NO-CLONING THEOREM

Ce théorème va prouver qu'il n'est pas possible de cloner (dupliquer) un état quantique en général.

Ce fait a des conséquences importantes dans le domaine de la cryptographie et des ordinateurs quantiques à venir.

En informatique classique, copier un bit ne pose pas de problème.

En mécanique quantique, on va prouver par l'absurde que copier un état quantique, par exemple un qbit représenté par un vecteur $|\psi>$ dans un espace complexe de Hilbert, est interdit, sauf cas très particuliers.

Supposons donc l'existence d'un opérateur de clonage U.

U va travailler sur l'état $|\psi>$ et un deuxième état, neutre $|b>$.

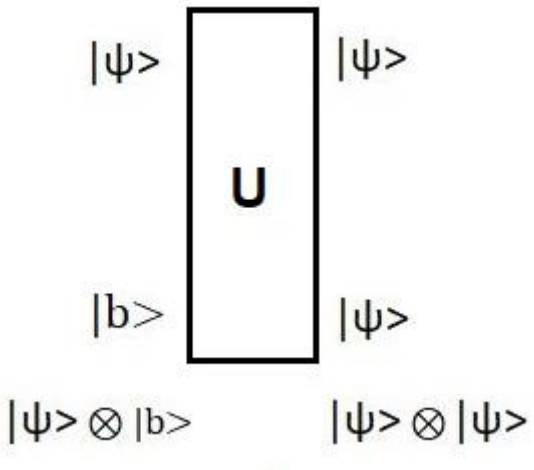
On peut comparer cet état $|b>$ à la feuille blanche d'une photocopieuse qui recevra donc l'état $|\psi>$.

L'état du système à l'entrée, produit tensoriel des deux états, s'écrit :

$$|\psi> \otimes |b>$$

et à la sortie du cloneur

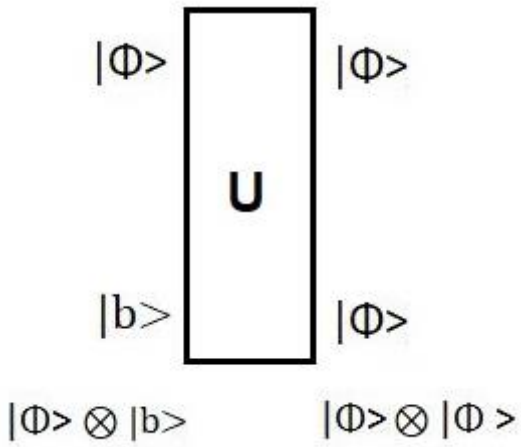
$$|\psi> \otimes |\psi>.$$



Le clonage s'écrit $U(|\psi\rangle \otimes |b\rangle) = |\psi\rangle \otimes |\psi\rangle$

On effectue la même opération avec un autre état quelconque

$|\Phi\rangle$

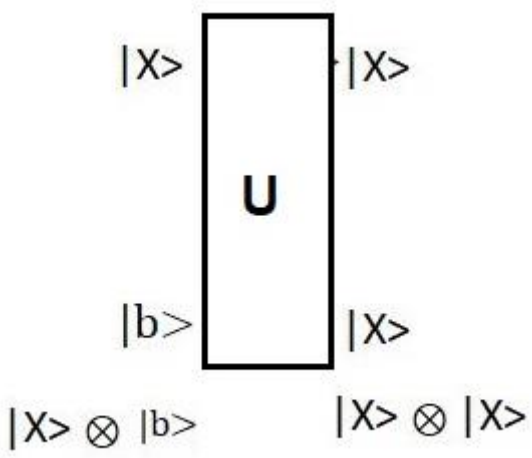


Le clonage s'écrit $U(|\Phi\rangle \otimes |b\rangle) = |\Phi\rangle \otimes |\Phi\rangle$

Contradiction avec un état superposé

Considérons |X>, un état superposé à cloner

$$|X\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\Phi\rangle)$$



Le clonage désiré s'écrit en développant

$$U(|X\rangle \otimes |b\rangle) = |X\rangle \otimes |X\rangle = \tfrac{1}{2}(|\psi\rangle + |\Phi\rangle) \otimes (|\psi\rangle + |\Phi\rangle)$$

$$= \tfrac{1}{2}\big(|\psi\rangle \otimes |\psi\rangle + |\Phi\rangle \otimes |\Phi\rangle + |\psi\rangle \otimes |\Phi\rangle + |\Phi\rangle \otimes |\psi\rangle\big)$$

Cette expression comporte donc 4 termes distincts.

Cependant, appliquons maintenant U directement aux composantes de |X>⊗|b>|*X*>⊗|*b*> en utilisant la linéarité de *U* :

$$U(|X\rangle \otimes |b\rangle) = \frac{1}{\sqrt{2}}\big(U(|\psi\rangle \otimes |b\rangle) + U(|\Phi\rangle \otimes |b\rangle)\big)$$

$$= \frac{1}{\sqrt{2}}\big(|\psi\rangle \otimes |\psi\rangle + |\Phi\rangle \otimes |\Phi\rangle\big)$$

Cette dernière expression ne comporte que deux termes distincts.

Conclusion

Nous observons une contradiction : le résultat attendu du clonage contient quatre termes distincts, alors que le résultat imposé par la linéarité de l'opérateur U n'en contient que deux. Cette contradiction prouve donc qu'une machine capable de cloner un état quantique arbitraire ne peut pas exister.

ANNEXE(Merci Perplexity.ai)

Le théorème de non-clonage quantique stipule qu'il est impossible de cloner parfaitement un état quantique arbitraire et inconnu. Cependant, il existe quelques cas particuliers où le clonage d'un état quantique est possible :

1. États orthogonaux : Il est possible de cloner des états quantiques qui sont mutuellement orthogonaux. Par exemple, les états de base $|0\rangle$ et $|1\rangle$ d'un qubit peuvent être clonés car ils sont orthogonaux.
2. États classiques : Les états classiques, qui sont essentiellement des états quantiques qui peuvent être mesurés sans perturbation, peuvent être copiés.
3. Clonage approximatif : Bien que le clonage parfait soit impossible, un clonage approximatif est réalisable. Cette approche permet de créer des copies imparfaites d'un état quantique, avec une certaine fidélité.
4. Clonage probabiliste : Dans certains cas, il est possible de cloner un état quantique avec une certaine probabilité de succès, mais pas de manière déterministe.
5. Clonage d'ensembles d'états connus : Si on connaît à l'avance l'ensemble des états possibles d'un système quantique, il peut être possible de concevoir une machine à cloner spécifique pour ces états.

Il est important de noter que ces exceptions ne contredisent pas le théorème de non-clonage, qui s'applique spécifiquement aux états quantiques arbitraires et inconnus. Ces cas particuliers ont des applications importantes dans divers domaines de l'informatique et de la communication quantiques.

Ph Loutrel www.loutrel.org 12/2/25