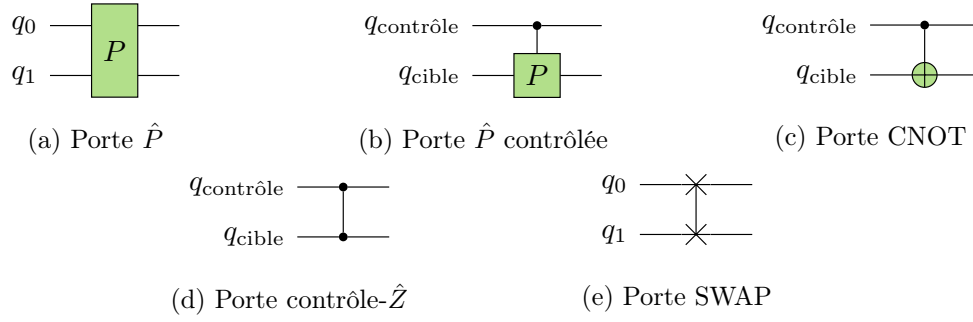


FIGURE 2.1 – Représentations diagrammatiques de portes quantiques à deux qubits. Ces représentations seront utilisées pour construire des circuits quantiques.

En règle générale, on peut générer un état à deux qubits intriqués en appliquant une porte contrôlée à partir d'un qubit de contrôle qui est dans un état de superposition.

Info notation B.1 : Les portes contrôlées

Il existe de nombreuses notations pour les portes contrôlées. Nous allons utiliser la notation suivante pour une porte \hat{P} appliquée au qubit q_{cible} et contrôlée par le qubit $q_{\text{contrôle}}$

$$C\hat{P}_{q_{\text{cible}}q_{\text{contrôle}}}.$$

Par exemple, la porte CNOT appliquée au qubit 1 à partir du qubit 0 s'écrit $C\hat{X}_{10}$. Pour alléger l'écriture, on omet parfois les indices des qubits. Dans ce cas, on suppose un système de deux qubits dans l'ordre suivant

$$|q_{\text{cible}}, q_{\text{contrôle}}\rangle.$$

On illustre les portes quantiques contrôlées comme à la figure 2.1b. Selon ce diagramme, la porte contrôlée ressemble à une porte quantique à un qubit appliquée sur le qubit cible (une boîte qui recouvre la ligne associée au qubit cible), à la différence que son application est contrôlée par le qubit de contrôle (la boîte est reliée par une ligne connectée à la ligne associée au qubit de contrôle).

Exemple B.1 : La porte contrôle- \hat{X}

Un bon exemple de porte contrôlée est la porte contrôle- \hat{X} aussi nommée CNOT. Comme son nom l'indique, cette porte applique un \hat{X} sur le qubit cible si le qubit de contrôle est dans l'état $|1\rangle$. Explicitons comment cette porte transforme chacun des états de base à deux qubits

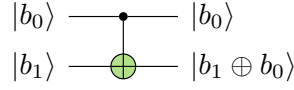
$$C\hat{X}|00\rangle = |00\rangle \quad C\hat{X}|01\rangle = |11\rangle \quad C\hat{X}|10\rangle = |10\rangle \quad C\hat{X}|11\rangle = |01\rangle.$$

En termes vectoriels, la porte CNOT transforme les quatre vecteurs de base (dans la base habituelle de l'équation 2.4) de la manière suivante

$$C\hat{X} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C\hat{X} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad C\hat{X} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad C\hat{X} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

La forme matricielle de cette porte est donc

$$C\hat{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

FIGURE 2.2 – La porte contrôle- \hat{X} agit comme une fonction XOR.

B.3 Quelques portes quantiques à deux qubits

La porte contrôle- \hat{X}

Cette porte, illustrée à la figure 2.1c est une version contrôlée de la porte \hat{X} , c'est-à-dire qu'elle applique une porte \hat{X} au qubit cible si le qubit de contrôle est dans l'état $|1\rangle$. On a déjà établi à l'exemple B.1 que la matrice qui représente cette porte à deux qubits est

$$C\hat{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Comme la porte \hat{X} , la porte contrôle- \hat{X} est sa propre inverse.

Fait intéressant, la porte contrôle- \hat{X} agit comme une fonction XOR (voir la section ?? au besoin) qui combine les états des qubits de contrôle et cible et les retourne sur le qubit cible, laissant le qubit de contrôle inchangé, comme illustré à la figure 2.2.

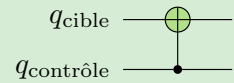
Exercice B.1 : Porte contrôle- \hat{X} vers le haut

La porte contrôle- \hat{X} est généralement définie de sorte que le qubit de contrôle est celui du haut et le qubit cible est celui du bas

$$|q_1, q_0\rangle = |q_{\text{cible}}, q_{\text{contrôle}}\rangle.$$

On peut spécifier l'ordre de ces qubits en écrivant $C\hat{X}_{\text{cible,contrôle}}$. Déduisez la matrice pour la porte $C\hat{X}_{01}$ où le qubit de contrôle est le qubit du bas

$$|q_1, q_0\rangle = |q_{\text{contrôle}}, q_{\text{cible}}\rangle.$$



La porte contrôle- \hat{Z}

Cette porte applique une porte \hat{Z} au qubit cible si le qubit de contrôle est dans l'état $|1\rangle$. Or, comme la porte \hat{Z} n'a pas d'effet si le qubit cible est dans l'état $|0\rangle$, cette porte agit uniquement si les deux qubits sont dans l'état $|1\rangle$, c'est-à-dire si le système est dans l'état $|11\rangle$. Dans ce cas, la phase de l'état est inversée, alors que rien ne se produit pour tous les autres états de base. Comme l'effet de la porte \hat{Z} est d'inverser la phase, la forme matricielle de cette porte se déduit facilement comme étant

$$C\hat{Z} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Cette porte apparaît donc comme symétrique par rapport au qubit de contrôle et au qubit cible, d'où sa représentation diagrammatique illustrée à la figure 2.1d.

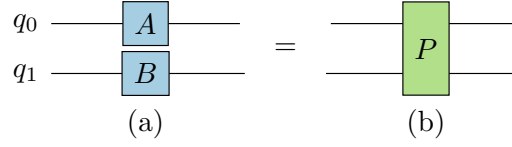


FIGURE 2.3 – L’application de portes quantiques à un qubit sur deux qubits peut être vue comme une seule porte à deux qubits.

Exercice B.2 : Porte contrôlée par $|0\rangle$

Il est parfois utile d’appliquer une porte contrôlée par l’état $|0\rangle$, c’est-à-dire que la porte est appliquée sur le qubit cible seulement si le qubit de contrôle est dans l’état $|0\rangle$ (la porte n’est pas appliquée s’il est dans l’état $|1\rangle$). Il est possible de construire une porte contrôlée par l’état $|1\rangle$ en *habillant* une porte contrôlée, c’est-à-dire en appliquant des portes avant et après celle-ci. Dessinez le circuit qui permet de faire cela.

La porte SWAP

Il est parfois nécessaire de transporter l’état d’un qubit vers un autre. Comme les portes quantiques sont unitaires, il est uniquement possible d’échanger les états quantiques entre deux qubits. Cette opération s’effectue grâce à une porte SWAP. En termes des états de base, l’échange de deux qubits n’affecte pas les états $|00\rangle$ et $|11\rangle$, mais échange les coefficients associés aux états $|01\rangle$ et $|10\rangle$, d’où la représentation matricielle suivante

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

La figure 2.1e illustre une porte SWAP.

Exercice B.3 : Construction d’une porte SWAP

Montrez qu’on peut construire une porte SWAP en assemblant trois CNOT consécutifs de la manière suivante :



B.4 Portes à un qubit pour un système de deux qubits

Supposons que l’on applique des portes à un qubit \hat{A} et \hat{B} sur deux qubits (q_0 et q_1) qui font partie d’un système de deux qubits comme c’est illustré à la figure 2.3a. Comment cela affecte-t-il l’état à deux qubits du système ? Comment construit-on une porte à deux qubits (figure 2.3b) qui aurait le même effet ?

Pour répondre à ces deux questions, commençons par considérer deux qubits, respectivement dans des états $|a\rangle$ et $|b\rangle$. Notons l’état initial à deux qubits comme le produit tensoriel de ces deux états à un qubit

$$|\psi\rangle = |b\rangle \otimes |a\rangle. \quad (2.11)$$

Ensuite, appliquons la porte \hat{A} sur q_0 et \hat{B} sur q_1 de manières séparées. Cela transforme les deux états à un qubit en

$$|a'\rangle = \hat{A}|a\rangle \quad \text{et} \quad |b'\rangle = \hat{B}|b\rangle.$$

L’état final à deux qubits est le produit tensoriel de ces deux états

$$|\psi'\rangle = |b'\rangle \otimes |a'\rangle = (\hat{B}|b\rangle) \otimes (\hat{A}|a\rangle).$$

On cherche à exprimer cet état final en fonction de l'état initial à deux qubits. En d'autres termes on veut construire une porte \hat{P} telle que

$$|\psi'\rangle = \hat{P} |\psi\rangle \quad (2.12)$$

Les propriétés du produit tensoriel nous permettent d'écrire

$$|\psi'\rangle = (\hat{B} |b\rangle) \otimes (\hat{A} |a\rangle) = (\hat{B} \otimes \hat{A})(|b\rangle \otimes |a\rangle). \quad (2.13)$$

Alors que le produit tensoriel permet d'unir les états $|a\rangle$ et $|b\rangle$ en un état à deux qubits, il permet également d'unir les opérateurs \hat{A} et \hat{B} en un opérateur à deux qubits. En combinant, les équations 2.11, 2.12 et 2.13, on déduit alors que

$$\hat{P} = \hat{B} \otimes \hat{A}. \quad (2.14)$$

L'opérateur \hat{P} agit sur un espace à deux qubits en appliquant l'opérateur \hat{A} dans l'espace du qubit q_0 et l'opérateur \hat{B} dans l'espace du qubit q_1 .

En termes matriciels, le produit tensoriel à l'équation 2.14 permet de construire la matrice 4×4 représentant l'opérateur \hat{P} à partir des matrices 2×2 représentant les opérateurs \hat{A} et \hat{B} . Ainsi, avec

$$\hat{A} = \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix} \quad \text{et} \quad \hat{B} = \begin{pmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{pmatrix}$$

la matrice qui représente \hat{P} peut être construite de la manière suivante

$$\hat{P} = \begin{pmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{pmatrix} \otimes \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix} = \begin{pmatrix} B_{00} \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix} & B_{01} \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix} \\ B_{10} \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix} & B_{11} \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix} \end{pmatrix} \quad (2.15)$$

et on obtient la forme générale

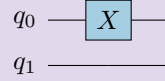
$$\hat{P} = \begin{pmatrix} B_{00}A_{00} & B_{00}A_{01} & B_{01}A_{00} & B_{01}A_{01} \\ B_{00}A_{10} & B_{00}A_{11} & B_{01}A_{10} & B_{01}A_{11} \\ B_{10}A_{00} & B_{10}A_{01} & B_{11}A_{00} & B_{11}A_{01} \\ B_{10}A_{10} & B_{10}A_{11} & B_{11}A_{10} & B_{11}A_{11} \end{pmatrix}.$$

Remarque

Notez comment la construction de la matrice représentant l'opérateur à deux qubits \hat{P} à l'aide du produit tensoriel à l'équation 2.15 est cohérente avec la construction du vecteur d'état pour un système de deux qubits présentée à l'équation 2.5.

Exemple B.2 : Application d'une porte à un qubit sur un système à deux qubits

Illustrons le produit tensoriel d'opérateurs à un qubit en construisant la matrice 4×4 représentant le circuit à deux qubits suivant.



L'absence d'opération sur le qubit q_1 est équivalente à l'utilisation de la porte identité \hat{I} . Ainsi, la porte à deux qubits équivalente au circuit précédent est donc

$$\hat{I} \otimes \hat{X}$$

La matrice 4×4 qui applique ces opérations se construit donc de la manière suivante

$$\hat{P} = \hat{I} \otimes \hat{X} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 0 \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ 0 \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 1 \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Appliquons l'opération $\hat{I} \otimes \hat{X}$ à l'état $|00\rangle$ pour vérifier la validité de cette matrice. D'abord, son effet sur l'état initial devrait être d'inverser l'état du qubit de droite

$$\hat{I} \otimes \hat{X} |00\rangle = \hat{I} |0\rangle \otimes \hat{X} |0\rangle = |01\rangle$$

ce qui correspond au deuxième vecteur de base. L'application de la matrice représentant cette opération sur le premier vecteur de base

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

retourne effectivement le deuxième vecteur de base. On peut ensuite répéter la même procédure pour chacun des trois autres états de base.

Info notation B.2 : Produit tensoriel de portes

Comme pour les états quantiques, les portes quantiques issues d'un produit tensoriel peuvent être écrites en utilisant différentes notations. Les notations suivantes sont équivalentes

$$\hat{Z}_b \otimes \hat{X}_a |0\rangle_b \otimes |1\rangle_a = \hat{Z}_b \hat{X}_a |0\rangle_b |1\rangle_a = \hat{Z} \otimes \hat{X} |01\rangle = \hat{Z} \hat{X} |01\rangle.$$

Dans les deux dernières expressions, l'ordre des portes quantique permet d'identifier avec un minimum de notation à quel qubit chaque porte est appliquée.

Cependant, cette notation est susceptible de créer de la confusion. En effet, prise hors contexte on pourrait penser qu'il s'agit du produit entre les \hat{Z} et \hat{X} , alors qu'en réalité ces deux opérations sont appliquées sur deux qubits différents. Elle est néanmoins régulièrement utilisée dans certains contextes qui ne laissent pas de place à l'ambiguïté. En cas de doute, il est préférable d'identifier les qubits et les opérations qui s'y appliquent.

Dans la notation la plus compact, le nombre de portes devrait donc toujours correspondre au nombre de qubits. Si un qubit reste inchangé, l'utilisation de la porte identité permet de le spécifier. Par exemple,

$$\hat{Z}_b |0\rangle_b |1\rangle_a = \hat{Z} \hat{I} |01\rangle.$$

Exercice B.4 : Produits tensoriels de portes quantiques

Construisez les matrices 4×4 qui représentent les opérations construites à partir de portes à un qubits suivantes :

(a) $\hat{X} \hat{X}$

(b) $\hat{Z} \hat{Z}$

(c) $\hat{Z} \hat{X}$

(d) $\hat{I} \hat{H}$

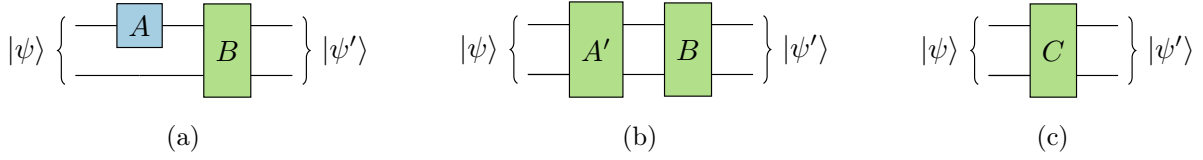


FIGURE 2.4 – La composition d’une porte quantique à un qubit avec une porte quantique à deux qubits (a) nécessite d’abord de réécrire la porte à un qubit comme une porte à deux qubits (b). Ensuite la composition des portes à deux qubits peut s’effectuer afin d’obtenir la porte quantique à deux qubits équivalente (c).

B.5 Composition de portes quantiques

Avec l’objectif de pouvoir décrire comment un circuit quantique transforme l’état quantique d’un système de qubit, il est essentiel de comprendre comment on peut composer des portes quantiques à un et deux qubits. Par exemple, le circuit quantique à la figure 2.4a transforme un état quantique initial à deux qubits $|\psi\rangle$ en un état quantique final $|\psi'\rangle$ en y appliquant successivement une porte à un qubit et une porte à deux qubits.

Afin de composer la porte \hat{A} avec la porte \hat{B} on doit d’abord obtenir une porte à deux qubits \hat{A}' équivalente à l’application de la porte \hat{A} . En d’autres mots, on doit construire une porte \hat{A}' qui agit sur un système de deux qubits de manière à appliquer \hat{A} sur le premier et à laisser le second inchangé. Cela peut être fait à l’aide d’un produit tensoriel avec l’identité (voir l’exemple B.2)

$$\hat{A}' = \hat{I} \otimes \hat{A}.$$

L’état quantique à deux qubits final peut alors être obtenu en composant les deux portes à deux qubits comme à la figure 2.4b

$$|\psi'\rangle = \hat{B}\hat{A}'|\psi\rangle.$$

Comme pour les portes à un qubit (voir la section B.5), on peut composer des portes à deux qubits pour obtenir une porte quantique équivalente (figure 2.4c) qui, lorsqu’appliquée à l’état $|\psi\rangle$, donne directement $|\psi'\rangle$. Cette porte est construite grâce au produit matriciel

$$\hat{C} = \hat{B}\hat{A}'$$

de sorte que

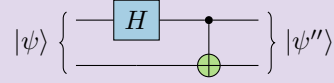
$$|\psi'\rangle = \hat{C}|\psi\rangle.$$

Bien qu’on ait ici réussi à composer deux portes à un et deux qubits respectivement, la même approche pourra être appliquée afin de composer des portes quantiques agissant sur des nombres différents de qubits. La stratégie sera toujours d’utiliser le produit tensoriel avec l’identité afin d’équilibrer le nombre de qubits de deux portes.

On constate qu’il est toujours possible de composer les portes quantiques entre elles pour combiner leurs actions en une seule porte quantique. Ultimement, il est toujours possible de résumer l’effet de la portion unitaire d’un circuit quantique de n qubits comme une seule porte quantique à n qubits.

Exemple B.3 : Composition de portes à un et deux qubits

Voyons comment on peut combiner les portes du circuit présenté à la figure 2.6b pour obtenir la matrice qui représente l'application de celui-ci.



On obtient d'abord la porte à deux qubits équivalente à l'application de la porte Hadamard au premier qubit. On effectue donc le produit tensoriel suivant

$$\hat{I} \otimes \hat{H} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

La porte quantique à deux qubits équivalente au circuit complet est obtenue en effectuant le produit matriciel entre cette dernière et la matrice de la porte CNOT. On obtient ainsi,

$$C\hat{X} \times (\hat{I}\hat{H}) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \end{pmatrix}.$$

C Circuits quantiques

Du moment qu'on a accès à au moins deux qubits sur lesquels on peut appliquer des portes à un ou deux qubits, il devient intéressant de construire des circuits quantiques. La figure 2.6 illustre des circuits quantiques très simples qui n'impliquent que deux qubits.

De manière plus générale, un circuit quantique est une séquence de portes quantiques qui modifie l'état d'un système de plusieurs qubits. On l'illustre d'abord comme une série de lignes horizontales, chacune représentant un qubit, sur lesquelles des portes quantiques sont appliquées en utilisant les représentations diagrammatiques introduites aux sections B.2 et B.1. Lors de l'exécution d'un tel circuit les opérations qui sont appliquées sur les qubits de la gauche vers la droite. L'état initial des qubits (à l'extrême gauche) est parfois spécifié. Dans le cas contraire, on suppose généralement que tous les qubits sont initialement dans l'état $|0\rangle$. En règle générale, les qubits sont mesurés à la fin du circuit (à l'extrême droite). Parfois, seulement un sous-ensemble de tous les qubits est mesuré.

C.1 Effet d'un circuit quantique

Lors de l'exécution d'un circuit quantique, les différentes portes quantiques sont appliquées au système de qubits pour produire un certain état quantique qui pourra ensuite être mesuré. Pour connaître l'état quantique juste avant la mesure, il est nécessaire d'appliquer les différentes portes quantiques à partir de l'état quantique initial. L'exemple suivant démontre comment obtenir l'état quantique produit par le circuit de la figure 2.6b.

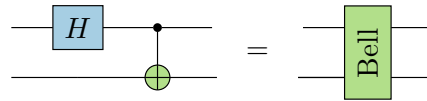


FIGURE 2.5 – Encapsulation du circuit quantique de préparation des états de Bell en une porte à deux qubits.

Exemple C.1 : L'effet d'un circuit quantique

À priori, l'état quantique initial pour le circuit à la figure 2.6b est l'état $|00\rangle$, ce qui correspond, dans la base computationnelle au vecteur d'état

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

La matrice qui représente l'action de ce circuit a été construite à l'exemple B.3. L'état quantique qui est produit par ce circuit s'obtient en effectuant le produit

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

L'état quantique ainsi produit peut également s'écrire comme

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Exercice C.1 : Préparation des quatre états de Bell

Montrez qu'il est possible de préparer les quatre états de Bell (équation 2.10) en appliquant le circuit quantique de la figure 2.6b aux quatre états de base à deux qubits.

C.2 Représentation matricielle

Les circuits quantiques utilisés dans les algorithmes quantiques sont généralement assez complexes. Pour aider à leur construction et les rendre plus faciles à comprendre, ils peuvent être décomposés en plusieurs circuits quantiques sous la forme de sous-routines. Il est alors pratique d'encapsuler ces sous-routines sous la forme de portes quantiques à plusieurs qubits. Ces sous-routines peuvent faire intervenir tous les qubits ou seulement un sous-ensemble.

Pour ces circuits quantiques de sous-routines, l'état initial des qubits n'est généralement pas spécifié, car il dépend du reste du circuit qui le précède. Également, à moins qu'il ne s'agisse d'une sous-routine de mesure, un tel circuit ne comporte pas de mesure à la fin. Par exemple, le circuit de préparation de paires de Bell peut être encapsulé dans une porte à deux qubits, comme c'est illustré à la figure 2.5.

C.3 Quelques circuits quantiques à deux qubits

Introduisons deux circuits quantiques notables, soit le circuit de préparation de superposition uniforme et le circuit de préparation de paires de Bell.



FIGURE 2.6 – Circuits quantiques à deux qubits notables : (a) préparation d’une superposition uniforme à deux qubits, (b) préparation d’une paire de Bell.

Circuit de superposition uniforme

On a introduit, à la section A.6, l’état de superposition uniforme à deux qubits. Le circuit qui permet de préparer cet état à partir de l’état initial $|00\rangle$ est illustré à la figure 2.6a. On constate que chaque qubit est alors placé dans l’état $|+\rangle$ et que l’état de superposition uniforme à deux qubits est l’état produit $|+\rangle \otimes |+\rangle$.

Nous allons voir au chapitre suivant que ce circuit se généralise facilement à plus de deux qubits et permet toujours de préparer une superposition uniforme de tous les états de base pour des systèmes de n qubits.

Exercice C.2 : Superposition uniforme à deux qubits

- Construisez la matrice 4×4 qui représente l’effet du circuit de préparation d’une superposition uniforme à deux qubits (figure 2.6a).
- Montrez que son application à l’état initial $|00\rangle$ permet de préparer l’état de superposition uniforme à deux qubits.
- Comment diffère l’état préparé si l’état initial est un autre état de base à deux qubits ($|01\rangle$, $|10\rangle$ ou $|11\rangle$) ?

Circuit de préparation de paires de Bell

Nous avons déjà introduit le circuit de préparation de paires de Bell, reproduit à la figure 2.6b. En utilisant ce circuit à partir d’un des quatre états de base à deux qubits, on arrive à préparer respectivement un des quatre états de Bell (voir équation 2.10). Ce circuit peut donc être vu comme une transformation depuis les états de base à deux qubits vers les états de Bell

$$\begin{aligned} |00\rangle &\rightarrow |\Phi^+\rangle & |01\rangle &\rightarrow |\Phi^-\rangle \\ |10\rangle &\rightarrow |\Psi^+\rangle & |11\rangle &\rightarrow |\Psi^-\rangle. \end{aligned}$$

Exercice C.3 : Circuit de Bell inverse

Trouvez le circuit quantique qui permet de transformer les états de Bell en états de base à deux qubits tel que

$$\begin{aligned} |\Phi^+\rangle &\rightarrow |00\rangle & |\Phi^-\rangle &\rightarrow |01\rangle \\ |\Psi^+\rangle &\rightarrow |10\rangle & |\Psi^-\rangle &\rightarrow |11\rangle. \end{aligned}$$

S Solutions aux exercices

Exercice A.3 : Probabilités pour un état produit

Pour vérifier qu'un état produit décrit bien un système de deux qubits indépendants, on peut vérifier que les probabilités d'obtenir les différents résultats lors des mesures des deux qubits sont cohérentes.

Par exemple, calculons la probabilité d'observer les deux qubits dans l'état 0. D'abord les probabilités d'obtenir 0 pour chacun des qubits isolés sont

$$p_0^{(a)} = |a_0|^2 \quad \text{et} \quad p_0^{(b)} = |b_0|^2.$$

La probabilité d'obtenir ces deux résultats est le produit de ces probabilités

$$p_{00} = p_0^{(b)} p_0^{(a)} = |b_0|^2 |a_0|^2 = |b_0 a_0|^2$$

ce qui correspond bien à la probabilité d'obtenir l'état $|00\rangle$ pour l'état produit de deux qubits à l'équation 2.7. De manière analogue, les probabilités d'obtenir les trois autres résultats possibles sont bien

$$p_{01} = |b_0 a_1|^2, \quad p_{10} = |b_1 a_0|^2 \quad \text{et} \quad p_{11} = |b_1 a_1|^2.$$

L'état produit de l'équation 2.7 permet donc d'obtenir les mêmes probabilités de mesure que si on considère les 2 qubits indépendamment.

Exercice A.5 : Factorisation impossible

La factorisation de l'état 2.9 dans des états à 1 qubit $|a\rangle$ et $|b\rangle$ impliquerait de pouvoir résoudre les équations suivantes

$$\begin{aligned} a_0 b_0 &= \frac{1}{\sqrt{2}} & a_1 b_1 &= \frac{1}{\sqrt{2}} \\ a_0 b_1 &= 0 & a_1 b_0 &= 0. \end{aligned}$$

Les équations du haut nécessitent qu'aucune composante ne soit nulle, alors que les équations du bas impliquent qu'au moins 2 d'entre elles soient nulles!

Exercice B.4 : Produits tensoriels de portes quantiques

(a)

$$\hat{X}\hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 1 \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ 1 \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 0 \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

(b)

$$\hat{Z}\hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & 0 \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ 0 \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & -1 \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

(c)

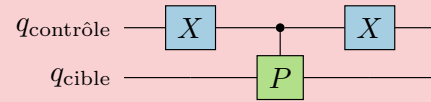
$$\hat{Z}\hat{X} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 0 \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ 0 \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & -1 \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

(d)

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

Exercice B.2 : Porte contrôlée par $|0\rangle$

En appliquant des portes \hat{X} sur le qubit de contrôle avant et après la porte contrôlée, on produit une porte contrôlée par l'état $|0\rangle$.



Chapitre 3

Plus de deux qubits

Les outils développés au chapitre 2 se généralisent naturellement pour des systèmes de plus de deux qubits.

Il peut parfois devenir encombrant de travailler et de manipuler des états à plusieurs qubits. Afin de nous aider dans cette tâche, il est pertinent de définir un certain nombre de notations utiles et judicieuses.

A État à n qubits

Un ordinateur quantique à deux qubits est certainement une machine intéressante à étudier d'un point de vue expérimental ou théorique, mais en pratique une telle machine n'a aucune utilité. Pour être en mesure d'aborder des problèmes d'intérêt, un ordinateur quantique devrait comporter au moins plusieurs dizaines, centaines ou milliers de qubits, voir plus. Considérant que les processeurs classiques actuels comportent plusieurs milliards de transistors, il est difficile de prédire combien de qubits auront les ordinateurs quantiques dans le futur.

Dans tous les cas, nous aurons besoin d'outils mathématiques efficaces et clairs pour décrire l'état de tels systèmes. Les notations choisies devraient aussi être applicables à des systèmes de dix ou un milliard de qubits.

A.1 Pour $n = 3$

Afin de faciliter la généralisation vers un état quantique à n qubits, recommençons la procédure du début de la section 2.A, mais cette fois pour trois ($n = 3$) qubits. La mesure de trois qubits dans des états quantiques quelconques peut possiblement retourner un des huit résultats suivants

000, 001, 010, 011, 100, 101, 110 ou 111.

On définit donc une base pour les états quantiques à trois qubits

$|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$ et $|111\rangle$.

qui nous permet d'écrire un état quantique général à trois qubits comme une combinaison linéaire de ces états de base

$$|\psi\rangle = \alpha |000\rangle + \beta |001\rangle + \gamma |010\rangle + \delta |011\rangle + \epsilon |100\rangle + \zeta |101\rangle + \eta |110\rangle + \theta |111\rangle. \quad (3.1)$$

On constate qu'avec seulement trois qubits l'écriture d'un état quantique commence déjà à être encombrante ! Pour alléger un peu l'écriture, il serait intéressant d'exprimer un état $|\psi\rangle$ comme une somme $\sum (\cdot)$. Pour ce faire, on doit d'abord pouvoir étiqueter ces 8 états de base clairement. Pour l'instant, les états de base sont étiquetés de la manière suivante

$$|b_2 b_1 b_0\rangle$$

$b_2 b_1 b_0$	j
0 0 0	0
0 0 1	1
0 1 0	2
0 1 1	3
1 0 0	4
1 0 1	5
1 1 0	6
1 1 1	7

TABLE 3.1 – Représentations binaires et décimales des 8 premiers entiers.

où les bits b_j peuvent prendre les valeurs 0 ou 1. Ces étiquettes sont en fait des chaînes de bits qui correspondent aux représentations binaires des entiers de 0 à 7. Le tableau 3.1 illustre cette correspondance. Chacun de ces entiers peut être obtenu grâce à une somme sur les trois premières puissances de 2 pondérées par les trois bits

$$j = \sum_{q=0}^2 2^q b_q.$$

Pour un système de trois qubits, on peut donc écrire un état quantique générale comme une somme sur huit termes

$$|\psi\rangle = \sum_{j=0}^7 \alpha_j |j\rangle \quad (3.2)$$

où les huit composantes $\alpha, \beta, \dots, \theta$ de l'équation 3.1, sont remplacées par $\alpha_0, \alpha_1, \dots, \alpha_7$ et donc, sous une forme générale, par α_j .

A.2 Forme générale

Pour généraliser l'équation 3.2 à un nombre arbitraire de qubits on peut d'abord identifier combien de termes une telle somme devrait comporter. On sait que pour un, deux et trois qubits les nombres d'états de base sont respectivement deux, quatre et huit : il double à chaque qubit supplémentaire. Le nombre d'états de base pour un système de n qubits est donc

$$N = 2^n. \quad (3.3)$$

En effet, en ajoutant un qubit à un système de n qubits, la nouvelle base d'états comporte tous les 2^n états de la base à n qubits augmentés de l'état $|0\rangle$ du nouveau qubit auxquels on ajoute un nombre égal d'états de base augmentés de l'état $|1\rangle$ du nouveau qubit.

Par exemple, au tableau 3.1, si on se concentre sur les bits b_0 et b_1 des quatre premières lignes et qu'on les compare à leurs valeurs sur les quatre dernières lignes, on constate qu'il s'agit des mêmes séquences. La différence entre ces deux groupes de lignes est la valeur de b_2 .

On voit donc que chaque qubit double le nombre d'états de base, ce qui justifie l'équation 3.3. L'état quantique général à n qubits comporte donc 2^n termes. Les états de base à n qubits peuvent être construits grâce au produit tensoriel de n états à un qubit ce qui s'écrit

$$|b_{n-1}\rangle \otimes \dots \otimes |b_1\rangle \otimes |b_0\rangle = |b_{n-1} \dots b_1 b_0\rangle = \bigotimes_{q=0}^{n-1} |b_q\rangle$$

où \otimes joue un rôle similaire à celui du produit \prod , mais pour le produit tensoriel.

Encore une fois, on peut étiqueter ces états plus succinctement en interprétant les chaînes de n bits comme des entiers compris entre 0 à $2^n - 1$. Ainsi, les états de base peuvent être identifiés comme

$$|j\rangle = \bigotimes_{q=0}^{n-1} |b_q\rangle \quad \text{avec les entiers} \quad j = \sum_{q=0}^{n-1} 2^q b_q.$$

L'expression générale pour un état quantique de n qubits peut donc finalement prendre la forme suivante

$$|\psi\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle \quad (3.4)$$

où la somme s'arrête à $2^n - 1$ car elle commence à 0. Comme tous les états quantiques, ses composantes sont soumises à une condition de normalisation. Pour un état à n qubits, cette condition est

$$\sum_{j=0}^{2^n-1} |\alpha_j|^2 = 1.$$

A.3 États quantiques notables

Comme il y a un nombre exponentiellement grand d'états quantiques possibles pour n qubits, il devient difficile d'en identifier des plus notables que d'autres. On va néanmoins en présenter quelques-uns qui nous permettront d'introduire les notations utilisées lorsqu'on considère un nombre arbitraire de qubits.

L'état du vide

L'état initial d'un circuit quantique, où tous les qubits sont dans l'état $|0\rangle$, est aussi appelé l'état du vide. On peut le noter de plusieurs manières différentes

$$|\mathbf{0}\rangle = |0\rangle^{\otimes n} = |0\dots 00\rangle = |0\rangle_{n-1} \otimes \dots \otimes |0\rangle_1 \otimes |0\rangle_0.$$

Info notation A.1 : Exposant tensoriel

De la même manière qu'un produit répété peut s'écrire plus brièvement grâce à un exposant

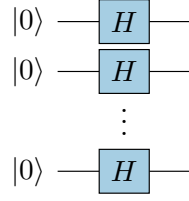
$$2 \times 2 \times \dots \times 2 = 2^n$$

un produit tensoriel répété peut être écrit comme

$$|0\rangle_{n-1} \otimes \dots \otimes |0\rangle_1 \otimes |0\rangle_0 = |0\rangle^{\otimes n}.$$

Le vecteur d'état de l'état du vide est toujours le produit états de base dont seule la première composante est non-nulle

$$|\mathbf{0}\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

FIGURE 3.1 – Circuit de préparation d'un état de superposition uniforme à n qubits.

L'état de superposition uniforme

On déjà vu l'état de superposition uniforme pour deux qubits à la section A.6. Cet état se généralise pour n qubits et peut être préparé à l'aide du circuit illustré à la figure 3.1. L'application d'une porte Hadamard sur chaque qubit, le place dans l'état $|+\rangle$ et on écrit cet état comme

$$|+\rangle^{\otimes n} = |+\rangle_{n-1} \otimes \cdots \otimes |+\rangle_1 \otimes |+\rangle_0.$$

Le produit tensoriel de plusieurs états $|+\rangle$ fait alors intervenir tous les états de base.

Exemple A.1 : Superposition uniforme à trois qubits

Illustrons que le produit tensoriel de trois états $|+\rangle$ génère un état qui fait intervenir tous les états de base pour trois qubits. D'abord, écrivons explicitement

$$|+\rangle^{\otimes 3} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

En distribuant les produits tensoriels on obtient alors,

$$|+\rangle^{\otimes 3} = \frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle).$$

Le vecteur d'état d'un tel état quantique a donc toutes ses composantes non-nulles et égales. Ce vecteur d'état doit cependant comporter la facteur commun qui assure la normalisation de l'état

$$|+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

L'annexe A.1 présente une démonstration générale de la préparation d'un état de superposition uniforme à n qubits à l'aide d'une transformation Hadamard à n qubits.

L'état GHZ

L'état Greenberger–Horne–Zeilinger (GHZ) est un état quantique enchevêtré qui implique au moins trois qubits. Il fait intervenir deux états de base, celui où tous les qubits sont dans l'état $|0\rangle$ et celui où tous les qubits sont dans l'état $|1\rangle$. Pour un système de trois qubit, il s'écrit

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

alors que sa forme générale à n qubits est

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}).$$

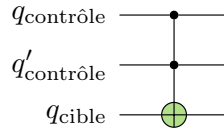


FIGURE 3.2 – La porte Toffoli

Exercice A.1 : État GHZ

- Écrivez le vecteur d'état pour l'état GHZ à trois qubits.
- Construisez un circuit quantique qui permet de préparer un état GHZ à trois qubits.
- Généralisez vos réponses aux deux questions précédentes pour un système de n qubits.

L'état W

L'état W (Wolfgang Dür) est également un état quantique enchevêtré à trois qubits. Il apparaît comme une combinaison des états quantiques où un seul qubit est dans l'état $|1\rangle$

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle).$$

Cet état se généralise également à un nombre arbitraire de qubits qui s'écrit alors

$$|W\rangle = \frac{1}{\sqrt{n}}(|0\dots 01\rangle + |0\dots 10\rangle + \dots + |1\dots 00\rangle).$$

Exercice A.2 : État W

- Montrez que l'état W à n qubit est normalisé.
- Construisez un circuit quantique qui prépare l'état W à trois qubits. Indice : commencez par une rotation à un qubit qui prépare une superposition qui a 1/3 des chances d'être mesuré dans un état et 1/3 des chances d'être mesuré dans l'autre.

B Portes quantiques à plus de deux qubits

La plus part des portes quantiques à trois qubit ou plus sont généralement des portes quantiques construite en assemblant plusieurs portes à un ou deux qubits. On en distingue plusieurs types, comme des portes contrôlées par plusieurs qubits ou encore des versions contrôlées de portes à plusieurs qubits. Il existe néanmoins au moins une porte quantique à trois qubits qui se démarque : la porte Toffoli.

Toffoli

La porte Toffoli, aussi appelée porte contrôle-contrôle- \hat{X} est une porte quantique contrôlée par deux qubits. Une porte \hat{X} est appliquée sur le qubit cible si les deux qubits de contrôle sont dans l'état $|11\rangle$. Une porte Toffoli est illustrée à la figure 3.2.

Exercice B.1 : Porte Toffoli

En énumérant comment la porte Toffoli affecte les huit états de base d'un système de trois qubits, construisez la matrice 8×8 qui représente l'application d'une porte Toffoli.

C Circuits quantiques et calcul quantique

Abordons maintenant comment un circuit quantique peut être utilisé pour effectuer un calcul quantique. Nous allons séparer le circuit quantique en deux sections : la transformation unitaire et la mesure.

C.1 Transformation unitaire

La transformation unitaire \hat{U} d'un circuit quantique qui agit sur n qubits transforme l'état initial du système vers un état quantique donné

$$|\psi\rangle = \hat{U} |\mathbf{0}\rangle \quad (3.5)$$

L'état ainsi préparé peut être représenté par un vecteur d'état comportant 2^n composantes

$$|\psi\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle. \quad (3.6)$$

Ultimement, la transformation unitaire représente donc une opération mathématique équivalente à la multiplication d'une matrice de dimensions $2^n \times 2^n$ sur un vecteur d'état de 2^n composantes pour générer un nouveau vecteur d'état de 2^n composantes

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{2^n-1} \end{pmatrix} = \begin{pmatrix} U_{00} & U_{01} & \cdots & U_{0,2^n-1} \\ U_{10} & U_{11} & \cdots & U_{1,2^n-1} \\ \vdots & \vdots & \ddots & \vdots \\ U_{2^n-1,0} & U_{2^n-1,1} & \cdots & U_{2^n-1,2^n-1} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Remarque : Simuler un ordinateur quantique

Pour simuler un circuit quantique de n qubits à l'aide d'un ordinateur classique, il est nécessaire de construire une matrice de dimensions $2^n \times 2^n$ et d'effectuer une multiplication entre celle-ci et un vecteur d'état de 2^n composantes.

Pour un circuit quantique de trois qubits, cela correspond à une matrice de $8 \times 8 = 64$ éléments. Simuler cela n'a rien d'extraordinaire. Cependant, pour un système qui comporte 20 qubits, la matrice correspondante comporte

$$2^{20} \times 2^{20} = 1\,048\,576 \times 1\,048\,576$$

éléments, soit un peu plus de mille milliards d'éléments ! Pour 150 qubits, ce nombre dépasse le nombre estimé d'atomes contenus dans l'univers ! Il apparaît alors évident qu'il est très difficile, voir impossible, de simuler à l'aide d'un ordinateur classique la transformation unitaire effectuée par un ordinateur quantique de taille raisonnable.

Insistons sur le fait que l'ordinateur quantique ne construit pas cette matrice et n'effectue pas un produit, mais effectue une opération équivalente. Le résultat est alors contenu dans le vecteur qui décrit l'état du système. Ce vecteur d'état n'est pas *parfaitement accessible* en pratique, c'est-à-dire qu'on ne peut pas le connaître en détail avec une précision infinie. On ne peut acquérir qu'une quantité d'information limitée sur celui-ci en effectuant une série de mesures.

C.2 Mesure

Une fois la transformation unitaire appliquée, le système est dans l'état $|\psi\rangle$. La mesure de chacun des qubits retournera un bit soit un 0 soit un 1. La chaîne de bits obtenue en rassemblant ces valeurs peut être interprétée comme un entier j . La probabilité d'obtenir la chaîne de bits associée à l'entier j est déterminé par l'état quantique du système avant la mesure (équation 3.6) et est directement donnée par la règle de Born

$$p_j = |\alpha_j|^2.$$

Qu'a-t-on appris après cette mesure ? Très peu ! Tout ce que l'on sait et que l'état $|j\rangle$ est un des résultats possibles, c'est-à-dire qu'il fait partie de la combinaison linéaire qui compose l'état préparé $|\psi\rangle$ (équation 3.6). On ne sait pas si ce résultat est très probable, peu probable, etc. On sait aussi que le système de qubits est maintenant dans l'état $|j\rangle$ à cause de l'effet projectif de la mesure.

Pour acquérir plus d'information sur l'état $|\psi\rangle$ on doit donc repartir de zéro, reconstruire l'état à l'aide de la transformation unitaire et le mesurer à nouveau, et ce, un très grand nombre de fois. Le nombre de répétitions (*shots* en anglais) est un paramètre important lorsqu'on lance un calcul quantique.

Il est alors possible d'accumuler des statistiques qui nous informe sur l'état $|\psi\rangle$. Par exemple, certains algorithmes sont construits de manière à ce qu'un résultat soit obtenu beaucoup plus souvent que les autres. D'autres algorithmes utilisent tous les résultats obtenus pour calculer une valeur moyenne. Tout cela dépend du type de problème et du type d'algorithme qu'on utilise pour tenter de le résoudre.

S Solutions aux exercices

Exercice B.1 : Porte Toffoli

La porte Toffoli inverse l'état du troisième qubit si les deux premiers sont dans l'état $|11\rangle$. Ainsi les deux états suivants sont échangés sous l'effet d'une porte Toffoli

$$|0\textcolor{red}{1}1\rangle \leftrightarrow |1\textcolor{red}{1}1\rangle$$

alors que tous les autres restent inchangés. Dans la base à huit états (0 à 7) pour un système de trois qubits ces états correspondent aux états 3 et 7. La matrice qui représente la porte Toffoli est donc

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

Chapitre 4

Mesures et observables

Jusqu'à maintenant, nous avons abordé la mesure d'un système quantique uniquement via la mesure des qubits dans la base computationnelle. En d'autres mots, la mesure d'un qubit retourne un 0 ou un 1 de manière aléatoire avec des probabilités qui sont données par les amplitudes de probabilités de l'état quantique du système. Nous allons voir que la mesure d'un système quantique peut être beaucoup plus riche que cela à partir du moment où on introduit le concept d'observable.

En mécanique quantique, une observable représente une quantité physique qui peut être observée. Par exemple, la position et l'énergie sont des observables. Jusqu'à maintenant, la seule observable que nous ayons considérée est la valeur du bit (0 ou 1). Dans le contexte du calcul quantique, les observables seront accessibles via la mesure de un ou plusieurs qubits. Elles peuvent être utilisées pour acquérir de l'information sur un système quantique, mais aussi pour calculer certaines quantités.

Nous allons introduire les observables en utilisant une approche axée sur le calcul quantique en tentant d'abord de reconstruire le vecteur d'état pour un qubit dont on ignore l'état. Nous verrons que le concept d'observable émerge naturellement dans ce contexte. Cela nous permettra de nous familiariser avec ce nouveau concept et sa représentation mathématique. Nous élargirons ensuite notre perspective en introduisant les observables à plusieurs qubits qui apparaîtront comme nécessaires à la description d'un système de plusieurs qubits. Nous nous intéresserons en particulier à un ensemble d'observables appelées les chaînes de Pauli qui peut servir de base pour tous les observables à plusieurs qubits.

Ce n'est qu'une fois ces introductions faites que nous aborderons les observables d'un point de vue plus abstrait et mathématique en établissant leur définition formelle et certaines de leurs propriétés.

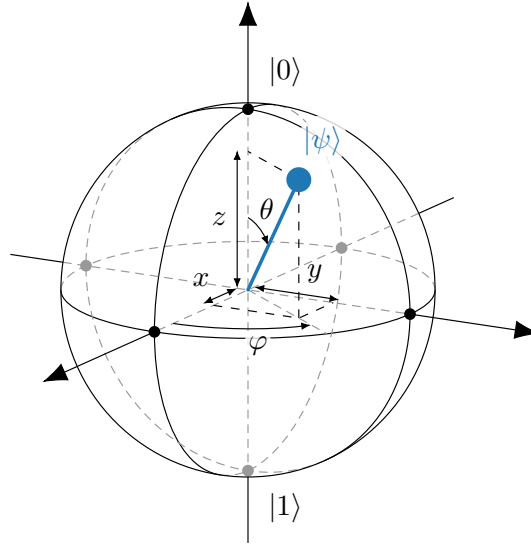
A Observables à un qubit

Supposez qu'on vous donne accès à une machine (un circuit quantique) qui peut être utilisée pour préparer un qubit dans un état quantique secret. On vous demande de déterminer quel est l'état quantique $|\psi\rangle$ que cette machine prépare. Pour remplir cette tâche, vous pouvez utiliser cette machine pour préparer cet état, le mesurer et répéter ces étapes autant de fois que vous le désirez.

A.1 Déterminer le vecteur d'état

Ce qu'on cherche à faire est donc de déterminer le vecteur d'état d'un qubit, ou autrement dit, trouver sa position sur la sphère de Bloch. Commençons par tenter de déterminer si l'état quantique se situe dans l'hémisphère nord (proche de $|0\rangle$) ou l'hémisphère sud (proche de $|1\rangle$).

Supposons que l'on mesure l'état secret une première fois et supposons que le résultat de cette mesure est 0. Que vient-on d'apprendre sur l'état secret ? Très peu. Nous savons définitivement que le qubit n'est pas exactement dans l'état $|1\rangle$. En fait, l'état pourrait être à n'importe quel endroit sur la sphère de Bloch, sauf exactement sur $|1\rangle$. À ce stade, il est légèrement plus probable que l'état se situe dans l'hémisphère

FIGURE 4.1 – Coordonnée x , y et z d'un état quantique sur la sphère de Bloch.

nord que dans l'hémisphère sud. Pour augmenter notre certitude, nous devrons mesurer l'état secret à nouveau.

Supposons que l'on effectue N mesures et que l'on obtienne N_0 fois l'état 0 et N_1 fois l'état 1. Si $N_0 > N_1$, il est raisonnable de croire que l'état se situe dans l'hémisphère nord. Notre niveau de certitude va cependant dépendre de la différence entre les nombres de fois qu'on a obtenu chacun des résultats $N_0 - N_1$.

Par exemple, supposons N égal à 100 pour illustrer notre propos. Si on obtient $N_0 = 95$ (et $N_1 = 5$), nous avons confiance que l'état se situe dans l'hémisphère nord. Par contre, si on obtient $N_0 = 55$ (et $N_1 = 45$), il est fort probable que l'état se situe proche de l'équateur ce qui rend toute conclusion un peu plus hasardeuse.

Si on augmente maintenant le nombre de mesures à 1000 et qu'au final on obtient $N_0 = 550$ (et $N_1 = 450$), la position de l'état est identique au cas $N_0 = 55$ (et $N_1 = 45$), mais notre certitude sur celle-ci est bien meilleure.

La différence normalisée

$$\frac{N_0 - N_1}{N}$$

semble donc être la quantité importante et elle nous informe si l'état sur la sphère de Bloch est plus proche de l'état $|0\rangle$ que de l'état $|1\rangle$. La précision de cette estimation dépend cependant de N .

A.2 Coordonnée en z

Tentons maintenant d'être plus quantitatifs et de déterminer avec précision la coordonnée en z de cet état quantique, comme illustré à la figure 4.1. D'abord, cette coordonnée peut être liée à l'angle θ par trigonométrie

$$z = \cos(\theta). \quad (4.1)$$

Si on peut obtenir l'angle θ , nous aurons directement accès à la coordonnée z via cette relation. Rappelons-nous que l'état quantique d'un qubit est donné par l'équation 1.10

$$|\psi\rangle = \cos(\theta/2) |0\rangle + e^{i\varphi} \sin(\theta/2) |1\rangle.$$

Or nous avons vu qu'on peut acquérir de l'information sur l'état quantique en effectuant un grand nombre de mesures sur celui-ci. Cela nous permet d'estimer les valeurs des probabilités p_0 et p_1 qui sont liées à l'angle θ via

$$p_0 = |\langle 0|\psi\rangle|^2 = \cos^2(\theta/2) \quad \text{et} \quad p_1 = |\langle 1|\psi\rangle|^2 = \sin^2(\theta/2).$$

Par trigonométrie, on constate que la quantité importante $p_0 - p_1$ donne directement l'information que l'on recherche

$$p_0 - p_1 = \cos^2(\theta/2) - \sin^2(\theta/2) = \cos(\theta) = z. \quad (4.2)$$

Donc, si on arrive à extraire les probabilités p_0 et p_1 pour un état quantique à un qubit, on sera capable de déterminer sa coordonnée z sur la sphère de Bloch. Nous continuerons cette discussion à la section A.7.

A.3 Observable \hat{Z}

Pour aborder le concept d'observable, réécrivons l'expression de la coordonnée z de la manière suivante

$$z = p_0 - p_1 = |\langle\psi|0\rangle|^2 - |\langle\psi|1\rangle|^2 = \langle\psi|0\rangle\langle 0|\psi\rangle - \langle\psi|1\rangle\langle 1|\psi\rangle.$$

En procédant à une mise en évidence de l'état quantique à gauche et à droite, on retrouve l'expression dyadique¹ de la matrice \hat{Z}

$$z = \langle\psi|(|0\rangle\langle 0| - |1\rangle\langle 1|)|\psi\rangle = \langle\psi|\hat{Z}|\psi\rangle.$$

On constate alors que la coordonnée z de l'état quantique peut être exprimée comme le produit $\langle\psi|\hat{Z}|\psi\rangle$. Ici, la matrice \hat{Z} correspond à l'observable \hat{Z} . On dit que l'expression

$$z = \langle\psi|\hat{Z}|\psi\rangle.$$

correspond au calcul de la *valeur moyenne* de l'*observable* \hat{Z} sur l'état quantique $|\psi\rangle$. Pour un état quantique quelconque $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, cela revient à effectuer le produit matriciel suivant

$$z = \langle\psi|\hat{Z}|\psi\rangle = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = |\alpha|^2 - |\beta|^2$$

ce qui revient bien à l'expression 4.2.

Remarque : Observables, portes et opérateurs

Dans ce chapitre, nous allons manipuler des observables et décrire leurs propriétés. Les observables, comme les opérateurs et les portes quantiques peuvent être représentés par des matrices. Cela implique que plusieurs manipulations mathématiques qui seront présentées ici pourraient également s'appliquer aux opérateurs et aux portes quantiques.

Par exemple, la matrice \hat{Z} peut à la fois représenter un opérateur, une porte quantique et une observable même si ces trois choses sont conceptuellement différentes.

Typiquement, les propriétés des matrices sont d'abord présentées de manière abstraite sous le thème de l'algèbre linéaire et sont ensuite appliquées aux opérateurs, aux observables et aux portes quantiques. Nous tentons ici une approche différente en appliquant directement ces concepts aux observables en espérant que cela permette de se familiariser plus facilement avec ceux-ci. L'abstraction pourra se faire dans un deuxième temps.

1. Consultez la section B.11 si vous avez besoin d'un rafraîchissement sur la notation dyadique.

A.4 Observable \hat{X}

Afin d'identifier l'état quantique $|\psi\rangle$, nous aurons également besoin de connaître ses coordonnées x et y . Concentrons-nous sur x pour l'instant. Par analogie avec l'observable \hat{Z} , le calcul de la valeur moyenne de l'observable \hat{X} permet d'obtenir la composante x de l'état $|\psi\rangle$ sur la sphère de Bloch. Vérifions cette affirmation en effectuant explicitement ce calcul

$$\begin{aligned} x = \langle \psi | \hat{X} | \psi \rangle &= \begin{pmatrix} \cos(\theta/2) & e^{-i\varphi} \sin(\theta/2) \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi} \sin(\theta/2) \end{pmatrix} \\ &= \sin(\theta/2) \cos(\theta/2) (e^{i\varphi} + e^{-i\varphi}) \\ &= \sin(\theta) \cos(\varphi) \end{aligned} \quad (4.3)$$

ce qui correspond effectivement à la coordonnée x (en coordonnées sphériques) de l'état $|\psi\rangle$ sur la sphère de Bloch.

Pour un état quantique quelconque $\alpha|0\rangle + \beta|1\rangle$, cela revient à effectuer le produit matriciel suivant

$$x = \langle \psi | \hat{X} | \psi \rangle = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\beta^* + \alpha^*\beta.$$

A.5 Observable \hat{Y}

Un calcul similaire permet de montrer que la valeur moyenne de l'observable \hat{Y} est égale à la coordonnée y de l'état quantique, sur la sphère de Bloch

$$y = \langle \psi | \hat{Y} | \psi \rangle = \sin(\theta) \sin(\varphi). \quad (4.4)$$

A.6 Observable \hat{I}

Il est également utile de définir l'observable identité. La valeur moyenne de cette observable est toujours

$$\langle \psi | \hat{I} | \psi \rangle = 1.$$

pour un état normalisé. Il n'est pas nécessaire de mesurer un qubit pour évaluer la valeur moyenne de l'identité sur celui-ci.

A.7 Estimation sur un ordinateur quantique

Nous avons établi qu'on peut exprimer les coordonnées x , y et z d'un état quantique à un qubit comme les valeurs moyennes des observables \hat{X} , \hat{Y} et \hat{Z} sur cet état quantique. Il nous reste cependant à décrire comment on peut utiliser des mesures sur un qubit afin de déduire ses coordonnées x , y et z .

La coordonnée en z

On a déjà vu à l'équation 4.2 que la coordonnée z peut être exprimée comme la différence entre les probabilités d'obtenir 0 et 1 lors de la mesure du qubit

$$z = p_0 - p_1.$$

On peut estimer ces probabilités en effectuant un certain nombre N de mesures. On utilise ensuite le nombre de fois qu'on a obtenu chacun des deux résultats possibles (N_0 et N_1) afin d'estimer les probabilités

$$p_0 \approx \frac{N_0}{N} \quad \text{et} \quad p_1 \approx \frac{N_1}{N}.$$

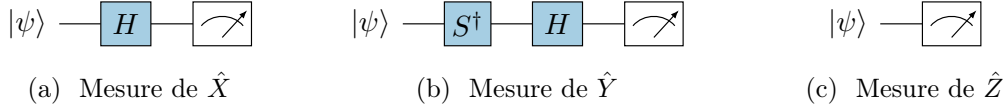


FIGURE 4.2 – Circuits de mesure pour les trois observables à un qubit.

Coordonnée en x

Alors que les états $|0\rangle$ et $|1\rangle$ correspondent respectivement aux coordonnées $z = 1$ et $z = -1$, les états $|+\rangle$ et $|-\rangle$ correspondent aux coordonnées $x = 1$ et $x = -1$. Imaginons donc qu'on puisse mesurer le qubit d'une manière que les résultats possibles soient $+$ et $-$ au lieu des habituels 0 et 1 . Pour un qubit dans un état quantique $|\psi\rangle$, les probabilités d'obtenir chacun de ces résultats se calculent comme d'habitude par la règle de Born

$$p_+ = |\langle +|\psi\rangle|^2 \quad \text{et} \quad p_- = |\langle -|\psi\rangle|^2$$

Par analogie avec la coordonnée z , la coordonnée en x peut alors être exprimée comme

$$x = p_+ - p_-.$$

Certaines architectures d'ordinateur quantique permettent d'effectuer des mesures dans la base $\{|+\rangle, |-\rangle\}$ et ainsi d'évaluer directement ces probabilités. Pour les autres, tout n'est pas perdu. En effet, on peut émuler une mesure dans cette base en modifiant l'état du qubit avant de le mesurer. En effet, on peut utiliser l'identité $\hat{X} = \hat{H}\hat{Z}\hat{H}$ pour écrire

$$x = \langle \psi | \hat{X} | \psi \rangle = \langle \psi | \hat{H} \hat{Z} \hat{H} | \psi \rangle = \langle \psi^{(x)} | \hat{Z} | \psi^{(x)} \rangle \quad (4.5)$$

où on a défini l'état quantique modifié

$$|\psi^{(x)}\rangle = \hat{H} |\psi\rangle.$$

On constate donc qu'il est possible d'émuler une mesure selon l'observable \hat{X} sur un état quantique $|\psi\rangle$, en effectuant une mesure selon \hat{Z} sur l'état quantique modifié $|\psi^{(x)}\rangle$, c'est-à-dire en effectuant une mesure *standard* d'un qubit sur lequel on a préalablement appliqué une porte Hadamard. Le circuit de la mesure pour l'observable \hat{X} est donc celui présenté à la figure 4.2a.

La porte Hadamard effectue une transformation qui déplace l'état $|+\rangle$ vers $|0\rangle$ de sorte que la probabilité d'obtenir 0 pour l'état transformé $|\psi^{(x)}\rangle$ est égale à la probabilité d'obtenir $+$ pour l'état initial $|\psi\rangle$. Un raisonnement analogue s'applique pour les états $|-\rangle$ et $|1\rangle$. Cela peut se résumer simplement par

$$p(+|\psi) = p(0|\psi^{(x)}) \quad \quad p(-|\psi) = p(1|\psi^{(x)}).$$

où on utilise la notation $p(\phi|\psi)$ pour indiquer la probabilité d'obtenir le résultat ϕ étant donné que l'état du qubit est $|\psi\rangle$.

Remarque

On a utilisé la porte Hadamard pour transformer l'état du qubit avant la mesure, car elle est typiquement plus facile à implémenter en pratique. Cependant, on aurait tout aussi bien pu utiliser une porte $R_y(-\pi/2)$ à la place et obtenir les mêmes résultats.

Coordonnée en y

De manière analogue aux coordonnées z et x , la troisième coordonnée peut être exprimée comme

$$y = p_{+i} - p_{-i}.$$

où les probabilités de mesure dans la $\{|+i\rangle, |-i\rangle\}$ peuvent être obtenues par une mesure émulée dans cette base. Dans ce cas-ci, on utilise l'identité $\hat{Y} = \hat{S}\hat{X}\hat{S}^\dagger$ pour écrire

$$y = \langle \psi | \hat{Y} | \psi \rangle = \langle \psi | \hat{S}\hat{X}\hat{S}^\dagger | \psi \rangle = \langle \psi | \hat{S}\hat{H}\hat{Z}\hat{H}\hat{S}^\dagger | \psi \rangle = \langle \psi^{(y)} | \hat{Z} | \psi^{(y)} \rangle \quad (4.6)$$

où on a défini l'état quantique modifié

$$|\psi^{(y)}\rangle = \hat{H}\hat{S}^\dagger |\psi\rangle.$$

Cette transformation permet de déplacer les états $|+i\rangle$ et $|-i\rangle$ respectivement vers les états de la base computationnelle $|0\rangle$ et $|1\rangle$. Le circuit de la mesure en \hat{Y} est présenté à la figure 4.2b.

En utilisant la même notation, les probabilités recherchées pour l'état $|\psi\rangle$ peuvent être exprimées grâce aux probabilités de mesure pour l'état modifié

$$p(+i|\psi) = p(0|\psi^{(y)}) \quad p(-i|\psi) = p(1|\psi^{(y)}).$$

A.8 Reconstruire le vecteur d'état

Une fois que les coordonnées x , y et z ont été estimées, on devrait être capable d'estimer la position du vecteur d'état sur la sphère de Bloch.

Remarque

Étant donné que les coordonnées ont été estimées, il n'est pas garanti qu'elles respectent la condition de normalisation

$$x^2 + y^2 + z^2 = 1$$

à laquelle on s'attend. On pourrait utiliser un modèle sophistiqué pour exploiter cette relation pour donner plus d'importance aux coordonnées dont l'estimation est plus précise, mais nous ne le ferons pas pour l'instant.

En utilisant les relations 4.1, 4.3 et 4.4 on peut exprimer les angles comme étant

$$\theta = \arccos(z) \quad \text{et} \quad \varphi = \arctan2(y, x).$$

Le vecteur d'état est alors simplement donné par l'équation 1.10, c'est-à-dire

$$|\psi\rangle = \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi} \sin(\theta/2) \end{pmatrix}.$$

A.9 Autres observables à un qubit

En ajoutant la matrice identité \hat{I} aux matrices de Pauli \hat{X} , \hat{Y} et \hat{Z} on forme une base pour toutes les matrices 2×2 à coefficient complexes. Autrement dit, toute matrice 2×2 à coefficients complexes peut être écrite comme une combinaison linéaire

$$\hat{A} = a_i \hat{I} + a_x \hat{X} + a_y \hat{Y} + a_z \hat{Z} \quad (4.7)$$

où les coefficients a_i à a_z sont des nombres complexes. Ces matrices servent donc également de base pour toute observable à un qubit. Nous verrons à la section C.5 que pour que \hat{A} soit une observable, elle doit être Hermitienne, ce qui impose que les coefficients a_i à a_z soient des nombres réels.

Par exemple, l'observable

$$\hat{A}(\theta) = \cos(\theta) \hat{Z} + \sin(\theta) \hat{X}$$

permet de mesurer un qubit selon un axe qui fait un angle θ avec l'axe des z tout en étant dans le plan xz .

La valeur moyenne d'une observable telle que construite à l'équation 4.7 peut être estimée de deux manières.

Première approche

D'abord, on peut l'exprimer comme une combinaison linéaire de valeurs moyennes

$$\langle \psi | \hat{A} | \psi \rangle = a_i + a_x \langle \psi | \hat{X} | \psi \rangle + a_y \langle \psi | \hat{Y} | \psi \rangle + a_z \langle \psi | \hat{Z} | \psi \rangle$$

où on a utilisé le fait que l'état $|\psi\rangle$ est normalisé et donc que $\langle \psi | \hat{I} | \psi \rangle = 1$. Cette approche nécessite donc d'exécuter trois circuits quantiques, un pour chaque observable.

Seconde approche

L'autre approche généralise l'approche utilisée pour estimer les valeurs moyennes de \hat{X} et \hat{Y} , c'est-à-dire d'appliquer une transformation qui diagonalise l'observable \hat{A} . En théorie, il est possible de trouver une transformation unitaire \hat{U} telle que

$$\hat{U} \hat{A} \hat{U}^\dagger = \hat{D}$$

où \hat{D} est un opérateur diagonal dans la base computationnelle. Comme \hat{D} est diagonal, on peut toujours l'exprimer comme une combinaison linéaire des observables \hat{I} et \hat{Z}

$$\hat{D} = d_i \hat{I} + d_z \hat{Z}.$$

On peut donc écrire la valeur moyenne de l'observable \hat{A} pour un état quantique quelconque, comme

$$\langle \psi | \hat{A} | \psi \rangle = \langle \psi | \hat{U}^\dagger \hat{D} \hat{U} | \psi \rangle$$

Comme \hat{U} est unitaire, il existe un circuit quantique qui applique cette transformation. En appliquant ce circuit sur un qubit dans l'état $|\psi\rangle$, on prépare l'état transformé

$$|\psi^{(a)}\rangle = \hat{U} |\psi\rangle$$

La mesure du qubit après cette transformation permet alors d'estimer la valeur moyenne de l'observable comme étant

$$\langle \psi | \hat{A} | \psi \rangle = \langle \psi^{(a)} | \hat{D} | \psi^{(a)} \rangle = d_i + d_z \langle \psi^{(a)} | \hat{Z} | \psi^{(a)} \rangle.$$

Cette approche nécessite l'exécution d'un seul circuit, mais requiert de connaître la transformation \hat{U} . Cela s'avère, difficile, voire pratiquement impossible, pour des systèmes de plus grande taille.

Remarque

Notons également que cette approche ne peut pas être utilisée pour faciliter l'estimation du vecteur d'état d'un qubit dans un état quelconque. Pour que ce soit le cas, il faudrait déjà connaître l'orientation du vecteur d'état sur la sphère de Bloch.

B Observables à plusieurs qubits

À la section précédente, nous avons établi que pour estimer le vecteur d'état d'un qubit, il est nécessaire d'estimer les valeurs moyennes des observables $\{\hat{X}, \hat{Y}, \hat{Z}\}$. Si maintenant on considère un système de deux qubits $|q_0\rangle$ et $|q_1\rangle$, on peut appliquer la même recette à chacun d'eux et estimer les valeurs moyennes de leurs observables à un qubit, soient $\{\hat{X}_0, \hat{Y}_0, \hat{Z}_0\}$ et $\{\hat{X}_1, \hat{Y}_1, \hat{Z}_1\}$. Cela ne permet cependant pas de décrire complètement l'état à deux qubits. En effet, un système de deux qubits comporte une richesse supplémentaire qui fait intervenir l'intrication et qui demande d'estimer la valeur moyenne d'observables à deux qubits pour pouvoir le décrire complètement.

On peut construire des observables à deux qubits de la même manière qu'on a construit les premiers états à deux qubits, c'est-à-dire en combinant les espaces des deux qubits à l'aide du produit tensoriel. Par exemple, l'observable

$$\hat{Z}\hat{Z} = \hat{Z}_1 \otimes \hat{Z}_0.$$

est une observable à deux qubits qui permet de caractériser si les deux qubits sont parallèles ou antiparallèles le long de l'axe z .

Remarque

Bien que notre intérêt pour les observables à plusieurs qubits soit motivé par leur importance dans la description de l'état d'un système de plusieurs qubits, nous ne parviendrons pas à remplir cet objectif dans cette section. En effet, cette tâche requiert des notions que nous n'avons pas encore vues.

Exemple B.1 : Valeur moyenne pour des états de base

Pour débiter notre compréhension des observables à deux qubits, calculons les valeurs moyennes de l'observable $\hat{Z}\hat{Z}$ pour les différents états de base à deux qubits. Comme ces observables ainsi que les états de base sont construits à l'aide de produits tensoriels, les valeurs moyennes peuvent être exprimées comme le produit des valeurs moyennes pour des observables à un qubit. Par exemple,

$$\langle 01 | \hat{Z}\hat{Z} | 01 \rangle = (\langle 0 | \otimes \langle 1 |)(\hat{Z}_1 \otimes \hat{Z}_0)(|0\rangle \otimes |1\rangle) = \langle 0 | \hat{Z} | 0 \rangle \langle 1 | \hat{Z} | 1 \rangle = 1 \times -1 = -1.$$

Les valeurs moyennes pour tous les états de base s'obtiennent de manière similaire et sont

$$\langle 00 | \hat{Z}\hat{Z} | 00 \rangle = 1 \quad \langle 01 | \hat{Z}\hat{Z} | 01 \rangle = -1 \quad \langle 10 | \hat{Z}\hat{Z} | 10 \rangle = -1 \quad \langle 11 | \hat{Z}\hat{Z} | 11 \rangle = 1.$$

On constate que la valeur moyenne de l'observable $\hat{Z}\hat{Z}$ permet en fait de déterminer si, dans l'état de base, les deux qubits sont pareils (00 ou 11 ; valeur moyenne 1) ou s'ils sont différents (01 ou 10 ; valeur moyenne -1).

Cela est toujours valide pour des états tels que les états de Bell

$$|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2} \quad \text{et} \quad |\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}.$$

En effet, on montre facilement que

$$\langle \Phi^+ | \hat{Z}\hat{Z} | \Phi^+ \rangle = 1 \quad \text{et} \quad \langle \Psi^+ | \hat{Z}\hat{Z} | \Psi^+ \rangle = -1.$$

B.1 Les chaines de Pauli

Nous avons vu à la section précédente qu'une observable à un qubit quelconque peut être exprimée comme une combinaison linéaire des opérateurs de Pauli et de l'identité (voir l'équation 4.7). De manière analogue, nous allons voir que les observables à plusieurs qubits peuvent être exprimées à l'aide de chaines de Pauli

Les expressions telles que $\hat{Z}\hat{Z}$ et $\hat{I}\hat{X}$ sont des chaines de Pauli à deux qubits. De manière générale, une chaîne de Pauli de longueur n est composée de n opérateurs de Pauli ou l'identité qui s'appliquent sur autant de qubits. Ces opérateurs sont assemblés à l'aide d'un produit tensoriel. De la même manière que les opérateurs \hat{I} , \hat{X} , \hat{Y} et \hat{Z} forment une base pour exprimer des observables à 1 qubit, les chaines de Pauli de longueur n forment une base pour exprimer toutes les observables à n qubits.

Formellement, une chaîne de Pauli à n qubits est définie comme

$$\hat{\mathcal{P}} = \bigotimes_{q=0}^{n-1} \hat{\sigma}_q \quad \text{avec} \quad \hat{\sigma}_q \in \{\hat{I}_q, \hat{X}_q, \hat{Y}_q, \hat{Z}_q\}.$$

Chaque chaîne de Pauli de longueur n peut être représentée dans la base computationnelle par une matrice de taille $2^n \times 2^n$ en appliquant le produit tensoriel comme on l'a fait à la section B.4 du chapitre 2.

Comme chaque élément d'une chaîne de Pauli est un opérateur parmi les quatre possibles, il existe donc 4^n chaines de Pauli différentes de longueur n .

B.2 Observables à n qubits

Lorsqu'on affirme que les chaînes de Pauli de longueur n constituent une base pour les observables à n qubits, cela signifie que chacune de ces observables \hat{A} peut être exprimée comme une combinaison linéaire de chaînes de Pauli

$$\hat{A} = \sum_i a_i \hat{\mathcal{P}}_i$$

où les coefficients a_i doivent être réels pour que \hat{A} soit Hermitien (voir section C.5). Les coefficients a_i (non nuls) définissent en quelque sorte l'observable \hat{A} . Cette combinaison linéaire est particulièrement intéressante lorsqu'elle ne fait intervenir qu'un petit sous-ensemble des 4^n chaînes de Pauli possibles.

Le calcul de la valeur moyenne d'une telle observable \hat{A} pour un état quantique $|\psi\rangle$ peut se faire en évaluant les valeurs moyennes des chaînes de Pauli qui le constituent

$$\langle\psi|\hat{A}|\psi\rangle = \sum_i a_i \langle\psi|\hat{\mathcal{P}}_i|\psi\rangle.$$

Il apparaît alors essentiel de pouvoir évaluer les valeurs moyennes de différentes chaînes de Pauli.

B.3 Estimation de la valeur moyenne d'une chaîne de Pauli

L'évaluation des valeurs moyennes de chaînes de Pauli est au centre de l'évaluation de la valeur moyenne d'observables. Afin de pouvoir effectuer une estimation de ces valeurs moyennes en utilisant un ordinateur quantique, nous allons d'abord considérer les chaînes de Pauli dites diagonales qui sont directement mesurables sur un ordinateur quantique. Nous généraliserons ensuite aux autres chaînes de Pauli.

Chaînes de Pauli diagonales

On identifie les chaînes de Pauli diagonales comme étant celles qui sont représentées par des matrices diagonales dans la base computationnelle. Ces chaînes de Pauli sont faciles à identifier, car elles comportent uniquement des opérateurs \hat{I} et \hat{Z} . En effet, on peut facilement se convaincre que le produit tensoriel de matrices diagonales produit toujours une matrice diagonale. En contrepartie, si on inclut au moins une matrice non diagonale dans le produit tensoriel, la matrice résultante ne sera pas diagonale.

On utilisera la notation suivante pour spécifier qu'une chaîne de Pauli est diagonale

$$\hat{\mathcal{Z}} = \bigotimes_{q=0}^{n-1} \hat{\sigma}_q \quad \text{avec} \quad \hat{\sigma}_q \in \{\hat{I}_q, \hat{Z}_q\}.$$

De la même manière que la mesure d'un qubit permet d'estimer la valeur moyenne de l'observable \hat{Z} , la mesure d'un système de n qubits permet d'estimer les valeurs moyennes de toutes les chaînes de Pauli diagonales de longueur n . En effet, comme on va le voir à la section C.2, les états de base à n qubits sont des états propres des chaînes de Pauli diagonales de longueur n . Illustrons cela grâce à l'exemple sur deux qubits suivant.

Exemple B.2 : Chaînes de Pauli diagonales pour deux qubits

On aimerait estimer les valeurs moyennes des chaînes de Pauli diagonales pour un système de deux qubits dans un état quelconque $|\psi\rangle$. En excluant l'observable identité $\hat{I}\hat{I}$, ces observables sont

$$\hat{I}\hat{Z}, \quad \hat{Z}\hat{I} \quad \text{et} \quad \hat{Z}\hat{Z}.$$

Un état à deux qubits est une superposition des états de base à deux qubits $|00\rangle$, $|01\rangle$, $|10\rangle$ et $|11\rangle$. Un tel état

peut donc être écrit sous la forme suivante

$$|\psi\rangle = \sum_{b_0=0}^1 \sum_{b_1=0}^1 \alpha_{b_1 b_0} |b_1 b_0\rangle$$

où le coefficient $\alpha_{b_1 b_0}$ est l'amplitude de probabilité devant l'état de base $|b_1 b_0\rangle$. Pour traiter les trois observables en même temps, considérons une observable de la forme $\hat{\sigma}_1 \hat{\sigma}_0$. La valeur moyenne d'une telle observable s'exprime comme

$$\langle \psi | \hat{\sigma}_1 \hat{\sigma}_0 | \psi \rangle = \left(\sum_{b'_0=0}^1 \sum_{b'_1=0}^1 \alpha_{b'_1 b'_0}^* \langle b'_1 b'_0 | \right) \hat{\sigma}_1 \hat{\sigma}_0 \left(\sum_{b_0=0}^1 \sum_{b_1=0}^1 \alpha_{b_1 b_0} |b_1 b_0\rangle \right)$$

où on a pris soin de distinguer les éléments des sommes à gauche et à droite et d'appliquer le complexe conjugué au terme de droite. Chaque état de base étant un état produit, on peut appliquer une approche similaire à celle de l'exemple précédent pour rassembler les observables et les états associés au même qubit. On obtient ainsi

$$\langle \psi | \hat{\sigma}_1 \hat{\sigma}_0 | \psi \rangle = \sum_{b'_0=0}^1 \sum_{b'_1=0}^1 \sum_{b_0=0}^1 \sum_{b_1=0}^1 \alpha_{b'_1 b'_0}^* \alpha_{b_1 b_0} \langle b'_1 | \hat{\sigma}_1 | b_1 \rangle \langle b'_0 | \hat{\sigma}_0 | b_0 \rangle$$

Étant donné que $\hat{\sigma}_q \in \{\hat{I}_q, \hat{Z}_q\}$, les expressions $\langle b'_0 | \hat{\sigma}_0 | b_0 \rangle$ et $\langle b'_1 | \hat{\sigma}_1 | b_1 \rangle$ sont des éléments de matrices diagonales. On peut donc les exprimer simplement à l'aide des valeurs moyennes

$$\langle b'_0 | \hat{\sigma}_0 | b_0 \rangle = \langle b_0 | \hat{\sigma}_0 | b_0 \rangle \delta_{b_0, b'_0} \quad \text{et} \quad \langle b'_1 | \hat{\sigma}_1 | b_1 \rangle = \langle b_1 | \hat{\sigma}_1 | b_1 \rangle \delta_{b_1, b'_1}.$$

On remplace ensuite ces éléments de matrices dans l'expression précédente et on effectue les sommes sur b'_0 et b'_1 pour obtenir

$$\langle \psi | \hat{\sigma}_1 \hat{\sigma}_0 | \psi \rangle = \sum_{b_0=0}^1 \sum_{b_1=0}^1 |\alpha_{b_1 b_0}|^2 \langle b_1 | \hat{\sigma}_1 | b_1 \rangle \langle b_0 | \hat{\sigma}_0 | b_0 \rangle. \quad (4.8)$$

On voit donc qu'il est possible de calculer la valeur moyenne d'une observable à deux qubits $\hat{\sigma}_1 \hat{\sigma}_0$ à partir des valeurs moyennes des observables à un qubit $\hat{\sigma}_0$ et $\hat{\sigma}_1$. Cela est uniquement possible parce que les observables impliquées sont diagonales dans la base computationnelle.

Appliquons l'expression 4.8 à l'observable $\hat{Z}\hat{Z}$. Comme les valeurs moyennes de l'observable \hat{Z} sur les états de base sont respectivement +1 et -1 pour les états $|0\rangle$ et $|1\rangle$, on peut les écrire

$$\langle b_0 | \hat{Z} | b_0 \rangle = (-1)^{b_0} \quad \text{et} \quad \langle b_1 | \hat{Z} | b_1 \rangle = (-1)^{b_1}.$$

La valeur moyenne de l'observable $\hat{Z}\hat{Z}$ devient alors

$$\langle \psi | \hat{Z}\hat{Z} | \psi \rangle = \sum_{b_0=0}^1 \sum_{b_1=0}^1 p_{b_1 b_0} (-1)^{b_0+b_1}$$

où $p_{b_1 b_0} = |\alpha_{b_1 b_0}|^2$ est la probabilité d'obtenir le résultat $b_1 b_0$ lors de la mesure des qubits. On note au passage que $(-1)^{b_0+b_1}$ correspond à la valeur propre de $\hat{Z}\hat{Z}$ pour l'état $|b_1 b_0\rangle$. En estimant les probabilités de mesure grâce à

$$p_{b_1 b_0} \approx \frac{N_{b_1 b_0}}{N}$$

l'estimation de la valeur moyenne peut être obtenue grâce au calcul suivant

$$\langle \psi | \hat{Z}\hat{Z} | \psi \rangle \approx \frac{N_{00} - N_{01} - N_{10} + N_{11}}{N}$$

Des calculs similaires à partir de l'équation 4.8 permettent d'estimer les valeurs moyennes pour les deux autres observables

$$\langle \psi | \hat{I}\hat{Z} | \psi \rangle \approx \frac{N_{00} - N_{01} + N_{10} - N_{11}}{N} \quad \text{et} \quad \langle \psi | \hat{Z}\hat{I} | \psi \rangle \approx \frac{N_{00} + N_{01} - N_{10} - N_{11}}{N}.$$

Dans l'exemple précédent, on constate que les données recueillies lors de l'exécution du circuit (N_{00} , N_{01} , N_{10} et N_{11}) peuvent être combinées de différentes manières afin de calculer les valeurs moyennes de différentes observables.

Chaines de Pauli non diagonales

Pour pouvoir estimer la valeur moyenne d'une chaîne de Pauli non diagonale, c'est-à-dire qui comporte au moins un \hat{X} ou \hat{Y} , on devra appliquer une transformation pour la rendre diagonale. De la même manière qu'on a transformé les observables \hat{X} et \hat{Y} vers \hat{Z} pour le cas à un qubit, cela se résume à modifier l'état quantique avant de le mesurer.

La transformation \hat{U} qu'on cherche doit donc transformer une chaîne de Pauli $\hat{\mathcal{P}}$ de sorte que

$$\hat{U}\hat{\mathcal{P}}\hat{U}^\dagger = \hat{\mathcal{Z}}$$

où $\hat{\mathcal{Z}}$ est une chaîne de Pauli diagonale. Il existe plusieurs transformations qui permettent cela, mais on s'intéresse ici à la méthode la plus simple qui implique uniquement des portes à un qubit. En effet, en s'inspirant de ce qu'on a appris sur la mesure d'observable à un qubit, la transformation \hat{U} peut simplement consister à appliquer les transformations présentées aux équations 4.5 et 4.6, c'est-à-dire

$$\hat{X} = \hat{H}\hat{Z}\hat{H} \quad \text{et} \quad \hat{Y} = \hat{S}\hat{H}\hat{Z}\hat{H}\hat{S}^\dagger$$

sur chacun des qubits de la chaîne de Pauli qui possède respectivement un \hat{X} ou un \hat{Y} . Le résultat de cette transformation sera une chaîne de Pauli diagonale.

Exemple B.3 : Diagonalisation d'une chaîne de Pauli

On veut estimer la valeur moyenne de l'observable à quatre qubits suivante

$$\hat{Z}\hat{I}\hat{X}\hat{Y}.$$

Les opérateurs associés aux qubits $|q_0\rangle$ et $|q_1\rangle$ peuvent être transformés grâce à

$$\hat{Y}_0 = \hat{S}_0\hat{H}_0\hat{Z}_0\hat{H}_0\hat{S}_0^\dagger \quad \text{et} \quad \hat{X}_1 = \hat{H}_1\hat{Z}_1\hat{H}_1.$$

On exprime ainsi la valeur moyenne de l'observable en remplaçant ces expressions pour obtenir

$$\langle\psi|\hat{Z}\hat{I}\hat{X}\hat{Y}|\psi\rangle = \langle\psi|\hat{Z}_3\hat{I}_2(\hat{H}_1\hat{Z}_1\hat{H}_1)(\hat{S}_0\hat{H}_0\hat{Z}_0\hat{H}_0\hat{S}_0^\dagger)|\psi\rangle$$

Étant donné que les opérateurs associés à un qubit commutent avec les opérateurs associés aux autres, on peut les réorganiser pour écrire

$$\langle\psi|\hat{Z}\hat{I}\hat{X}\hat{Y}|\psi\rangle = \langle\psi|\hat{H}_1\hat{S}_0\hat{H}_0(\hat{Z}_3\hat{I}_2\hat{Z}_1\hat{Z}_0)\hat{H}_1\hat{H}_0\hat{S}_0^\dagger|\psi\rangle.$$

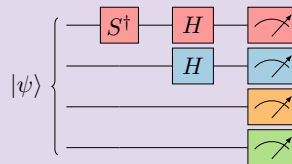
La valeur moyenne pour la chaîne de Pauli originale sur l'état quantique $|\psi\rangle$ peut donc être obtenue via la valeur moyenne d'une chaîne de Pauli diagonale

$$\langle\psi|\hat{Z}\hat{I}\hat{X}\hat{Y}|\psi\rangle = \langle\psi'|\hat{Z}\hat{I}\hat{Z}\hat{Z}|\psi'\rangle$$

laquelle est évaluée sur l'état quantique modifié qu'on a défini comme

$$|\psi'\rangle = \hat{H}_1\hat{H}_0\hat{S}_0^\dagger|\psi\rangle.$$

Le circuit de mesure qui permet l'estimation de la valeur moyenne de la chaîne de Pauli $\hat{Z}\hat{I}\hat{X}\hat{Y}$ est donc le suivant.



C Observables en général

Maintenant que nous avons fait un survol pratique, mais introductif aux observables à un ou plusieurs qubits, il est pertinent d'établir plus formellement la définition d'une observable ainsi que ses propriétés. Dans cette section, nous allons considérer une observable quelconque \hat{A} . Nous établirons d'abord les conséquences liées au fait que la mesure d'une observable soit projective, c'est-à-dire que la mesure projette le système quantique dans un état quantique associé au résultat obtenu. Cela nous amènera à introduire les concepts d'états propres et de valeurs propres pour une observable. Nous poursuivrons la discussion en établissant quelques propriétés importantes des observables.

C.1 Mesures projectives

Nous avons présenté aux sections A.6 et A.7 du chapitre 1 le concept de mesure projective sans nécessairement le nommer. Comme son nom l'indique, une mesure projective projette un système quantique vers l'état quantique associé au résultat obtenu. Nous avons également vu que si on répète la mesure d'un système, le résultat restera inchangé à moins qu'on altère le système entre deux mesures ou qu'on effectue une mesure différente. Nous allons montrer dans cette section que cela implique que les états vers lesquels le système peut être projeté par la mesure sont orthogonaux et forment une base.

Projecteurs

Afin de mieux décrire l'effet de la mesure, nous aurons besoin de définir des projecteurs. Introduisons ceux-ci grâce à un exemple familier.

Exemple C.1 : Projecteurs et mesure d'un qubit

Lorsqu'un qubit dans un état quantique quelconque $|\psi\rangle$ est mesuré, les deux résultats qu'on peut obtenir sont 0 et 1. En fonction du résultat obtenu, l'état du qubit, après la mesure, est respectivement $|0\rangle$ ou $|1\rangle$. Pour représenter mathématiquement cette projection, on peut utiliser les projecteurs qui sont définis comme

$$\hat{P}_0 = |0\rangle\langle 0| \quad \text{et} \quad \hat{P}_1 = |1\rangle\langle 1|.$$

Par exemple, l'action du projecteur \hat{P}_0 sur l'état $|\psi\rangle$ produit un état qui s'apparente à l'état $|0\rangle$

$$\hat{P}_0 |\psi\rangle = |0\rangle \langle 0|\psi\rangle \propto |0\rangle$$

à l'exception qu'il n'est pas normalisé. En effet, l'état $\hat{P}_0 |\psi\rangle$ fait intervenir un facteur $\langle 0|\psi\rangle$. On peut normaliser l'état résultant en le divisant par sa norme (voir l'équation 1.6 chapitre 1) et ainsi obtenir

$$|0\rangle = \frac{\hat{P}_0 |\psi\rangle}{\sqrt{\langle \psi | \hat{P}_0^\dagger \hat{P}_0 | \psi \rangle}}.$$

Ainsi, à l'aide du projecteur \hat{P}_0 on est capable de représenter l'effet de la mesure sur l'état quantique étant donné le résultat de cette mesure. Notons que l'opération appliquée à l'état $|\psi\rangle$ pour produire l'état résultant $|0\rangle$ n'est manifestement pas linéaire, ce qui traduit bien le fait que la mesure d'un système quantique n'est pas un phénomène linéaire.

Considérons maintenant la mesure d'une observable quelconque \hat{A} . Pour l'instant, on ne s'intéresse pas aux résultats de la mesure en tant que tels, mais plutôt à l'état résultant. Il existe un certain nombre d'états quantiques vers lesquels le système peut être projeté lors de la mesure de l'observable \hat{A} . Notons ces états $|\phi_j\rangle$ où l'indice j sert à les identifier. Le projecteur associé à chacun de ces états est défini comme

$$\hat{P}_j = |\phi_j\rangle\langle \phi_j|.$$

Les principales caractéristiques d'un projecteur sont qu'il est Hermitien ($\hat{P}_j^\dagger = \hat{P}_j$) et idempotent, c'est-à-dire que l'application d'un projecteur sur lui-même retourne le même projecteur

$$\hat{P}_j \hat{P}_j = |\phi_j\rangle\langle\phi_j| \phi_j\rangle\langle\phi_j| = |\phi_j\rangle\langle\phi_j| = \hat{P}_j.$$

Mesures projectives

Supposons que le système était initialement dans un état quelconque $|\psi\rangle$ et qu'à la suite d'une première mesure celui-ci est projeté dans l'état $|\phi_j\rangle$. On peut écrire l'état résultant normalisé grâce à son projecteur \hat{P}_j comme étant

$$|\phi_j\rangle = \frac{\hat{P}_j |\psi\rangle}{\sqrt{\langle\psi|\hat{P}_j^\dagger \hat{P}_j|\psi\rangle}}.$$

Il est alors intéressant de calculer la probabilité d'obtenir différents résultats en effectuant une seconde mesure subséquente à la première. On écrit $p(\phi_k|\phi_j)$ la probabilité que le système soit projeté dans l'état $|\phi_k\rangle$ lors d'une seconde mesure étant donné que celui-ci a été projeté dans l'état $|\phi_j\rangle$ lors de la première mesure. Cette probabilité se calcule ainsi

$$p(\phi_k|\phi_j) = |\langle\phi_k|\phi_j\rangle|^2 = \frac{|\langle\phi_k|\hat{P}_j|\psi\rangle|^2}{\langle\psi|\hat{P}_j^\dagger \hat{P}_j|\psi\rangle}.$$

Or, des mesures subséquentes d'un même système devraient toujours retourner le même résultat. Ainsi cette probabilité devrait être nulle si k et j sont différents. En revanche, cette probabilité devrait être de 100% si $k = j$. On résume cela avec l'équation suivante

$$p(\phi_k|\phi_j) = \frac{|\langle\phi_k|\hat{P}_j|\psi\rangle|^2}{\langle\psi|\hat{P}_j^\dagger \hat{P}_j|\psi\rangle} = \delta_{kj}.$$

En remplaçant l'expression du projecteur dans cette dernière équation, on obtient

$$\frac{|\langle\phi_k|\phi_j\rangle\langle\phi_j|\psi\rangle|^2}{|\langle\phi_j|\psi\rangle|^2} = \delta_{kj}.$$

où on a utilisé le fait que l'état $|\phi_j\rangle$ est normalisé. On constate que cette relation est vérifiée pourvu que

$$\langle\phi_k|\phi_j\rangle = \delta_{kj} \tag{4.9}$$

ce qui implique que les états quantiques $|\phi_j\rangle$ et $|\phi_k\rangle$ qui peuvent résulter de la mesure projective sont nécessairement orthogonaux entre eux (ou identiques dans le cas $k = j$).

Ce résultat est central pour la mesure projective. Il implique que les états vers lesquels une mesure peut projeter un système quantique doivent être orthogonaux et forment donc une base. Si ce n'était pas le cas, des mesures successives d'un même système pourraient retourner des résultats différents.

C.2 Équation aux valeurs propres

Les états $|\phi_j\rangle$ associés à l'observable \hat{A} , tels qu'introduits à la section précédente, sont nommés les états propres de \hat{A} . De manière générale, toute observable \hat{A} est caractérisée par un ensemble d'états propres $\{|\phi_j\rangle\}$. Chaque état propre répond à l'équation aux valeurs propres

$$\hat{A} |\phi_j\rangle = \lambda_j |\phi_j\rangle \tag{4.10}$$

où λ_j est la valeur propre de l'observable \hat{A} associée à l'état propre $|\phi_j\rangle$. L'indice j sert à énumérer tous les états propres et leurs valeurs propres correspondantes.

Les valeurs propres λ_j correspondent aux résultats possibles lors de la mesure de l'observable \hat{A} . À cause de l'effet projectif de la mesure en mécanique quantique, si le résultat de la mesure retourne la valeur λ_j , le système sera alors dans l'état associé $|\phi_j\rangle$ après la mesure².

Comme les états $|\phi_j\rangle$ forment une base, on peut appliquer par la gauche un état $\langle\phi_k|$ à l'équation aux valeurs propres 4.10 pour exprimer l'*élément de matrice* de \hat{A} dans la base $\{|\phi_j\rangle\}$ comme étant

$$\langle\phi_k|\hat{A}|\phi_j\rangle = \langle\phi_k|\lambda_j|\phi_j\rangle = \lambda_j\delta_{kj}. \quad (4.11)$$

Ainsi, dans la base des états de propres $\{|\phi_j\rangle\}$ l'observable \hat{A} prend la forme d'une matrice diagonale. Ceci n'a rien d'étonnant, car c'est la définition même de l'équation aux valeurs propres.

Exemple C.2 : Observables \hat{X} , \hat{Y} et \hat{Z}

Identifions les valeurs propres et les états de propres des observables \hat{X} , \hat{Y} et \hat{Z} en guise d'exemple.

Pour l'observable \hat{X} , les deux états qui se retrouvent sur l'axe x de la sphère de Bloch ($|+\rangle$ et $|-\rangle$) restent inchangés sous l'effet de l'opérateur \hat{X} . Ceux-ci répondent donc à l'équation aux valeurs propres de la manière suivante

$$\hat{X}|+\rangle = +1|+\rangle \quad \text{et} \quad \hat{X}|-\rangle = -1|-\rangle.$$

La valeur propre associée à l'état propre $|+\rangle$ est $+1$, et la valeur propre associée à l'état propre $|-\rangle$ est -1 . De manière similaire, les états propres de l'observable \hat{Y} sont les états $|+i\rangle$ et $|-i\rangle$ avec les valeurs propres respectives $+1$ et -1

$$\hat{Y}|+i\rangle = +1|+i\rangle \quad \text{et} \quad \hat{Y}|-i\rangle = -1|-i\rangle.$$

Finalement, l'observable la plus simple d'entre elles, \hat{Z} , est caractérisée par des états propres qui ne sont rien d'autre que les états de la base computationnelle

$$\hat{Z}|0\rangle = +1|0\rangle \quad \text{et} \quad \hat{Z}|1\rangle = -1|1\rangle.$$

Remarque

L'opérateur \hat{Z} est diagonal dans la base computationnelle, et donc ces états propres sont $|0\rangle$ et $|1\rangle$ par définition. C'est pour cette raison qu'on fait généralement référence à la mesure standard d'un qubit comme étant une mesure en \hat{Z} .

C.3 Dégénérescence

Il arrive que deux (ou plusieurs) états propres d'une observable partagent la même valeur propre. On dit alors que cette valeur propre est dégénérée. Dans ce cas, les états propres associés à cette même valeur propre forment un sous-espace. Ainsi, toute combinaison linéaire de ces états propres est également un état propre avec la même valeur.

Cela implique qu'il existe un choix dans la base des états propres de \hat{A} associé à ce sous-espace. La seule condition sur les états choisis pour ce sous-espace est qu'ils soient orthogonaux.

2. Si cette valeur propre est dégénérée les choses sont un peu plus compliquées que cela (voir section C.3).

Exemple C.3 : Dégénérescence

Considérons l'observable à nouveau $\hat{Z}\hat{Z}$. On a déjà établi (sans le mentionner) à l'exemple 4.B que les états de base

$$|00\rangle, |01\rangle, |10\rangle \text{ et } |11\rangle$$

sont des états propres de $\hat{Z}\hat{Z}$ avec les valeurs propres respectives

$$+1, -1, -1 \text{ et } +1.$$

La valeur propre +1 est dégénérée, car elle est associée à deux états propres, soient $|00\rangle$ et $|11\rangle$. La valeur propre -1 est également dégénérée pour les mêmes raisons. Ces deux valeurs propres sont associées aux sous-espaces

$$\{|00\rangle, |11\rangle\} \text{ et } \{|01\rangle, |10\rangle\}.$$

Ainsi tout état qui se retrouve dans un de ces sous-espaces est également un état propre de $\hat{Z}\hat{Z}$ avec la valeur propre associée. Par exemple,

$$|\Psi^+\rangle = \alpha |01\rangle + \beta |10\rangle$$

est un état propre de $\hat{Z}\hat{Z}$ avec la valeur propre +1. En effet,

$$\begin{aligned} \hat{Z}\hat{Z}|\Psi^+\rangle &= \alpha \hat{Z}\hat{Z}|01\rangle + \beta \hat{Z}\hat{Z}|10\rangle \\ &= \alpha (-1)|01\rangle + \beta (-1)|10\rangle = (-1)|\Psi^+\rangle. \end{aligned}$$

On pourrait donc choisir les états

$$|\Psi^+\rangle = \alpha |01\rangle + \beta |10\rangle \quad \text{et} \quad |\Psi^-\rangle = \beta^* |01\rangle - \alpha^* |10\rangle$$

comme base du sous-espace associé à la valeur propre (-1). En effet, ceux-ci sont bien orthogonaux

$$\langle \Psi^+ | \Psi^- \rangle = (\beta \langle 01| - \alpha \langle 10|)(\alpha |01\rangle + \beta |10\rangle) = \beta\alpha - \alpha\beta = 0$$

Remarque

La dégénérescence d'états quantiques peut amener son lot de complexités dans la description des phénomènes quantiques.

C.4 Forme spectrale

Tout opérateur qui répond à une équation aux valeurs propres telle que l'équation 4.10 peut être exprimée sous sa forme spectrale

$$\hat{A} = \sum_j \lambda_j |\phi_j\rangle\langle\phi_j| \quad (4.12)$$

qui apparait comme une combinaison linéaire des projecteurs des états propres de \hat{A} pondérés par leurs valeurs propres. On peut rapidement voir que cette formulation permet de respecter trivialement l'équation aux valeurs propres. En effet,

$$\hat{A}|\phi_j\rangle = \sum_k \lambda_k |\phi_k\rangle\langle\phi_k|\phi_j\rangle = \sum_k \lambda_k |\phi_k\rangle \delta_{kj} = \lambda_j |\phi_j\rangle$$

Exemple C.4 : Forme spectrale de \hat{Z}

La forme spectrale de l'opérateur \hat{Z} est simplement donnée par

$$\hat{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

Elle fait intervenir deux types d'ingrédients principaux. D'abord, les $|\cdot\rangle\langle\cdot|$ sont les projecteurs. La décomposition spectrale d'un opérateur est une combinaison linéaire des projecteurs pour les états propres de l'opérateur. Les coefficients devant chaque projecteur sont les valeurs propres associées à chaque état propre. Cette construction assure que l'équation aux valeurs propres de l'opérateur soit respectée. En effet, dans ce cas-ci on a

$$\hat{Z}|0\rangle = |0\rangle\langle 0|0\rangle - |1\rangle\langle 1|0\rangle = |0\rangle \quad \text{et} \quad \hat{Z}|1\rangle = |0\rangle\langle 0|1\rangle - |1\rangle\langle 1|1\rangle = -|1\rangle.$$

Remarque

L'écriture sous forme spectrale 4.12 n'est pas exclusive aux observables, mais s'applique également à tout opérateur qui répond à une équation aux valeurs propres de la forme 4.10.

Une forme spectrale particulièrement utile est celle de l'opérateur identité. Toutes les valeurs propres de l'opérateur identité sont égales à 1. Sa forme spectrale est donc simplement

$$\hat{I} = \sum_j |\phi_j\rangle\langle\phi_j|. \quad (4.13)$$

Comme toutes les valeurs propres de cet opérateur sont égales à 1, elles sont donc également toutes dégénérées. Cela implique qu'on peut définir une forme spectrale pour l'opérateur identité pour n'importe quelle base pourvu que celle-ci soit orthonormée. On fait souvent référence à cette équation comme étant la *relation de fermeture* et elle est régulièrement utilisée dans diverses démonstrations.

Exemple C.5 : Relation de fermeture à deux qubits

Pour un système à deux qubits, on peut écrire une relation de fermeture dans la base computationnelle comme étant

$$\hat{I} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|.$$

ou en utilisant les états définis à l'exemple C.3 qui sont une généralisation des états de Bell

$$\hat{I} = |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|.$$

Ces deux expressions sont égales et totalement équivalentes.

C.5 Opérateur Hermitien

Lorsqu'on spécifie une quantité physique d'un système, on lui attribue généralement une valeur (et des unités, mais notre discussion n'ira pas dans cette direction). Cette valeur est donnée sous la forme d'un nombre réel. On exige donc que toutes les valeurs propres d'une observable soient des nombres réels. On exige aussi que les états propres d'une observable soient orthogonaux. Ces deux conditions réunies impliquent qu'une observable est un opérateur Hermitien. La caractéristique qui définit un opérateur Hermitien est qu'il est égal à son conjugué Hermitien

$$\hat{A}^\dagger = \hat{A}.$$

On peut facilement démontrer qu'un opérateur Hermitien remplit ces deux critères en utilisant la forme spectrale de l'observable 4.12, le fait que ses valeurs propres soient réelles ainsi que les propriétés des projecteurs.

C.6 Probabilités de mesure

La mesure d'une observable \hat{A} sur un état $|\psi\rangle$ retourne donc un résultat parmi l'ensemble des valeurs propres $\{\lambda_j\}$ associées à cette observable. La probabilité d'obtenir chacun de ces résultats dépend de l'état du système avant la mesure. En effet, la probabilité d'obtenir que le système soit mesuré dans l'état $|\phi_j\rangle$ est donnée par la règle de Born

$$p_j = |\langle\phi_j|\psi\rangle|^2.$$

Dans le cas sans dégénérescence, cette probabilité donne directement la probabilité d'obtenir la valeur λ_j lors de cette mesure.

En revanche, s'il existe plus d'un état propre associé à une valeur propre $\lambda^{(g)}$, la probabilité d'obtenir cette valeur lors d'une mesure est égale à la somme des probabilités d'obtenir chacun des états propres associés à cette même valeur propre

$$p^{(g)} = \sum_{j \in g} |\langle\phi_j|\psi\rangle|^2.$$

C.7 Valeur moyenne

Comme les résultats de mesure d'un système quantique sont aléatoires, nos efforts pour acquérir de l'information sur celui-ci doivent donc reposer sur la répétition. En particulier, on peut s'intéresser à la valeur moyenne d'une observable. Comme chaque résultat de mesure λ_j a une probabilité p_j de survenir, la moyenne des valeurs propres λ_j pondérées par leurs probabilités de survenir est donc

$$\langle\hat{A}\rangle_\psi = \sum_j p_j \lambda_j. \quad (4.14)$$

Dans cette section, nous allons montrer que cette même valeur moyenne peut en fait être exprimée comme le produit suivant

$$\langle\hat{A}\rangle_\psi = \langle\psi|\hat{A}|\psi\rangle$$

que nous avons déjà rencontré aux sections 4.A et 4.B.

Valeur moyenne d'un état propre

Tentons d'abord d'exprimer la valeur moyenne pour un état propre de l'observable en question. À l'aide de l'expression pour un élément de matrice d'une observable dans sa base d'états propres 4.11, on peut facilement montrer que la valeur moyenne d'une observable \hat{A} sur un état propre $|\phi_j\rangle$ donne directement la valeur propre associée à cet état propre. En effet,

$$\langle\hat{A}\rangle_{\phi_j} = \langle\phi_j|\hat{A}|\phi_j\rangle = \lambda_j \delta_{jj} = \lambda_j \quad (4.15)$$

car l'état propre est normalisé. La probabilité d'obtenir la valeur propre λ_j lorsque le système est dans l'état $|\phi_j\rangle$ étant de 100% (et 0% pour tous les autres états), on constate que ce résultat est cohérent avec l'équation 4.14.

Valeur moyenne d'un état quelconque

Nous avons vu à l'équation 3.4 du chapitre 3 qu'un état quantique quelconque $|\psi\rangle$ peut toujours être écrit comme une combinaison linéaire de tous les états de base parce que ceux-ci constituent (justement) une base. Comme les états propres d'une observable forment une base (voir équation 4.9) on peut écrire un état quantique quelconque comme une combinaison linéaire de ceux-ci. On peut faire usage de la

relation de fermeture afin d'obtenir cette combinaison linéaire. En effet, en appliquant la forme spectrale de l'opérateur identité à un état quantique quelconque, on obtient

$$|\psi\rangle = \hat{I}|\psi\rangle = \sum_j |\phi_j\rangle\langle\phi_j|\psi\rangle = \sum_j \alpha_j |\phi_j\rangle$$

où les coefficients sont donnés par

$$\alpha_j = \langle\phi_j|\psi\rangle.$$

On peut donc toujours écrire un état quantique comme une combinaison linéaire des états propres d'une observable donnée.

Cette décomposition sur la base des états propres de l'observable nous permet de calculer la valeur moyenne d'une observable pour un état quantique quelconque. D'abord, on écrit cette valeur moyenne grâce au produit

$$\langle\hat{A}\rangle_\psi = \langle\psi|\hat{A}|\psi\rangle = \left(\sum_k \alpha_k^* \langle\phi_k|\right) \hat{A} \left(\sum_j \alpha_j |\phi_j\rangle\right)$$

où on a pris soin d'utiliser des indices différents pour les deux sommes et de prendre le complexe conjugué des coefficients du *bra*. En distribuant les produits, on fait apparaître les éléments de matrice de l'observable dans sa base propre

$$\langle\hat{A}\rangle_\psi = \sum_{k,j} \alpha_k^* \alpha_j \langle\phi_k|\hat{A}|\phi_j\rangle.$$

En utilisant l'équation 4.11, on obtient l'expression

$$\langle\hat{A}\rangle_\psi = \sum_j |\alpha_j|^2 \lambda_j$$

qui est exactement l'expression de la valeur moyenne de l'équation 4.14 car $p_j = |\alpha_j|^2 = |\langle\phi_j|\psi\rangle|^2$ est la probabilité d'obtenir l'état $|\phi_j\rangle$ lorsqu'on mesure l'observable \hat{A} sur l'état $|\psi\rangle$. L'appellation *valeur moyenne* prend alors tout son sens. En effet, celle-ci est une moyenne de toutes les valeurs propres de l'observable pondérée par les probabilités d'obtenir chacun des états propres.

D Précision de l'estimation

À chaque fois qu'on exécute et mesure un circuit quantique à n qubits on obtient un des 2^n états de base, et ce, de manière aléatoire. Chacun de ces états a une probabilité plus ou moins élevée de survenir. En réalité, chaque exécution du circuit correspond à un échantillon d'une variable aléatoire. En utilisant des concepts fondamentaux liés aux variables aléatoires (voir annexe D), nous allons établir comment évaluer la précision de l'estimation d'une valeur moyenne pour une observable quelconque.

À venir...

Chapitre 5

Algorithmes quantiques jouets

Les algorithmes jouets sont des algorithmes quantiques qui n'ont pas nécessairement d'applications pratiques. Cependant, ce sont les premiers à avoir été imaginés qui exploitent les phénomènes de superposition, d'intrication et d'interférence afin d'effectuer des opérations plus efficacement que pourrait le faire un ordinateur classique. Ces algorithmes ont contribué de manière importante à l'émergence du domaine de l'information et de la programmation quantique en suscitant l'intérêt des scientifiques.

En plus d'offrir une perspective historique sur les débuts de la programmation quantique, les algorithmes jouets permettent également de se familiariser avec certaines astuces qui peuvent être utilisées pour exploiter les phénomènes quantiques.

A Algorithme de Deutsch

L'algorithme de Deutsch est probablement l'exemple le plus élémentaire d'un algorithme qui utilise le traitement quantique de l'information pour résoudre un problème plus efficacement que la meilleure solution classique. Cet algorithme illustre également comment il est possible de sacrifier une partie de l'information acquise lors d'une solution classique pour répondre plus rapidement une question bien précise.

Nous allons d'abord présenter le problème ainsi que sa solution classique. On présentera ensuite comment le problème peut être posé de manière quantique et nous tenterons de construire de manière intuitive une solution quantique qui exploitera le parallélisme quantique.

L'algorithme de Deutsch fait usage de fonctions binaires qui prennent en entrée un bit d'information x (0 ou 1) et qui retournent un bit d'information $f(x)$ (0 ou 1). Il n'existe que quatre fonctions de ce type. Leurs effets sont présentés au tableau 5.1.

	x	0	1
f_0	$f(x)$	0	0
f_1		0	1
f_2		1	0
f_3		1	1

TABLE 5.1 – Les quatre fonctions binaires.

On distingue deux types parmi ces fonctions : les fonctions *constantes* où le résultat est toujours le même ($f(0) = f(1)$) et les fonctions *balancées* dont le résultat est différent pour différentes entrées ($f(0) \neq f(1)$).

A.1 Problème

Le problème de Deutsch se formule ainsi. On vous donne accès à une fonction $f(x)$ sans vous dire de laquelle il s'agit. On vous demande d'identifier si cette fonction est une fonction *constante* ou une fonction

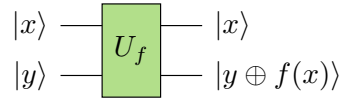


FIGURE 5.1 – Forme de l’oracle pour l’algorithme de Deutsch sous la forme d’une porte quantique à 2 qubits qui évalue la fonction $f(x)$.

balancée en utilisant celle-ci le moins souvent possible.

A.2 Solution classique

La solution classique à ce problème demande d’évaluer la fonction deux fois. On l’évalue d’abord pour $f(x = 0)$ et ensuite pour $f(x = 1)$ pour finalement comparer les deux résultats obtenus. Si les résultats sont identiques, la fonction est constante, sinon elle est balancée.

Remarque

Avec deux évaluations, on possède toute l’information pour identifier laquelle des quatre fonctions il s’agit ; pas seulement si elle est constante ou balancée. En quelque sorte, on a acquis trop d’information. La solution quantique au problème de Deutsch que nous allons voir est un bon exemple où l’on sacrifie une certaine quantité d’information (qui nous n’est pas essentielle) pour répondre à une question plus rapidement.

A.3 Solution quantique

Dans la version quantique de ce problème, la fonction est fournie sous la forme d’une porte quantique à deux qubits qui agit de la manière suivante sur les états de base

$$\hat{U}_f |y\rangle |x\rangle = |y \oplus f(x)\rangle |x\rangle \quad (5.1)$$

où x et y peuvent prendre les valeurs 0 et 1. Celle-ci peut également être présentée sous forme du circuit quantique à la figure 5.1. Cette porte utilise l’état $|x\rangle$ pour calculer $f(x)$. Elle modifie ensuite l’état du second qubit en effectuant une addition modulo 2 entre sa valeur initiale y et le résultat de $f(x)$.

Info notation A.1 : L’oracle

La porte \hat{U}_f qui définit le problème de Deutsch est souvent appelée un oracle. Le concept d’oracle revient régulièrement pour de nombreux algorithmes quantiques. En règle générale, l’oracle est une porte quantique qui permet de distinguer différents états quantiques. Pour la plupart des algorithmes jouets, l’oracle est souvent présenté comme une boîte noire dont on ignore le fonctionnement. Il apparait également nécessaire de déjà connaître la solution au problème pour pouvoir construire l’oracle, rendant le concept totalement inutile.

Cela n’est (heureusement) qu’une conséquence de la simplicité inhérente des problèmes jouets. Pour des problèmes suffisamment complexes, il sera possible de construire un oracle sans nécessairement être capable de décrire son effet sur les différents états quantiques.

Exemple A.1 : Application de la porte unitaire U_{f_2}

Supposons que la fonction utilisée est f_2 (voir le tableau 5.1). Voici comment cette porte modifie les quatre états de base à deux qubits :

$$\begin{aligned} \hat{U}_{f_2} |0\rangle |0\rangle &= |0 \oplus f(0)\rangle |0\rangle = |0 \oplus 1\rangle |0\rangle = |1\rangle |0\rangle \\ \hat{U}_{f_2} |0\rangle |1\rangle &= |0 \oplus f(1)\rangle |1\rangle = |0 \oplus 0\rangle |1\rangle = |0\rangle |1\rangle \\ \hat{U}_{f_2} |1\rangle |0\rangle &= |1 \oplus f(0)\rangle |0\rangle = |1 \oplus 1\rangle |0\rangle = |0\rangle |0\rangle \\ \hat{U}_{f_2} |1\rangle |1\rangle &= |1 \oplus f(1)\rangle |1\rangle = |1 \oplus 0\rangle |1\rangle = |1\rangle |1\rangle. \end{aligned}$$

Exercice A.1 : Application de la porte unitaire U_{f_3}

Évaluez comment la porte unitaire \hat{U}_{f_3} transforme les quatre états de base à deux qubits à l'aide de la fonction f_3 . En vous basant sur vos résultats et sur l'exemple précédent, discuter si \hat{U}_f est une transformation unitaire en général.

Remarque

La porte \hat{U}_f ne fait pas simplement évaluer la fonction $f(x)$, mais fait intervenir son évaluation dans le cadre d'une transformation unitaire. En effet, il n'est pas possible de simplement construire une transformation unitaire qui aurait l'effet suivant

$$\hat{U}_f |x\rangle = |f(x)\rangle$$

car celle-ci ne serait pas inversible et donc non unitaire.

En ayant accès à la porte \hat{U}_f on peut exploiter la superposition d'états quantique afin de résoudre le problème de Deutsch avec une seule évaluation et donc faire mieux que la solution classique qui en requiert deux.

Parallélisme quantique

Le parallélisme quantique consiste à appliquer une porte quantique sur un état en superposition afin d'effectuer plusieurs évaluations en parallèle. Comme on aimerait évaluer $f(x)$ pour $x = 0$ et $x = 1$ en même temps, on est tenté de placer le premier qubit dans une superposition d'états. Voyons voir comment \hat{U}_f agit sur l'état $|y\rangle |+\rangle$ où le second qubit est laissé dans un état de base arbitraire. Comme l'effet de \hat{U}_f est bien défini sur les états de base, écrivons d'abord,

$$|y\rangle |+\rangle = |y\rangle \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) = \frac{|y\rangle |0\rangle + |y\rangle |1\rangle}{\sqrt{2}}.$$

L'application de \hat{U}_f , à l'aide de l'équation 5.1, est alors triviale

$$\hat{U}_f |y\rangle |+\rangle = \frac{\hat{U}_f |y\rangle |0\rangle + \hat{U}_f |y\rangle |1\rangle}{\sqrt{2}} = \frac{|y \oplus f(0)\rangle |0\rangle + |y \oplus f(1)\rangle |1\rangle}{\sqrt{2}}. \quad (5.2)$$

L'état obtenu fait intervenir les deux évaluations $f(0)$ et $f(1)$ en même temps, alors qu'on a utilisé \hat{U}_f qu'une seule fois ! Malheureusement, si l'on mesure les qubits alors que le système est dans cet état, on ne pourra connaître qu'une seule de ces deux évaluations.

Exemple A.2 : Algorithme de Deutsch incomplet

Illustrons ce que la mesure des qubits pour un système dans l'état quantique de l'équation 5.2 pourrait retourner. Dans le cas où $y = 0$, l'état quantique est

$$\hat{U}_f |0\rangle |+\rangle = \frac{|f(0)\rangle |0\rangle + |f(1)\rangle |1\rangle}{\sqrt{2}}.$$

Les résultats de mesure possibles sont

$$|f(0)\rangle |0\rangle \quad \text{et} \quad |f(1)\rangle |1\rangle$$

et les deux ont autant de chances de survenir. Si la mesure du premier qubit retourne 0 le second qubit est projeté dans l'état $f(0)$, et si on obtient 1 le second qubit est projeté dans l'état $f(1)$. Dans tous les cas, la mesure du second qubit ne nous permet d'obtenir d'une seule des deux évaluations de la fonction f . On arrive à une conclusion équivalente pour $y = 1$.

Jeu de phase

Placer le premier qubit dans une superposition d'états n'est pas suffisant pour résoudre le problème de Deutsch. Il est nécessaire de faire intervenir l'interférence pour obtenir le résultat recherché en une seule évaluation. Et, qui dit interférence, dit phase. Notre objectif est alors de faire intervenir l'évaluation de $f(x)$ dans une phase quantique.

Il est possible de faire cela en initialisant le second qubit dans l'état $|-\rangle$. Voyons voir comment la porte \hat{U}_f agit sur l'état $|-\rangle |x\rangle$ où c'est maintenant l'état du premier qubit est laissé arbitraire. D'abord, écrivons l'état

$$|-\rangle |x\rangle = \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) |x\rangle = \frac{|0\rangle |x\rangle - |1\rangle |x\rangle}{\sqrt{2}}.$$

Appliquons ensuite l'opérateur unitaire

$$\hat{U}_f |-\rangle |x\rangle = \frac{\hat{U}_f |0\rangle |x\rangle - \hat{U}_f |1\rangle |x\rangle}{\sqrt{2}} = \frac{|0 \oplus f(x)\rangle |x\rangle - |1 \oplus f(x)\rangle |x\rangle}{\sqrt{2}} = \left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \right) |x\rangle$$

où on a refactorisé l'état $|x\rangle$ du premier qubit. On distingue alors deux possibilités pour l'état du second qubit. Soit $f(x) = 0$ et son état reste inchangé ($|-\rangle$), soit $f(x) = 1$ et son état devient

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

faisant apparaître une phase -1 . On peut alors résumer l'effet de \hat{U}_f en général comme étant,

$$\hat{U}_f |-\rangle |x\rangle = (-1)^{f(x)} |-\rangle |x\rangle \quad (5.3)$$

où on utilise le fait que

$$(-1)^{f(x)} = \begin{cases} (-1)^0 = 1 & \text{pour } f(x) = 0, \text{ ou} \\ (-1)^1 = -1 & \text{pour } f(x) = 1. \end{cases}$$

Info notation A.2 : Des phases et des exposants

L'utilisation d'exposants appliqués à -1 (ou encore à i) revient régulièrement dans les développements d'algorithmes quantiques. On exploite simplement la structure des nombres complexes (voir l'annexe B). En particulier, n'importe quel nombre à l'exposant 0 retourne 1 et n'importe quel nombre à l'exposant 1 retourne ce même nombre

$$b^0 = 1$$

$$b^1 = b.$$

Jeu d'interférence

Combinons le parallélisme quantique avec le jeu de phase pour voir si cela nous permet de résoudre le problème de Deutsch. En d'autres termes, on veut appliquer l'unitaire \hat{U}_f sur l'état $|-\rangle |+\rangle$. Comme on sait écrire son effet lorsque le second qubit est dans l'état $|-\rangle$ (équation 5.3) il est suffisant d'écrire seulement l'état du premier qubit dans la base computationnelle

$$|-\rangle |+\rangle = \frac{|-\rangle |0\rangle + |-\rangle |1\rangle}{\sqrt{2}} \quad (5.4)$$

L'application de l'unitaire, à l'aide de l'équation 5.3, produit alors l'état

$$\hat{U}_f |-\rangle |+\rangle = \frac{(-1)^{f(0)} |-\rangle |0\rangle + (-1)^{f(1)} |-\rangle |1\rangle}{\sqrt{2}} = |-\rangle \left(\frac{(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle}{\sqrt{2}} \right). \quad (5.5)$$

On constate que cet état est un état produit et que chaque qubit peut être étudié indépendamment de l'autre. Le second qubit restant dans l'état $|-\rangle$, il est inutile de le mesurer.

En contrepartie, l'état du premier qubit est alors très intéressant, car il fait intervenir les deux évaluations de f en même temps. En particulier, si $f(0) = f(1)$ les phases devant les deux états de base sont les mêmes, alors qu'une phase relative de -1 apparaît si $f(0) \neq f(1)$. En d'autres termes, le premier qubit est (à une phase globale près) dans l'état

$$|+\rangle \text{ si } f(0) = f(1) \quad \text{ou} \quad |-\rangle \text{ si } f(0) \neq f(1).$$

Pour distinguer entre ces deux possibilités, on doit simplement introduire une porte Hadamard sur ce premier qubit pour transformer les états $|+\rangle$ et $|-\rangle$ en $|0\rangle$ et $|1\rangle$ respectivement. On peut alors mesurer ce qubit. Si l'on obtient la valeur 0 on sait que $f(0) = f(1)$ et que la fonction est constante, alors que si l'on obtient 1 on sait que $f(0) \neq f(1)$ et que la fonction est balancée.

On peut rendre cela plus explicite en modifiant l'écriture de l'état du premier qubit dans l'équation 5.5. En effet, isolons une phase globale pour écrire,

$$\frac{(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle}{\sqrt{2}} \propto \frac{|0\rangle + (-1)^{f(0) \oplus f(1)} |1\rangle}{\sqrt{2}}$$

ce qui rend plus explicite que cet état est soit $|+\rangle$ ou $|-\rangle$.

Info notation A.3 : Ignorer une phase globale

Nous avons introduit le symbole *proportionnel* à (\propto) pour indiquer que la phase globale $(-1)^{f(0)}$ pouvait être ignorée. En effet,

$$\frac{(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle}{\sqrt{2}} = (-1)^{f(0)} \left(\frac{|0\rangle + (-1)^{f(1)-f(0)} |1\rangle}{\sqrt{2}} \right) \propto \frac{|0\rangle + (-1)^{f(1)-f(0)} |1\rangle}{\sqrt{2}}.$$

Info notation A.4 : Des phases et des exposants pairs ou impairs

Nous avons également introduit l'addition modulo 2 (\oplus ou XOR) dans l'exposant de la phase relative. En effet, le facteur de phase relatif

$$(-1)^{f(1)-f(0)}$$

ne peut prendre que les valeurs ± 1 dépendamment si l'exposant est pair ou impair. Or, la parité d'une soustraction est la même que celle d'une addition ou d'une addition modulo 2

$$f(1) - f(0) \pmod{2} = f(1) + f(0) \pmod{2} = f(0) \oplus f(1).$$

Finalement, l'application d'une porte Hadamard sur cet état permet d'obtenir l'état final,

$$\hat{H} \frac{|0\rangle + (-1)^{f(0) \oplus f(1)} |1\rangle}{\sqrt{2}} = |f(0) \oplus f(1)\rangle$$

ou encore, pour l'ensemble de deux qubits,

$$|-\rangle |f(0) \oplus f(1)\rangle. \tag{5.6}$$

La mesure du premier qubit retourne donc directement

$$f(0) \oplus f(1) = \begin{cases} 0 & \text{si } f(0) = f(1) \text{ ou} \\ 1 & \text{si } f(0) \neq f(1). \end{cases}$$

Ainsi, si ce qubit est mesuré dans l'état 0, on apprend que la fonction est constante. S'il est mesuré dans l'état 1, cela veut dire que la fonction est balancée.

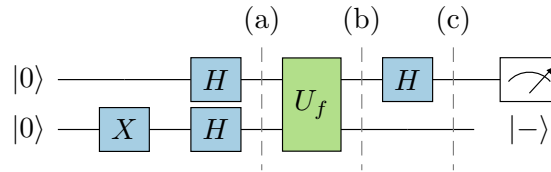


FIGURE 5.2 – Circuit quantique de l’algorithme de Deutsch.

Circuit quantique

Le circuit quantique présenté à la figure 5.2 résume l’implémentation de l’algorithme de Deutsch. Les états quantiques aux points (a), (b) et (c) sont respectivement donnés par les équations 5.4, 5.5 et 5.6.

Comme on le voit l’algorithme de Deutsch permet de déterminer si une fonction $f(x)$ est constante ou balancée en exécutant une seule fois le circuit présenté à la figure 5.2 et, par conséquent, en appelant la fonction qu’une seule fois. Notez également que le résultat obtenu après l’exécution de ce circuit ne permet pas de distinguer de laquelle des 4 fonctions il s’agit. On a donc sacrifié l’information qui nous aurait permis de faire cette distinction pour répondre au problème de Deutsch plus rapidement.

Exercice A.2 : Circuits quantiques pour les fonctions binaires

Construisez quatre circuits à deux qubits qui implémentent l’évaluation des quatre fonctions $f(x)$ sous la forme donnée à l’équation 5.1 et à la figure 5.1. (*Indice* : Retournez voir la figure 2.2 pour vous aider.)

B Algorithme de Deutsch-Jozsa

L’algorithme de Deutsch-Jozsa est une tentative de généraliser l’algorithme de Deutsch afin d’impliquer un plus grand nombre de qubits. Cette version de l’algorithme fait intervenir des fonctions qui prennent en entrée n bits qu’on note x_0 à x_{n-1} et qui retourne un seul bit

$$y = f(x_0, x_1, \dots, x_{n-1}).$$

Comme un ensemble de n bits peut être interprété comme un entier situé entre 0 et $2^n - 1$, on peut également ces fonctions comme prenant en entrée un entier x et retournant un bit

$$y = f(x).$$

Pour cet algorithme on se limite aux mêmes types de fonction que pour l’algorithme de Deutsch, c’est-à-dire des fonctions constantes qui retournent toujours la même chose, et des fonctions balancées qui elles sont garanties de retourner 0 pour la moitié des entrées possibles et 1 pour l’autre moitié. Comme il y a 2^n entrées possibles, une fonction balancée retourne 0 pour $2^n/2 = 2^{n-1}$ entrées possibles et retourne 1 pour les autres 2^{n-1} entrées possibles.

B.1 Problème

Le problème de Deutsch-Jozsa se formule exactement de la même manière que pour l’algorithme de Deutsch. On vous donne accès à une fonction $f(x)$ sans vous dire de quel type il s’agit. On vous demande d’identifier si cette fonction est une fonction *constante* ou une fonction *balancée* en utilisant celle-ci le moins souvent possible.

B.2 Solution classique

Comme pour la version originale de l’algorithme de Deutsch, la solution classique de l’algorithme de Deutsch-Jozsa consiste à essayer un certain nombre d’entrées différentes pour vérifier si la fonction utilisée

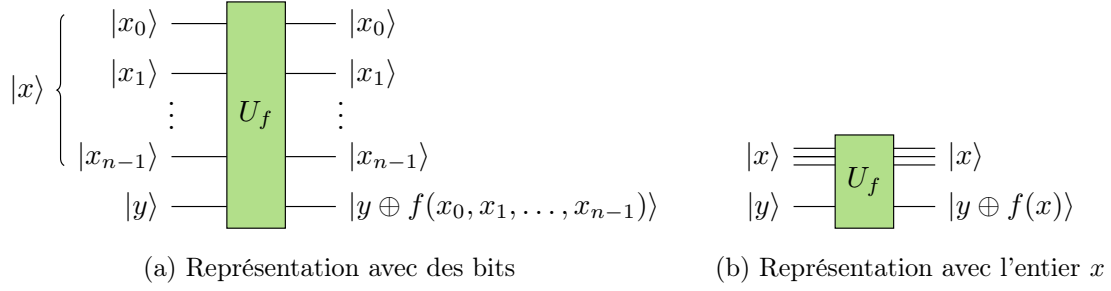


FIGURE 5.3 – Forme de l'oracle pour l'algorithme de Deutsch-Jozsa sous la forme d'une porte quantique à $n + 1$ qubits qui évalue la fonction $f(x)$.

est constante ou balancée. Combien d'entrées différentes doit-on essayer avant d'être complètement certain que la fonction est constante ou balancée ?

D'un côté, du moment que la fonction retourne deux résultats différents, on sait que la fonction balancée (elle ne peut pas être constante). De l'autre côté, si on n'est vraiment pas chanceux, il se peut qu'on essaie les 2^{n-1} entrées qui produisent le même résultat. Il faut donc évaluer la fonction sur $2^{n-1} + 1$ entrées possibles pour s'assurer qu'elle est constante.

B.3 Solution quantique

La solution quantique de ce problème est très similaire à celle du problème de Deutsch à l'exception que la porte quantique de l'oracle doit maintenant évaluer une fonction de n bits

$$\hat{U}_f |y\rangle |x_{n-1} \cdots x_0\rangle = |y \oplus f(x_0, \dots, x_{n-1})\rangle |x_{n-1} \cdots x_0\rangle. \quad (5.7)$$

Le circuit représentant cette porte est illustré à la figure 5.3a. En interprétant les bits comme un entier, le circuit de la porte quantique s'exprime de manière plus compacte (voir figure 5.3b) et l'effet de l'oracle se résume à

$$\hat{U}_f |y\rangle |x\rangle = |y \oplus f(x)\rangle |x\rangle \quad (5.8)$$

avec

$$|x\rangle = |x_{n-1} \cdots x_0\rangle.$$

Encore une fois, nous allons placer le qubit $|y\rangle$ dans l'état $|-\rangle$ de sorte que l'application de cette porte évalue la fonction $f(x)$ dans un facteur de phase

$$\begin{aligned} \hat{U}_f |-\rangle |x\rangle &= \hat{U}_f \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) |x\rangle \\ &= \frac{1}{\sqrt{2}}(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) |x\rangle \\ &= (-1)^{f(x)} |-\rangle |x\rangle. \end{aligned} \quad (5.9)$$

Circuit quantique

Nous allons construire le circuit quantique pour l'algorithme de Deutsch-Jozsa en nous inspirant directement du circuit quantique pour l'algorithme de Deutsch à la figure 5.2. Dans ce cas-ci, pour exploiter le parallélisme quantique, nous allons appliquer des portes Hadamard sur les n premiers qubits qui encode l'entier x . Cela va nous permettre d'évaluer la fonction $f(x)$ pour les 2^n valeurs possibles de x en même temps. Le circuit quantique à utiliser pour l'algorithme de Deutsch-Jozsa est illustré à la figure 5.4.

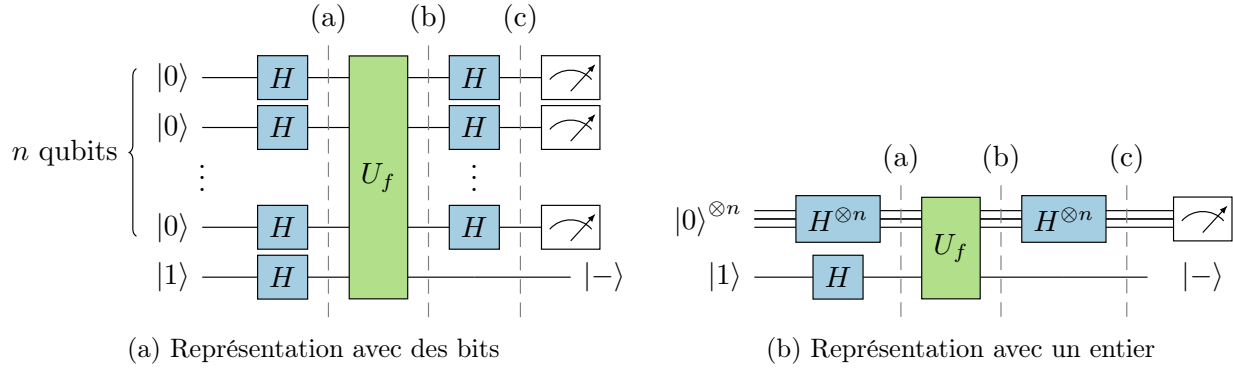


FIGURE 5.4 – Circuit quantique de l’algorithme de Deutsch-Jozsa.

Transformation unitaire

Voyons voir comment ce circuit modifie l’état des qubits. Procédons étape par étape pour bien comprendre comment fonctionne l’algorithme de Deutsch-Jozsa. D’abord, les portes Hadamard appliquées sur les n premiers qubits préparent une superposition uniforme de tous les états de base¹

$$\hat{H}^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle. \quad (5.10)$$

Une porte Hadamard est également appliquée sur le dernier qubit (initialement dans l’état $|1\rangle$) pour le placer dans l’état $|-\rangle$. L’état quantique du système au point (a) est donc

$$|\psi^{(a)}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |-\rangle |x\rangle. \quad (5.11)$$

Ensuite, on applique la porte \hat{U}_f à cet état. L’état quantique devient

$$|\psi^{(b)}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \hat{U}_f |-\rangle |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |-\rangle |x\rangle \quad (5.12)$$

où on a utilisé l’équation 5.9. Il ne reste qu’à appliquer une transformation d’Hadamard sur les n premiers qubits. Nous devons ici faire usage de l’équation suivante

$$\hat{H}^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle.$$

qui décrit l’effet d’une transformation Hadamard appliquée à n’importe quel état de base. Consultez l’annexe A.1 pour une démonstration. En résumé, la transformation Hadamard d’un état de base produit une superposition uniforme de tous les états de base où chacun d’eux est affecté par une phase qui dépend du produit scalaire (modulo 2) entre les bits de l’entier z et les bits de l’entier x de l’état de base initial.

En appliquant cette transformation à l’état $|\psi^{(b)}\rangle$ on obtient l’état quantique final²

$$\begin{aligned} |\psi^{(c)}\rangle &= |-\rangle \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \hat{H}^{\otimes n} |x\rangle \\ &= |-\rangle \frac{1}{2^n} \sum_{z=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{x \cdot z \oplus f(x)} |z\rangle. \end{aligned} \quad (5.13)$$

1. Voir l’équation A.3 à l’annexe A.1 pour vous en convaincre.

2. Consultez l’info notation A.4 si la présence du \oplus dans le facteur de phase vous laisse perplexe.

Résultats de mesure

Voyons maintenant comment les résultats de mesure nous informent si la fonction $f(x)$ est balancée ou constante. Fait étonnant, il est nécessaire de considérer uniquement la probabilité de mesurer les n premiers qubits dans l'état $|0\rangle$. Avant la mesure, les n premiers qubits sont, à priori dans un état de superposition de tous les états de base

$$\sum_{z=0}^{2^n-1} \alpha_z |z\rangle = \frac{1}{2^n} \sum_{z=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{x \cdot z \oplus f(x)} |z\rangle.$$

Pour calculer la probabilité de mesurer tous les qubits dans l'état 0 on doit d'abord obtenir l'amplitude de probabilité devant l'état $|z=0\rangle$. On l'obtient facilement comme étant

$$\alpha_0 = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}.$$

Dans l'éventualité où la fonction est constante, elle est indépendante de x . Notons sa valeur simplement par f . Dans ce cas,

$$\alpha_0 = \frac{(-1)^f}{2^n} \sum_{x=0}^{2^n-1} 1 = \frac{(-1)^f}{2^n} 2^n = (-1)^f \quad \text{et} \quad p_0 = |\alpha_0|^2 = 1.$$

Dans l'éventualité où la fonction est balancée, la somme sur x comporte autant de termes positifs que négatifs; elle est donc nulle. Dans ce cas,

$$\alpha_0 = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} = \frac{1}{2^n} (2^n/2 - 2^n/2) = 0 \quad \text{et} \quad p_0 = |\alpha_0|^2 = 0.$$

En résumé, l'algorithme de Deutch permet de distinguer en une seule exécution du circuit de la figure 5.4 si la fonction $f(x)$ est constante ou balancée. Si tous les qubits sont mesurés dans l'état $|0\rangle$, la fonction est constante, dans tous les autres cas elle est balancée.

L'algorithme de Deutch-Jozsa est plutôt contraignant au niveau du type de fonctions qu'il peut considérer. En particulier, il n'existe seulement que deux fonctions constantes, peu importe le nombre de bits d'entrée.

C Algorithme de Bernstein-Vazirani

Supposons que vous participiez à un jeu où vous devez deviner un nombre s choisi au hasard entre 0 et 15 inclusivement. Pour le découvrir, vous avez le droit de poser au meneur de jeu des questions qui se répondent par oui ou non. Quelle stratégie devriez-vous utiliser pour déterminer de quel nombre il s'agit en posant le moins de questions possible?

D'une certaine manière, l'algorithme de Bernstein-Vazirani permet de déterminer ce nombre en une seule question! Un autre aspect intéressant de cet algorithme est qu'il utilise exactement le même circuit que l'algorithme de Deutch-Jozsa.

C.1 Problème

Pour ce problème, le nombre à deviner est noté s . Pour cet exemple, on suppose qu'il est situé entre 0 et 15, mais dans un cas général il serait situé entre 0 et $2^n - 1$ où n est un nombre de bits donné. Ce nombre est encodé dans une fonction du type

$$f_s(x) = s \cdot x \pmod{2}$$

qui prend en entrée un entier x . On sous la forme binaire

$$f_s(x_0, x_1, \dots, x_{n-1}) = s_0x_0 + s_1x_1 + \dots + s_{n-1}x_{n-1} \pmod{2}.$$

Celle-ci effectue un produit scalaire entre les bits des entiers x et s et applique une opération modulo 2 pour retourner 0 ou 1. En d'autres termes, ce type de fonction compte le nombre de 1 que x a en commun (au même endroit) avec s et retourne 0 si ce nombre est pair ou 1 s'il est impair.

C.2 Solution classique

Une approche systématique pour identifier l'entier s est d'utiliser des entiers qui sont caractérisés par une décomposition binaire qui ne comporte qu'un seul 1. Par exemple, en utilisant

$$x = 8 \quad (x_3x_2x_1x_0 = 1000)$$

on peut confirmer la valeur du bit le plus à gauche pour l'entier s . En effet, si la fonction retourne 0, c'est que ce bit est 0, sinon ce bit est 1. L'utilisation de $x = 8$ revient à demander « Est-ce que s est plus grand ou égal à 8 ? ». En effet, tous les nombres plus grands ou égaux à 8 ont un 1 à cet endroit dans leur représentation binaire.

Pour un nombre s ayant une représentation binaire d'au maximum 4 bits, il faudra appeler la fonction 4 fois. Le tableau 5.2 dresse l'exemple des résultats obtenus dans le cas où $s = 6$ (0110) et dresse la liste des possibilités à chaque étape.

x	$s = 0110$	$f_s(x)$	Possibilités
8	1000	0	0, 1, 2, 3, 4, 5, 6 ou 7
4	0100	1	4, 5, 6, 7
2	0010	1	6 ou 7
1	0001	0	6

TABLE 5.2 – Exemple d'élimination pour le problème de Bernstein-Vazirani

De manière générale, pour un nombre situé entre 0 et $2^n - 1$, il faudra appeler la fonction n fois pour déterminer les n bits qui composent sa représentation binaire.

C.3 Solution quantique

Pour solutionner le problème de Bernstein-Vazirani avec un algorithme quantique on utilise exactement le même circuit quantique que pour l'algorithme de Deutsch-Jozsa, tel qu'illustré à la figure 5.4. La porte quantique de l'oracle doit alors avoir l'effet suivant

$$\hat{U}_f |y\rangle |x\rangle = |y \oplus f_s(x)\rangle |x\rangle. \quad (5.14)$$

Comme le circuit quantique et la forme de l'oracle sont identiques à ceux de l'algorithme de Deutsch-Jozsa, on peut facilement comprendre le fonctionnement de l'algorithme de Bernstein-Vazirani en réutilisant l'équation 5.13. En y remplaçant simplement la fonction $f_s(x)$ on obtient l'état quantique suivant

$$|\psi^{(c)}\rangle = |-\rangle \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{z=0}^{2^n-1} (-1)^{x \cdot (z \oplus s)} |z\rangle. \quad (5.15)$$

En effectuant une simple mise en évidence des produits scalaires dans le facteur de phase, l'état quantique des n premiers qubits peut s'écrire

$$\sum_{z=0}^{2^n-1} \alpha_z |z\rangle = \frac{1}{2^n} \sum_{z=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{x \cdot (z \oplus s)} |z\rangle.$$

L'amplitude de probabilité devant l'état $|z\rangle$ est donc,

$$\alpha_z = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{x \cdot (z \oplus s)}.$$

On peut montrer que toutes ces amplitudes sont nulles sauf celle pour $z = s$ qui est égale à 1. Pour démontrer cela, supposons que les représentations binaires de z et s diffèrent pour un seul bit. L'addition modulo 2 $z \oplus s$ possède donc un 1 à cet endroit. Parmi tous les entiers x qui font partie de la somme, il y en a autant qui ont un 0 qu'il y en a qui ont un 1 à cet endroit. Il y a donc autant de phases positives que négatives et la somme est nulle. Ce raisonnement tient pour toutes les valeurs de z sauf pour $z = s$. Pour celui-ci, on obtient

$$\alpha_s = \frac{1}{2^n} \sum_{x=0}^{2^n-1} 1 = 1.$$

et on a 100% des chances de mesurer l'état $|s\rangle$. Ce faisant, on peut déterminer le nombre s en exécutant ce circuit qu'une seule fois.

S Solutions aux exercices

Exercice A.1 : Application de la porte unitaire U_{f_3}

La porte unitaire \hat{U}_{f_3} transforme les quatre états de base à deux qubits de la manière suivante

$$\begin{aligned}\hat{U}_{f_3} |0\rangle |0\rangle &= |0 \oplus f(0)\rangle |0\rangle = |0 \oplus 1\rangle |0\rangle = |1\rangle |0\rangle \\ \hat{U}_{f_3} |0\rangle |1\rangle &= |0 \oplus f(1)\rangle |1\rangle = |0 \oplus 1\rangle |1\rangle = |1\rangle |1\rangle \\ \hat{U}_{f_3} |1\rangle |0\rangle &= |1 \oplus f(0)\rangle |0\rangle = |1 \oplus 1\rangle |0\rangle = |0\rangle |0\rangle \\ \hat{U}_{f_3} |1\rangle |1\rangle &= |1 \oplus f(1)\rangle |1\rangle = |1 \oplus 1\rangle |1\rangle = |0\rangle |1\rangle.\end{aligned}$$

Comme chaque état de base apparaît une seule fois dans les résultats obtenus à partir des quatre états de base (\hat{U}_{f_3} agit comme une bijection), et que ceux-ci sont normalisés, \hat{U}_{f_3} doit être unitaire.

Annexe A

Démonstrations

Cette annexe contient des démonstrations qui trouvent des applications à plusieurs endroits dans les notes ou qui sont trop lourdes et auraient nui à la lecture.

1 Transformation Hadamard à plusieurs qubits

La transformation Hadamard à plusieurs qubits est impliquée dans de nombreux algorithmes. En particulier, on s'intéresse ici à la transformation des états de base à n qubits.

1.1 Transformation du premier état de base

Comme tous les qubits du premier état de base sont dans l'état $|0\rangle$, l'application d'une porte Hadamard sur chacun d'eux va produire un état $|+\rangle$. On peut expliciter cela en écrivant.

$$\hat{H}^{\otimes n} |0\rangle^{\otimes n} = \bigotimes_{q=0}^{n-1} \hat{H} |0\rangle = \bigotimes_{q=0}^{n-1} |+\rangle = |+\rangle^{\otimes n}.$$

On va montrer ici, qu'un tel état est en fait une superposition uniforme de tous les états de base à n qubits. D'abord, on écrit chacun des états $|+\rangle$ en fonction des états de base à un qubit

$$|+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \bigotimes_{q=0}^{n-1} (|0\rangle + |1\rangle).$$

On explicite ensuite le produit tensoriel pour obtenir n paires de termes

$$\frac{1}{\sqrt{2^n}} \bigotimes_{q=0}^{n-1} (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2^n}} \underbrace{(|0\rangle + |1\rangle) \otimes \dots \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)}_{n \text{ fois}}.$$

On peut facilement se convaincre que le produit de ces n paires de termes va produire une somme 2^n termes

$$\underbrace{(|0\rangle + |1\rangle) \otimes \dots \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)}_{n \text{ fois}} = \underbrace{|0\dots 00\rangle + |0\dots 01\rangle + |0\dots 10\rangle + \dots + |1\dots 11\rangle}_{2^n \text{ termes}} \quad (\text{A.1})$$

qui ne sont rien d'autre que tous les états de base à n qubits. Ainsi, on peut résumer que le produit tensoriel de n qubits dans l'état $|+\rangle$ retourne une superposition de tous les états de base

$$\frac{1}{\sqrt{2^n}} \bigotimes_{q=0}^{n-1} (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \quad (\text{A.2})$$

On conclut donc que la transformation Hadamard à n qubits appliqués au premier état de base produit une superposition uniforme de tous les états de base à n qubits

$$\hat{H}^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle. \quad (\text{A.3})$$

1.2 Relations utiles

L'état obtenu à la section précédente peut être exprimé de plusieurs manières différentes. En les décrivant et en sachant qu'elles sont toutes équivalentes, on pourra établir des relations qui nous seront fort utiles pour la suite. La première expression est déjà donnée à l'équation A.3

$$|+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle. \quad (\text{A.4})$$

La seconde s'obtient en écrivant chacun des états $|+\rangle$ comme une somme sur les deux états de base du qubit q on peut écrire

$$|+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \bigotimes_{q=0}^{n-1} \sum_{x_q=0}^1 |x_q\rangle. \quad (\text{A.5})$$

Pour la troisième, on constate que le côté droit de l'équation A.1 peut également être exprimé comme le résultat de n sommes sur les deux états de base de chacun des qubits

$$\underbrace{\sum_{x_{n-1}=0}^1 \dots \sum_{x_0=0}^1}_{n \text{ sommes}} |x_{n-1} \dots x_0\rangle = \underbrace{|0 \dots 00\rangle + |0 \dots 01\rangle + |0 \dots 10\rangle + \dots + |1 \dots 11\rangle}_{2^n \text{ termes}}.$$

En écrivant l'état $|x_{n-1} \dots x_0\rangle$ comme un produit tensoriel, on obtient la dernière expression

$$|+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \underbrace{\sum_{x_{n-1}=0}^1 \dots \sum_{x_0=0}^1}_{n \text{ sommes}} \bigotimes_{q=0}^{n-1} |x_q\rangle. \quad (\text{A.6})$$

En mettant en relation les équations A.4 et A.6, on déduit qu'une somme sur les 2^n état de base à n qubits est équivalente à n sommes sur les deux états de base de chacun des qubits

$$\sum_{x=0}^{2^n-1} (\dots) = \underbrace{\sum_{x_{n-1}=0}^1 \dots \sum_{x_0=0}^1}_{n \text{ sommes}} (\dots). \quad (\text{A.7})$$

En mettant en relation les équations A.5 et A.6, constate qu'on peut sortir une somme sur les deux états de base à un qubit d'un produit tensoriel en la remplaçant par les n sommes sur chacun des n qubits

$$\bigotimes_{q=0}^{n-1} \sum_{x_q=0}^1 (\dots) = \underbrace{\sum_{x_{n-1}=0}^1 \dots \sum_{x_0=0}^1}_{n \text{ sommes}} \bigotimes_{q=0}^{n-1} (\dots). \quad (\text{A.8})$$

1.3 Transformation générale d'un état de base

On peut maintenant se pencher sur la transformation Hadamard des autres états de base à n qubits. D'abord, un état de base est un état produit

$$|x\rangle = |x_{n-1} \cdots x_0\rangle = \bigotimes_{q=0}^{n-1} |x_q\rangle$$

où chacun des bits x_q peut être dans les états $|0\rangle$ ou $|1\rangle$. L'application d'une porte Hadamard sur un qubit dans chacun de ces états va respectivement produire les états $|+\rangle$ et $|-\rangle$. On peut résumer cela avec l'équation suivante

$$\hat{H} |x_q\rangle = \frac{|0\rangle + (-1)^{x_q} |1\rangle}{\sqrt{2}}$$

où on obtient bien $|+\rangle$ si $x_q = 0$ et $|-\rangle$ si $x_q = 1$. La transformation Hadamard d'un état de base peut donc s'exprimer comme

$$\hat{H}^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{q=0}^{n-1} (|0\rangle + (-1)^{x_q} |1\rangle). \quad (\text{A.9})$$

Comme à la section 1.1, le produit tensoriel de n paires de termes va produire une superposition des 2^n états de base. Cependant, dans ce cas-ci, chacun des différents états de base sera affecté d'une phase. Pour identifier la phase de chaque état de base, notons qu'on peut écrire l'état de chaque qubit après la transformation Hadamard comme étant une somme sur ses deux états de base

$$\frac{|0\rangle + (-1)^{x_q} |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \sum_{z_q=0}^1 (-1)^{x_q z_q} |z_q\rangle.$$

Le facteur de phase devient $(-1)^{x_q z_q}$ pour s'assurer que la phase -1 est appliquée uniquement quand $|z_q\rangle = |1\rangle$. L'expression A.9 devient alors

$$\hat{H}^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{q=0}^{n-1} \sum_{z_q=0}^1 (-1)^{x_q z_q} |z_q\rangle.$$

Insistons ici sur le fait que les bits x_q décrivent l'état initial, alors que les bits z_q servent à décrire l'état transformé.

On fait ensuite usage de la relation A.8 pour sortir la somme sur z_q du produit tensoriel

$$\hat{H}^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \underbrace{\sum_{z_{n-1}=0}^1 \cdots \sum_{z_0=0}^1}_{n \text{ sommes}} \bigotimes_{q=0}^{n-1} (-1)^{x_q z_q} |z_q\rangle. \quad (\text{A.10})$$

On voit que l'état $\hat{H}^{\otimes n} |x\rangle$ est une superposition d'états qui ne sont rien d'autre que les états de base accompagnés d'un facteur de phase. En effet,

$$\bigotimes_{q=0}^{n-1} (-1)^{x_q z_q} |z_q\rangle = (-1)^{x_0 z_0 + \cdots + x_{n-1} z_{n-1}} \bigotimes_{q=0}^{n-1} |z_q\rangle$$

où on a sorti les n facteurs de phase du produit tensoriel pour les combiner en un seul. Pour simplifier l'expression de l'état $\hat{H}^{\otimes n} |x\rangle$ notons les états de base qui décrivent l'état transformé à l'aide d'entiers z tel que

$$|z\rangle = \bigotimes_{q=0}^{n-1} |z_q\rangle.$$

On peut alors écrire l'état

$$\bigotimes_{q=0}^{n-1} (-1)^{x_q z_q} |z_q\rangle = (-1)^{x \cdot z} |z\rangle$$

où

$$x \cdot z = \sum_{q=0}^{n-1} x_q z_q = x_0 z_0 + \dots + x_{n-1} z_{n-1} \quad (\text{A.11})$$

est un produit scalaire entre les bits qui composent l'entier x et ceux qui composent l'entier z . En réécrivant l'équation A.10 à l'aide de cette expression et en utilisant l'équivalence A.7 pour remplacer les sommes sur les z_q par une somme sur z , on obtient

$$\hat{H}^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle. \quad (\text{A.12})$$

Ainsi, la transformation Hadamard d'un état de base retourne une superposition uniforme de tous les états de base où chacun d'eux est affecté par une phase qui dépend du produit scalaire entre les bits de l'entier z et les bits de l'entier x de l'état de base initial.

Annexe B

Nombres complexes

Les nombres complexes sont un outil extrêmement utile dans la théorie de la mécanique quantique pour représenter les phases nécessaires pour décrire un état quantique. L'objectif de cette section est d'introduire de manière originale les nombres complexes.

1 Représentation géométrique des nombres réels

Nous utiliserons une représentation géométrique des nombres complexes pour les introduire. Considérons d'abord l'équation suivante

$$x^2 = 4. \quad (\text{B.1})$$

Pour solutionner cette équation, on doit trouver une valeur de x qui, lorsque mise au carré, donne 4. La réponse est triviale : $x = 2$.

Malgré cela, réécrivons la même équation de la manière suivante,

$$1 \times x \times x = 4.$$

et interprétons $\times x$ comme une transformation qui permet de nous déplacer sur l'axe des nombres réels. Par exemple, l'application de $\times 2$ agit comme une transformation qui double la coordonnée sur l'axe des réels.

Dans ce contexte, on cherche donc une transformation qui, lorsqu'appliquée deux fois, à partir de 1, nous amène à 4. La figure B.1 illustre comment on peut utiliser la transformation $\times x$ pour se déplacer sur l'axe des réels, à partir de la position 1, et comment elle peut être appliquée deux fois pour nous amener à la position 4. La solution est encore une fois évidente $x = 2$.

Cependant, on constate qu'il y a un autre chemin pour passer de 1 à 4 en appliquant deux fois la même transformation : on peut doubler la coordonnée tout en effectuant une rotation de π radians (ou 180°). La rotation de π peut être représentée par le nombre -1 ($x = 2 \times -1$). La solution $x = -2$ est la seconde solution possible à l'équation B.1.

On peut donc représenter la multiplication par un nombre réel comme étant une transformation géométrique d'un vecteur où on peut changer sa longueur ainsi que sa direction par un angle π s'il est négatif.

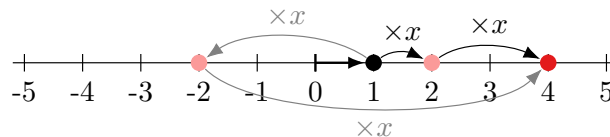
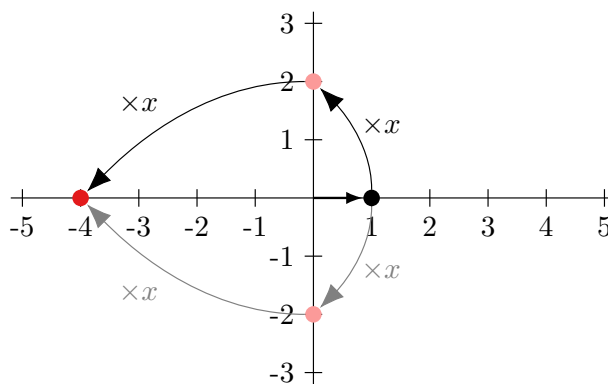


FIGURE B.1 – Représentations géométriques des solutions à l'équation $x^2 = 4$

FIGURE B.2 – Représentation géométrique de la solution à l'équation $x^2 = -4$

2 Représentation géométrique des nombres complexes

Les nombres complexes sont une invention qui permet de trouver les solutions à l'équation suivante

$$x^2 = -4 \qquad 1 \times x \times x = -4. \qquad (\text{B.2})$$

Notre réflexe pour solutionner une équation quadratique est de prendre la racine carrée. Malheureusement, l'équation

$$x = \sqrt{-4}?$$

n'a pas vraiment de sens dans le contexte des nombres réels.

Avec notre approche géométrique, cela revient à chercher une transformation qui, lorsqu'appliquée deux fois, à partir du nombre 1, nous amènent au nombre -4 . En utilisant uniquement une dimension comme à la figure précédente, cela est impossible. Pour y arriver, on doit « penser à l'extérieur de la boîte ». En effet, on doit sortir de l'axe des nombres réels (horizontal) et passer par l'axe imaginaire (vertical) comme cela est illustré à la figure B.2.

Une première solution consisterait donc à appliquer une transformation qui double la longueur d'un vecteur tout en effectuant une rotation de $\pi/2$ radians (90°) dans le sens antihoraire. Écrivons cette rotation d'un quart de tour comme la lettre i de sorte que la solution soit $x = 2 \times i$. Une seconde solution similaire consiste à tourner de $3\pi/2$ (270°) ou bien $-\pi/2$, c'est-à-dire dans l'autre sens. On donc peut représenter cette transformation comme $x = 2 \times i \times -1$.

Exercice 2.1 : Rotations en i

La multiplication par un nombre complexe permet d'effectuer une rotation dans le plan complexe. Donnez l'angle de la rotation provoquée par la multiplication des nombres complexes suivants. Supposez une rotation dans le sens contraire des aiguilles d'une montre. Les angles négatifs sont admissibles.

a) $-i$ b) i^3 c) \sqrt{i}

Mais que vaut i ? Pour le savoir, remplaçons notre première solution dans l'équation B.2. On trouve alors

$$(2 \times i)^2 = -4$$

$$4i^2 = -4$$

$$i^2 = -1.$$

Ce qui signifie que $i = \pm\sqrt{-1}$!

On peut ensuite se demander où se trouve le nombre i sur le plan de la figure B.2? On sait que i effectue une rotation de $\pi/2$ dans le sens antihoraire. En appliquant $\times i$ sur 1 on obtient $1 \times i = i$. La rotation de $\pi/2$ à partir de 1 nous amène une unité au-dessus de l'origine, directement sur l'axe vertical. Il est illustré par un point [bleu](#) à la figure B.3. On l'appelle l'axe des *imaginaires* et i est l'unité imaginaire.

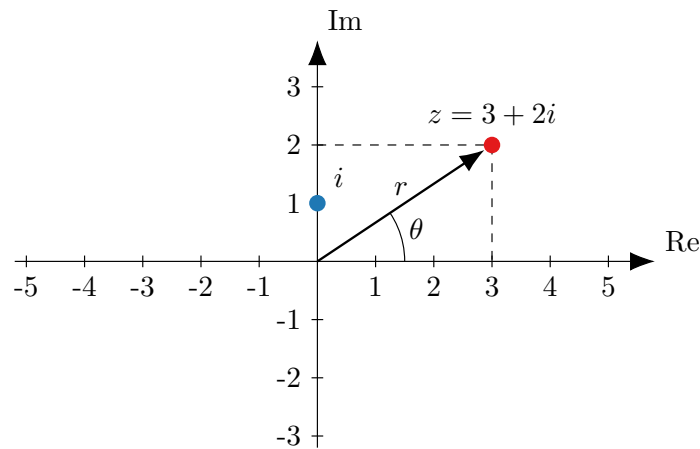


FIGURE B.3 – Représentation d'un nombre complexe dans un espace à 2 dimensions.

3 Représentation des nombres complexes

On peut alors construire un nombre *complexe* en combinant une partie réelle (Re) et une partie imaginaire (Im) comme on le ferait pour un vecteur à deux dimensions. La figure B.3 illustre le nombre complexe z ayant une partie réelle égale à 3 et une partie imaginaire égale à 2. On peut écrire ce nombre comme

$$z = 3 + 2i.$$

De manière générale, un nombre complexe écrit sous la forme

$$z = \operatorname{Re}\{z\} + i \operatorname{Im}\{z\}$$

est dit écrit dans sa forme algébrique.

Toujours sur la figure B.3, nous avons représenté le nombre z sous la forme polaire, c'est-à-dire en utilisant une longueur r (module) et une direction θ (angle en radians ou phase). Un peu de trigonométrie nous permet d'identifier les composantes réelle et imaginaire de z comme étant

$$\operatorname{Re}\{z\} = r \cos \theta \quad \text{et} \quad \operatorname{Im}\{z\} = r \sin \theta,$$

ce qui nous permet d'écrire un nombre complexe général grâce à ses coordonnées polaires

$$z(r, \theta) = r \cos \theta + ir \sin \theta = r(\cos \theta + i \sin \theta).$$

Considérons maintenant cette forme comme une suite de transformations

$$z(r, \theta) = 1 \times r \times (\cos \theta + i \sin \theta).$$

Nous identifions la transformation $\times r$ comme la modification de la distance par rapport à l'origine. La transformation $\times (\cos \theta + i \sin \theta)$ doit donc représenter une rotation dans le sens antihoraire d'un angle θ . Si l'on fait grandir la valeur de θ , le point z va tourner autour de l'origine sur un cercle de rayon r . La direction de son déplacement est toujours perpendiculaire au vecteur qui relie z à l'origine.

Exercice 3.1 : Racine cubique

En utilisant le même genre d'arguments introduits pour la représentation géométrique des nombres complexes qui nous a permis de définir $\sqrt{-1}$, illustrez les positions dans le plan complexe des 3 solutions possibles pour chacune des racines cubiques suivantes :

a) $\sqrt[3]{1}$

b) $\sqrt[3]{-1}$

c) $\sqrt[3]{-8}$

4 Relation d'Euler

Une autre manière d'étudier comment z change sous une variation de θ est de dériver z par rapport à θ . On obtient assez facilement

$$\begin{aligned}\frac{dz}{d\theta} &= r \left(\frac{d}{d\theta} \cos \theta + i \frac{d}{d\theta} \sin \theta \right) \\ &= r(-\sin \theta + i \cos \theta) \\ &= ir(i \sin \theta + \cos \theta) = iz.\end{aligned}\tag{B.3}$$

L'égalité B.3 cache une dernière information cruciale : la dérivée de z par rapport à θ est égale à z avec un facteur multiplicatif i . Cela nous permet d'identifier que la rotation d'un angle θ peut être exprimée grâce à la fonction exponentielle. En effet, on sait que la fonction exponentielle $f(x) = be^{ax}$ se dérive de la manière suivante

$$\frac{df}{dx} = \frac{d}{dx}(be^{ax}) = abe^{ax} = af(x).\tag{B.4}$$

Les équations B.3 et B.4 sont parfaitement équivalentes, seules les noms de variables et fonctions ont été changés. Ainsi, on déduit que l'équation B.3 permet d'écrire

$$\frac{dz}{d\theta} = \frac{d}{d\theta}(re^{i\theta}) = ire^{i\theta} = iz.$$

et on voit que $re^{i\theta}$ se comporte comme un nombre complexe z .

$$\frac{dz}{d\theta} = iz \quad \Leftrightarrow \quad \frac{d}{d\theta} re^{i\theta} = ire^{i\theta}.$$

On peut donc écrire un nombre complexe sous une forme polaire plutôt compacte

$$z = z(r, \theta) = re^{i\theta}.$$

En particulier, si on s'intéresse uniquement aux nombres complexes de module $r = 1$, on obtient une relation extrêmement utile, appelée relation d'Euler

$$e^{i\theta} = \cos \theta + i \sin \theta.\tag{B.5}$$

On se rappelle que la transformation $\times e^{i\theta}$ doit donc représenter une rotation dans le sens antihoraire d'un angle θ . Que se passe-t-il si l'on applique 2 rotations successives pour des angles θ et ϕ ? La figure B.4 montre bien que cela produit une rotation d'un angle $\theta + \phi$. La forme exponentielle des nombres complexes est cohérente avec cela. En effet, on obtient alors une rotation

$$1 \times e^{i\theta} \times e^{i\phi} = e^{i(\theta+\phi)}$$

pour un angle total de $\theta + \phi$. La forme exponentielle est donc très utile et plutôt simple à utiliser !

Exercice 4.1 : Racine cubique et formule d'Euler

Écrivez toutes les racines cubiques que vous avez illustrées à l'exercice 3.1 sous la forme exponentielle. Rappel : l'angle dans la forme exponentielle doit être exprimé en radians.

Exercice 4.2 : Racine $n^{\text{ième}}$

Donnez une forme générale pour les racines $n^{\text{ième}}$ de 1

$$z^n = 1 \qquad z = \sqrt[n]{1} = ?$$

Indice : vous pouvez commencer par refaire l'exercice précédent pour les racines d'ordre 4.

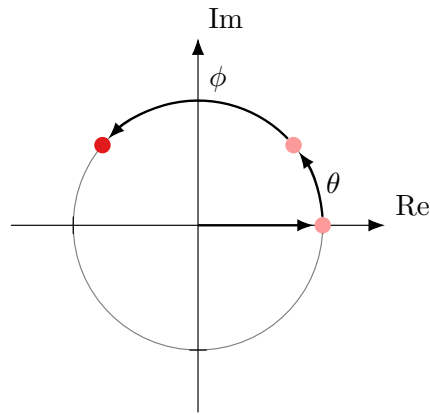


FIGURE B.4 – Addition des phases de deux nombres complexes

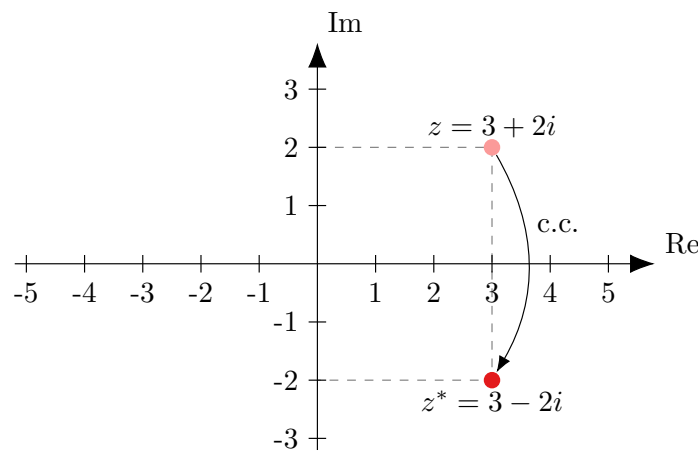


FIGURE B.5 – Complexe conjugué d'un nombre complexe

Exercice 4.3 : Transformations pures

Quelle condition un nombre complexe z doit-il respecter pour produire une transformation dans le plan complexe qui soit

1. uniquement une rotation ;
2. uniquement une mise à l'échelle (étirement ou compression).

5 Complexe conjugué

Terminons cette section en introduisant le complexe conjugué d'un nombre complexe. Pour obtenir le complexe conjugué z^* d'un nombre complexe z , on doit simplement effectuer la transformation $i \rightarrow -i$. Cela correspond à une réflexion par rapport à l'axe des réels dans le plan complexe comme illustré à la figure B.5.

Le produit d'un nombre complexe avec son complexe conjugué permet d'obtenir la norme au carré qui est toujours un nombre réel et positif. On note souvent cela sous la forme suivante

$$|z|^2 = z^* z = r^2$$

et on désigne cette opération comme le *module au carré*.

Exercice 5.1 : Module au carré

Calculez les modules au carré de nombres complexes suivants

a) $3 - 4i$

c) $1 + i$

e) $\frac{1}{\sqrt{3}} + i\sqrt{\frac{2}{3}}$

b) i

d) $\cos \theta + i \sin \theta$

f) $\sqrt{\frac{2}{3}} - i\frac{1}{\sqrt{3}}$

Exercice 5.2 : Formes algébrique et exponentielle

Convertissez les nombres complexes suivants qui sont sous formes algébriques en leurs formes exponentielles et vice versa.

a) $\frac{1-i}{\sqrt{2}}$

c) $2e^{-i\pi/2}$

e) $\cos(\theta) - i \sin(\theta)$

b) $e^{i\pi/3}$

d) $4e^{i\pi}$

f) $\frac{\sqrt{3}}{2} - i\frac{1}{2}$

Annexe C

Notation indicielle

La notation indicielle n'est qu'une manière plus compacte d'écrire certaines équations qui pourraient autrement être plus longues à écrire. Prenons l'exemple d'un système de deux équations linéaires

$$\begin{aligned}2x + 5y &= 4 \\ x - 4y + 7z &= 0.\end{aligned}$$

L'algèbre linéaire nous a appris qu'on peut écrire un tel système d'équations sous une forme matricielle

$$\begin{pmatrix} 2 & 5 & 0 \\ 1 & -4 & 7 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 4 \\ 0 \end{pmatrix}.$$

En définissant la matrice et les vecteurs suivants

$$\mathbf{M} = \begin{pmatrix} 2 & 5 & 0 \\ 1 & -4 & 7 \end{pmatrix} \quad \mathbf{x} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \quad \mathbf{b} = \begin{pmatrix} 4 \\ 0 \end{pmatrix}$$

nous arrivons à écrire tout cela de manière beaucoup plus courte

$$\mathbf{M} \cdot \mathbf{x} = \mathbf{b}. \tag{C.1}$$

1 Matrices et vecteurs comme tenseurs

Afin de donner une adresse à chaque élément d'une matrice où d'un vecteur on identifie avec M_{ij} l'élément situé à la ligne i et à la colonne j dans la matrice \mathbf{M} . On peut faire cela pour des matrices et des vecteurs¹

$$\mathbf{M} = \begin{pmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \end{pmatrix} \quad \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \quad \mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}.$$

Ainsi, on a par exemple $M_{12} = 5$ et $b_1 = 4$.

On peut accéder à un *élément* d'une matrice en spécifiant les numéros de ligne et de colonne de celui-ci. Une notation fréquemment utilisée est la suivante,

$$(\mathbf{M})_{12} = M_{12} = 5.$$

1. On choisit ici de commencer la numérotation à 1, ce qui n'est pas cohérent avec les sections principales de ces notes.

Selon cette notation on a donc de manière générale

$$(\mathbf{M})_{ij} = M_{ij}.$$

La matrice \mathbf{M} (comme toutes les matrices) est équivalente à un *tenseur* d'ordre 2, car il est nécessaire de spécifier 2 indices pour aller chercher chacun de ses éléments. Les vecteurs sont équivalents à des tenseurs d'ordre 1. Les scalaires sont des tenseur d'ordre 0 car ils ne contiennent qu'une seule valeur.

Le terme tenseur est donc un terme très général pour désigner un objet qui prend la forme d'un tableau de quantités ou de variables.

En général, les indices d'un tenseur peuvent prendre autant de valeurs que le nombre de dimensions que comportent les espaces dans lesquels ils existent. Chaque valeur d'indice est associée à une direction de cet espace. Par exemple, les indices i et j pour M_{ij} peuvent chacun prendre les valeurs $i \in \{1, 2\}$ et $j \in \{1, 2, 3\}$ respectivement. Ainsi l'indice i existe dans un espace à deux dimensions et j dans un espace à trois dimensions.

2 Produit matricielle en notation indicielle

Explicitons le produit de l'équation C.1

$$\begin{pmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} M_{11}x_1 + M_{12}x_2 + M_{13}x_3 \\ M_{21}x_1 + M_{22}x_2 + M_{23}x_3 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}.$$

On voit que les composantes du vecteur \mathbf{b} sont égaux à l'addition de trois termes. Il est possible de résumer cela grâce à une somme. Par exemple, la première composante de \mathbf{b} s'écrit

$$b_1 = M_{11}x_1 + M_{12}x_2 + M_{13}x_3 = \sum_{j=1}^3 M_{1j}x_j \quad (\text{C.2})$$

ce qui est manifestement plus compact.

On pourrait faire la même chose pour l'autre composante de \mathbf{b} . On généralise ce résultat pour le $i^{\text{ième}}$ élément de \mathbf{b} . La notation indicielle nous permet d'écrire une forme générale pour les composantes du vecteur \mathbf{b}

$$b_i = \sum_{j=1}^3 M_{ij}x_j. \quad (\text{C.3})$$

Cette expression est totalement équivalente au produit présenté à l'équation C.1.

3 Tenseurs d'ordre supérieur à 2

Comme nous résolvons des problèmes mathématiques sur une feuille de papier qui est un espace à deux dimensions, il nous est impossible d'écrire explicitement et simplement des tenseurs d'ordre supérieur à deux ! Nous pouvons néanmoins faire référence à chaque élément en spécifiant les indices correspondants. On peut alors travailler avec des tenseurs d'ordre trois ou supérieur. Il est facile de généraliser l'écriture des tenseurs d'ordre supérieur : on ajoute des indices ! Les éléments d'un tenseur \mathbf{T} d'ordre trois seraient donc

$$T_{ijk}.$$

On pourrait représenter le tenseur \mathbf{T} si on avait accès à une représentation en trois dimensions. Comme une matrice \mathbf{M} prend la forme d'un rectangle, un tenseur \mathbf{T} d'ordre trois prendrait alors la forme d'un prisme rectangulaire.

4 Analogie avec la programmation

Les indices dans cette notation peuvent être comparés aux compteurs utilisés dans les boucles **for** d'un programme informatique. Cette analogie est limitée, mais peut aider à comprendre le rôle des indices lors d'un premier contact avec cette notation. Par exemple, la somme de l'équation C.3 se traduirait ainsi en Python.

```
b = [0, 0]
for i in range(2):
    for j in range(3):
        b[i] = b[i] + M[i,j] * x[j]
```

Ce code permet de calculer les valeurs des composantes de **b** à partir des tenseurs **M** et **x**.

5 Notation d'Einstein

Supposons le produit de trois matrices (**A**, **B** et **C**) qui résulte en une quatrième matrice (**D**).

$$\mathbf{D} = \mathbf{A} \cdot \mathbf{B} \cdot \mathbf{C}$$

On peut écrire l'élément de matrice D_{ij} à l'aide de la notation indicielle. Procédons étape par étape.

$$D_{ij} = (\mathbf{A} \cdot \mathbf{B} \cdot \mathbf{C})_{ij} = \sum_k A_{ik} (\mathbf{B} \cdot \mathbf{C})_{kj} = \sum_k A_{ik} \left(\sum_m B_{km} C_{mj} \right) = \sum_{k,m} A_{ik} B_{km} C_{mj} \quad (\text{C.4})$$

Dans la dernière expression, on remarque qu'on peut reconnaître les indices sur lesquels on effectue une somme car ils apparaissent toujours 2 fois. Le fait qu'il y ait un indice *répété* implique généralement qu'il y a une *somme* associée à celui-ci. Pour rendre la notation encore plus compacte, on peut omettre les symboles de sommation. Cette pratique s'appelle la convention de sommation d'Einstein². On reconnaîtra qu'une sommation est implicite chaque fois qu'on identifiera 2 fois le même indice. En utilisant cette convention, les équations C.3 et C.4 deviennent,

$$b_i = M_{ij} x_j \quad (\text{C.5})$$

et

$$D_{ij} = A_{ik} B_{km} C_{mj}. \quad (\text{C.6})$$

Les indices répétés sur lesquels on effectue une somme implicite sont dits *muets*. Dans l'équation C.5, l'indice j est muet. Dans l'équation C.6, les indices k et m sont muets.

Exercice 5.1 : Ordre de tenseur

Déterminez l'ordre de chacun de ces tenseurs. Écrivez également leur forme explicite en supposant des espaces vectorielles à 3 dimensions.

a) $K_{ij} = 2$

d) δ_{ii}

g) M_{ij}^4

b) $\epsilon_{ijk} \delta_{ij}$

e) $2\delta_{i3}$

h) $\epsilon_{ijk} \epsilon_{ijk}$

c) $\epsilon_{ij2} \delta_{i1}$

f) $1 - \delta_{ij}$

2. La description faite ici est simplifiée. La version complète fait intervenir des indices en bas ou en haut faisant référence à l'aspect covariant ou contravariant des tenseurs impliqués en relativité restreinte. Nous n'accorderons pas d'importance à cela dans ce document.

6 Tenseurs importants

Certains tenseurs sont régulièrement utilisés. En utilisant toujours la même notation on évite d'avoir à les redéfinir à chaque utilisation.

6.1 Symbole de Kronecker

On le note δ_{ij} . C'est un tenseur d'ordre 2. Il peut être utilisé dans des espaces de toutes les dimensions, mais ses indices i et j doivent vivre dans des espaces de dimensions identiques. En d'autres termes, δ_{ij} est carré. Il est défini comme suit :

$$\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases} \quad (\text{C.7})$$

Son application est triviale, tout comme la multiplication avec une matrice identité. On n'a qu'à remplacer l'indice sommé par l'autre indice du Kronecker. Par exemple,

$$M_{ik}\delta_{kj} = M_{ij}.$$

On peut s'en convaincre en réintroduisant le symbole de sommation

$$\sum_{k=1}^n M_{ik}\delta_{kj} = M_{i1}\delta_{1j} + M_{i2}\delta_{2j} + \dots + M_{in}\delta_{nj} = M_{ij}$$

et en effectuant cette somme. La somme comporte n termes. Tous les δ_{kj} sont nuls, sauf celui pour lequel $k = j$. Ce terme est donc $M_{ij} \times 1 = M_{ij}$.

6.2 Levi-Civita

On le note ϵ_{ijk} . C'est un tenseur³ d'ordre 3 dont chacun des indices désigne une direction dans un espace à 3 dimensions. On le définit ainsi :

$$\epsilon_{ijk} = \begin{cases} 1 & \text{si } (i, j, k) \in \{(1, 2, 3), (2, 3, 1), (3, 1, 2)\} \text{ (ordres cycliques)} \\ -1 & \text{si } (i, j, k) \in \{(3, 2, 1), (2, 1, 3), (1, 3, 2)\} \text{ (ordres anti-cycliques)} \\ 0 & \text{si } i = j \text{ ou } j = k \text{ ou } k = i \end{cases} \quad (\text{C.8})$$

Par définition, ce tenseur possède une propriété de cyclicité avec ses indices ; et est antisymétrique sous inversion de 2 indices⁴. Les six permutations sont liées de la manière suivante

$$\epsilon_{ijk} = \epsilon_{kij} = \epsilon_{jki} = -\epsilon_{jik} = -\epsilon_{ikj} = -\epsilon_{kji}.$$

Le tenseur de Levi-Civita permet, en particulier, de définir le produit vectoriel en notation indicielle.

$$\mathbf{c} = \mathbf{a} \times \mathbf{b} \quad \rightarrow \quad c_i = \epsilon_{ijk} a_j b_k \quad (\text{C.9})$$

3. Rigoureusement ϵ_{ijk} est un pseudo tenseur.

4. Les indices sont en couleur pour aider la lecture.

Exemple 6.1 : Superposition uniforme à trois qubits

Calculons la première composante de \mathbf{c} à titre d'exemple. La double somme comporte 9 termes au total

$$\begin{aligned} c_1 &= \sum_{jk} \epsilon_{1jk} a_j b_k \\ &= \epsilon_{111} a_1 b_1 + \epsilon_{112} a_1 b_2 + \epsilon_{113} a_1 b_3 + \epsilon_{121} a_2 b_1 + \epsilon_{122} a_2 b_2 + \underbrace{\epsilon_{123}}_{=1} a_2 b_3 + \epsilon_{131} a_3 b_1 + \underbrace{\epsilon_{132}}_{=-1} a_3 b_2 + \epsilon_{133} a_3 b_3 \\ &= a_2 b_3 - a_3 b_2 \end{aligned}$$

dont seulement 2 ne s'annulent pas. Le même calcul pour chacune des composantes de \mathbf{c} nous donne

$$\mathbf{c} = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} a_2 b_3 - a_3 b_2 \\ a_3 b_1 - a_1 b_3 \\ a_1 b_2 - a_2 b_1 \end{pmatrix}.$$

Exercice 6.1 : Levi-Civita

a) Écrivez le produit triple sous forme indicielle. En utilisant les propriétés de ϵ_{ijk} démontrez l'identité suivante

$$\mathbf{a} \cdot \mathbf{b} \times \mathbf{c} = \mathbf{b} \cdot \mathbf{c} \times \mathbf{a} = \mathbf{c} \cdot \mathbf{a} \times \mathbf{b}.$$

b) En utilisant la propriété de cyclicité de ϵ_{ijk} , démontrez l'identité suivante

$$\epsilon_{ijk} \epsilon_{ilm} = \delta_{jl} \delta_{km} - \delta_{jm} \delta_{kl},$$

ce qui vous permettra de démontrer cette dernière identité

$$\mathbf{a} \times \mathbf{b} \times \mathbf{c} = \mathbf{b}(\mathbf{a} \cdot \mathbf{c}) - \mathbf{c}(\mathbf{a} \cdot \mathbf{b}).$$

7 Quelques astuces et mises en garde

7.1 Cohérence dans les indices

L'opération qu'on effectue le plus souvent sur un tenseur est une somme selon un indice. Par exemple, une multiplication d'un tenseur d'ordre trois (\mathbf{T}) avec un tenseur d'ordre un (\mathbf{r}) sur le deuxième indice du tenseur T résulte en un tenseur d'ordre deux

$$S_{ik} = T_{ijk} r_j.$$

On verra toujours à vérifier que les indices, de part et d'autre, d'une équation sont cohérents. C'est-à-dire que tous les indices d'un côté se retrouvent également de l'autre côté, à l'exception des indices muets (sur lesquels une somme est effectuée ; j dans l'exemple précédent). Cette condition équivaut à dire qu'un vecteur doit toujours être égal à un vecteur avec le même nombre de composantes, une matrice égale à une matrice de même taille, un tenseur d'ordre n à un tenseur d'ordre n ,...

Remarque

Dans certaines situations particulières, il arrive qu'un indice se retrouve d'un seul côté d'une équation. Un tel indice est dit *libre*. L'équation est généralement posée ainsi dans un but particulier. Cela veut généralement dire que l'équation est vérifiée, peu importe la valeur de cet indice. Par exemple, $r_i = 2$ définit un vecteur \mathbf{r} dont toutes les composantes sont égales à 2.

7.2 Commutation des éléments de tenseurs

Les éléments des tenseurs sont généralement des scalaires. L'élément $M_{12} = 5$ est un scalaire. Les scalaires sont des objets qui commutent. On peut donc effectuer des opérations de commutation en notation

indicielle. Prenons l'exemple d'un produit entre 2 matrices qu'on écrit sous forme indicielle

$$\mathbf{S} = \mathbf{M} \cdot \mathbf{Q} \quad \rightarrow \quad S_{ij} = M_{ik} Q_{kj}.$$

On peut changer l'ordre des éléments de matrice sans problème.

$$S_{ij} = M_{ik} Q_{kj} = Q_{kj} M_{ik}$$

Cela ne signifie pas que \mathbf{M} et \mathbf{Q} commutent ! La position de l'indice k s'assure qu'on effectuera le produit matriciel correctement. L'ordre des indices est donc important. Pour s'en convaincre considérons à nouveau l'expression explicite de produit C.5

$$b_i = M_{ij} x_j = M_{i1} x_1 + M_{i2} x_2 + M_{i3} x_3 = x_1 M_{i1} + x_2 M_{i2} + x_3 M_{i3} = x_j M_{ij}.$$

7.3 Matrice transposée

Lorsqu'on transpose une matrice, on échange ses lignes pour ses colonnes. En notation indicielle, cela revient donc à échanger les indices de ligne avec les indices de colonnes. Ainsi, on peut écrire

$$(\mathbf{M})_{ij} = (\mathbf{M}^\top)_{ji}.$$

Si on identifie les éléments de la matrice \mathbf{M}^\top comme étant M_{ij}^\top on peut alors également écrire

$$M_{ij} = M_{ji}^\top.$$

Cela est particulièrement utile lorsqu'on manipule des matrices unitaires. La matrice inverse d'une matrice unitaire étant donnée par sa conjuguée hermitienne (transposée, conjuguée complexe)

$$\mathbf{U}^{-1} = \mathbf{U}^\dagger = (\mathbf{U}^*)^\top$$

on peut obtenir les éléments de cette matrice simplement en écrivant

$$(\mathbf{U}^{-1})_{ij} = ((\mathbf{U}^*)^\top)_{ij} = (\mathbf{U}^*)_{ji} = U_{ji}^*.$$

En résumé,

$$U_{ij}^{-1} = U_{ji}^*$$

signifie que l'élément ij de la matrice inverse de \mathbf{U} est égal au complexe conjugué de l'élément ji .

7.4 Choix des indices

Il est crucial de garder en tête le rôle de chacun des indices. On doit éviter d'utiliser deux fois le même indice pour désigner des sommes différentes. En effet, écrite comme ceci

$$D_{ij} = (\mathbf{A} \cdot \mathbf{B} \cdot \mathbf{C})_{ij} \neq \sum_k \sum_k A_{ik} B_{kk} C_{kj}$$

l'équation C.6 n'a plus le même sens. Un peu comme en programmation, il ne faut pas utiliser deux fois le même nom pour deux variables différentes. Les lettres qu'on utilise n'ont pas d'importance, mais elles doivent être désignées correctement. Par exemple, les équations suivantes sont équivalentes :

$$S_{ij} = M_{ik} Q_{kj} \quad \text{et} \quad S_{\alpha\beta} = M_{\alpha\gamma} Q_{\gamma\beta}.$$

Les indices muets peuvent être renommés à volonté pour accommoder certains calculs, en respectant toutefois la signification de chacun des indices. Par exemple, on peut changer la lettre de l'indice de sommation du deuxième terme de l'équation suivante

$$A_{ij} = B_{ik} C_{kj} + D_{il} C_{lj} = B_{ik} C_{kj} + D_{ik} C_{kj} = (B_{ik} + D_{ik}) C_{kj}$$

ce qui nous a permis d'effectuer une mise en évidence.

7.5 Piège : redondance accidentelle d'indices muets

Considérons maintenant les deux produits suivants.

$$A_{ij} = B_{ik}C_{kj} \qquad D_{ij} = E_{ik}F_{kj}$$

On désire faire le produit matriciel de \mathbf{A} avec \mathbf{D} , ce qui s'écrit ainsi sous forme indicielle.

$$\mathbf{G} = \mathbf{A} \cdot \mathbf{D} \quad \rightarrow \quad G_{ij} = A_{im}D_{mj}$$

Les indices de cette dernière équation ne correspondent pas à la notation utilisée pour définir \mathbf{A} et \mathbf{D} . On doit donc réécrire les éléments de ces matrices en utilisant d'autres lettres pour les indices.

$$A_{im} = B_{ik}C_{km} \qquad D_{mj} = E_{mk}F_{kj}$$

Ces deux expressions comportent l'indice muet k . Le même indice désignerait deux sommes distinctes. Ainsi, on ne peut pas directement écrire,

$$G_{ij} = A_{im}D_{mj} \neq (B_{ik}C_{km})(E_{mk}F_{kj}) = B_{ik}C_{km}E_{mk}F_{kj}$$

La somme sur l'indice k poserait problème, car il apparaît quatre fois !

On introduit alors de nouveaux caractères, autant que nécessaire, pour ne pas associer accidentellement 2 indices qui n'ont rien à voir ensemble. Dans le cas du produit de \mathbf{A} et \mathbf{D} on devrait faire quelque chose comme suit

$$G_{ij} = A_{im}D_{mj} = (B_{ik}C_{km})(E_{ml}F_{lj}) = B_{ik}C_{km}E_{ml}F_{lj}.$$

Les indices muets viennent par paires. Cela correspond bien à une multiplication de plusieurs matrices.

7.6 Mélanger les notations

Il arrive parfois qu'on veuille mélanger les notations vectorielle et indicielle. En restant rigoureux, on évitera de faire des erreurs mathématiques et conceptuelles. Par exemple, cette égalité n'est pas valable

$$\mathbf{M} \neq M_{ij}.$$

La matrice \mathbf{M} n'est pas égale à tous ses éléments ! Lorsqu'on désire spécifier l'élément du résultat d'un calcul, on peut mettre l'expression entre parenthèses et le décorer d'indices. Par exemple, dans le cas du produit $\mathbf{S} = \mathbf{M}\mathbf{Q}$, on peut écrire,

$$S_{ij} = (\mathbf{M} \cdot \mathbf{Q})_{ij}$$

Il est rigoureux de mélanger les notations si les résultats sont strictement les mêmes. En particulier dans le cas du produit scalaire qui donne ... un scalaire.

$$\mathbf{q} \cdot \mathbf{r} = q_i r_i$$

8 Les dérivées

La notation indicielle est également utile dans le contexte du calcul différentiel vectoriel.

8.1 Gradient

On peut exprimer le gradient d'une fonction en notation indicielle. Par exemple, si en notation vectorielle on a,

$$\mathbf{a} = \nabla f(\mathbf{r})$$

la composante i du gradient est

$$a_i = \frac{df}{dr_i}.$$

Ce résultat est à l'origine de l'abus de notation suivante pour exprimer un gradient

$$\nabla f(\mathbf{r}) = \frac{df}{d\mathbf{r}}.$$

8.2 Différentielle d'une fonction à n variables

Considérons une fonction à n variables

$$f(x_1, x_2, \dots, x_n) = f(\{x_i\}).$$

On peut rapidement exprimer sa différentielle

$$df = \sum_i \frac{\partial f}{\partial x_i} dx_i = \frac{\partial f}{\partial x_i} dx_i.$$

Si tous les x_i sont dépendants de la variable t on peut exprimer la dérivée de f par rapport à t

$$\frac{df}{dt} = \sum_i \frac{\partial f}{\partial x_i} \frac{dx_i}{dt} = \frac{\partial f}{\partial x_i} \frac{dx_i}{dt} = \frac{\partial f}{\partial x_i} \dot{x}_i.$$

Ce résultat s'applique en particulier aux fonctions qui dépendent de la position. Par exemple, si on a $f(\mathbf{r}(\mathbf{t}))$ et qu'on désire calculer la dérivée temporelle de f on peut écrire

$$\frac{df}{dt} = \frac{\partial f}{\partial r_i} \frac{dr_i}{dt} = \frac{\partial f}{\partial \mathbf{r}} \cdot \frac{d\mathbf{r}}{dt}.$$

Dans la dernière égalité, on a simplement exprimé la somme sur i comme un produit scalaire.

Expression	Ordre	Vectorielle	Explicite	Indicielle	Einstein
Scalaire	0	k	k	k	k
Vecteur	1	\mathbf{r}	$\begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix}$	r_i	r_i
Matrice	2	\mathbf{M}	$\begin{pmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \\ M_{31} & M_{32} & M_{33} \end{pmatrix}$	M_{ij}	M_{ij}
Tenseur Ordre 3	3	—	—	M_{ijk}	M_{ijk}
Tenseur Ordre n	n	—	—	$M_{ijk\dots}$	$M_{ijk\dots}$
Matrice identité	2	\mathbf{I}	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	δ_{ij}	δ_{ij}
Levi-Civita	3	—	$\epsilon_{1ij} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \epsilon_{2ij} = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \epsilon_{3ij} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	ϵ_{ijk}	ϵ_{ijk}

TABLE C.1 – Liste de tenseurs communs exprimés sous plusieurs formes. On suppose un espace à 3 dimensions.

Opération	Vectorielle	Explicite	Indicielle	Einstein
Transposée	$\mathbf{Q} = \mathbf{M}^\top$	$\begin{pmatrix} Q_{11} & Q_{12} & Q_{13} \\ Q_{21} & Q_{22} & Q_{23} \\ Q_{31} & Q_{32} & Q_{33} \end{pmatrix} = \begin{pmatrix} M_{11} & M_{21} & M_{31} \\ M_{12} & M_{22} & M_{32} \\ M_{13} & M_{23} & M_{33} \end{pmatrix}$	$Q_{ij} = M_{ji}$	$Q_{ij} = M_{ji}$
Addition	$\mathbf{S} = \mathbf{M} + \mathbf{Q}$	$\begin{pmatrix} S_{11} & S_{12} & S_{13} \\ S_{21} & S_{22} & S_{23} \\ S_{31} & S_{32} & S_{33} \end{pmatrix} = \begin{pmatrix} M_{11} + S_{11} & M_{12} + S_{12} & M_{13} + S_{13} \\ M_{21} + S_{21} & M_{22} + S_{22} & M_{23} + S_{23} \\ M_{31} + S_{31} & M_{32} + S_{32} & M_{33} + S_{33} \end{pmatrix}$	$S_{ij} = M_{ij} + Q_{ij}$	$S_{ij} = M_{ij} + Q_{ij}$
Produit scalaire	$k = \mathbf{q} \cdot \mathbf{r}$	$k = (q_1 \quad q_2 \quad q_3) \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} = q_1 r_1 + q_2 r_2 + q_3 r_3$	$k = \sum_i q_i r_i$	$k = q_i r_i$
Produit matrice-vecteur	$\mathbf{q} = \mathbf{M} \cdot \mathbf{r}$	$\begin{pmatrix} q_1 \\ q_2 \\ q_3 \end{pmatrix} = \begin{pmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \\ M_{31} & M_{32} & M_{33} \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} = \begin{pmatrix} M_{11}r_1 + M_{12}r_2 + M_{13}r_3 \\ M_{21}r_1 + M_{22}r_2 + M_{23}r_3 \\ M_{31}r_1 + M_{32}r_2 + M_{33}r_3 \end{pmatrix}$	$q_i = \sum_j M_{ij} r_j$	$q_i = M_{ij} r_j$
Produit identique	$\mathbf{r} = \mathbf{I} \cdot \mathbf{r}$	$\begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix}$	$r_i = \sum_j \delta_{ij} r_j$	$r_i = \delta_{ij} r_j$
Produit matriciel	$\mathbf{S} = \mathbf{M} \cdot \mathbf{Q}$	$\begin{pmatrix} S_{11} & S_{12} & S_{13} \\ S_{21} & S_{22} & S_{23} \\ S_{31} & S_{32} & S_{33} \end{pmatrix} = \begin{pmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \\ M_{31} & M_{32} & M_{33} \end{pmatrix} \begin{pmatrix} Q_{11} & Q_{12} & Q_{13} \\ Q_{21} & Q_{22} & Q_{23} \\ Q_{31} & Q_{32} & Q_{33} \end{pmatrix} = \dots$	$S_{ij} = \sum_k M_{ik} Q_{kj}$	$S_{ij} = M_{ik} Q_{kj}$
Carré d'une matrice	$\mathbf{S} = \mathbf{M}^2$	$\begin{pmatrix} S_{11} & S_{12} & S_{13} \\ S_{21} & S_{22} & S_{23} \\ S_{31} & S_{32} & S_{33} \end{pmatrix} = \begin{pmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \\ M_{31} & M_{32} & M_{33} \end{pmatrix} \begin{pmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \\ M_{31} & M_{32} & M_{33} \end{pmatrix} = \dots$	$S_{ij} = \sum_k M_{ik} M_{kj} \neq M_{ij}^2$	$S_{ij} = M_{ik} M_{kj}$
Produit quadratique	$k = \mathbf{q} \cdot \mathbf{M} \cdot \mathbf{r}$	$k = (q_1 \quad q_2 \quad q_3) \begin{pmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \\ M_{31} & M_{32} & M_{33} \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} = M_{11} q_1 r_1 + M_{12} q_1 r_2 + \dots$	$k = \sum_{ij} M_{ij} q_i r_j$	$k = M_{ij} q_i r_j$
Produit vectoriel	$\mathbf{p} = \mathbf{q} \times \mathbf{r}$	$\begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} = \det \begin{pmatrix} \hat{\mathbf{u}}_1 & \hat{\mathbf{u}}_2 & \hat{\mathbf{u}}_3 \\ q_1 & q_2 & q_3 \\ r_1 & r_2 & r_3 \end{pmatrix} = \begin{pmatrix} q_2 r_3 - q_3 r_2 \\ q_3 r_1 - q_1 r_3 \\ q_1 r_2 - q_2 r_1 \end{pmatrix}$	$p_i = \sum_{jk} \epsilon_{ijk} q_j r_k$	$p_i = \epsilon_{ijk} q_j r_k$
Gradient	$\mathbf{g} = \frac{\partial f}{\partial \mathbf{r}} = \nabla f$	$\begin{pmatrix} g_1 \\ g_2 \\ g_3 \end{pmatrix} = \begin{pmatrix} \partial f / \partial r_1 \\ \partial f / \partial r_2 \\ \partial f / \partial r_3 \end{pmatrix}$	$g_i = \frac{\partial f}{\partial r_i}$	$g_i = \frac{\partial f}{\partial r_i}$

TABLE C.2 – Liste d'opérations tensorielles courantes sous plusieurs formes. On suppose un espace à 3 dimensions.

Annexe D

Variables aléatoires

Soit x une variable aléatoire. La seule chose que l'on peut faire avec une variable aléatoire est de l'échantillonner, c'est-à-dire lui demander qu'elle est sa valeur. À chaque fois qu'on effectue un échantillonnage, la variable aléatoire nous retourne une valeur aléatoire parmi un ensemble de valeurs possibles.

Une variable aléatoire ne peut pas retourner n'importe quelle valeur. Les valeurs qu'elle peut retourner sont imposées. Par exemple, lors d'un jeu de pile ou face, les deux valeurs possibles sont pile et face. Pour un dé à six faces, les valeurs possibles sont les nombres de 1 à 6.

En échantillonnant plusieurs fois une variable aléatoire, on peut acquérir de l'information sur celle-ci. Les informations caractéristiques les plus fondamentales sont l'espérance et la variance.

1 Espérance

La première information caractéristique qu'on peut tenter d'obtenir à propos d'une variable aléatoire est son espérance. L'espérance d'une variable aléatoire correspond à la valeur moyenne qu'on obtiendrait si on pouvait effectuer un nombre infini d'échantillons. Pour une variable aléatoire x on note l'espérance

$$\mathbb{E}[x].$$

L'espérance est linéaire, c'est-à-dire que l'espérance d'une variable renormalisée ax est simplement

$$\mathbb{E}[ax] = a\mathbb{E}[x] \tag{D.1}$$

et que l'espérance de la somme de deux variables aléatoires est simplement

$$\mathbb{E}[x + y] = \mathbb{E}[x] + \mathbb{E}[y]. \tag{D.2}$$

Mentionnons que l'espérance d'une quantité qui n'est pas aléatoire est simplement égale à cette quantité

$$\mathbb{E}[a] = a.$$

2 Variance

Chaque échantillon de x peut retourner différentes valeurs en fonction de sa distribution. La variance d'une variable aléatoire caractérise en quelque sorte, la différence moyenne entre les résultats aléatoires avec l'espérance. On parle aussi de la largeur de cette distribution. Pour calculer la variance, on doit d'abord connaître l'espérance. Ensuite, on échantillonne x et on calcule le carré de la différence entre l'échantillon et l'espérance. En faisant cela un très grand nombre de fois ça revient à calculer

$$\sigma_x^2 = \text{Var}(x) = \mathbb{E}\left[(x - \mathbb{E}[x])^2\right].$$

La variance peut également être exprimée grâce à l'espérance du carré de la variable aléatoire

$$\begin{aligned}\text{Var}(x) &= \mathbb{E}[x^2 + \mathbb{E}^2[x] - 2x\mathbb{E}[x]] \\ &= \mathbb{E}[x^2] - \mathbb{E}^2[x] - 2\mathbb{E}[x]\mathbb{E}[x] \\ &= \mathbb{E}[x^2] - \mathbb{E}^2[x].\end{aligned}$$

Comme pour l'espérance, établissons quelques propriétés. D'abord, la variance d'une variable aléatoire renormalisée ax est quadratique avec le scalaire a

$$\begin{aligned}\text{Var}(ax) &= \mathbb{E}[(ax - \mathbb{E}[ax])^2] \\ &= \mathbb{E}[a^2(x - \mathbb{E}[x])^2] \\ &= a^2 \text{Var}(x).\end{aligned}\tag{D.3}$$

Ensuite, la variance d'une somme de variables aléatoires est donnée par les variances de chacune

$$\begin{aligned}\text{Var}(x + y) &= \mathbb{E}[(x + y - \mathbb{E}[x + y])^2] \\ &= \mathbb{E}[(x - \mathbb{E}[x] + y - \mathbb{E}[y])^2] \\ &= \mathbb{E}[(x - \mathbb{E}[x])^2 + (y - \mathbb{E}[y])^2 + 2(x - \mathbb{E}[x])(y - \mathbb{E}[y])] \\ &= \text{Var}(x) + \text{Var}(y) + 2\text{Covar}(x, y)\end{aligned}\tag{D.4}$$

auxquelles on ajoute ce qu'on appelle la covariance

$$\text{Covar}(x, y) = \mathbb{E}[(x - \mathbb{E}[x])(y - \mathbb{E}[y])].$$

qui est non nulle si les deux variables aléatoires ne sont pas complètement indépendantes. Dans le cas, où les deux variables aléatoires sont indépendantes, la covariance entre les deux variables est nulle et on a simplement

$$\text{Var}(x + y) = \text{Var}(x) + \text{Var}(y). \quad (\text{Variables indépendantes})$$

3 Covariance

La covariance entre deux variables aléatoires x et y permet de décrire si elles sont indépendantes l'une de l'autre ou si le résultat obtenu sur l'une influence d'une quelconque manière le résultat de l'autre

$$\text{Covar}(x, y) = \mathbb{E}[(x - \mathbb{E}[x])(y - \mathbb{E}[y])].$$

On peut également exprimer la covariance à l'aide de l'espérance du produit des variables aléatoires et du produit de leurs espérances respectives

$$\begin{aligned}\text{Covar}(x, y) &= \mathbb{E}[xy - x\mathbb{E}[y] - y\mathbb{E}[x] + \mathbb{E}[x]\mathbb{E}[y]] \\ &= \mathbb{E}[xy] - \mathbb{E}[x]\mathbb{E}[y].\end{aligned}$$

Établissons quelques propriétés de la covariance. La covariance est linéaire avec la renormalisation de chacune des variables aléatoires

$$\text{Covar}(ax, by) = ab \text{Covar}(x, y)\tag{D.5}$$

Cela implique également que

$$\begin{aligned}\text{Covar}(x, y + z) &= \mathbb{E}[x(y + z)] - \mathbb{E}[x]\mathbb{E}[y + z] \\ &= \mathbb{E}[xy] - \mathbb{E}[x]\mathbb{E}[y] + \mathbb{E}[xz] - \mathbb{E}[x]\mathbb{E}[z] \\ &= \text{Covar}(x, y) + \text{Covar}(x, z).\end{aligned}\tag{D.6}$$

Finalement, notons que la covariance d'une variable aléatoire avec elle-même revient à sa variance

$$\text{Covar}(x, x) = \text{Var}(x)$$

et que la variance est symétrique sous l'échange des deux variables aléatoires

$$\text{Covar}(x, y) = \text{Covar}(y, x).$$

4 Estimation de l'espérance

Pour obtenir de l'information sur une variable aléatoire x on effectue un échantillonnage, c'est-à-dire qu'on interroge cette variable aléatoire qui nous retourne une valeur. On note un échantillon, aussi appelé réalisation, de la variable aléatoire comme

$$x^{(i)}$$

où l'indice i indique qu'il s'agit du $i^{\text{ième}}$ échantillon.

Une fois qu'on a accumulé plusieurs échantillons, notons ce nombre N , on peut calculer la valeur moyenne à partir de ceux-ci. Cela nous permet en fait d'estimer l'espérance de la variable aléatoire. On note cette estimation de l'espérance

$$\tilde{\mathbb{E}}[x] = \frac{1}{N} \sum_{i=1}^N x^{(i)}.$$

On fera référence à cette quantité comme une valeur moyenne ou encore comme l'estimation de l'espérance. Comme il s'agit d'une estimation, on a donc que

$$\mathbb{E}[x] \approx \tilde{\mathbb{E}}[x]$$

et non une égalité. En effet, si on effectue plusieurs rondes d'échantillonnages de la variable x on obtiendra plusieurs estimations. Notons les $\tilde{\mathbb{E}}^{(1)}[x]$, $\tilde{\mathbb{E}}^{(2)}[x]$ et $\tilde{\mathbb{E}}^{(j)}[x]$. Chacune de ces estimations est donnée par

$$\tilde{\mathbb{E}}^{(j)}[x] = \frac{1}{N} \sum_{i=1}^N x^{(i,j)}$$

où $x^{(i,j)}$ est la $i^{\text{ième}}$ réalisation de la variable aléatoire pour la ronde j . Celles-ci sont sans doute similaires, mais fort probablement différentes. Si on fait ce processus plusieurs fois, on constate que l'estimation $\tilde{\mathbb{E}}^{(j)}[x]$ est en fait, elle aussi, une variable aléatoire. Ainsi, si on considère qu'on peut échantillonner $\tilde{\mathbb{E}}[x]$, cette variable aléatoire est une somme de variables aléatoires

$$\tilde{\mathbb{E}}[x] = \frac{1}{N} \sum_{i=1}^N x_i$$

où x_i représente la variable aléatoire qui sera échantillonnée à la $i^{\text{ième}}$ étape.

La figure D.1 aide à illustrer cela. On y considère plusieurs rondes d'échantillonnage. La ronde j permet de faire une estimation de l'espérance $\tilde{\mathbb{E}}^{(j)}[x]$. Les échantillons pris à la $i^{\text{ième}}$ étape peuvent être considéré

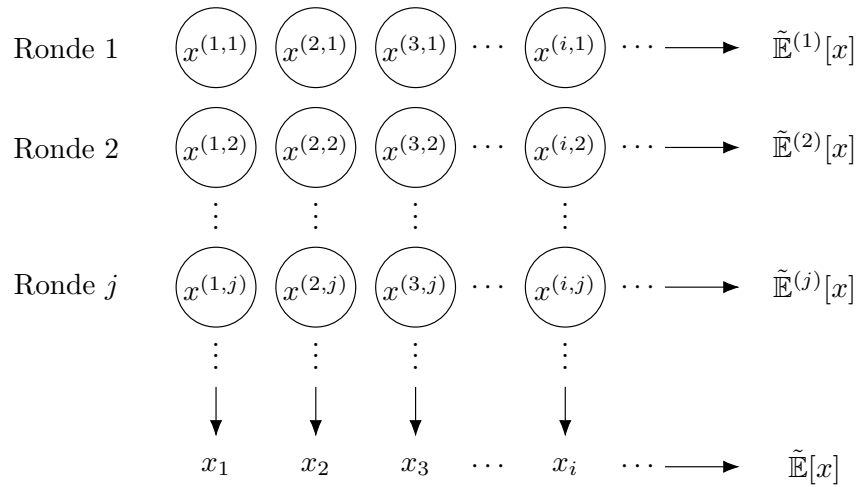


FIGURE D.1 – Une variable aléatoire x est échantillonnée lors de plusieurs rondes. La valeur moyenne calculer à chaque ronde peut être vue comme un échantillon d'une variable aléatoire $\mathbb{E}[x]$. Celle-ci apparaît comme une somme des variables aléatoires x_i .

comme étant des réalisations de la variable aléatoire x_i . Ainsi, l'espérance $\tilde{\mathbb{E}}[x]$ est en fait une somme de variables aléatoires.

Les distributions qui caractérisent chacune des variables aléatoires x_i sont les mêmes que pour x . On conclut donc que

$$\mathbb{E}[x_i] = \mathbb{E}[x] \quad (\text{D.7})$$

et

$$\text{Var}(x_i) = \text{Var}(x). \quad (\text{D.8})$$

Finalement, on considère qu'un résultat obtenu à la $i^{\text{ième}}$ étape est indépendant de celui obtenu à la $j^{\text{ième}}$, sauf si $j = i$. On résume cela en spécifiant la covariance entre les échantillons pris aux étapes i et j

$$\text{Covar}(x_i, x_j) = \text{Var}(x_i)\delta_{ij}. \quad (\text{D.9})$$

4.1 Espérance

Ainsi, on peut utiliser les propriétés D.1 et D.2 de l'espérance pour exprimer l'espérance de l'estimation de l'espérance de x

$$\mathbb{E}[\tilde{\mathbb{E}}[x]] = \mathbb{E}\left[\frac{1}{N} \sum_{i=1}^N x_i\right] = \frac{1}{N} \sum_{i=1}^N \mathbb{E}[x_i]$$

En utilisant le fait que les distributions de x et x_i sont identiques (équation D.7), on peut conclure que l'espérance de la valeur moyenne d'une ronde d'échantillonnage est égale, sans surprise, à l'espérance de la variable aléatoire x

$$\mathbb{E}[\tilde{\mathbb{E}}[x]] = \frac{1}{N} \sum_{i=1}^N \mathbb{E}[x] = \mathbb{E}[x].$$

4.2 Variance

Il est surtout intéressant d'exprimer la variance de l'estimation de l'espérance. En supposant que chaque échantillon de la variable x est indépendant des autres (équation D.9) et à l'aide des propriétés D.3 et D.4, on peut écrire

$$\text{Var}(\tilde{\mathbb{E}}[x]) = \text{Var}\left(\frac{1}{N} \sum_{i=1}^N x_i\right) = \frac{1}{N^2} \sum_{i=1}^N \text{Var}(x_i).$$

Encore en utilisant le fait que les distributions de x et x_i sont identiques (équation D.7) on obtient que la variance de l'estimation de l'espérance de x est donnée par

$$\text{Var}(\tilde{\mathbb{E}}[x]) = \frac{1}{N} \text{Var}(x).$$

Ainsi, lorsqu'on augmente le nombre d'échantillons N pour calculer une valeur moyenne, la variance sur celle-ci diminue comme l'inverse de N . Autrement dit, plus le nombre d'échantillons est grand, plus la valeur moyenne devrait être proche de l'espérance. Cela est cohérent avec notre intuition qu'on peut améliorer la précision d'une estimation en accumulant plus de données.

4.3 Covariance

On peut également s'intéresser à la covariance entre des estimations d'espérance pour deux variables aléatoires. Ici, il est important de noter que lorsque plusieurs variables aléatoires sont impliquées, on considère un échantillon comme comprenant une valeur pour chaque variable aléatoire. Ainsi pour des variables aléatoires x et y , un échantillon consiste en

$$\{x^{(i)}, y^{(i)}\}.$$

En utilisant une approche similaire à celle qu'on a utilisée plutôt, on peut identifier les estimations des espérances de x et y comme des sommes de variables aléatoires

$$\tilde{\mathbb{E}}[x] = \frac{1}{N} \sum_{i=1}^N x_i \quad \text{et} \quad \tilde{\mathbb{E}}[y] = \frac{1}{N} \sum_{j=1}^N y_j$$

La covariance entre les estimations des espérances pour deux variables aléatoires s'exprime donc comme

$$\text{Covar}(\tilde{\mathbb{E}}[x], \tilde{\mathbb{E}}[y]) = \text{Covar}\left(\frac{1}{N} \sum_{i=1}^N x_i, \frac{1}{N} \sum_{j=1}^N y_j\right)$$

En utilisant les propriétés D.5 et D.6, on peut réécrire cette covariance en fonction de la covariance entre x_i et y_j

$$\text{Covar}(\tilde{\mathbb{E}}[x], \tilde{\mathbb{E}}[y]) = \frac{1}{N^2} \sum_{ij} \text{Covar}(x_i, y_j)$$

Or, si on suppose que les échantillons pris à des étapes différentes sont indépendants on doit avoir

$$\text{Covar}(x_i, y_j) = \text{Covar}(x_i, y_i) \delta_{ij} = \text{Covar}(x, y) \delta_{ij}.$$

Ainsi, la covariance entre les estimations des espérances pour deux variables aléatoires x et y est donnée par

$$\text{Covar}(\tilde{\mathbb{E}}[x], \tilde{\mathbb{E}}[y]) = \frac{1}{N} \text{Covar}(x, y).$$

Ce résultat indique, qu'en augmentant le nombre d'échantillons, les estimations des espérances de x et y sont de moins en moins affectées par la covariance entre celle-ci.

5 Estimation de la variance

Pour estimer la variance d'une variable aléatoire, on doit d'abord en connaître l'espérance, ou du moins avoir fait une bonne estimation de celle-ci. Assumons qu'on la connaisse. L'estimation de la variance à partir de N d'échantillons $x^{(i)}$ s'obtient en calculant

$$\tilde{\text{Var}}(x) = \frac{1}{N} \sum_{i=1}^N \left(x^{(i)} - \mathbb{E}[x] \right)^2.$$

6 Estimation de la covariance

Pour estimer la covariance entre deux variables aléatoires, on doit d'abord connaître leurs espérances. L'estimation de la variance à partir de N d'échantillons $\{x^{(i)}, y^{(i)}\}$ s'obtient en calculant

$$\tilde{\text{Covar}}(x) = \frac{1}{N} \sum_{i=1}^N \left(x^{(i)} - \mathbb{E}[x] \right) \left(y^{(i)} - \mathbb{E}[y] \right).$$