Méthodes mathématiques de la théorie quantique - 2022

Bases de l'Information quantique - Day 1

Nana Engo
serge.nana-engo@facsciences-uy1.cm

Department of Physics
Faculty of Science
University of Yaounde I

https://github.com/NanaEngo/Memaquan2022

Bénin, 11-15 Juillet 2022

Sommaire - Day 1 - 11 Juillet 2022

Definition (Information quantique)

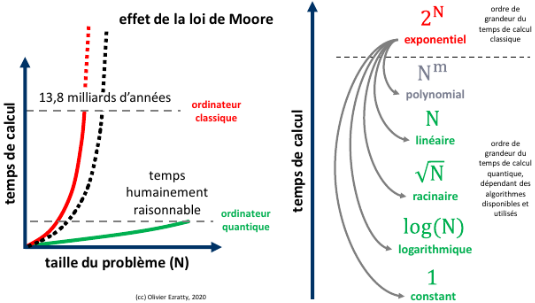
- La théorie de l'information quantique, ou simplement l'information quantique, est un développement de la théorie de l'information de Claude Shannon exploitant les propriétés de la théorie quantique, comme
  - le principe de superposition
  - l'intrication quantique
  - le non-clonage quantique
- L'unité utilisée pour quantifier l'information quantique est le qubit ou quantum bit, par analogie avec le bit d'information classique

Les principales sous-branches de l'information quantique sont

- L'informatique ou le calcul quantique
- La cryptographie quantique
- Les codes correcteurs quantiques
- Les communications quantiques

- L'informatique quantique sert à dépasser les limites des processeurs traditionnels pour des applications spécifiques
  - d'optimisation, de simulation
  - de prédiction
  - de cryptographie

  dont la complexité croit de manière exponentielle avec la taille du problème



Atouts information quantique

Problèmes d'optimisation - véhicules autonomes

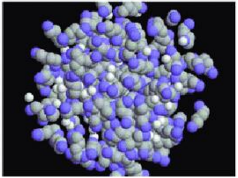
- Lorsque la combinatoire à optimiser est très grande, les algorithmes classiques trouvent leurs limites sur les calculateurs (ordinateurs) traditionnels
- Cela se complique avec l'optimisation du trafic de parcs de véhicules autonomes de villes intelligentes du futur
  - Flotte intégralement autonome $\Rightarrow$ il faut théoriquement optimiser le trajet individuel de chaque véhicule en f(départ,destination)
  - Algorithmes classiques $\equiv$ fonctionner avec $\sim$ 100 véhicules et trajets, mais au-délà, les capacités de calcul traditionnelles seraient largement saturées. La quantique arriverait alors à la rescousse !

Atouts information quantique

Simulation du fonctionnement de la matière au niveau nanoscopique

- La matière est régie par les règles de la théorie quantique qui dépendent d'équations connues
  - mais dont la résolution est un problème d'optimisation complexe à résoudre
  - passant par la recherche d'un minimum énergétique

  $\Rightarrow$ comprendre l'interaction de nombreux atomes dans des molécules ou des structures cristallines complexes
- Cela concerne les simulations chimiques et moléculaires (matériaux et biologique) : $100 - 10^4$ atomes, $10^5 - 10^8$ configurations

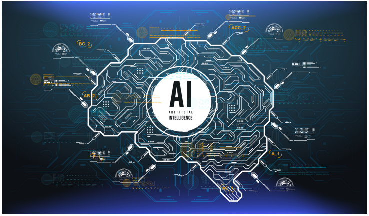


- L'informatique quantique pourrait servir à simuler la quantique du monde réel dans l'infiniment petit

Atouts information quantique

Entraînement de modèles de machine learning et des réseaux de neurones

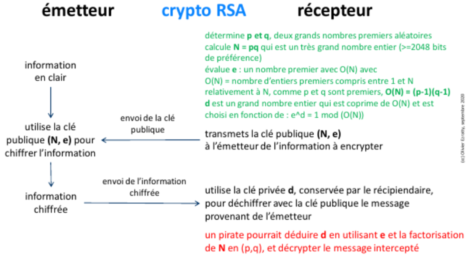
- Il est à la portée des ordinateurs classiques, équipés
  - de GPU (Graphics Processing Unit)
  - de processeurs neuromorphiques qui mettent en œuvre dans le silicium des portes logiques dont l'organisation est très proche de la logique des réseaux de neurones
- Cependant, la puissance de calcul disponible rend difficile l'entraînement des réseaux de grande taille
  - Par exemple, les réseaux convolutifs de reconnaissance d'images ont une résolution d'image en entrée généralement limitée à 227×227 pixels



Atouts information quantique

Factorisation de nombres entiers

- La factorisation de nombres entiers intéresse les services de renseignement pour casser les codes de sécurité sur Internet de type RSA qui reposent sur l'envoi de clés publiques

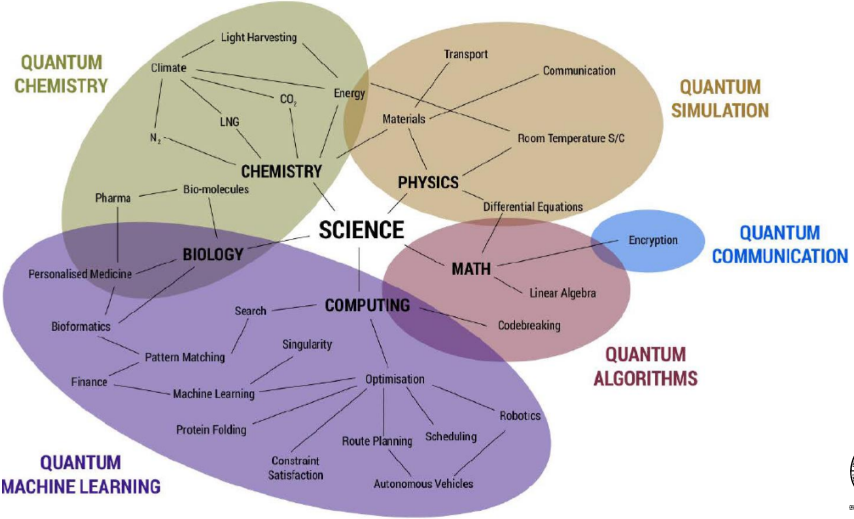


- L'algorithme quantique de Shor pourrait mettre à mal les systèmes de cryptographiques courants qui reposent sur la notion de clé publique
  - Il devrait permettre de factoriser dans un temps raisonnable des nombres entiers, proportionnel à leur logarithme
  - C'est donc une factorisation en un temps linéaire en fonction du nombre de bits de la clé

- Les algorithmes quantiques existant sont dans l'ensemble de bien bas niveau. Il reste à les assembler dans des solutions métiers, marché par marché
- Le secteur du calcul quantique est encore des plus immatures puisque les calculateurs quantiques sont encore très limités
- Il est donc difficile de prédire à quelle vitesse les applications quantiques émergeront marché par marché
- Cependant, il existe, depuis 2018, un inventaire des applications de l'informatique quantique classifiées par secteurs d'activités
- Il existe déjà un marché des outils de modélisation et de développement des solutions quantiques
    - Ces outils sont déjà bien nombreux et vont continuer de gagner en maturation et s'adapter aux évolutions du matériel
    - Des bibliothèques adaptées aux besoins de marchés spécifiques feront sans doute leur apparition comme dans la simulation moléculaire ou la finance

Applications métiers I

Inventaire par secteurs d'activité



Applications métiers II

Inventaire par secteurs d'activité

INDUSTRIES	SELECTION OF USE-CASES	ENTERPRISES (EXAMPLES)	
High-tech	• Machine learning and artificial intelligence, such as neural networks • Search • Bidding strategies for advertisements • Cybersecurity • Online and product marketing • Software verification and validation	IBM Alibaba Google Microsoft	Telstra Baidu Samsung
Industrial goods	• Logistics: scheduling, planning, product distribution, routing • Automotive: traffic simulation, e-charging station and parking search, autonomous driving • Semiconductors: manufacturing, such as chip layout optimization • Aerospace: R&D and manufacturing, such as fault-analysis, stronger polymers for airplanes • Material science: effective catalytic converters for cars, battery cell research, more-efficient materials for solar cells, and property engineering uses such as OLEDS	Airbus NASA Northrop Grumman Daimler Raytheon	BMW Volkswagen Lockheed Martin Honeywell Bosch

Applications métiers III

Inventaire par secteurs d'activité

INDUSTRIES	SELECTION OF USE-CASES	ENTERPRISES (EXAMPLES)	
Chemistry and Pharma	• Catalyst and enzyme design, such as nitrogenase • Pharmaceuticals R&D, such as faster drug discovery • Bioinformatics, such as genomics • Patient diagnostics for health care, such as improved diagnostic capability for MRI	BASF Biogen Dow Chemical	JSR DuPont Amgen
Finance	• Trading strategies • Portfolio optimization • Asset pricing • Risk analysis • Fraud detection • Market simulation	J.P. Morgan Commonwealth Bank	Barclays Goldman Sachs
Energy	• Network design • Energy distribution • Oil well optimization	Dubai Electricity & Water Authority	BP

Quantum Computing as a service - QCaaS

- Jusqu'à un passé très récent, l'informatique quantique était réservée aux labos de Recherche et Developpement (R&D) et aux centres universitaires
  - Les contraintes techniques pour assurer la stabilité des qubits sont particulièrement draconiennes
  - Isolé du monde extérieur, le calculateur doit être protégé des interférences magnétiques et refroidi à des températures proches du zéro absolu ($-273.15\,^{\circ}\mathrm{C}$)
- Des considérations techniques qui n'ont pas fait reculer les géants du numérique qui ont conçu des services de calcul quantique managés en mode cloud
  - IBM a été le premier, en 2016, à proposer une offre de Quantum Computing as a service (QCaaS)
  - Il est suivi en 2018 par Alibaba Cloud
  - Et en 2019, par Microsoft Azure et Amazon Web Services (AWS)

Comparatif des services cloud d'informatique quantique

	IBM Quantum Experience	Microsoft Azure Quantum	AWS Braket	Alibaba Cloud
Année Start	2016	2019	2019	2018
Calculateurs	Calculateurs quantiques en propre	Honeywell, IonQ, QCI	IonQ, Rigetti, D-Wave	Calculateurs quantiques en propre
SDK	Qiskit	Quantum Development Kit	SDK Amazon Braket	Alibaba Cloud Quantum Development Platform
Langages supportés	OpenQASM, Python	Q#, Python, C++, C	Python	Python
Partenaires académiques	Université de Princeton, The Coding School	Membre des réseaux Quantum Science Center (QSC) et Q-NEXT, Pacific Northwest National Laboratory	California Institute of Technology, universités de Stanford, du MIT et de Chicago	Académie chinoise des sciences

Definition (Produit tensoriel de deux espaces de Hilbert)

- L'espace d'états $\mathcal{H}$ est appelé **produit tensoriel** de $\mathcal{H}_A$ et $\mathcal{H}_B$, et noté $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, si

$$\boxed{\begin{aligned} &\mathcal{H}_A \times \mathcal{H}_B \mapsto \mathcal{H} \\ &(|\psi_A\rangle, |\psi_B\rangle) \mapsto |\psi_A\rangle \otimes |\psi_B\rangle = |\psi_A\rangle|\psi_B\rangle = |\psi_A\psi_B\rangle \end{aligned}} \tag{1}$$

- $|\psi_A\rangle \otimes |\psi_B\rangle$, le produit tensoriel de $|\psi_A\rangle$ et $|\psi_B\rangle$ (outer product en anglais), est linéaire par rapport à la multiplication (2a), et distributive par rapport à l'addition vectorielle (2b)

$$[|\psi_A\rangle + \lambda|\psi'_A\rangle] \otimes |\psi_B\rangle = |\psi_A\rangle \otimes |\psi_B\rangle + \lambda|\psi'_A\rangle \otimes |\psi_B\rangle \tag{2a}$$
$$|\psi_A\rangle \otimes [|\psi_B\rangle + \lambda|\psi'_B\rangle] = |\psi_A\rangle \otimes |\psi_B\rangle + \lambda|\psi_A\rangle \otimes |\psi'_B\rangle \tag{2b}$$

Produit tensoriel de deux états II

Definition (Produit scalaire dans un espace produit tensoriel)

Le **produit scalaire** sur $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ se définit de la manière suivante

$$\boxed{\langle \psi'_B \psi'_A | \psi_A \psi_B \rangle = \langle \psi'_A | \psi_A \rangle \langle \psi'_B | \psi_B \rangle} \tag{3}$$

Si $\{|n\rangle\}$ et $\{|m\rangle\}$ sont les bases orthonormées de $\mathcal{H}_A$ et $\mathcal{H}_B$ telles que

$$|\psi_A\rangle = \sum_{n=1}^{N} \alpha_n |n\rangle \qquad |\psi_B\rangle = \sum_{m=1}^{M} \alpha_m |m\rangle \tag{4}$$

alors

$$\boxed{|\psi_A \psi_B\rangle = \sum_{n,m} \alpha_n \alpha_m |nm\rangle \qquad \text{avec} \qquad \langle m' n' | nm \rangle = \delta_{n'n} \delta_{m'm}} \tag{5}$$

Produit tensoriel de deux états III

Exemple 4.1 – Produit tensoriel de deux états

On considère dans la base $\{|0\rangle, |1\rangle\}$ $|\psi_A\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\binom{1}{-1}$ *et* $|\psi_B\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\binom{1}{1}$. *Dans la base* $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ *le produit tensoriel* $|\psi_A\rangle \otimes |\psi_B\rangle$ *s'écrit :*

- sous forme matricielle

$$|\psi_A\rangle \otimes |\psi_B\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1.|\psi_B\rangle \\ -1.|\psi_B\rangle \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix} \tag{6}$$

- sous forme vectorielle

$$\begin{aligned} |\psi_A\rangle \otimes |\psi_B\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle) \end{aligned} \tag{7}$$

Definition (Produit tensoriel de deux opérateurs)

Soient $\mathtt{A}$ et $\mathtt{B}$ deux opérateurs agissant respectivement dans $\mathcal{H}_A$ et $\mathcal{H}_B$. Un opérateur $\mathtt{A} \otimes \mathtt{B}$ agissant dans $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ est tel que

$$\boxed{(\mathtt{A} \otimes \mathtt{B})|\psi_A \psi_B\rangle = \mathtt{A}|\psi_A\rangle \otimes \mathtt{B}|\psi_B\rangle} \tag{8}$$

Si $\mathtt{A}$ et $\mathtt{B}$ sont hermitiens, alors $\mathtt{A} \otimes \mathtt{B}$ est un opérateur hermitien

- Une classe simple des opérateurs de $\mathcal{H}$ est

$$\mathtt{A} \otimes \mathbb{I}_B \text{ et } \mathbb{I}_A \otimes \mathtt{B} \tag{9}$$

- Comme

$$(\mathtt{A} \otimes \mathtt{B}) \cdot (\mathtt{C} \otimes \mathtt{D}) = (\mathtt{AC}) \otimes (\mathtt{BD}) \tag{10}$$

$$[\mathtt{A} \otimes \mathbb{I}_B, \mathbb{I}_A \otimes \mathtt{B}] = (\mathtt{A} \otimes \mathbb{I}_B) \cdot (\mathbb{I}_A \otimes \mathtt{B}) - (\mathbb{I}_A \otimes \mathtt{B}) \cdot (\mathtt{A} \otimes \mathbb{I}_B) = 0 \tag{11}$$

Produit tensoriel des opérateurs II

- Si $\mathtt{A}|\psi_A\rangle = a|\psi_A\rangle$, alors $|\psi_A \otimes \psi_B\rangle$ est aussi vecteur propre de $\mathtt{A} \otimes \mathbb{I}_B$ avec la valeur propre a :

$$\mathtt{A} \otimes \mathbb{I}_B|\psi_A \otimes \psi_B\rangle = a|\psi_A\rangle \otimes \psi_B \tag{12}$$

- On omet très souvent d'écrire explicitement les opérateurs identités $\mathbb{I}_A$ et $\mathbb{I}_B$ pour écrire simplement

$$\mathtt{A}|\psi_A \otimes \psi_B\rangle = a|\psi_A \otimes \psi_B\rangle \qquad \text{ou} \qquad \mathtt{A}|\psi_A\psi_B\rangle = a|\psi_A\psi_B\rangle \tag{13}$$

en supprimant le produit tensoriel

Produit tensoriel des opérateurs III

Exemple 4.2 – Produit tensoriel des opérateurs

1. *La matrice représentant le produit tensoriel des matrices de Pauli* $\mathtt{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ *et* $\mathtt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ *est*

$$\mathtt{X} \otimes \mathtt{Z} = \begin{pmatrix} 0.\mathtt{Z} & 1.\mathtt{Z} \\ 1.\mathtt{Z} & 0.\mathtt{Z} \end{pmatrix} = \begin{pmatrix} \mathbb{O} & \mathtt{Z} \\ \mathtt{Z} & \mathbb{O} \end{pmatrix} = \left(\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ \hline 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{array}\right) \tag{14}$$

2. *Évaluer* $\mathtt{Z} \otimes \mathtt{X}$ *et conclure*

Exemple 4.3 – Probability of finding a 2-qubit and a 1-qubit

A system is in the state

$$|\psi\rangle = \frac{1}{\sqrt{8}}|00\rangle + \sqrt{\frac{3}{8}}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \tag{15}$$

1. *What is the probability that measurement finds the system in the state $|\phi\rangle = |01\rangle$?*
2. *What is the probability that measurement finds the first qubit in the state $|0\rangle$? What is the state of the system after measurement ?*

1. Given that the system is in the state $|\psi\rangle$, the probability of finding it in the state $|\phi\rangle = |01\rangle$ is calculated using the Born

rule, that is $\mathcal{P} = |\langle\phi|\psi\rangle|^2$. Since $\langle 0|1\rangle = \langle 1|0\rangle = 0$, we have

$$\begin{aligned}\langle\phi|\psi\rangle &= \langle 10|\left(\frac{1}{\sqrt{8}}|00\rangle + \sqrt{\frac{3}{8}}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\right) \\ &= \sqrt{\frac{3}{8}}\langle 0|0\rangle\langle 1|1\rangle = \sqrt{\frac{3}{8}}\end{aligned} \tag{16}$$

Therefore the probability is

$$\mathcal{P} = |\langle\phi|\psi\rangle|^2 = \frac{3}{8} \tag{17}$$

2. To find the probability that measurement finds the first qubit in the state $|0\rangle$, we can apply $P_0 \otimes \mathbb{I} = |0\rangle\langle 0| \otimes \mathbb{I}$ to the state. So the projection operator P_0 is applied to the first qubit and the identity operator to the second qubit, leaving the second qubit unchanged

Then,

$$P_0 \otimes \mathbb{I}|\psi\rangle = |0\rangle\langle 0| \otimes \mathbb{I}\left(\frac{1}{\sqrt{8}}|00\rangle + \sqrt{\frac{3}{8}}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\right)$$

$$= \frac{1}{\sqrt{8}}|0\rangle\langle 0|0\rangle \otimes |0\rangle + \sqrt{\frac{3}{8}}|0\rangle\langle 0|0\rangle \otimes |1\rangle = \frac{1}{\sqrt{8}}|00\rangle + \sqrt{\frac{3}{8}}|01\rangle$$

The probability of obtaining this result (Born's rule) is

$$\mathcal{P} = \langle\psi|P_0 \otimes \mathbb{I}|\psi\rangle = \left(\frac{1}{\sqrt{8}}\langle 00| + \sqrt{\frac{3}{8}}\langle 01| + \frac{1}{2}\langle 10| + \frac{1}{2}\langle 11|\right)\left(\frac{1}{\sqrt{8}}|00\rangle + \sqrt{\frac{3}{8}}|01\rangle$$

$$= \frac{1}{8} + \frac{3}{8} = \frac{1}{2}$$

According to the postulate 5, the state of the system after measurement is found to be

$$\frac{\frac{1}{\sqrt{8}}|00\rangle + \sqrt{\frac{3}{8}}|01\rangle}{\sqrt{\langle\psi|P_0 \otimes \mathbb{I}|\psi\rangle}} = \sqrt{2}\left(\frac{1}{\sqrt{8}}|00\rangle + \sqrt{\frac{3}{8}}|01\rangle\right) = \frac{1}{2}|00\rangle + \frac{\sqrt{3}}{2}|01\rangle$$

États Intriqués - États de Bell I

États intriqués (*entangled states* en anglais)

- **Un état intriqué ou corrélé est un état <u>non factorisable</u> !**
- Lorsqu'un système est dans un état intriqué, les propriétés du système global sont définies, mais pas celles de chacun des sous-systèmes.

- Parmi les états intriqués les plus populaires, on a les 4 états de Bell

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |B_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{18a}$$

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |B_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{18b}$$

- Sous une forme compact,

$$\boxed{|B_{xy}\rangle = \frac{1}{\sqrt{2}}(|0y\rangle + (-1)^x|1(1-y)\rangle), \qquad x, y \in \{0, 1\}} \tag{19}$$

États Intriqués - États de Bell II

- On montre facilement que

$$\mathtt{Z}\otimes\mathtt{Z}|B_{xy}\rangle = (-1)^y|B_{xy}\rangle \quad \mathtt{X}\otimes\mathtt{X}|B_{xy}\rangle = (-1)^x|B_{xy}\rangle \quad \mathtt{Y}\otimes\mathtt{Y}|B_{xy}\rangle = (-1)^{x+y}|B_{xy}\rangle \tag{20}$$

  - Par exemple, comme

$$\mathtt{Z}|y\rangle = (-1)^y|y\rangle \text{ et } \mathtt{Z}|1-y\rangle = (-1)^{1-y}|1-y\rangle \tag{21}$$

  on a

$$\begin{aligned}\mathtt{Z}\otimes\mathtt{Z}|B_{xy}\rangle &= \frac{1}{\sqrt{2}}[\mathtt{Z}|0\rangle\otimes\mathtt{Z}|y\rangle + (-1)^x\mathtt{Z}|1\rangle\otimes\mathtt{Z}|1-y\rangle] \\ &= \frac{1}{\sqrt{2}}[(-1)^y|0y\rangle + (-1)^x(-1)(-1)^{1-y}|1(1-y)\rangle \\ &= (-1)^y\frac{1}{\sqrt{2}}[|0y\rangle + (-1)^x|1(1-y)\rangle = (-1)^y|B_{xy}\rangle\end{aligned} \tag{22}$$

États Intriqués - États de Bell III

- Soient deux qubits de $\mathcal{H}_A$ et $\mathcal{H}_B$,

$$|\varphi_A\rangle = a_0|0_A\rangle + a_1|1_A\rangle, \qquad |a_0|^2 + |a_1|^2 = 1 \tag{23a}$$

$$|\varphi_B\rangle = b_0|0_B\rangle + b_1|1_B\rangle, \qquad |b_0|^2 + |b_1|^2 = 1 \tag{23b}$$

$$|\varphi_A\varphi_B\rangle = a_0 b_0|0_A 0_B\rangle + a_0 b_1|0_A 1_B\rangle + a_1 b_0|1_A 0_B\rangle + a_1 b_1|1_A 1_B\rangle \tag{24}$$

  - Un vecteur arbitraire $|\Psi\rangle$ de $\mathcal{H}$ est

$$|\Psi\rangle = \alpha|0_A 0_B\rangle + \beta|0_A 1_B\rangle + \gamma|1_A 0_B\rangle + \delta|1_A 1_B\rangle \tag{25}$$

n'est en général pas de la forme (24) !. On dit qu'il est dans un état intriqué

États Intriqués - États de Bell IV

- Pour que $|\Psi\rangle$ soit de la forme $|\varphi_A \varphi_B\rangle$ (produit tensoriel), une condition nécessaire et suffisante est que

$$\alpha = a_0 b_0, \quad \beta = a_0 b_1, \quad \gamma = a_1 b_0, \quad \delta = a_1 b_1 \quad \Rightarrow \boxed{\alpha\delta = \beta\gamma} \tag{26}$$

ce qui *à priori* n'a aucune raison d'être valide.

L'état de Bell

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|0_A 1_B\rangle + |1_A 0_B\rangle) \tag{27}$$

est manifestement intriqué puisque

$$\alpha = 0, \qquad \beta = \gamma = \frac{1}{\sqrt{2}}, \qquad \delta = 0 \qquad \Rightarrow \alpha\delta \neq \beta\gamma \tag{28}$$