Calcul quantique:le cadre mathématique.

Géraud Sénizergues

LaBRI, Bordeaux.

Séminaire LIS, 21 et 28 Mars 2023

Le cadre mathématique

contents

Un peu d'histoire

Calcul/Information classique et logique

- [Gödel 1926], [Kleene 1937] : Fonctions récursives
- [Church 1936] : Lambda-calcul
- [Turing 1936] : Machines de Turing

Thèse de Church-Turing (logique) :
Les fonctions calculables en un sens mathématique naturel sont les fonctions Turing-calculables.
Thèse de Church-Turing (physique) :
les fonctions calculables par un dispositif physique sont les fonctions Turing-calculables

Calcul/Information classique et logique

Autres questions :
Q1 tout phénomène physique est-il descriptible par une loi déterministe Turing-calculable ?
Q2 toute fonction Turing-calculable est-elle calculable par un dispositif physique ?
Réponses(dans le monde de la physique classique) :
Q1
OUI : preuve mathématique [Gandi 1985],[Dershowitz,Gurevich 2008].
Q2
2.1 OUI fabrication d'un ordinateur [ENIAC, Eckert-Maughli 1945].
2.2 OUI preuve mathématique [Bennett, Toffoli $\sim$ 1980].

Calcul/Information classique et physique classique

- Brillouin 1956 : Science and information theory
- Landauer, Bennett, Toffoli [$\sim$ 1960] : calcul réversible
- Gandi 1985 : déduit la thèse de Church-Turing des lois de la physique classique.

Calcul/Information quantique et physique quantique

- Feynmann 1982 : faire calculer les lois de la mécanique quantique ...par des systèmes quantiques
- Deutsch 1985 : machine de Deutsch i.e. machine de Turing , mais quantique
démontre l'existence d'une machine universelle quantique.
- Arrighi-Dowek 2012 : déduisent la thèse de Church-Turing des lois de la physique quantique.

Physique "informationelle"

J.A. Wheeler [directeur de thèse de Feynmann] : "Everything is information" changement de paradigme, voir [Gruska, 2007, poly de calcul quantique].
P. Höhn : déduit la formulation de la mécanique quantique (espaces de Hilbert, opérateurs linéaires hermitiens (resp. unitaires), amplitude de probabilité) d'axiomes "informationels" i.e. sur l'acquisition et la communication d'informations.

Produit tensoriel

Produit tensoriel :definition

Soient E, F deux espaces vectoriels de dimension finie sur un corps commutatif K. Soit $\mathcal{B}$ (resp. $\mathcal{C}$) une base de E (resp. de F). Considérons l'ensemble

$$T := K^{\mathcal{B}\times\mathcal{C}}$$

muni des opérations suivantes :
addition :

$$\varphi + \psi : (b, c) \mapsto \varphi(b, c) + \psi(b, c)$$

produit par un scalaire :

$$k \cdot \varphi : (b, c) \mapsto k \cdot \varphi(b, c)$$

On vérifie que T, muni de ces deux opérations, est un espace vectoriel sur K.

Produit tensoriel :definition

Définissons, pour tout $b \in \mathcal{B}$ et tout $c \in \mathcal{C}$, l'élément suivant de T, que nous noterons $b \otimes c$:

$$b \otimes c : (b, c) \mapsto 1, (b', c') \mapsto 0(\text{ pour tout } (b', c') \neq (b, c)$$

On vérifie alors que tout élément φ de T s'écrit sous la forme :

$$\varphi = \sum_{b \in \mathcal{B}, c \in \mathcal{C}} \varphi(b, c) \cdot b \otimes c$$

et que, d'autre part, si

$$\varphi = \sum_{b \in \mathcal{B}, c \in \mathcal{C}} k_{b,c} \cdot b \otimes c$$

pour une famille $(k_{b,c})_{(b,c) \in \mathcal{B} \times \mathcal{C}}$, alors

$$\forall b \in \mathcal{B}, \forall c \in \mathcal{C}, k_{b,c} = \varphi(b, c).$$

Produit tensoriel :definition

Donc $\{b \otimes c \mid b \in \mathcal{B}, c \in \mathcal{C}\}$ est une base de T. L'application $(b, c) \mapsto b \otimes c$ peut être étendue, par bilinéarité, à l'espace produit :

$$(\sum_{b \in \mathcal{B}} \lambda_b b) \otimes (\sum_{c \in \mathcal{C}} \mu_c c) := \sum_{b \in \mathcal{B}, c \in \mathcal{C}} \lambda_b \mu_c \cdot (b \otimes c).$$

Cette application bilinéaire $\otimes : E \times F \to T$ est l'application bilinéaire la plus générale que l'on puisse définir depuis $E \times F$ vers n'importe quel autre e.v. sur K.

Proposition

Soit B une application bilinéaire de $E \times F$ dans un espace vectoriel T' sur K. Alors, il existe une unique application linéaire $\tilde{B} : T \to T'$ telle que :

$$B = \tilde{B} \circ \otimes.$$

Produit tensoriel :definition

La proposition 1 énonce la *propriété universelle* du produit tensoriel :
- elle est universelle, en ce qu'elle parle de *toutes* les applications bilinéaires
- elle *caractérise* le couple (espace T, application bilinéaire $\otimes$) à isomorphisme près.

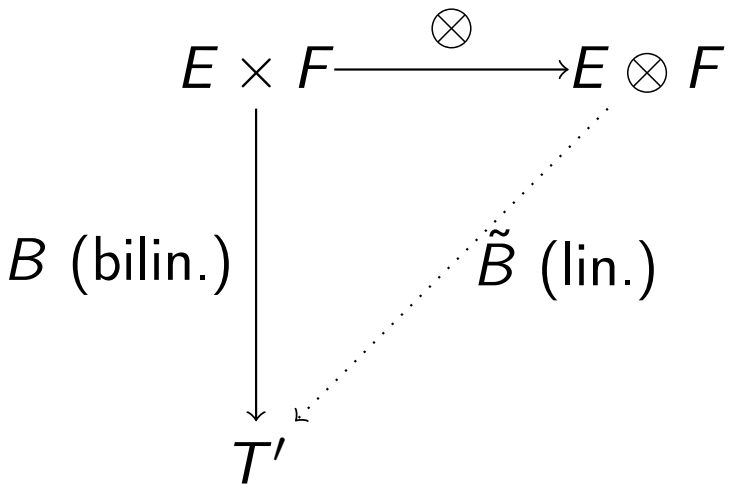

Figure – La propriété universelle du produit tensoriel.

Produit tensoriel :definition

Une construction qui partirait de bases $\mathcal{B}', \mathcal{C}'$ différentes, aboutirait à un espace vectoriel T',isomorphe à l'espace T, par un isomorphisme compatible avec les applications $\otimes : E \times F \to T$ et $\otimes : E \times F \to T'$.

Produit tensoriel :un exemple

Soit $K = \mathbb{R}, E = \mathbb{C}, F = \mathbb{R}^3$

$$E = \mathrm{Vec}\{1, i\}, \quad F = \mathrm{Vec}\{e_1, e_2, e_3\}$$

où $e_1 = (1, 0, 0), e_2 = (0, 1, 0), e_3 = (0, 0, 1)$.

$$E \otimes F = \mathrm{Vec}\{1 \otimes e_1, i \otimes e_1, 1 \otimes e_2, i \otimes e_2, 1 \otimes e_3, i \otimes e_3\}.$$

$F_{\mathbb{C}} = \mathbb{C} \otimes F$ est le complexifié de F.
C'est un e.v. sur $\mathbb{C}$ pour la loi externe :

$$(a + ib) \odot u = (a + ib) \otimes u$$

Produit tensoriel :un exemple

Une base de $F_{\mathbb{C}}$ sur $\mathbb{C}$ est $\{e_1, e_2, e_3\}$:
- elle est génératrice
- elle est libre :

si

$$\sum_{j=1}^{3}(a_j + ib_j) \otimes e_j = 0$$

alors

$$\sum_{j=1}^{3} a_j(1 \otimes e_j) + \sum_{j=1}^{3} b_j(i \otimes e_j) = 0$$

donc

$$\forall j \in [1,3], a_j = b_j = 0.$$

Couramment utilisé pour démontrer des formes normales pour les endomorphimes de $\mathbb{R}^n$.

Produit tensoriel d'applications linéaires

Soient E, E, F, F' des espaces vectoriels de dimension finie sur un corps commutatif K. Première définition :
pour toutes applications linéaires

$$\varphi \in \mathcal{L}(E, E'), \psi \in \mathcal{L}(F, F')$$

nous définissons une application linéaire

$$\varphi \hat{\otimes} \psi \in \mathcal{L}(E \otimes F, E' \otimes F'),$$

de la façon suivante : supposons que $\mathcal{B}$ (resp. $\mathcal{C}$) est une base de E (resp. de F). On pose

$$\varphi \hat{\otimes} \psi\Big(\sum_{(b,c)\in\mathcal{B}\times\mathcal{C}} \lambda_{b,c}\, b \otimes c\Big) := \sum_{(b,c)\in\mathcal{B}\times\mathcal{C}} \lambda_{b,c}\varphi(b) \otimes \psi(c).$$

Produit tensoriel d'applications linéaires

Deuxième définition :
l'application $(u, v) \mapsto \varphi(u) \otimes \psi(v)$ est une application bilinéaire de $E \times F$ dans $E' \otimes F'$, donc il existe une unique application linéaire

$$\Phi : E \otimes F \to E' \otimes F'$$

qui fait commuter le diagramme ci-dessous.

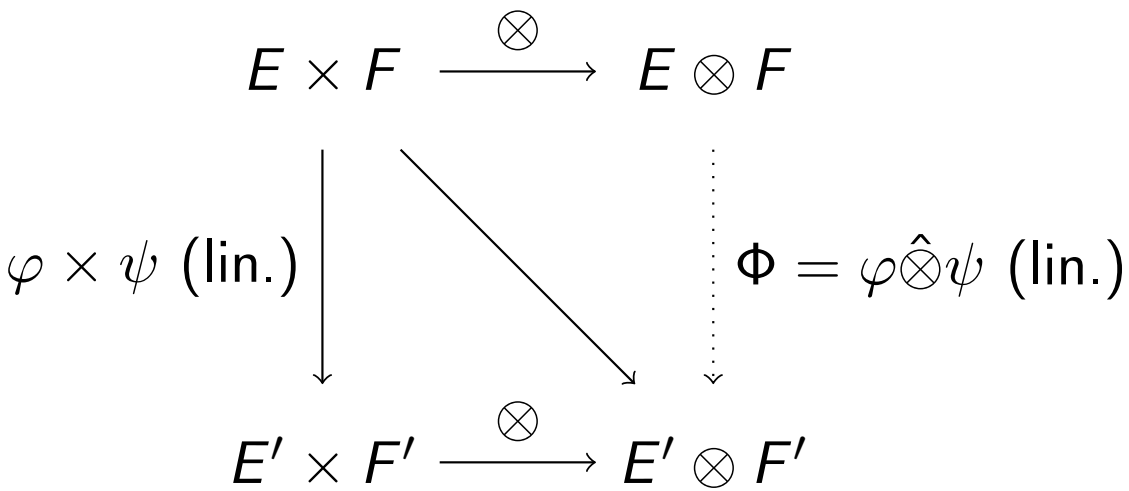

Figure – Produit tensoriel d'applications linéaires.

Produit tensoriel d'applications linéaires

1-Comme l'application définie par la première définition fait commuter le diagramme, les deux définitions sont équivalentes.
2- L'application $\varphi\hat{\otimes}\psi$ ne dépend *que* des applications φ, ψ (vu la deuxième définition)

Produit tensoriel d'applications linéaires

Considérons maintenant l'application :

$$\hat{\otimes} : \mathcal{L}(E, E') \times \mathcal{L}(F, F') \to \mathcal{L}(E \otimes F, E' \otimes F')$$

$$(\varphi, \psi) \mapsto (\varphi \hat{\otimes} \psi)$$

Cette application est bilinéaire. Par la propriété universelle, il existe une unique application linéaire

$$H : \mathcal{L}(E, E') \otimes \mathcal{L}(F, F') \to \mathcal{L}(E \otimes F, E' \otimes F')$$

faisant commuter le diagramme :

Produit tensoriel d'applications linéaires

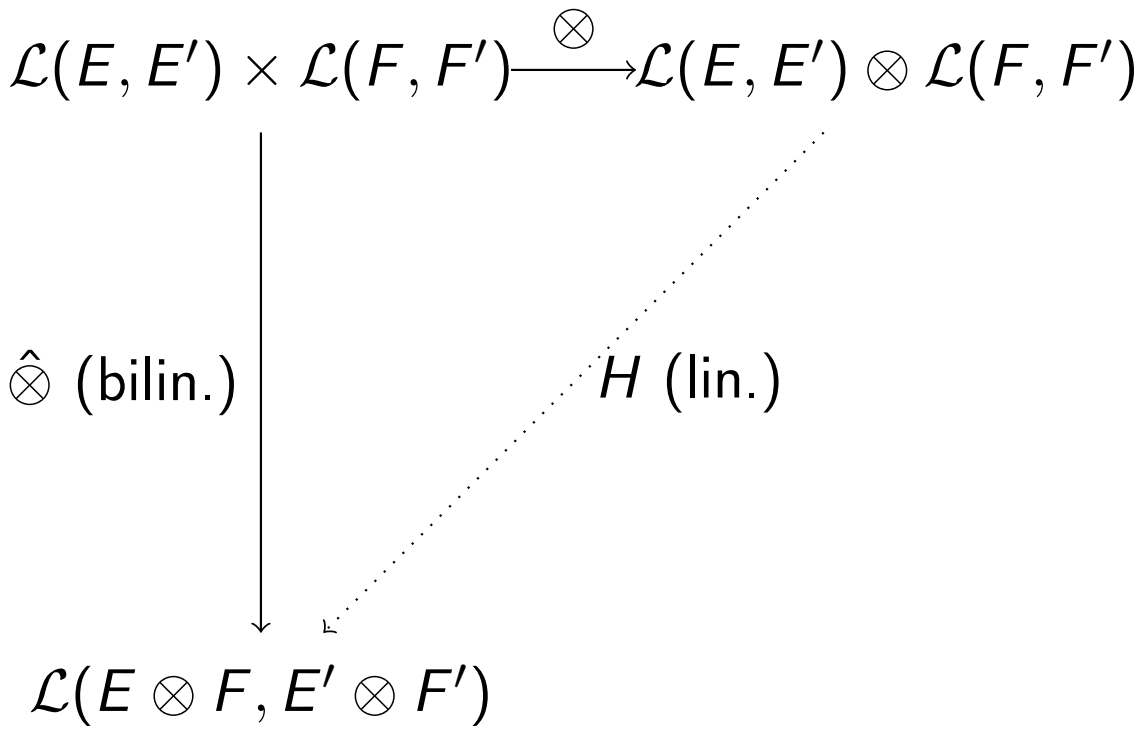

Figure – L'isomorphisme H.

i.e. vérifiant que, $H(\varphi \otimes \psi) = \varphi \hat{\otimes} \psi$.

Produit tensoriel d'applications linéaires : exemple

Un automate fini avec multiplicités dans K (K-automate, en abrégé) est un 5-uplet $\mathcal{A} =< X, Q, I, T, \tau >$ où

- X est un ensemble fini, l'alphabet d'entrée
- $Q = \{q_0, \ldots, q_{d-1}\}$ est un ensemble fini, l'ensemble des états
- $I \in K^{1\times d}$ est le vecteur-ligne initial
- $T \in K^{d\times 1}$ est le vecteur-colonne terminal
- $\tau \subseteq Q \times X \times K \times Q$ est l'ensemble des transitions

Pour toutre lettre $x \in X$, on note $\mu_{\mathcal{A}}(x) \in K^{d\times d}$ la matrice dont le coefficient en ligne i, colonne j est :

$$\mu_{\mathcal{A}}(x)_{i,j} := \sum_{(q_i,x,k,q_j)\in\tau} k$$

$$\mathrm{S}(\mathcal{A}) : w \mapsto I \cdot \mu_{\mathcal{A}}(w) \cdot T$$

Produit tensoriel d'applications linéaires : exemple

Soient deux automates finis avec multiplicité $\mathcal{A}_1, \mathcal{A}_2$.
Posons $I = I_1 \otimes I_2 \in K^{1 \times d_1 \cdot d_2}$,

$$\mu(x) = \mu_1(x) \otimes \mu_2(x) \in K^{d_1 \cdot d_2 \times d_1 \cdot d_2},$$

$T = T_1 \otimes T_2 \in K^{d_1 \cdot d_2 \times 1}$. Alors :

$$(S_1 \odot S_2)(w) = I \cdot \mu(w) \cdot T$$

autrement dit, le produit tensoriel des représentations linéaires de S_1, S_2 représente $S_1 \odot S_2$.

Produit tensoriel d'applications linéaires

Theorem

L'application H est un isomorphisme de $\mathcal{L}(E, E') \otimes \mathcal{L}(F, F')$ dans $\mathcal{L}(E \otimes F, E' \otimes F')$.

On peut donc "identifier" l'objet $\varphi \otimes \psi$ avec son image par H i.e. $\varphi \hat{\otimes} \psi$.

Fait

Pour tous
$L_1 \in \mathcal{L}(E_1, E_1'), L_1' \in \mathcal{L}(E_1', E_1''), L_2 \in \mathcal{L}(E_2, E_2'), L_2'' \in \mathcal{L}(E_2', E_2'')'$,
$(L_1' \otimes L_2') \cdot (L_1 \otimes L_2) = (L_1' \cdot L_1) \otimes (L_2' \cdot L_2)$

Preuve. Ces deux applications sont linéaires et coincident sur les vecteurs de $E_1 \otimes E_2$. ■

Espaces de Hilbert

Produit scalaire

Espaces de Hilbert :produit scalaire

Soit $\mathcal{H}$ un espace vectoriel sur le corps des nombres complexes $\mathbb{C}$. On appelle "produit scalaire" sur $\mathcal{H}$ toute application de $\mathcal{H} \times \mathcal{H}$ dans $\mathbb{C}$, notée :

$$(u, v) \mapsto (u|v)$$

qui vérifie les propriétés suivantes :

linéarité à droite :pour tous $u, v_1, v_2 \in \mathcal{H}, \lambda_1, \lambda_2 \in \mathbb{C}$

$$(u|\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 (u|v_1) + \lambda_2 (u|v_2) \tag{2}$$

anti-linéarité à gauche :pour tous $u_1, u_2, v \in \mathcal{H}, \lambda_1, \lambda_2 \in \mathbb{C}$

$$(\lambda_1 u_1 + \lambda_2 u_2|v) = \overline{\lambda_1}(u_1|v) + \overline{\lambda_2}(u_2|v) \tag{3}$$

symétrie hermitienne :pour tous $u, v \in \mathcal{H}$

$$(u|v) = \overline{(v|u)} \tag{4}$$

Espaces de Hilbert :produit scalaire

Remarquons que :
(2) et (4) entrainent (3) ; (4) entraine que $(u|u)$ est un nombre réel.
positivité :pour tout $u \in \mathcal{H}$

$$(u|u) \geq 0 \tag{5}$$

non-dégénérescence :pour tout $u \in \mathcal{H}$

$$\forall v \in \mathcal{H}, (u|v) = 0 \Rightarrow u = 0 \tag{6}$$

Espaces de Hilbert :produit scalaire

Inégalité de cauchy-Schwartz :
si $(*|*)$ est sesquilinéaire et positive , alors, pour tous $u, v \in \mathcal{H}$:

$$|(u|v)|^2 \leq |(u|u)| \cdot |(v|v)|.$$

Sachant que $(*|*)$ est positive, la non-dégénérescence équivaut à :

$$\forall u \in \mathcal{H}, (u|u) = 0 \Rightarrow u = 0. \tag{7}$$

(forme sequilinéaire *définie* positive).

Espaces de Hilbert :produit scalaire

On appelle *espace pré-hilbertien* tout espace vectoriel $\mathcal{H}$ sur $\mathbb{C}$ muni d'un produit scalaire $(*|*)$ vérifiant les propriétés ci-dessus.

Lorsque $\mathcal{H}$ est de dimension finie, il s'agit d'un espace *de Hilbert*.

Cas général : un espace de Hilbert est un espace pré-Hilbertien, qui est complet et qui admet une partie dénombrable dense.

Dans ce qui suit, on ne considérera que des espaces de Hilbert de dimension finie $\mathcal{H}$.

Espaces de Hilbert :produit scalaire

On rappelle que le dual de $\mathcal{H}$, noté $\mathcal{H}^*$ est l'espace des formes linéaires sur $\mathcal{H}$: $\mathcal{H}^* := \mathcal{L}(\mathcal{H}, \mathbb{C})$.
$\mathcal{H}$ admet au moins une base orthonormée i.e. une famille de vecteurs $e_1, e_2, \ldots, e_n$ qui est une base et telle que

$$\forall i, j \in [1, n], (e_i | e_j) = \delta_i^j$$

où δ_i^j, le symbole de Kronecker signifie 1 si $i = j$ et 0 si $i \neq j$.
Fixons une base orthonormée de $\mathcal{H}$. Si les vecteurs u, v ont pour coordonnées respectives $X, Y \in \mathbb{M}_{n,1}(\mathbb{C})$ dans cette base, alors leur produit scalaire vaut

$$(u|v) = X^\dagger \cdot Y.$$

(dans le membre droit, $\cdot$ dénote le produit matriciel).

Espaces de Hilbert :produit scalaire

Autrement écrit : si

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ \vdots \\ x_n \end{pmatrix}, Y = \begin{pmatrix} y_1 \\ \vdots \\ y_k \\ \vdots \\ k_n \end{pmatrix}$$

alors

$$X^\dagger = \begin{pmatrix} \bar{x}_1 & \dots & \bar{x}_k & \dots & \bar{x}_n \end{pmatrix}$$

$$(u|v) = \sum_{k=1}^{n} \bar{x}_k \cdot y_k.$$

Espaces de Hilbert :adjoint

Considérons une application linéaire $L : \mathcal{H} \to \mathcal{H}$. L'application adjointe, L^* est définie par :

$$\forall u, v \in \mathcal{H}, (u|Lv) = (L^* u|v). \tag{8}$$

On vérifie que si M est la matrice de L dans une bases orthonormée $\mathcal{E}$, alors la matrice de L^* dans la même base est $M^\dagger$ définie par

$$M = (m_{i,j})_{i,j\in[1,n]}, \quad M^\dagger := (\bar{m}_{j,i})_{i,j\in[1,n]}.$$

Espaces de Hilbert :adjoint

Les propriétés suivantes des applications linéaires sont souvent utilisées en mécanique quantique :
L est *hermitien* ssi

$$\forall u, v \in \mathcal{H}, (u|Lv) = (Lu|v)$$

ce qui revient à $L = L^*$ ou encore au fait que sa matrice M (dans une base orthonormée) vérifie $M = M^\dagger$.
L est *unitaire* ssi

$$\forall u, v \in \mathcal{H}, (Lu|Lv) = (u|v)$$

ce qui revient à $L^*L = \mathrm{Id}_{\mathcal{H}}$, ou encore au fait que sa matrice M (dans une base orthonormée) vérifie $M \cdot M^\dagger = \mathrm{I}_n$.

Espaces de Hilbert :Endomorphismes normaux

L'endomorphisme $L \in \mathcal{L}(\mathcal{H}, \mathcal{H})$ est dit *normal* ssi

$$L \cdot L^* = L^* \cdot L$$

Théorème

Si L est normal, alors, il existe une base orthonormée de $\mathcal{H}$, formée de vecteurs propres de L.

Idée de la preuve :
Tout sous-espace $F \subseteq \mathcal{H}$ stable par L, a un orthogonal $F^{\perp}$ stable par L^*.
Cas particuliers :
Endomorphismes hermitiens : $L^* = L$
Endomorphismes unitaires : $L^* = L^{-1}$

Notation de Dirac

Notation de Dirac

La propriété de non-dégénérescence du produit scalaire entraine que l'application :

$$G : \mathcal{H} \to \mathcal{H}^*$$

definie par

$$G(u) : v \mapsto (u|v) \tag{9}$$

est semi-linéaire et injective (puisque son noyau est réduit à $\{0\}$). Comme $\mathcal{H}$ est de dimension finie, $\mathcal{H}$ et $\mathcal{H}^*$ ont même dimension, ce qui entraîne que G est un anti-isomorphisme.
Pour tous vecteurs $u, v \in \mathcal{H}$

$$(u|v) = G(u)(v)$$

i.e. le produit scalaire du vecteur u par le vecteur v est égal à la valeur de la forme linéaire $G(u)$ appliquée à l'argument v.

Notation de Dirac

Décidons de noter

$$|u\rangle, |v\rangle, |w\rangle, |0\rangle, |1\rangle, \ldots$$

les vecteurs de $\mathcal{H}$, puis de noter

$$\langle u|, \langle v|, \langle w|, \langle 0|, \langle 1|, \ldots$$

leurs images par G.
L'équation précédente devient alors

$$(u|v) = G(u)(v) = \langle u||v\rangle$$

Décidons maintenant de ne retenir qu'une barre verticale dans le membre droit, on obtient alors

$$(u|v) = G(u)(v) = \langle u|v\rangle$$

Notation de Dirac : quelques usages

Soit $L \in \mathcal{L}(\mathcal{H}, \mathcal{H})$, La notation

$$\langle u|L|v\rangle$$

signifie : la forme $\langle u|$ appliquée à l'argument $L(|v\rangle)$, i.e.

$$(u|Lv)$$

Si nous déplaçons les parenthèses d'un cran vers la gauche, la notation devient

$$(\langle u|\, L)|v\rangle$$

qui signifie : la forme $\langle u|\, L$ appliquée à l'argument $|v\rangle$;
où

$$\langle u|\, L := \langle u| \circ L$$

est la forme linéaire composée de l'endomorphisme L par la forme $\langle u|$: le résultat est le même.

Notation de Dirac : quelques usages

Remarquons aussi que :

$$\langle u|L = \langle L^* u|.$$

(ces deux formes, appliquées à un même argument $|v\rangle$ donnent le même résultat).

Notation de Dirac : quelques usages

Une notation, plus étrange, est la suivante :

$$|v\rangle\langle u| \tag{10}$$

Elle désigne l'application linéaire :

$$|w\rangle \mapsto |v\rangle\langle u||w\rangle = |v\rangle(\langle u|w\rangle)$$

L'expression entre parenthèses est un nombre ; (10) désigne l'application linéaire :

$$|w\rangle \mapsto \langle u|w\rangle|v\rangle$$

On vérifie que

$$\mathrm{Tr}(|v\rangle\langle u|) = \langle u|v\rangle$$

Produit tensoriel d'espaces de Hilbert

Produit scalaire

Supposons que $\mathcal{B} = \{b_1, \ldots, b_i, \ldots, b_n\}$ est une base orthonormée de E et $\mathcal{C} = \{c_1, \ldots, c_j, \ldots, c_m\}$ est une base orthonormée de F. Considérons la forme sesqui-linéaire S (i.e. semi-linéaire à gauche, linéaire à droite) définie sur la base $\{b_i \otimes c_j | i \in [1, n], j \in [1, m]\}$ par

$$S(b_i \otimes c_j, b_k \otimes c_\ell) := (b_i|b_k) \cdot (c_j|c_\ell).$$

Elle est (par définition) sesqui-linéaire. La matrice de S, dans la base $\{b_i \otimes c_j | i \in [1, n], j \in [1, m]\}$ est :

$$\mathrm{I}_{nm}.$$

Donc S est "hermitienne, définie-positive". L'espace $E \otimes F$, muni de la forme S, est un espace de Hilbert.

Produit tensoriel d'espaces de Hilbert

La forme S sera noté $(*|*)$ (comme dans E et F). On montre que, pour tous $u, u' \in E, v, v' \in F$

$$(u \otimes v | u' \otimes v') = (u|u')(v|v').$$

Preuve : le lhs et le rhs définissent des applications $E \times F \times E \times F \to \mathbb{C}$ qui sont linéaires par rapport à v, v' et anti-linéaires par rapport à u, u'. Comme elles coincident sur les quadruplets formés d'éléments des bases $\mathcal{B}, \mathcal{C}$, elles sont égales. □

N.B. le produit scalaire sur $E \otimes F$ ne dépend donc que des produits scalaires sur les facteurs E, F.

Produit tensoriel d'espaces de Hilbert

Compatibilité avec l'anti-isomorphisme G
Pour tous $u \in E, v \in F$.

$$\langle u \otimes v| = \langle u| \otimes \langle v|.$$

Esquisse de preuve. On prouve que ces deux éléments de $(E \otimes F)^*$ coincident sur les vecteurs de la forme $|u_1\rangle \otimes |v_1\rangle$. ■

Postulats physiques

Espace des états

Un système physique $\mathcal{S}$ est décrit par un espace de Hilbert $\mathcal{H}$.
Chaque état du système est décrit par un vecteur unitaire :

$$|\psi\rangle \in \mathcal{H}, \quad \langle\psi|\psi\rangle = 1.$$

Système $\mathcal{S}$ formé de deux particules A_1, A_2 :
$\mathcal{H}_1$ (resp. $\mathcal{H}_2$) est l'espace de A_1 (resp. A_2).
L'espace du système entier est

$$\mathcal{H} := \mathcal{H}_1 \otimes \mathcal{H}_2.$$

Système $\mathcal{S}$ formé de n sous-systèmes $\mathcal{S}_1, \ldots, \mathcal{S}_n$:

$$\mathcal{H} := \bigotimes_{j=1}^{n} \mathcal{H}_j.$$

Evolution

Espace des états : sphère unité d'un espace de Hilbert $\mathcal{H}$.
Équation de Schrödinger :

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

où $\mathrm{H}(t) \in \mathcal{L}(\mathcal{H})$, $\mathrm{H}(t) = \mathrm{H}^*(t)$.
Si $\mathrm{H}(t)$ est constant, il existe une application dérivable $U : \mathbb{R} \times \mathbb{R} \to \mathrm{U}(\mathcal{H})$ telle que, $\forall t \in \mathbb{R}, U(t,t) = \mathrm{I}$ et, pour tous $(t_0, t) \in \mathbb{R} \times \mathbb{R}$ et $|\psi_0\rangle \in \mathcal{H}$

$$|\psi\rangle (t) = U(t_0, t) |\psi_0\rangle$$

est l'unique solution de l'équation sur $\mathbb{R}$ t.q. $|\psi\rangle (t_0) = |\psi_0\rangle$.
NB : il suffit de poser $U(t_0, t) = \exp(-i \frac{t-t_0}{\hbar} \mathrm{H})$.

Mesure

Observable $\mathcal{M}$: protocole de mesure d'une grandeur sur le système.
Opérateur hermitien associé

$$M \in \mathcal{L}(\mathcal{H}, \mathcal{H})$$

tel que

$$M^* = M.$$

Soit $\mathcal{H}_\lambda = \mathrm{Ker}(M - \lambda \mathrm{I})$, pr_λ la projection orthogonale sur le sous-espace propre $\mathcal{H}_\lambda$.

Mesure

Résultat d'une mesure :

$\mu : \Omega \to \mathbb{R}$ est une variable aléatoire. Si le système est dans l'état $|\psi\rangle$

$$\Pr\{\mu = \lambda\} = \| \mathrm{pr}_\lambda |\psi\rangle \|^2$$

État après la mesure :

$$\frac{1}{\| \mathrm{pr}_\lambda |\psi\rangle \|} \cdot \mathrm{pr}_\lambda |\psi\rangle$$

la fonction d'onde "s'effondre".

Mesure et évolution de sous-systèmes

Système $\mathcal{S}$ formé de deux sous-systèmes $\mathcal{S}_1, \mathcal{S}_2$, dont les espaces sont $\mathcal{H}_1$ (resp. $\mathcal{H}_2$).
Evolution : si U_1, U_2 sont des évolutions possibles de $\mathcal{S}_1, \mathcal{S}_2$, alors $U_1 \otimes U_2$ est une évolutions possible de $\mathcal{S}_1, \mathcal{S}_2$.
NB : $U_1 \otimes U_2 = (U_1 \otimes \mathrm{I}_2) \cdot (\mathrm{I}_1 \otimes U_2)$
Mesure : la mesure de l'observable $\mathcal{M}_1$ sur $\mathcal{S}_1$ est representée par l'endomorphisme

$$M_1 \otimes \mathrm{I}_2$$

sur $\mathcal{S}$.
la mesure de l'observable $\mathcal{M}_2$ sur $\mathcal{S}_2$ est representée par l'endomorphisme

$$\mathrm{I}_1 \otimes M_2$$

sur $\mathcal{S}$.

Circuits quantiques

un qbit : espace $\mathcal{B} = \mathrm{Vect}_{\mathbb{C}}(|0\rangle, |1\rangle) \simeq \mathbb{C}^2$.
n qbits : espace $\mathcal{B}^{\otimes n}$.
transition d'évolution : une application unitaire de la forme

$$\mathrm{I}_{2^p} \otimes P \otimes \mathrm{I}_{2^{n-p-r}}$$

pour un ensemble fini de portes $P \in \mathrm{U}(\mathcal{B}^{\otimes r})$ avec $r \leq 3$.
mesure : une famille de projecteurs orthogonaux $(\mathrm{pr}_j)_{j\in J}$ tels que

$$\sum_{j\in J} \mathrm{pr}_j = \mathrm{I}_{2^n}, \quad \mathrm{pr}_j \circ \mathrm{pr}_k = \mathrm{pr}_k \circ \mathrm{pr}_j$$

(i.e. $\mathcal{H} = \bigoplus_{j=1}^{\ell} \mathrm{Im}\ \mathrm{pr}_j$ et $k \neq j \Rightarrow \mathrm{Im}\ \mathrm{pr}_j \subseteq (\mathrm{Im}\ \mathrm{pr}_k)^{\perp}$).
résultat :$\Pr(\mu = j) = \|\mathrm{pr}_j |\psi\rangle\|^2$
transition :$|\psi\rangle \mapsto \frac{1}{\|\mathrm{pr}_j|\psi\rangle\|} \mathrm{pr}_j |\psi\rangle$

Circuits quantiques

Réalisation des mesures :
Cas 1 : $J = \mathbb{B}^n$,$\mathrm{pr}_{\overrightarrow{b}}$= projection orthogonale sur $\mathbb{C} \cdot \left|\overrightarrow{b}\right\rangle$.
On considère une observable $\mathcal{M}$ sur un qbit, de matrice M (dans la base $(|0\rangle, |1\rangle)$) :

$$M = \begin{pmatrix} \lambda_0 & 0 \\ 0 & \lambda_1 \end{pmatrix}$$

On considère l'observable $\mathcal{M}_k$: mesurer $\mathcal{M}$ sur le qbit numéro k.
Elle est représentée par l'endomorphisme :

$$\mathrm{I}_{2^{k-1}} \otimes M \otimes \mathrm{I}_{2^{n-k+1}}.$$

la variable aléatoire :$\mu_k : \Omega \to \mathbb{R}$
l'espace propre de $\mathcal{M}_k$ associé à λ_b est :

$$E_{k,b} = \mathcal{B}^{\otimes(k-1)} \otimes |b\rangle \otimes \mathcal{B}^{\otimes(n-k+1)}$$

la projection sur ce sous-espace est : $\mathrm{pr}_{k,b}$

Circuits quantiques

Si on mesure successivement $\mathcal{M}_1$ sur le qbit 1, puis $\mathcal{M}_2$ sur 2 , puis ...$\mathcal{M}_n$ sur n, on obtient un vecteur de résultats :

$$\lambda_{b_1}, \lambda_{b_2}, \ldots, \lambda_{b_n}.$$

avec probabilité :

$$\Pr(\forall k, \mu_k = \lambda_{b_k}) = \| \mathrm{pr}_{n,b_n} \cdots \mathrm{pr}_{k,b_k} \cdots \mathrm{pr}_{1,b_1} |\psi\rangle \|^2.$$

et transition vers l'état :

$$\frac{1}{\| \mathrm{pr}_{n,b_n} \cdots \mathrm{pr}_{k,b_k} \cdots \mathrm{pr}_{1,b_1} |\psi\rangle \|} \mathrm{pr}_{n,b_n} \cdots \mathrm{pr}_{k,b_k} \cdots \mathrm{pr}_{1,b_1} |\psi\rangle .$$

On a donc simulé la famille de projecteurs :

$$(\mathrm{pr}_{\overrightarrow{b}})_{\overrightarrow{b} \in \mathbb{B}^n}$$

et les résultats de mesures

$$\overrightarrow{b} \in \mathbb{B}^n.$$

Circuits quantiques

Cas 2 : J= une partition de $\mathbb{B}^n$,
pr_j= projection orthogonale sur $\mathrm{Vect}_{\mathbb{C}}(\{\left|\overrightarrow{b}\right\rangle \mid \overrightarrow{b} \in j\})$.
On simule ces mesures via la famille de projecteurs précédente :
- on fait les mêmes mesures
- on pose $\mu = j$ si le résultat est un vecteur $\overrightarrow{b} \in j$

Circuits quantiques

Cas 3 : J ensemble ($|J| \leq 2^n$) et $\mathcal{H} = \bigoplus_{j \in J} \mathrm{Im}\ \mathrm{pr}_j$ avec $k \neq j \Rightarrow \mathrm{Im}\ \mathrm{pr}_j \subseteq (\mathrm{Im}\ \mathrm{pr}_k)^\perp$
On réalise un circuit C qui envoie une décomposition de la forme du cas 2, vers cette décomposition.
On applique le circuit C^{-1}, puis on fait une mesure comme dans le cas 2, puis on applique le circuit C.

États mixtes

États mixtes :mesures de probabilité

Lorsqu'on effectue une mesure de $\mathcal{S}$ dans l'état $|\psi\rangle$ avec la famille de projecteurs $(\mathrm{pr}_j)_{j\in J}$, le nouvel état peut être vu comme la distribution de probabilité :

$$p := (p_j, |\psi_j\rangle)_{j\in J}$$

où

$$p_j = \|\mathrm{pr}_j |\psi\rangle\|^2, \quad |\psi_j\rangle = \frac{1}{\|\mathrm{pr}_j |\psi\rangle\|} \cdot \mathrm{pr}_j |\psi\rangle .$$

Si on applique un opérateur d'évolution U au système, la distribution de probabilité évolue vers :

$$(p_j, U|\psi_j\rangle)_{j\in J}$$

États mixtes :mesures de probabilité

Si on mesure le système, dans l'état $|\psi_j\rangle$,
avec une famille de projecteurs $(q_k)_{k\in K}$,

$$\Pr(\mu = k) = \| q_k \, |\psi_j\rangle \, \|^2$$

La distribution de probabilité p transite vers :

$$p' := (p_j \cdot \| q_k \, |\psi_j\rangle \, \|^2, q_k \, |\psi_j\rangle)_{(j,k)\in J\times K}$$

États mixtes : Opérateurs de densité

Associons à l'état $|\psi\rangle$, l'opérateur : $\rho := |\psi\rangle \langle\psi|$
Après une évolution par U :

$$\rho' = U\rho U^*.$$

Effet d'une mesure par $(\mathrm{pr}_j)_{j\in J}$:
$\Pr\{\mu = j\} = \|\mathrm{pr}_j |\psi\rangle\|^2 = \mathrm{Tr}(\mathrm{pr}_j |\psi\rangle \langle\psi| \mathrm{pr}_j^*) =$
$\mathrm{Tr}(\mathrm{pr}_j^* \mathrm{pr}_j |\psi\rangle \langle\psi|) = \mathrm{Tr}(\mathrm{pr}_j |\psi\rangle \langle\psi|)$.

$$\Pr\{\mu = j\} = \mathrm{Tr}(\mathrm{pr}_j \rho).$$

$$\rho' = \sum_{j\in J} p_j |\psi_j\rangle \langle\psi_j| = \sum_{j\in J} \mathrm{pr}_j |\psi\rangle \langle\psi| \mathrm{pr}_j^*$$

$$\rho' = \sum_{j\in J} \mathrm{pr}_j \rho \mathrm{pr}_j^*$$

Conclusion : évolution et mesures s'expriment sur ρ.

États mixtes : Opérateurs de densité

Proposition

Soit $\rho \in \mathcal{L}(\mathcal{H})$. Les propriétés suivantes sont équivalentes :
1- il existe des vecteurs unitaires $(|\psi_j\rangle)_{j\in J}$ et des nombres $p_j \in \mathbb{R}^+$ tels que $\sum_{j\in J} p_j = 1$ et $\rho = \sum_{j\in J} p_j |\psi_j\rangle \langle\psi_j|$.
2- $\rho = \rho^*$, $\forall |\psi\rangle \in \mathcal{H}, \langle\psi| \rho |\psi\rangle \geq 0$, $\mathrm{Tr}(\rho) = 1$.

lorsque (1) ou (2) est vrai, on dit que ρ est un opérateur de densité.

États mixtes : Opérateurs de densité

Opération	loi de proba sur états	op. de densité
Etat initial	$p = (p_j, \|\psi_j\rangle)_{j\in J}$	ρ
Evolution selon U	$(p_j, U\|\psi_j\rangle)_{j\in J}$	$U\rho U^*$
$\Pr\{\mu = k\}$	$\sum_{j\in J} p_j \mathrm{Tr}(\mathrm{pr}_k \|\psi_j\rangle\langle\psi_j\|)$	$\mathrm{Tr}(\mathrm{pr}_k \rho)$
Etat après $\mu = k$	$(p_{j,k}, \frac{\mathrm{pr}_k\|\psi_j\rangle}{\|\mathrm{pr}_k\|\psi_j\rangle\|})_{(j,k)\in J\times K}$	$\sum_{k\in K} \mathrm{pr}_k \rho \mathrm{pr}_k^*$

où $p_{j,k} = p_j \cdot \|\mathrm{pr}_k |\psi_j\rangle\|^2$.

États mixtes : Trace partielle

$$\mathrm{Tr}_{\mathcal{F}} : \mathcal{L}(\mathcal{E},\mathcal{E}) \otimes \mathcal{L}(\mathcal{F},\mathcal{F}) \to \mathcal{L}(\mathcal{E},\mathcal{E}) :$$

est l'application linéaire telle que, pour tous $L_1 \in \mathcal{L}(\mathcal{E},\mathcal{E}),\ \ L_2 \in \mathcal{L}(\mathcal{F},\mathcal{F})$:

$$\mathrm{Tr}_{\mathcal{F}}(L_1 \otimes L_2) = \mathrm{Tr}(L_2) \cdot L_1.$$

(L'existence et unicité de $\mathrm{Tr}_{\mathcal{F}}$ découle, via la propriété universelle, du fait que $(L_1, L_2) \mapsto \mathrm{Tr}(L_2) \cdot L_1$ est bilinéaire).
On nomme $\mathrm{Tr}_{\mathcal{F}}$ la trace partielle sur $\mathcal{F}$.
Elle consiste, informellement, à "oublier" l'espace $\mathcal{F}$.

États mixtes : Trace partielle

Considérons un état pur dans un espace de Hilbert : $|\psi\rangle \in \mathcal{E} \otimes \mathcal{F}$.

$$|\psi\rangle = \sum_{j \in J} \alpha_j \, |\xi_j\rangle \otimes |\psi_j\rangle$$

où $\alpha_j \in \mathbb{C}, \xi_j \in \mathcal{E}, \langle \xi_j | \xi_j \rangle = 1$, et $(|\psi_j\rangle)_{j \in J}$ est une base orthonormée de $\mathcal{F}$.
Une mesure avec la famille de projecteurs $(\mathrm{pr}_j)_{j \in J}$, (où pr_j est la projection orthogonale sur $\mathcal{E} \otimes |\psi_j\rangle$) transforme l'état en la distribution de probabilité :

$$p = (|\alpha_j|^2, |\xi_j\rangle \otimes |\psi_j\rangle)_{j \in J}$$

si on "oublie" les $|\psi_j\rangle$ i.e. on envoie tout $|\xi\rangle \otimes |\psi_j\rangle$ sur $|\xi\rangle$ (pour $|\xi\rangle \in \mathcal{E}$), on obtient :

$$p' = (|\alpha_j|^2, |\xi_j\rangle)_{j \in J}$$

États mixtes : Trace partielle

$$\psi = \sum_{j \in J} \alpha_j \left|\xi_j\right\rangle \otimes \left|\psi_j\right\rangle$$

est représenté par l'opérateur de densité :

$$\rho = \sum_{j,k \in J} \alpha_j \bar{\alpha_k} \left|\xi_j\right\rangle \left\langle\xi_k\right| \otimes \left|\psi_j\right\rangle \left\langle\psi_k\right| .$$

$$\begin{aligned} \mathrm{Tr}_{\mathcal{F}}(\rho) &= \sum_{j,k \in J} \alpha_j \bar{\alpha_k} \left|\xi_j\right\rangle \left\langle\xi_k\right| \cdot \mathrm{Tr}(\left|\psi_j\right\rangle \left\langle\psi_k\right|) \\ &= \sum_{j \in J} |\alpha_j|^2 \left|\xi_j\right\rangle \left\langle\xi_j\right| \\ &= \rho'. \end{aligned}$$

États mixtes : Trace partielle

NB0 : ρ' représente p'.
NB1 : ρ' ne dépend pas de la base orthonormée $|\psi_j\rangle$.
NB2 : Si on part d'une distribution de probabilité p sur $\mathcal{E} \otimes \mathcal{F}$ on a la même équivalence entre :
- mesurer avec la famille de projecteurs $(\mathrm{pr}_j)_{j\in J}$, puis projeter $\mathcal{E} \otimes |\psi_j\rangle$ sur $\mathcal{E}$
- prendre la trace partielle de l'opérateur de densité ρ associé à p.

L'algorithme de Simon via les états mixtes

Algorithme de Simon

DONNÉE :$f : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$
fortement périodique i.e. $\exists D \subseteq (\mathbb{Z}/2\mathbb{Z})^n$ s.t.

$$\forall x, y \in (\mathbb{Z}/2\mathbb{Z})^n, \quad f(x) = f(y) \Leftrightarrow (x - y \in D)$$

RÉSULTAT : Une base de D.

Donnée : la "boîte noire" U_f :

$$U_f \left|x\right\rangle \left|y\right\rangle := \left|x\right\rangle \left|y \oplus f(x)\right\rangle .$$

Algorithme de Simon

Notons $G = (\mathbb{Z}/2\mathbb{Z})^n$.

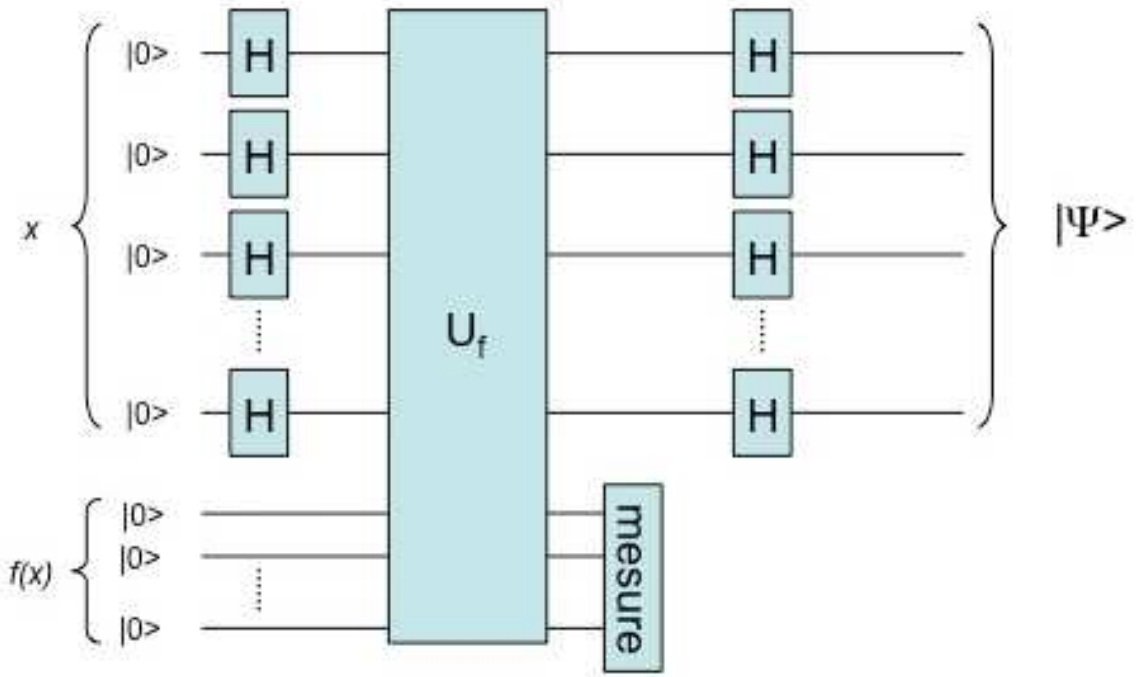

Figure – Le circuit.

Algorithme de Simon

État initial : $|\psi_0\rangle = |0^n\rangle \otimes |0^n\rangle$
Étape 1 :

$$\begin{aligned} |\psi_1\rangle &= H^{\otimes n} \otimes \mathrm{I}_{2^n} |\psi_0\rangle \\ &= \frac{1}{2^{n/2}} \sum_{x \in G} |x\rangle \otimes |0^n\rangle \end{aligned}$$

Algorithme de Simon

Étape 2 :

$$\begin{aligned} |\psi_2\rangle &= U_f |\psi_1\rangle \\ &= \frac{1}{2^{n/2}} \sum_{x \in G} |x\rangle \otimes |f(x)\rangle \\ &\sim \rho_2 \\ &= \frac{1}{2^n} \sum_{x,y \in G} |x\rangle \langle y| \otimes |f(x)\rangle \langle f(y)| \end{aligned}$$

Algorithme de Simon

Étape 3 :

$$\begin{aligned} \rho_3 &= \mathrm{Tr}_2(\rho_2) \\ &= \frac{1}{2^n} \sum_{x-y \in D} |x\rangle \langle y| \end{aligned}$$

Algorithme de Simon

Étape 4 :

$$
\begin{aligned}
\rho_4 &= H^{\otimes n}\rho_3(H^{\dagger})^{\otimes n} \\
&= \frac{1}{2^n}\sum_{x-y\in D} H^{\otimes n}\left|x\right\rangle\left\langle y\right|H^{\otimes n} \\
&= \frac{1}{2^{2n}}\sum_{x-y\in D}\sum_{a,b\in G}(-1)^{ax+by}\left|a\right\rangle\left\langle b\right| \\
&= \frac{1}{2^{2n}}\sum_{a,b\in G}\sum_{x-y\in D}(-1)^{ax+by}\left|a\right\rangle\left\langle b\right|
\end{aligned}
$$

Algorithme de Simon

On analyse le coefficient

$$c(a,b) = \sum_{x-y \in D} (-1)^{ax+by}$$

cas 1 : $a = b \in D^{\perp}$
$c(a,b) = \sum_{x-y \in D} (-1)^{a(x-y)} = |G| \cdot |D|$.

Algorithme de Simon

cas 2 : $a = b \in D \setminus D^{\perp}$
Soit $d_0 \in D, a \cdot d_0 = 1$.

$$\begin{aligned} c(a,b) &= \sum_{x \in G, d \in D} (-1)^{ad} \\ &= \sum_{x \in G, d \in D \cap a^{\perp}} (-1)^{a(d_0+d)} + \sum_{x \in G, d \in D \cap a^{\perp}} (-1)^{ad} \\ &= (-1)^{ad_0} \sum_{x \in G, d \in D \cap a^{\perp}} (-1)^{ad} + \sum_{x \in G, d \in D \cap a^{\perp}} (-1)^{ad} \\ &= 0. \end{aligned}$$

Algorithme de Simon

cas 3 : $a \neq b$
Soit $x_0 \in G \setminus (a+b)^{\perp}$.

$$
\begin{aligned}
c(a,b) &= \sum_{x\in G, d\in D} (-1)^{ax+b(x+d)} = \sum_{x\in G, d\in D} (-1)^{ax+bx}(-1)^{bd} \\
&= \sum_{x\in G}(-1)^{(a+b)x} \sum_{d\in D}(-1)^{bd} \\
&= \Big(\sum_{x\in x_0+(a+b)^{\perp}} (-1)^{(a+b)x} + \sum_{x\in (a+b)^{\perp}} (-1)^{(a+b)x} \Big) \sum_{d\in D}(-1)^{bd} \\
&= \Big((-1)^{(a+b)x_0} \sum_{x\in (a+b)^{\perp}} (-1)^{(a+b)x} + \sum_{x\in (a+b)^{\perp}} (-1)^{(a+b)x} \Big) \sum_{d\in D}(\\
&= 0.
\end{aligned}
$$

Algorithme de Simon

Finalement :

$$\begin{aligned}\rho_4 &= \frac{1}{2^{2n}} \sum_{a=b\in D^\perp} |G| \cdot |D| \, |a\rangle \langle b| \\ &= \frac{|D|}{|G|} \sum_{a\in D^\perp} |a\rangle \langle a|\end{aligned}$$

ρ_4 est la loi uniforme sur $D^\perp$.

Algorithme de Simon

La fin est un algorithme probabiliste (classique) :
On tire aléatoirement ℓ vecteurs $x_1, x_2, \ldots, x_\ell$ de $D^\perp$ selon la loi de ρ_4 :

$$\Pr(\langle x_1, x_2, \ldots, x_\ell \rangle = D^\perp) \geq 1 - \frac{|D^\perp|}{2^\ell}.$$

La décohérence via les états mixtes

La décohérence

Soit

$$\rho = \sum_{a \in \mathbb{B}^n, b \in \mathbb{B}^n} \rho_{a,b} \left|a\right\rangle \left\langle b\right|$$

un opérateur de densité.
On se demande par quel processus il peut se transformer en

$$\rho' = \sum_{a \in \mathbb{B}^n} \rho_{a,a} \left|a\right\rangle \left\langle a\right|$$

qui représente la loi de probabilité $(\rho_{a,a}, \{\left|a\right\rangle) \mid a \in \mathbb{B}^n\}$.

La décohérence

Une copie dans la base canonique, suivie d'une trace partielle, a cet effet.
Soit $U : (\mathcal{B}^{\otimes n} \otimes \mathcal{B}^{\otimes n}) \to (\mathcal{B}^{\otimes n} \otimes \mathcal{B}^{\otimes n})$:

$$U |x\rangle |y\rangle := |x\rangle |x \oplus y\rangle.$$

$$\begin{aligned}
\rho_1 &= \rho \otimes |0^n\rangle \langle 0^n| \\
\rho_2 &= U \rho_1 U^* \\
&= \sum_{a \in \mathbb{B}^n, b \in \mathbb{B}^n} \rho_{a,b} (U |a\rangle |0^n\rangle)(\langle b| \langle 0^n| U^*) \\
&= \sum_{a \in \mathbb{B}^n, b \in \mathbb{B}^n} \rho_{a,b} (|a\rangle |a\rangle)(\langle b| \langle b|)
\end{aligned}$$

La décohérence

$$\begin{aligned}
\rho_3 &= \mathrm{Tr}_2(\rho_2) \\
&= \sum_{a\in\mathbb{B}^n, b\in\mathbb{B}^n} \rho_{a,b}(|a\rangle\langle b|)\cdot \mathrm{Tr}(|a\rangle\langle b|) \\
&= \sum_{a\in\mathbb{B}^n} \rho_{a,a}(|a\rangle\langle a|) \\
&= \rho'.
\end{aligned}$$