

Information Quantique

Frédéric Magniez

Cours 2 :
Paradoxe EPR
Téléportation, surperdense coding
Tirage à pile ou face
Algorithmes élémentaires

La transformation c -NOT

2

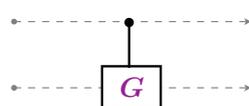
Définition

$$\begin{aligned}c\text{-NOT}|0b\rangle &= |0b\rangle \\c\text{-NOT}|1b\rangle &= |1\rangle|1 - b\rangle \\c\text{-NOT}|ab\rangle &= |a\rangle|a \oplus b\rangle\end{aligned} \quad c\text{-NOT} = \begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{pmatrix}$$

Représentation



Généralisation



$$\begin{aligned}c\text{-}G|0b\rangle &= |0b\rangle \\c\text{-}G|1b\rangle &= |1\rangle G|b\rangle\end{aligned}$$

Exercice 1

- Montrer qu'il n'existe pas de transformation quantique à 2-qubit telle que

$$G|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$$

Exercice 2

- Montrer que



- Réaliser un SWAP avec des c-NOT.

L'état singlet

Exercice 3

- Soit la paire EPR $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Montrer qu'effectuer une transformation unitaire U sur le premier qubit de $|\psi\rangle$ est équivalent à effectuer la transformation U^t sur le deuxième qubit.

Exercice 4

- Considérer la paire EPR $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
 La probabilité d'observer 0 ou 1 sur le premier qubit est 1/2
 Quand est-il dans une autre base ?
- Intuitivement, quelle est la matrice densité représentant l'état du 1er qubit

Définition informelle

- Matrice densité du qubit restant après l'observation de l'autre qubit (et en oubliant le résultat) (peut importe la base !)

Exemples

- Etats séparés : $\text{Tr}_2(|\psi_1\rangle|\psi_2\rangle) = |\psi_1\rangle\langle\psi_1| \approx |\psi_1\rangle$
- Paire EPR : $\text{Tr}_2(|\text{EPR}\rangle) = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \frac{1}{2}\text{Id}$

Définition formelle

$${}_2\langle b|\psi\rangle_{12} = (\langle 0b|\psi\rangle)|0\rangle + (\langle 1b|\psi\rangle)|1\rangle$$

$$\text{Tr}_2(|\psi\rangle) = {}_2\langle 0|\psi\rangle\langle\psi|0\rangle_2 + {}_2\langle 1|\psi\rangle\langle\psi|1\rangle_2$$

Exercice

- Vérifier les exemples ci-dessus
- Pourquoi le nom de trace partielle ?

Définition

- Soit ρ une matrice densité sur n -qubit
- Soit $|\psi\rangle$ une superposition sur $(n+m)$ -qubit, avec $m \geq 0$
- L'état pur $|\psi\rangle$ purifie l'état mélangé ρ si

$$\text{tr}_S|\psi\rangle\langle\psi| = \rho$$

où S représente les m derniers qubits de $|\psi\rangle$

Théorème

- Si $2^m \geq \text{rang}(\rho)$ alors il existe une purification de ρ

Exercice

- Prouver le théorème de purification en diagonalisant ρ

Jeu

- Alice et Bob partagent une information initiale mais ne communiquent pas
- Alice, resp. Bob, reçoit un bit aléatoire x , resp. y
- Alice, resp. Bob, retourne un bit a , resp. b



- **Objectif** : maximiser $p = \Pr_{x,y}(a \oplus b = x \wedge y)$

\wedge	0	1
0	0	0
1	0	1

\oplus	0	1
0	0	1
1	1	0

Classiquement

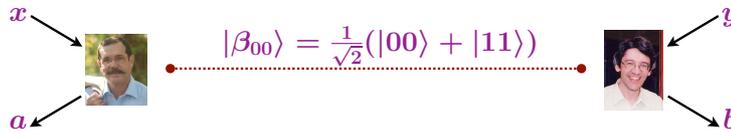
- Exercice : - Meilleur stratégie déterministe : $a = b = 0 \implies p = \frac{3}{4}$
- Exercice : - **Théorème** : la meilleure stratégie **probabiliste** n'est pas meilleure que la meilleure stratégie déterministe

Rappel

- **Objectif** : maximiser $p = \Pr_{x,y}(a \oplus b = x \wedge y)$

Quantiquement

- Alice et Bob partagent une paire EPR



Paradoxe : ce qu'observe Alice = ce qu'observe Bob

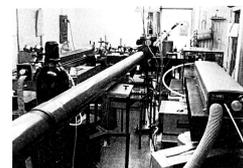
- Bob effectue une rotation d'angle $\frac{\pi}{8}$
- Si $x = 1$, Alice effectue une rotation d'angle $\frac{\pi}{4}$
- Si $y = 1$, Bob effectue une rotation d'angle $-\frac{\pi}{4}$

$y \setminus x$	0	1
0	$ \beta_{0, \frac{\pi}{8}}\rangle$	$ \beta_{\frac{\pi}{4}, \frac{\pi}{8}}\rangle$
1	$ \beta_{0, -\frac{\pi}{8}}\rangle$	$ \beta_{\frac{\pi}{4}, -\frac{\pi}{8}}\rangle$

- Alice et Bob observent leur qubit et renvoie la valeur obtenue

- Exercice : - **Théorème** : $p = \cos^2(\frac{\pi}{8}) \approx 0.85$

Réalisation : [Aspect-Grangier-Roger-Dalibard: Orsay'82]



Jeu

- Alice, Bob et Charlie partagent une information initiale mais ne communiquent pas
- Alice, Bob et Charlie reçoivent un bit aléatoire : x, y, z
- **Contrainte** : $x \oplus y \oplus z = 0 \implies xyz \in \{000, 011, 101, 110\}$
- Alice, Bob et Charlie renvoient un bit : a, b, c
- **Objectif** : maximiser $a \oplus b \oplus c = x \vee y \vee z$

Classiquement

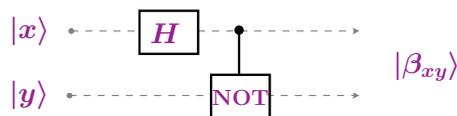
- Impossible avec une certitude absolue
- Exercice : Montrer que la probabilité de succès maximale est $3/4$

Quantiquement

- Alice, Bob et Charlie partagent $\frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$
- Protocole pour Alice/Bob/Charlie :
 - Si le bit détenu est **1** alors appliquer la porte Hadamard
 - Observer et renvoyer le bit obtenu
- Exercice : Montrer que ce protocole gagne le jeu avec certitude.

Application des mesures de Bell

Changement de base de Bell



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

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Superdense coding

$$\text{FLIP} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

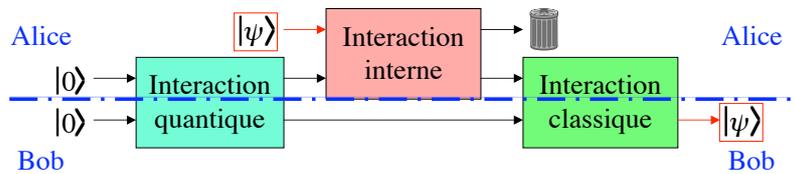
- Alice et Bob partagent une paire EPR $|\beta_{00}\rangle$
- Alice veut envoyer à Bob deux bits x, y
- Alice effectue les transformations locales $\text{NOT}^y \times \text{FLIP}^x$
- Alice envoie son qubit à Bob
- Bob fait une mesure de Bell et récupère x, y
- **Conclusion** : 1-qubit = 2 bits !

Problème

- Alice veut transmettre un qubit $|\psi\rangle$ à Bob
- Bob : position éloignée et inconnue d'Alice
- Communication possible : classique à sens unique Alice \rightarrow Bob

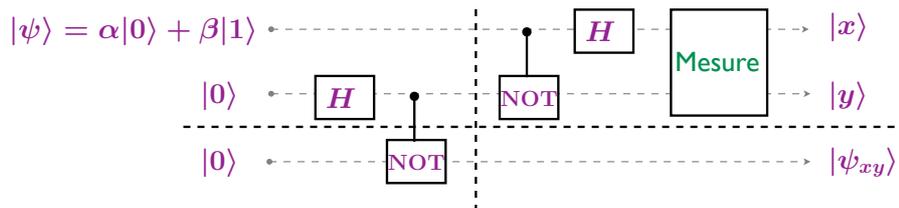


Réalisation



La communication classique ne révèle rien sur $|\psi\rangle$!

Circuit

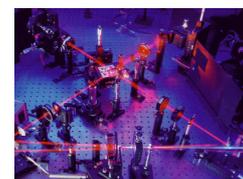


Exercice

- Calculer l'état du système avant mesure
- Ecrire l'état du qubit $|\psi_{xy}\rangle$ en fonction des valeurs x,y observées
- Quelle est la matrice densité correspondant au troisième qubit ? Expliquer la fin du protocole

Réalisations

- 1 photon [Zeilinger et al : Innsbruck'97]
- 1 photon, 6 km [Gisin et al : Genève'02]
- 1 atome [Blatt et al : Innsbruck'04]
- Vidéo YouTube'06 : http://www.youtube.com/watch?v=6_5KKeEq-FU



Problème

- Alice et Bob sont éloignés
- Ils veulent tirer à pile ou face de manière équitable



Classiquement

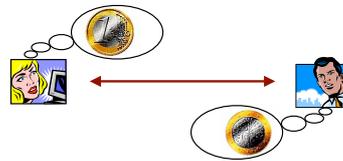
- Solutions basées sur des difficultés combinatoires
- Aucune solution inconditionnellement sûre

Quantiquement

- Biais possible : 0,25 [Ambainis 2001]
- Biais impossible : 0,207 [Kitaev 2002]

Version faible : élection

- Alice voudrait pile
- Bob voudrait face
- Aucune impossibilité connue !
- Biais possible : arbitrairement petit ! [Mochon 2007]



Exercice

Essai de protocole

$$|\psi_{b,x}\rangle = \begin{cases} |0\rangle, & \text{si } b = 0, x = 0 \\ |1\rangle, & \text{si } b = 0, x = 1 \\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), & \text{si } b = 1, x = 0 \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), & \text{si } b = 1, x = 1 \end{cases}$$

- Alice choisit deux bits aléatoires b, x
- Alice envoie $|\psi_{b,x}\rangle$ à Bob
- Bob choisit un bit aléatoire b' qu'il envoie à Alice
- Alice envoie b, x à Bob qui vérifie l'état reçu
- Le résultat du protocole est $b \oplus b'$

Exercice

- Montrer que si Alice et Bob sont honnêtes, alors $\Pr_{x,b,b'}(b \oplus b' = 0) = \frac{1}{2}$
- Montrer que Bob ne peut pas tricher
- Montrer qu'Alice peut tricher avec certitude : biais = 0.5

Indication : utiliser une paire EPR

Solutions

- Ne pas prendre $|\psi_{b,0}\rangle \perp |\psi_{b,1}\rangle \implies \text{biais} \leq 0.42$
- Augmenter la dimension $\implies \text{biais} \leq 0.25$

Protocole à 2 paires EPR

- Alice prépare 2 paires EPR $|\beta_{00}\rangle|\beta_{00}\rangle$
et envoie le second qubit de chaque paire à Bob
- Bob choisit aléatoirement une des 2 paires EPR à vérifier
- Alice envoie le qubit manquant de la paire EPR choisie par Bob
- Bob fait une mesure dans la base de Bell :
S'il observe $|\beta_{00}\rangle$, il continue sinon il annule le protocole
- Bob mesure le qubit de la paire EPR non utilisée
et annonce son résultat à Bob
- Alice vérifie que la mesure du qubit restant donne le même résultat

Théorème

- Le biais maximal de triche pour Alice et Bob est $1/4$

Exercice

- Prouver que Bob ne peut pas tricher avec un biais supérieur à $1/4$, et donner la triche correspondante.
- Est-ce que Bob peut se faire prendre en suivant votre triche ?

Exercice

- Alice va tricher en préparant l'état $\frac{1}{\sqrt{3}}(|00\rangle|\beta_{00}\rangle + |\beta_{00}\rangle|00\rangle)$
puis en suivant le protocole décrit
- Calculer la probabilité que Bob n'annule pas le protocole
- En supposant que Bob continue le protocole, calculer la probabilité que le résultat du protocole soit 0

Definition

- Etats purs

$$F(|\phi\rangle, |\psi\rangle) = \langle \phi | \psi \rangle^2$$

- Etat pur et état mélangé

$$F(\rho, |\psi\rangle) = \langle \psi | \rho | \psi \rangle$$

- Etats mélangés

$$F(\rho, \sigma) = \left(\text{tr} \left(\sqrt{\sqrt{\rho} \sigma \sqrt{\rho}} \right) \right)^2$$

Propriétés

- $0 \leq F(\cdot, \cdot) \leq 1$ et $F(\rho, \sigma) = 1$ ssi $\rho = \sigma$
- $F(\rho, \sigma) \leq F(\text{tr}_A(\rho), \text{tr}_A(\sigma))$
- $F(\rho, \sigma_0) + F(\rho, \sigma_1) \leq 1 + \sqrt{F(\sigma_0, \sigma_1)}$

Théorème

- $F(\rho, \sigma) = \max_{|\phi\rangle\langle\phi|=\rho, |\psi\rangle\langle\psi|=\sigma} F(|\phi\rangle, |\psi\rangle)$

Remarque

- La fidélité mesure la difficulté de distinguer 2 états
(Exercice : Pourquoi dans le cas d'états purs?)

Procéde de Salvail, triche d'Alice : cas général

Scénario

- Alice prépare un état différent $|\psi\rangle$ sur plusieurs (au moins 4) qubits
Parmi ces qubits, distinguons 4 positions : 1, 1', 2 et 2'
Les autres positions sont désignées par l'ensemble S
- Alice envoie 2 de ces qubits, numérotés 1 et 2
- Quand Bob lui demande le qubit qui complète la présumée paire EPR, Alice peut effectuer une transformation unitaire sur ces qubits, puis il envoie soit le qubit numéroté 1', soit le qubit numéroté 2'

Exercice

- Montrer qu'on peut supposer qu'Alice effectue une transformation unitaire uniquement lorsque Bob demande le qubit 2'.

On appellera par la suite cette transformation U

- Montrer que la probabilité que le résultat du protocole soit 0 est

$$\frac{1}{2} (F(\text{tr}_{2S}(|\psi\rangle\langle\psi|), |\beta\rangle_{11'}|0\rangle_{2'}) + F(\text{tr}_{1S}(U|\psi\rangle\langle\psi|U^*), |0\rangle_{1'}|\beta\rangle_{22'}))$$

où $|\beta\rangle = |\beta_{00}\rangle$

- Borné cette probabilité par la quantité suivante puis conclure :

$$\frac{1}{2} (1 + \sqrt{F(|0\rangle\langle 0|_{1'} \otimes \frac{\text{Id}_{2'}}{2}, \frac{\text{Id}_{1'}}{2} \otimes |0\rangle\langle 0|_{2'})})$$

Calculabilité

- Que veut dire calculer ?
- Qu'est-ce qu'une machine, un programme ?
- Comment modéliser un ordinateur ?
indépendamment de la technologie, du langage, du système utilisés

Difficulté d'un problème

- Définitions intrinsèques (indépendantes de la technologie, du langage, du système utilisés) pour
- Calculable / Non calculable
 - Facile / Intraitable

Rappels historiques

- Machine de Turing, calculabilité, universalité : [Turing 1936]
- Proposition : EDVAC (Electronic Discrete Variable Computer) [von Neumann 1945]
- Premier ordinateur : Mark I [Robinson-Tootill-Williams 1949]

Portes et circuits quantiques

Portes $U \in \mathcal{U}(2^k)$, $k = 1, 2, 3$

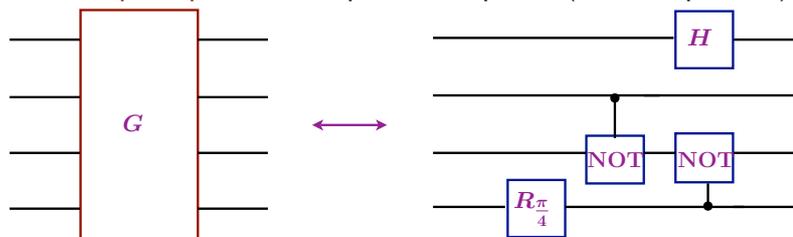
- Une **porte quantique** est une transformation unitaire qui agit sur au plus **3** qubits

Produit tensoriel de portes



Circuit

- Un **circuit quantique** est la composition de portes (étendues par $\otimes \text{Id}$)



Théorème. Familles universelles (au sens approché)

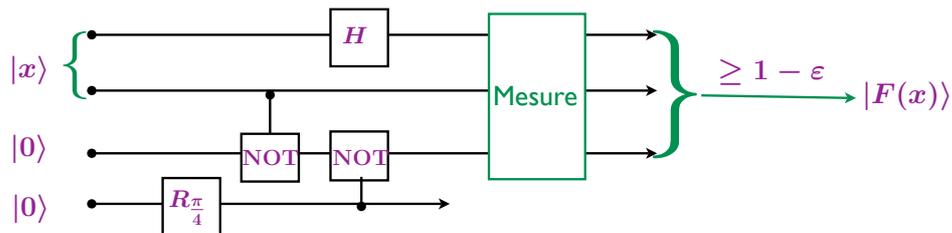
- NOT, H et Toffoli (c-c-NOT) (transformations uniquement réelles)
- NOT, \sqrt{H} et c-NOT
- La porte c-NOT et toutes les portes sur 1-qubit (**simulation exacte**)

Définition

- Un circuit $U = U_L \dots U_2 U_1$ calcule une fonction F avec erreur ϵ si pour toute entrée x :

$$\sum_z |\langle F(x), z | U | x, 0^k \rangle|^2 \geq 1 - \epsilon$$

- La **taille** d'un circuit est le nombre de portes utilisées pour le réaliser.
- La **complexité approchée** (resp. **exacte**) d'une fonction est la taille minimale du circuit qui la calcule avec erreur $1/3$ (resp. 0)



Remarques

- La complexité d'une fonction ne dépend pas du choix de base universelle
- L'erreur peut arbitrairement être réduite à ϵ par $\log(1/\epsilon)$ itérations

Définition

- Un **algorithme quantique** pour le calcul d'une fonction $F : \{0, 1\}^* \rightarrow \{0, 1\}^*$ est un algorithme classique qui calcule une famille de circuits $(C_n)_{n \in \mathbb{N}}$ telle que C_n calcule avec erreur $\epsilon < 1/3$ la fonction F restreinte aux entrées de $\{0, 1\}^n$
- La **complexité en temps** $T(n)$ d'un algorithme quantique est la taille du circuit C_n **PLUS** le temps qu'il faut pour décrire le circuit C_n avec précision $O(1/|C_n|)$

Remarques

- En règle générale la description du circuit est négligeable
- Les amplitudes des portes sont donc **calculables** !
- La complexité *ne dépend pas* du choix des portes

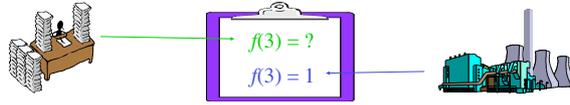
Classes de complexité

- Fonctions (problèmes) calculable (résoluble) en temps polynomial en la taille de l'entrée
 - déterministe : **P**
 - probabiliste avec erreur $\epsilon < 1/3$: **BPP**
 - quantique avec erreur $\epsilon < 1/3$: **BQP**

$$P \subseteq BPP \subseteq BQP$$

Problème

- Entrée : $f : \{0, 1\}^n \rightarrow \{0, 1\}$ soit constante, soit **balancée**
- Sortie : **0** ssi f est constante
- Contrainte : f est une **boîte noire**



Complexité en requêtes

- Déterministe : $1 + 2^{n-1}$
- Quantique : **1**

Cas $n = 1$

- Problème équivalent à décider si $f(0) = f(1)$ pour f quelconque

Solution quantique ($n = 1$)

 $x \mapsto f(x)$ n'est pas nécessairement réversible !

Implémentation de f

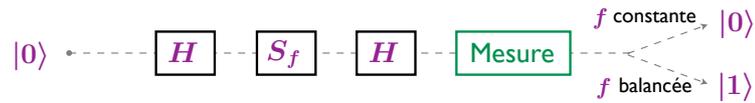
$$|b\rangle \longleftarrow \boxed{S_f} \longrightarrow (-1)^{f(b)}|b\rangle$$

Porte de Hadamard : lame demi-onde à $22,5^\circ$

$$|b\rangle \longleftarrow \boxed{H} \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$$

Circuit quantique

$$|0\rangle \longleftarrow \boxed{H} \longrightarrow \boxed{S_f} \longrightarrow \boxed{H} \longrightarrow \boxed{\text{Mesure}} \longrightarrow ?$$



Initialisation : $|0\rangle$

Parallélisation : $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Appel de la fonction : $\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)$

Interférences : $\frac{1}{2}((-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle))$

Au final : $\frac{1}{2}((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle$



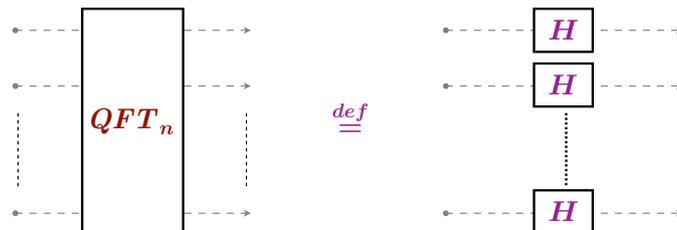
Dans ce cas la supériorité du quantique ne vient pas de l'enchevêtrement, mais des interférences **constructives** et **destructives**.

Solution quantique (cas général)

Implémentation de f



Transformée de Fourier quantique



Exercice

- Vérifier que

$$QFT_n|x\rangle = \frac{1}{2^{n/2}} \sum_y (-1)^{x \cdot y} |y\rangle$$

avec $x \cdot y = \sum_i x_i y_i \pmod 2$

Exercice 1

- Montrer que le circuit suivant résout le problème



Exercice 2

- Montrer que le même circuit permet de trouver f avec la promesse que

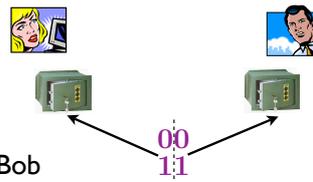
$$f(x) = a \cdot x$$

- Remarque : on montre que pour ce problème, la complexité probabiliste en requêtes est en $\Omega(2^{n/2})$

D'où le quantique tire-t-il sa supériorité ?

De l'enchevêtrement ?

- L'"enchevêtrement probabiliste" existe
 - Tirer à pile ou face **00** ou **11**
 - Partager chacun des bits entre Alice et Bob
 - Alice/Bob regarde son bit quand il le désire, son résultat est alors corrélé avec celui de Bob/Alice
- Mais l'enchevêtrement quantique est "plus fort"
 - Paradoxe EPR (violation des inégalités de Bell)



Des amplitudes complexes ?

- Non, on peut les simuler par des amplitudes réelles
- $$\alpha|0\rangle + \beta|1\rangle \simeq \alpha_r|00\rangle + \alpha_i|01\rangle + \beta_r|10\rangle + \beta_i|11\rangle \quad \mathcal{U}(2^n) \simeq \mathcal{O}(2^{2n})$$

Des amplitudes négatives ?

- Oui car possibilité d'interférences **destructives**

De la complexité des amplitudes ?

- Non, les amplitudes doivent être facilement calculables pour être physiquement réalisables