8. Mesure de l'intrication: entropies de Shannon et von Neumann

Préparation de n paires de qubits, chacune dans l'état: $|\Psi_{AB}> = \sqrt{\lambda_1}\,|\,1\,0> + \sqrt{\lambda_2}\,|\,0\,1>$. Le 1er bit de chaque paire «localisé» en A, le second en B.

Pour un cas pur (λ_1 ou $\lambda_2 = 0$), les mesures en A ou B dans la base (0,1) effectuées sur ces paires donnent une suite de résultats identiques (0,0,0,0,0…..ou 1,1,1,1…). →
On peut coder toute l'information «locale» en A ou B en remplaçant les n qubits par un seul.

Pour un état intriqué à poids égaux ($\lambda_1 = \lambda_2 = 1/2$) , les suites des mesures effectuées en A ou B dans la base (0,1) sont aléatoires avec des probabilités égales de trouver 0 ou 1. →
l 'information contenue dans ces suites ne peut pas être comprimée (n bits nécessaires). Par contre, l 'information contenue dans la somme des résultats des mesures en A et B est réductible à un seul bit: toute l'information est dans les corrélations « non-locales » entre bits.

Dans une situation intermédiaire ($\lambda_1 \neq \lambda_2$), les suites de mesures en A et B sont aléatoires avec des probabilités des bits 0 et 1 différentes. On peut alors (théorème de Shannon) comprimer l 'information en codant les 2^n « mots» de n «lettres» par $2^{nH(\lambda)}$ «mots codes» avec:

$$H(\lambda) = - < \log_2 \lambda > = -\Sigma_{i=1,2}(\lambda_i \log_2 \lambda_i) \quad \text{(H: Entropie de Shannon)}$$

H(λ) apparaît comme une «mesure» de l'intrication des deux qubits: vaut 1 (maximum) lorsque les poids de la décomposition de Schmidt sont égaux (pas de compression d'information «locale» possible) et 0 dans le cas où il n'y a pas d'intrication (compression totale de l'information locale).

Théorème de Shannon appliqué aux suites de bits 0,1

Considérons l'ensemble des suites de n bits prenant la valeur 1 avec la probabilité p et la valeur 0 avec la probabilité 1-p:

La loi des grands nombres dit que l'immense majorité de ces suites contient ~ np bits de valeur 1 et ~ n(1−p) bits de valeur 0, avec une fluctuation de ± √(np(1−p)) autour de ces valeurs. On appelle suites « typiques » les suites satisfaisant la condition précédente, suites «atypiques» les autres. Lorsque $n \to +\infty$, la probabilité d'une suite atypique tend vers zéro.

Le nombre A(n,p) de suites typiques est estimé en calculant le nombre de permutations de bits qui échangent les suites contenant exactement np bits égaux à 1 et en multipliant ce nombre par √(np(1-p)) pour tenir compte des fluctuations typiques:

$$A(n,p) \sim \frac{n!}{(np)!\left[n(1-p)\right]!} \times \sqrt{np(1-p)}$$

La formule de Stirling donne immédiatement:

$$\text{Limite}_{n\to\infty}\ (1/n)\log_2 A(n,p) = -p\log_2(p) - (1-p)\log_2(1-p) = H(p) \longrightarrow \boxed{A(n,p) \sim 2^{n\,H\,p)}}$$

On décide de coder les suites typiques et de laisser non codées les atypiques, avec une probabilité de non codage qui tend vers 0 lorsque $n \to +\infty$. On peut donc représenter toutes les suites typiques à l'aide de suites réduites de nH(p) bits. Cela équivaut à dire que chaque bit des suites typiques peut être comprimé en H(p) bits avec $H \leq 1$. L'analyse se généralise à des alphabets à plus de deux lettres (probabilités $\{p_i\} \to H(\{p_i\}) = -\Sigma_i\, p_i \log_2 p_i$).

Intrication et entropie de von Neumann

nH(p) est le logarithme du nombre de configurations les plus probables des suites de résultats des mesures sur n qubits. nH(p) décrit notre «ignorance» a priori d'une suite (avant la mesure). Notion semblable à la définition habituelle de l'entropie d'un système, égale au logarithme du nombre de configurations microscopiques correspondant à une configuration macroscopique.

Von Neumann a étendu la notion d'entropie à la physique quantique en définissant l'entropie d'un mélange statistique décrit par l'opérateur densité ρ:

$$S(\rho) = -\langle \log_2 \rho \rangle = -\, T_r\,(\rho \ \log_2 \rho) = -\ \Sigma_i\, p_i \log_2 p_i$$

Les p_i sont les valeurs propres de l'opérateur densité (probabilités de trouver le système dans l 'un des états orthogonaux d' une base où ρ est diagonal).

$\log_2$ choisis par convention informatique. L'usage physique (ln base e) multiplie S par ln(2).

L' entropie de von Neumann dans quelques cas particuliers importants:

1. L 'entropie d'un système dans un état pur est nulle.

2. L 'entropie d'un mélange statistique est maximum lorsque ρ a toutes ses valeurs propres non nulles égales. Elle vaut alors $\log_2 N$, où N est la dimension de l'espace des états de ρ de valeurs propres $\neq$ 0. Dans ce cas, l'ignorance a priori des résultats des mesures est maximum.

3. L' entropie d'un système A-B non corrélé est la somme des entropies de A et B:

$$\rho_{AB} = \rho_A \otimes \rho_B \ \rightarrow S(\rho_{AB}) = S(\rho_A) + S(\rho_B)$$

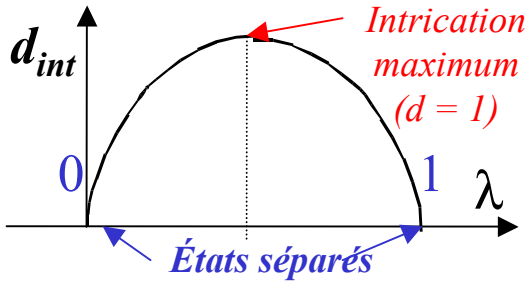
Interprétation de l'entropie comme mesure d'intrication

Définition: *Degré d 'intrication d'un système A-B dans l 'état* $|\Psi>_{AB}$:

$$d_{int} = S(\rho_A) = S(\rho_B) \quad \text{où } \rho_{A(B)} = Tr_{B(A)} (|\Psi>_{AB\ AB}<\Psi|)$$

$d_{int} = 0 \longleftrightarrow$ *A-B séparable*; $d_{int} = log\ (N_{schmidt}) \longleftrightarrow$ *intrication A-B maximale*

Le degré d 'intrication d_{int} ***d 'un système A-B apparaît comme la mesure de l 'augmentation de notre ignorance lorsque nous perdons la possibilité de faire des mesures sur le système dans son ensemble et que nous n 'avons accès localement qu' à l'un des deux sous-systèmes.***
Alors que l 'on peut prévoir à coup sûr la valeur des observables non locales dont $|\Psi>_{AB}$ ***est un état propre, on a une ignorance «partielle» de la valeur prise par toutes les observables locales associées à A ou B seul. Lorsque l'intrication est maximale, cette ignorance devient aussi maximale. On peut voir également*** d_{int} ***comme le nombre moyen de bits nécessaires pour transmettre le résultat d'une mesure sur un des sous-systèmes intriqués.***



Cas de deux qubits intriqués (coefficients de Schmidt $\sqrt{\lambda}$ *et* $\sqrt{1-\lambda}$*)*

$$\rightarrow S(\lambda) = -\lambda \log_2 \lambda - (1-\lambda) \log_2 (1-\lambda)$$

Sub-additivité de l'entropie

Pour un système bi-partite, dans le cas général (qu 'il soit dans un cas pur ou un mélange statistique d 'états):

$$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$$

Il y a plus d'information (moins d'ignorance) dans une paire corrélée que dans la somme de ses parties (égalité si A et B ne sont pas corrélés: $\rho_{AB} = \rho_A \otimes \rho_B$).

<u>Démonstration:</u>

Il suffit de montrer l'inégalité pour l'entropie définie en logarithmes néperiens (ln):

On a immédiatement: $S'(\rho_A) + S'(\rho_B) = -Tr\,[\rho_{AB}\ (\ln\rho_A + \ln\rho_B)] = -Tr\,\rho_{AB} \ln\ \rho_A \otimes \rho_B$

et: $S'(\rho_A) + S'(\rho_B) - S'(\rho_{AB}) = Tr\ \rho_{AB}[\ \ln\ \rho_{AB} - \ln\ \rho_A \otimes \rho_B]$

Introduisons les états propres et valeurs propres $\{|m>, p_m\}$ ***et*** $\{|\mu>, q_\mu\}$ ***de*** ρ_{AB} ***et*** $\rho_A \otimes \rho_B$ ***respectivement (avec*** $\Sigma_m\, p_m = \Sigma_\mu q_\mu = 1$***) . On a alors:***

$$S'(\rho_A) + S'(\rho_B) - S'(\rho_{AB}) = \Sigma_m\, p_m\,[\ \ln\, p_m - \langle m\,|\ln\ \rho_A \otimes \rho_B\,|m\rangle]$$

$$= \Sigma_{m,\mu}\, p_m\, |\langle m|\mu\rangle|^2\, \ln\ (p_m/q_\mu)$$

et puisque $\ln x \geq 1 - 1/x\ \ (\forall x)$***:***

$$S'(\rho_A) + S'(\rho_B) - S'(\rho_{AB}) \geq 1 - \Sigma_{m,\mu} |\langle m|\mu\rangle|^2 q_\mu = 0\ ,\ CQFD.$$

Sub-additivité de l 'entropie et intrication

Quand deux systèmes initialement non-corrélés interagissent, on a:

$$\rho_A(0) \otimes \rho_B(0) \rightarrow \rho_{AB}(t) = U(t,0)\ \rho_A(0) \otimes \rho_B(0)\ U^{\dagger}(t,0)$$

$$\text{avec}\ \ S(\rho_{AB}(t)) = S(\rho_A(0) \otimes \rho_B(0)) = S(\rho_A(0)) + S(\rho_B(0))$$

(L'évolution unitaire ne change pas le spectre de ρ_{AB}).

Le théorème de sub-additivité entraîne alors:

$$S(\rho_A(t)) + S(\rho_B(t)) \geq S(\rho_A(0)) + S(\rho_B(0))$$

La somme des entropies des deux parties A et B ne peut qu'augmenter (une forme du second principe de la thermodynamique!) $\rightarrow$

Pour un système bipartite A-B dans un état pur initialement séparé, puis intriqué par interaction A- B, on a $S(\rho_{AB}(0)) = S(\rho_A(0)) = S(\rho_B(0)) = 0$ et $d_{int}(t) = S(\rho_A(t)) = S(\rho_B(t)) > 0$. L'apparition d'une intrication non nulle entre A et B présente ainsi une certaine similtude avec le second principe. Elle correspond à une perte d'information «locale». L 'information se retrouve dans les corrélations entre A et B.

Variation du degré d' intrication d'une paire A-B dans un état pur sous l' effet d'opérations locales (sur A ou B seul).

1. Le degré d'intrication n'est pas modifié par une transformation unitaire U_A de A (ou B) seul:
$\rho_A = \Sigma_i p_i \, |\phi_i><\phi_i| \rightarrow \rho'_A = U_A \rho_A U^{\dagger}_A = \Sigma_i \; p_i \, |\psi_i><\psi_i|$ *avec* $|\psi_i> = U_A |\phi_i>$

U_A transforme l 'ensemble orthonormé $\{|\phi_i>\}$ en un autre, $\{|\psi_i>\}$, sans changer le spectre $\{p_i\}$ de ρ_A. L 'entropie partielle $S(\rho'_A) = S(\rho_A)$ reste inchangée.

2. L 'intrication est détruite par une <u>mesure</u> d'une observable quelconque de A dont le résultat est une valeur propre non dégénérée (mesure projective sur l'état propre $|\phi_a>$):
$\rho_A \rightarrow |\phi_a><\phi_a|$ et $S(|\phi_a><\phi_a|) = 0$. A est devenu un cas pur et l'intrication A-B a disparu $\rightarrow$ Dans le cas où A et B sont deux qubits, toute mesure sur l'un détruit l'intrication.

3. Dans le cas où l'espace de A est de dimension > 2, une mesure projetant A dans un espace propre dégénéré (projecteur P_α) effectue la transformation $\rho_A \rightarrow \rho'_A = P_\alpha \rho_A P_\alpha / Tr\,(P_\alpha \rho_A)$. La probabilité de ce résultat est $p_\alpha = Tr\,(P_\alpha \rho_A)$. Le spectre de ρ'_A est en général différent de celui de ρ_A et $S(\rho'_A) \neq S(\rho_A)$. Le degré d'intrication A-B peut ainsi être changé par la mesure locale, sans s'annuler. La variation ΔS d'entropie de A moyennée sur les probabilités des différents résultats de mesure est toujours ≤ 0: <u>en moyenne</u>, une opération de mesure sur A seul ne peut augmenter l'intrication du système A-B (nous admettrons ce résultat).

$\rightarrow$ On ne change pas le degré d 'intrication d'une paire intriquée dans un état $|\Psi>_{AB}$ par une opération locale unitaire. On ne peut, en moyenne, augmenter son intrication par une mesure projective.

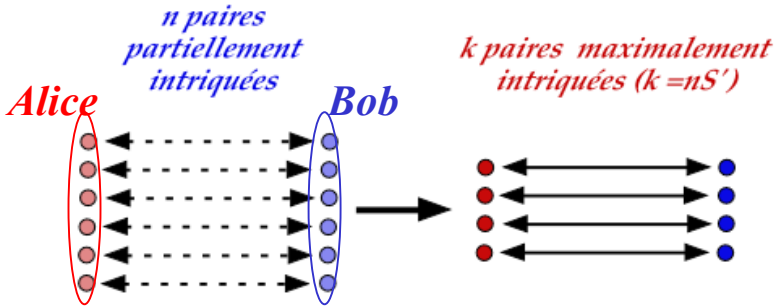
Distillation de l'intrication (un aperçu)

Nous verrons dans la prochaine leçon que les paires de qubits intriqués A-B sont des ressources essentielles pour la communication quantique. Les opérations «idéales» nécessitent des paires dans des états purs maximalement intriquées (S = 1). Si Alice et Bob ont en commun k paires indépendantes de ce type, ils partagent un système bi-partite de degré d'intrication $d_{AB} = kS = k$.

Peut-on comparer cette ressource à celle qu'ils ont s'ils partagent n paires indépendantes d'intrication S' < 1? Le degré d 'intrication est alors $d'_{AB} = n\,S' < n$.

On est tenté de dire que les deux « ressources » sont équivalentes si nS' = k. Le degré d'intrication partagée par Alice et Bob est alors le même, sous deux formes différentes. On doit pouvoir «compenser» le moindre degré d'intrication de chaque paire par un nombre plus grand de paires, dans le rapport S'/S des entropies par paire. Nous montrerons en effet qu'Alice et Bob peuvent, sans changer le degré d'intrication, modifier les états de leurs paires par des opérations locales. Ils peuvent transformer n paires partiellement intriquées en k < n paires d'intrication maximale par des opérations n'agissant que sur leur partie du système A-B.

Discussion limitée ici à des paires dans des états purs

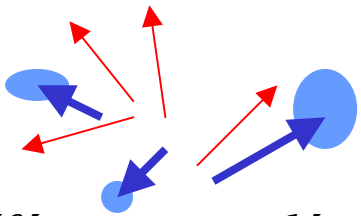


L'entropie de von Neumann d'un ensemble de n paires de qubits indépendants apparaît ainsi comme le nombre de paires maximalement intriquées «distillables» à partir de cet ensemble. Analogie avec l'entropie de Shannon de n bits classiques représentant le nombre de bits nécessaires au codage de l'information contenue dans ces bits.

Intrication, entropie et décohérence

Dans une mesure quantique, certains états « classiques » du mètre (M) (états cohérents ou états propres de la position X du curseur) sont «autorisés» alors que leurs superpositions sont «interdites» par le postulat de la mesure. La différence physique est que les états de la première catégorie ne s'intriquent pas avec l'environnement E, alors que ceux de la seconde s'intriquent rapidement avec E. L' augmentation de notre ignorance sur les résultats des mesures de M est représentée par le degré d'intrication entre M et E. Pour les états classiques de M, il n 'y a pas (ou peu) de perte d 'information vers l 'environnement alors qu 'il y en a beaucoup pour les états non-classiques interdits.

Critère de «classicité» des états de M pour un environnement (E) et un couplage M-E donnés:
On calcule (à l 'aide d 'une équation pilote) le degré d 'intrication d_{int} de M avec E au bout d 'un temps t, en fonction de l'état initial du système M. d_{int} apparaît comme une fonctionnelle de cet état initial. Les extrema de cette fonctionnelle correspondent aux « ilôts » classiques de l 'espace de Hilbert. (états ayant un comportement classique à l 'échelle de temps t). Ils correspondent aux états qui sont le plus «protégés» contre la perte d'information vers l'environnement. Ces états dépendent de la forme du couplage M-E. Ainsi, pour un oscillateur couplé à E par des termes linéaires en a et a†, les ilôts classiques sont les états voisins des états cohérents, états propres de a.



Représentation schématique de l 'espace de Hilbert avec ses ilots « classiques » extrema de la fonctionnelle d_{int}

<u>Références complémentaires</u>: Paz and Zurek, PRL, 82, 5181 (1999), Zurek, Habib et Paz, PRL, 70, 1187 (1993); Zurek, Prog.Theor.Phys. 89, 281 (1993).

9. Intrication et communication quantique

Nous allons décrire trois cas particuliers simples de traitement quantique de l 'information, la distribution de clé cryptographique, la téléportation et le codage dense. Nous insisterons sur le rôle joué par l'intrication dans ces applications.

Nous nous bornerons à l 'analyse des principes de ces opérations, sans décrire de systèmes spécifiques. (voir par exemple séminaires du 8/01 et du 29/01 par P.Zoller et N.Gisin).

La distribution de clé cryptographique et la téléportation sont deux exemples de communication quantique généralisant à la physique quantique des opérations classiques bien connues:

La cryptographie est la science très ancienne de l 'échange secret d 'information entre deux partenaires. On peut montrer classiquement que cet échange est absolument inviolable si les deux partenaires (appelés traditionnellement Alice et Bob) disposent d'une clé secrète, suite aléatoire de 0 et de 1 aussi longue que le message qu 'ils veulent échanger et utilisée une seule fois. La physique quantique n'intervient que pour fournir une méthode sure de partage de cette clé, basée sur des corrélations quantiques.

La téléportation n'est rien d 'autre que la communication à distance entre Alice et Bob d'un qubit dans un état inconnu (et fondamentalement inconnaissable). C'est la généralisation à la physique quantique de l 'échange classique de bits (ou fax).

Ces applications nécessitent le partage entre deux points A et B de paires de qubits préparés dans l 'un des quatre états d 'une base d'intrication maximale (états de Bell, $d_{int} = 1$). Nous commencerons par nous familiariser avec ces états.

Base de 4 états intriqués dans l 'espace de deux qubits arbitrairement séparés:

$$\left|\varphi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\overset{AB}{\left|00\right\rangle} \pm \overset{AB}{\left|11\right\rangle}\right)$$

$$\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\overset{AB}{\left|01\right\rangle} \pm \overset{AB}{\left|10\right\rangle}\right)$$

|0> et |1> correspondent par exemple aux états propres |+1/2> et |– 1/2> de v.p. ± 1 de σ_z*:*

$$\sigma_z|0\rangle = |0\rangle \,;\, \sigma_z|1\rangle = -|1\rangle$$

$|\varphi^{\pm}\rangle$ *et* $|\psi^{\pm}\rangle$ ***sont états propres des observables collectives*** $\sigma_z^A\,\sigma_z^B$ ***et*** $\sigma_x^A\,\sigma_x^B$***:***

$$\sigma_z^A\,\sigma_z^B\,|\varphi^{\pm}\rangle = |\varphi^{\pm}\rangle \,;\; \sigma_z^A\,\sigma_z^B\,|\psi^{\pm}\rangle = -|\psi^{\pm}\rangle$$

$\sigma_z^A\,\sigma_z^B$*: opérateur « parité » (répond à la question: les qubits sont-ils identiques?)*

$$\sigma_x^A\,\sigma_x^B\,|\varphi^{\pm}\rangle = \pm|\varphi^{\pm}\rangle;\; \sigma_x^A\,\sigma_x^B\,|\psi^{\pm}\rangle = \pm|\psi^{\pm}\rangle$$

$\sigma_x^A\,\sigma_x^B$*: opérateur «phase»(répond à la question: la superposition a-t-elle le signe+ ou -?*

Pas d 'information dans chaque qubit, mais seulement dans leur corrélations.

Impossibilité de changer l 'intrication par des <u>opérations locales</u> sur chaque qubit.

(Ces opérations transforment les états de Bell en d 'autres états d'intrication maximale):

Mêmes opérations en manipulant B.

$$\sigma_z^A |\varphi^+\rangle = |\varphi^-\rangle ; \sigma_z^A |\varphi^-\rangle = |\varphi^+\rangle$$

$$\sigma_z^A |\psi^+\rangle = |\psi^-\rangle ; \sigma_z^A |\psi^-\rangle = |\psi^+\rangle$$

σ_z^A change la phase de l'état de Bell

$$\sigma_x^A |\varphi^+\rangle = |\psi^+\rangle ; \sigma_x^A |\varphi^-\rangle = -|\psi^-\rangle$$

$$\sigma_x^A |\psi^+\rangle = |\varphi^+\rangle ; \sigma_x^A |\psi^-\rangle = -|\varphi^-\rangle$$

σ_x^A change la parité de l'état de Bell

Evolution unitaire générale de A <u>seul</u> fait « tourner » l 'état A dans la direction θ,ϕ:

$$U|\varphi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^A_{\theta,\phi}|0\rangle^B \pm |1\rangle^A_{\theta,\phi}|1\rangle^B\right)$$

Equivalent à un changement d'axe de quantification du qubit A sans modifier celui de B: le degré d 'intrication ne change pas

Opérations locales combinées à des communications classiques entre A et B

Supposons qu 'A et B partagent entre eux une paire de qubits dans l'un des quatre états de Bell (correspondant à une valeur ±1 de la parité et une valeur ±1 de la phase). Il est facile de voir qu'ils ne peuvent pas déterminer cet état de Bell, et donc les deux bits classiques correspondants, par des mesures locales, même accompagnées de la communication classique de leurs résultats:

En mesurant séparément σ_z^A et σ_z^B (opérateurs qui commutent avec $\sigma_z^A\ \sigma_z^B$) et en multipliant leurs résultats, ils auront déterminé, sans l 'altérer, la parité de l 'état de Bell. Mais ils auront perturbé sa phase car $[\sigma_z^{A,B},\ \sigma_x^A\ \sigma_x^B] \neq 0$.

De même, en mesurant séparément σ_x^A et σ_x^B (opérateurs qui commutent avec $\sigma_x^A\ \sigma_x^B$) et en multipliant leurs résultats, ils auront déterminé, sans l'altérer, la phase de l 'état de Bell . Mais ils auront perturbé sa parité car $[\sigma_x^{A,B}\ ,\ \sigma_z^A\ \sigma_z^B] \neq 0$.

Des opérations locales, même accompagnées de communication classique, ne permettent ni de mesurer ni de préparer un état de Bell. Il faut pour cela des opérations «non locales» agissant simultanément sur les deux qubits.

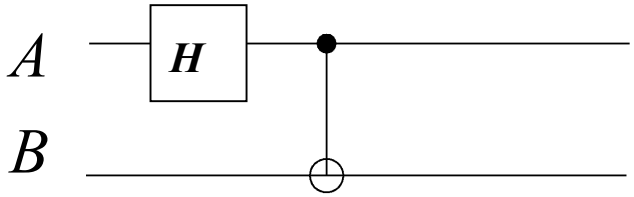
Opérations jointes sur deux qubits: exemples de circuits quantiques:

Nous avons vu (leçon 1) que deux qubits peuvent être intriqués par une porte C-NOT à deux qubits effectuant une pré-mesure dans laquelle un qubit (A) est la source et l'autre (B) la cible. L'intrication requiert que A soit initialement préparé dans une superposition d 'états par une opération unitaire U (porte à un qubit).

Choisissons U = $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$ ***(transfo. de Hadamard vérifiant H*** ^{2} ***=1)***

$$\longrightarrow \quad |0\rangle^A \to \frac{1}{\sqrt{2}}\left(|0\rangle^A + |1\rangle^A\right) \; ; \quad |1\rangle^A \to \frac{1}{\sqrt{2}}\left(|0\rangle^A - |1\rangle^A\right)$$

L 'intrication est alors réalisée, à partir de qubits séparés, par l 'opération schématisée par le circuit ci-dessous qui combine une porte à un qubit avec une porte à deux qubits:



$$|0,0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)^A |0\rangle^B \to |\varphi^+\rangle;$$

$$|0,1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)^A |1\rangle^B \to |\psi^+\rangle;$$

$$|1,0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)^A |0\rangle^B \to |\varphi^-\rangle;$$

$$|1,1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)^A |1\rangle^B \to |\psi^-\rangle.$$

Le trait vertical reliant les deux cercles différents symbolise la dynamique conditionnelle de la porte C-NOT à deux qubits

Ce circuit transforme la base « découplée » des deux qubits dans la base de Bell. A devient le bit de « phase » et B le bit de « parité ». En appliquant le circuit en sens inverse et en mesurant les bits A et B, on détermine complètement l'état de Bell, en obtenant simultanément sa phase et sa parité.