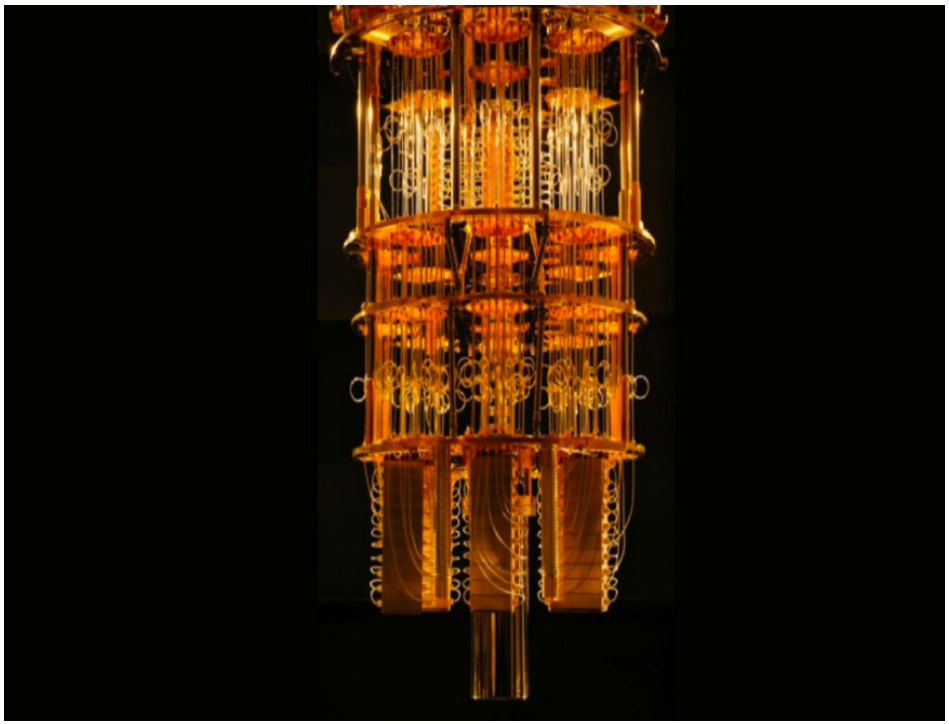
Calcul quantique

Olivier Lévêque, EPFL

IDIAP, 25 mars 2023



Calcul quantique : quelques dates

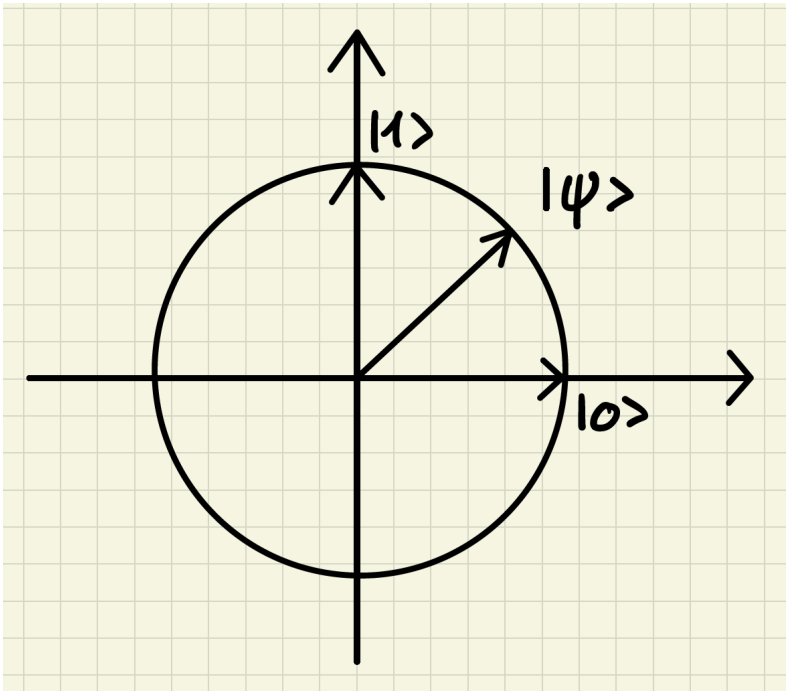
- 1920's : naissance de la physique quantique
- 1982 : Feynman/Manin : idée d'un ordinateur quantique
- 1986 : algorithmes de Deutsch, Deutsch-Josza
- 1993 : algorithme de Bernstein-Vazirani
- 1994 : algorithme de Simon
- 1994 : algorithme de Shor pour la factorisation des nombres
- 1996 : algorithme de Grover
- 2001 : premier ordinateur quantique (factorise $15 = 3 \cdot 5$)
- 2019 : "suprématie quantique" annoncée par Google
- 2023+ : "Il est difficile de faire des prédictions,
  surtout lorque celles-ci concernent l'avenir..."

Bits quantiques (Q-bits)

Un Q-bit peut valoir 0, 1 ou une *superposition* de ces deux valeurs !

On décrit son état par un *vecteur unité* dans l'espace vectoriel $\mathbb{R}^2$:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \quad \text{avec} \quad \alpha^2 + \beta^2 = 1$$



Note : En vrai, l'espace vectoriel est $\mathbb{C}^2$ et α et β sont des nombres complexes, mais oublions ça...

Bits quantiques (Q-bits)

Lorsqu'on mesure un Q-bit dans un état $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, il *change* d'état et prend la valeur

$$\begin{cases} |0\rangle & \text{avec probabilité} \quad \alpha^2 \\ \\ |1\rangle & \text{avec probabilité} \quad \beta^2 \end{cases}$$

C'est un des grands mystères de la physique quantique :

la mesure / l'observation d'un système change l'état de ce système !

Deux Q-bits

L'état joint de deux Q-bits est décrit par un vecteur unité dans l'espace vectoriel $\mathbb{R}^2 \otimes \mathbb{R}^2$.

A nouveau, il y a les états dits *purs* :

$$|00\rangle = |0\rangle \otimes |0\rangle, \quad |01\rangle = |0\rangle \otimes |1\rangle, \quad |10\rangle = |1\rangle \otimes |0\rangle, \quad |11\rangle = |1\rangle \otimes |1\rangle$$

et les états dits *superposés* :

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle \quad \text{avec} \quad \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1$$

et à nouveau, une *mesure* de ce système peut générer 4 états possibles : $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ (avec probabilités $\alpha^2, \beta^2, \gamma^2, \delta^2$, respectivement).

Intrication : un autre mystère de la physique quantique !

Si par exemple l'état $|\psi\rangle$ est donné par

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

alors on dit que les deux Q-bits sont *intriqués*, car quel que soit le résultat (aléatoire) de la mesure ($|00\rangle$ ou $|11\rangle$, chaque fois avec probabilité $1/2$), les deux Q-bits sortiront de cette mesure avec la même valeur.

Prix Nobel de physique 2022 (Aspect, Clauser, Zellinger) :

Les états intriqués existent !

Problème de Deutsch

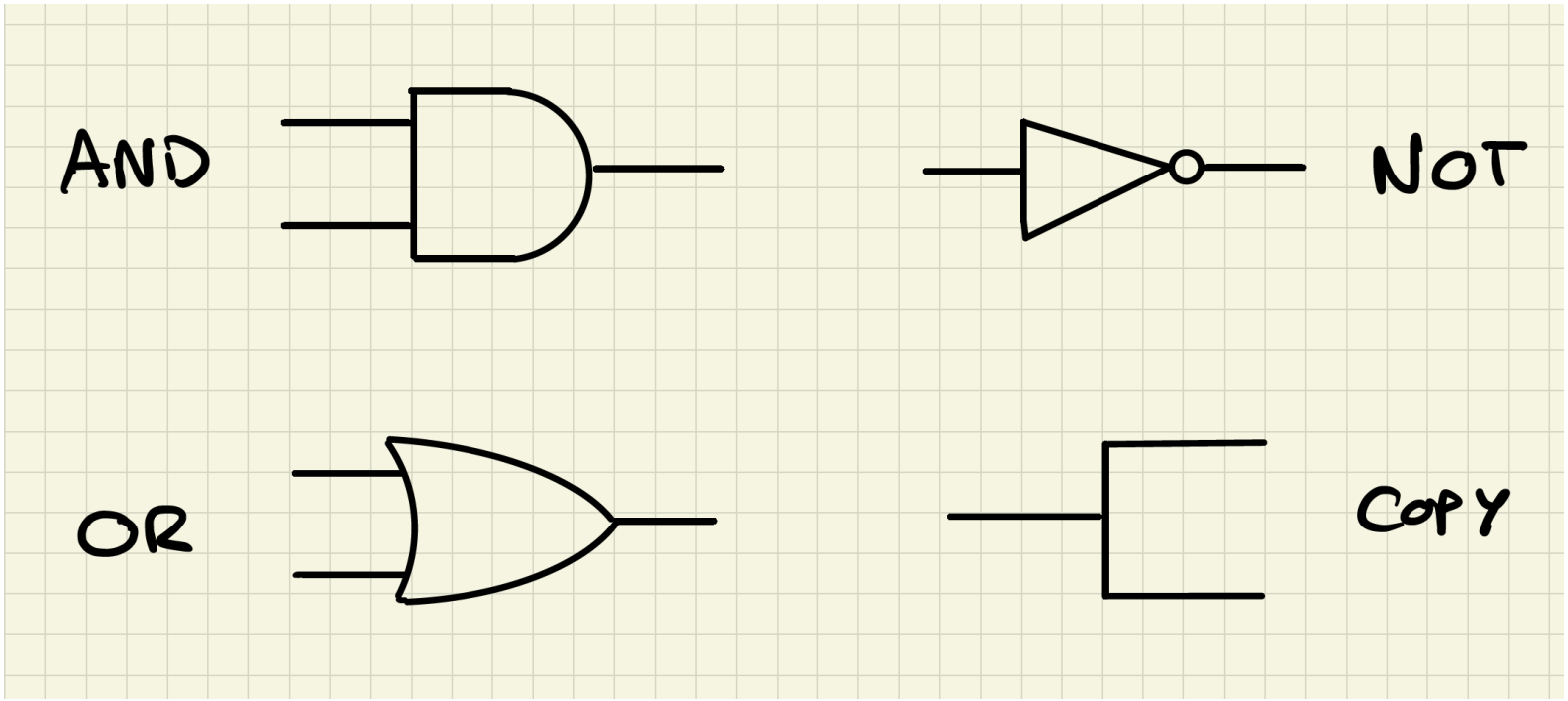
Soit $f : \{0,1\} \to \{0,1\}$: on aimerait savoir si

$$f(0) = f(1) \quad \text{ou} \quad f(0) \neq f(1) \quad ?$$

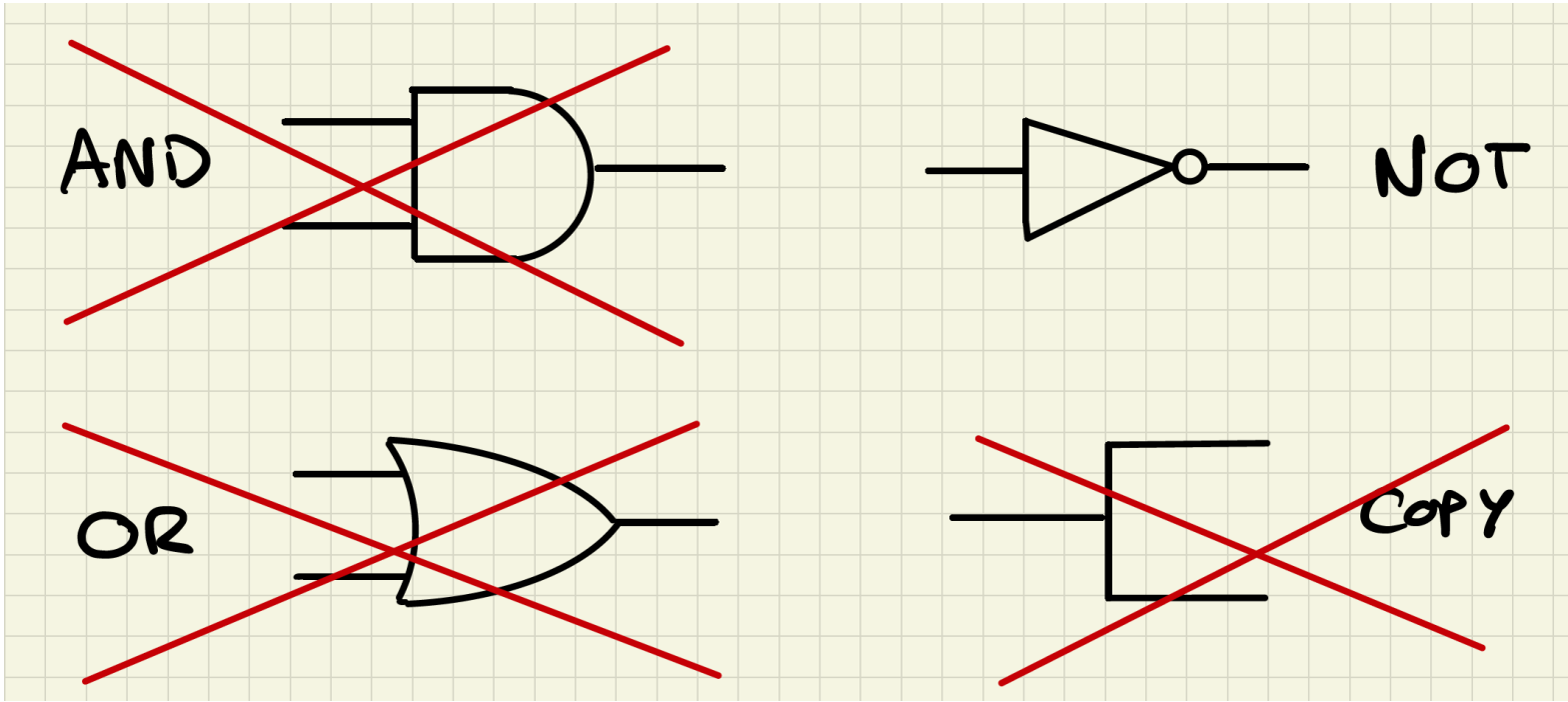
"Classiquement", deux évaluations de la fonction f sont nécessaires pour répondre à cette question.

Avec un circuit quantique, *une seule* évaluation suffit !

Portes classiques

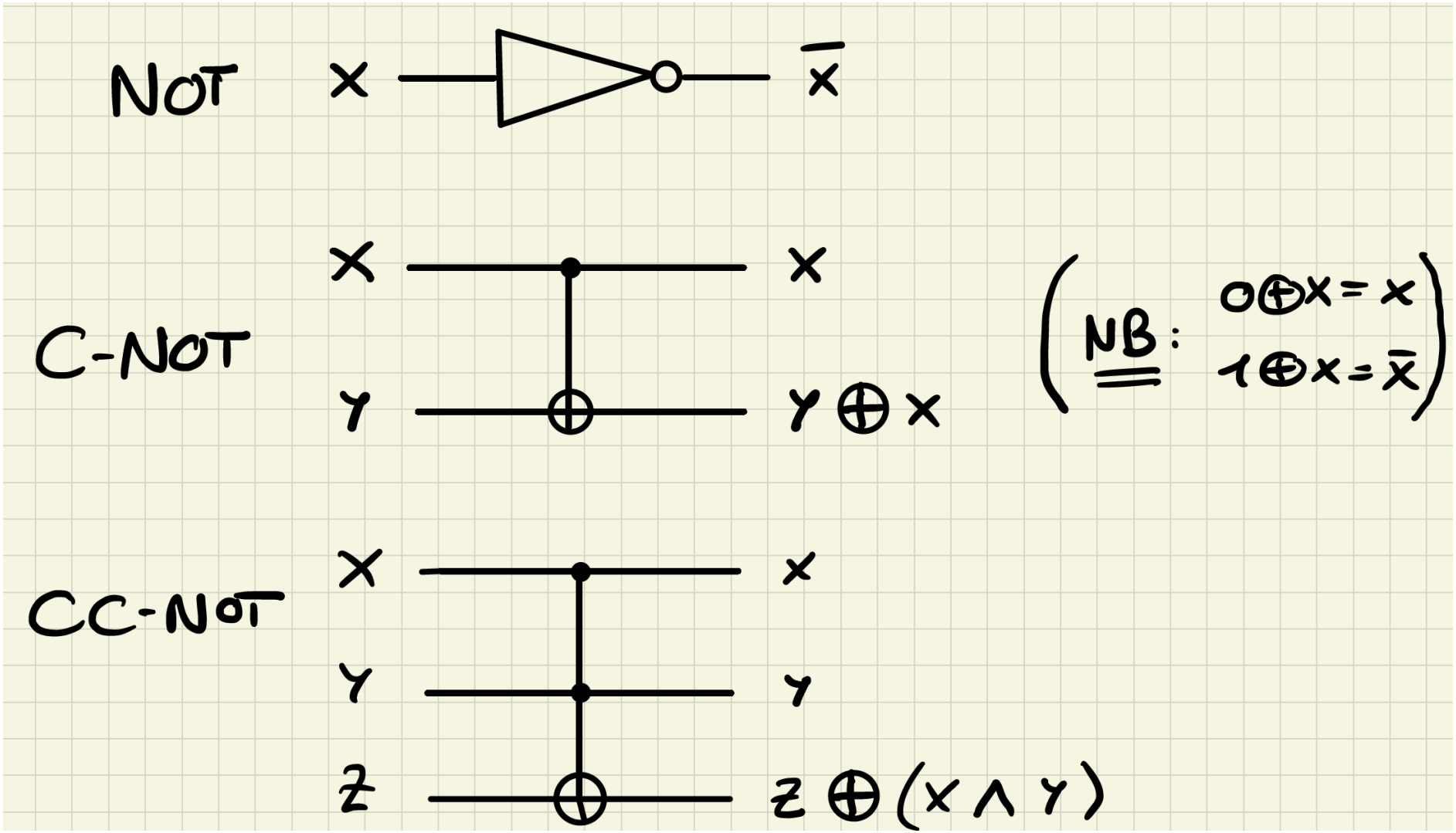


Portes classiques



En physique quantique, seules les portes *réversibles* sont admises !

Portes classiques utilisables dans un circuit quantique

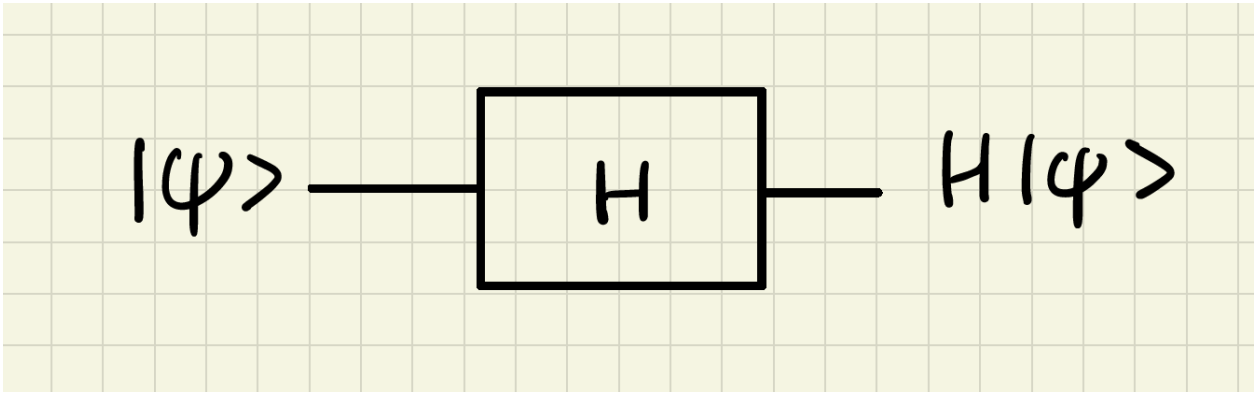


Exercice : recréer les portes AND, OR et COPY à partir des portes précédentes

Attention : on ne copie *jamais* un bit quantique !

Autres portes quantiques

1. La porte de Hadamard (1 Q-bit en entrée et en sortie)



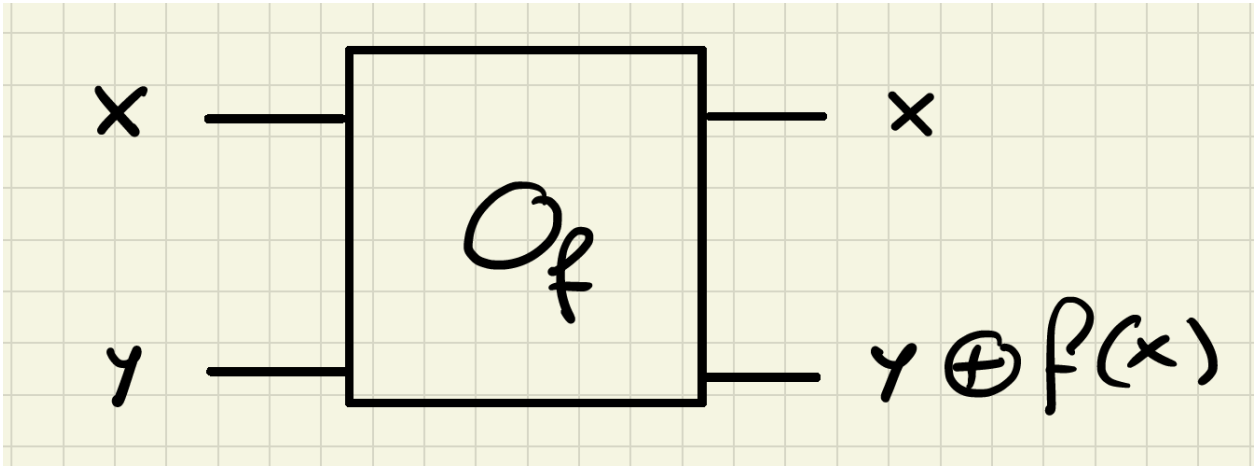
$$H|0\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \qquad H|1\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)$$

La porte H est une opération linéaire : si $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, alors

$$H|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

Autres portes quantiques

2. La porte "oracle" O_f (2 Q-bits en entrée et en sortie)



La porte O_f est également une opération linéaire (et réversible) :

si $|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$, alors

$$O_f\,|\psi\rangle = \alpha\,|0, 0 \oplus f(0)\rangle + \beta\,|0, 1 \oplus f(0)\rangle + \gamma\,|1, 0 \oplus f(1)\rangle + \delta\,|1, 1 \oplus f(1)\rangle$$

$$= \alpha\,|0, f(0)\rangle + \beta\,|0, \overline{f(0)}\rangle + \gamma\,|1, f(1)\rangle + \delta\,|1, \overline{f(1)}\rangle$$

Algorithme quantique de Deutsch

Rappel : Le but est de décider si une fonction $f : \{0,1\} \to \{0,1\}$ satisfait

$$f(0) = f(1) \quad \text{ou} \quad f(0) \neq f(1) \text{ (autrement dit, } f(0) = \overline{f(1)})$$

en évaluant *une seule fois* la fonction f, i.e., en faisant appel une seule fois à l'oracle O_f.

1. Pour utiliser le parallélisme quantique, on génère deux Q-bits dans l'état superposé

$$|\psi_0\rangle = \frac{1}{2}\Big(|00\rangle - |01\rangle + |10\rangle - |11\rangle\Big)$$

Exercice: Vous pouvez vérifier que

$$|\psi_0\rangle = H|0\rangle \otimes H|1\rangle = \frac{1}{2}\Big(|0\rangle + |1\rangle\Big) \otimes \Big(|0\rangle - |1\rangle\Big)$$

Algorithme quantique de Deutsch (suite)

2. On passe l'état $|\psi_0\rangle$ à travers la porte O_f :

$$|\psi_1\rangle = O_f\,|\psi_0\rangle = \frac{1}{2}\Big(|0, f(0)\rangle - |0, \overline{f(0)}\rangle + |1, f(1)\rangle - |1, \overline{f(1)}\rangle\Big)$$

3. Puis on passe *le premier bit uniquement* à travers une porte de Hadamard (formellement, on applique l'opérateur $H \otimes I$ à $|\psi_1\rangle$), pour obtenir

$$\begin{aligned}|\psi_2\rangle &= (H \otimes I)\,|\psi_1\rangle \\ &= \frac{1}{2^{3/2}}\Big(|0, f(0)\rangle + |1, f(0)\rangle - |0, \overline{f(0)}\rangle - |1, \overline{f(0)}\rangle \\ &\qquad + |0, f(1)\rangle - |1, f(1)\rangle - |0, \overline{f(1)}\rangle + |1, \overline{f(1)}\rangle\Big)\end{aligned}$$

Algorithme quantique de Deutsch (suite)

4. En regroupant les termes selon la valeur du premier Q-bit, on trouve

$$|\psi_2\rangle = \frac{1}{2^{3/2}} \Big(|0, f(0)\rangle - |0, \overline{f(0)}\rangle + |0, f(1)\rangle - |0, \overline{f(1)}\rangle + |1, f(0)\rangle - |1, \overline{f(0)}\rangle - |1, f(1)\rangle + |1, \overline{f(1)}\rangle \Big)$$

Si donc $f(0) = f(1)$, alors

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} \Big(|0, f(0)\rangle - |0, \overline{f(0)}\rangle \Big)$$

si par contre $f(0) = \overline{f(1)}$, alors

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} \Big(|1, f(0)\rangle - |1, \overline{f(0)}\rangle \Big)$$

Algorithme quantique de Deutsch (fin)

En conclusion, en mesurant la valeur du premier Q-bit de l'état $|\psi_2\rangle$, on saura que

$$\begin{cases} f(0) = f(1) & \text{si cette valeur vaut 0} \\ f(0) = \overline{f(1)} & \text{si cette valeur vaut 1} \end{cases}$$

...tout ceci en ayant évalué une seule fois la fonction f (i.e., en ayant fait appel une seule fois à l'oracle O_f).

Sur le même principe...

1. Algorithme de Deutsch-Josza

Soit $f : \{0,1\}^n \to \{0,1\}$ une fonction qui est :

$$\begin{cases} \text{soit constante, i.e.,} & f(x) = f(y) \text{ pour tous } x, y \in \{0,1\}^n \\ \text{soit balancée, i.e.,} & f(x) = 0 \text{ pour la moitié des valeurs de } x \in \{0,1\}^n \\ & \text{et } f(x) = 1 \text{ pour l'autre moitié} \end{cases}$$

Classiquement, il faut évaluer f en $2^{n-1} + 1$ points (dans le pire des cas) pour savoir à quelle catégorie appartient f.

Quantiquement, l'algorithme de Deutsch-Josza trouve la réponse en une seule évaluation de la fonction f (avec $n + 1$ Q-bits au lieu de deux).

Sur le même principe...

2. Algorithme de Bernstein-Vazirani

Soit $f : \{0,1\}^n \to \{0,1\}$ une fonction de la forme

$$f(x) = s \cdot x = s_1 x_1 + s_2 x_2 + \ldots + s_n x_n$$

Pour trouver le vecteur $s \in \{0,1\}^n$, il faut classiquement évaluer f en n positions différentes ($x = (1,0,\ldots,0)$, $x = (0,1,\ldots,0)$, etc.).

A nouveau, un algorithme quantique permet de trouver le vecteur $s \in \{0,1\}^n$ avec une seule évaluation de la fonction f.

Sur le même principe...

3. Algorithme de Grover

Soit $f : \{0,1\}^n \to \{0,1\}$ une fonction telle que

$$f(x_0) = 1 \quad \text{et} \quad f(x) = 0 \quad \text{pour toute valeur de } x \neq x_0$$

Classiquement, de l'ordre de 2^n évaluations de f sont nécessaires (dans le pire des cas) pour trouver la valeur de x_0.

Un algorithme quantique permet de trouver la valeur de x_0 en $\sqrt{2^n} = 2^{n/2}$ évaluations de la fonction f.

Sur le même principe...

4. Algorithme de Simon

Algorithme quantique efficace pour trouver la *période* d d'une fonction périodique $f : \{0,1\}^n \to \{0,1\}$ (i.e., $f(x \oplus d) = f(x)$, $\forall x \in \{0,1\}^n$).

5. Algorithme de Shor

Algorithme quantique efficace pour trouver la *période* d d'une fonction périodique $f : \mathbb{Z} \to \mathbb{Z}$ (i.e., $f(x+d) = f(x)$ pour tout $x \in \mathbb{Z}$)...

...qui peut ensuite être utilisé pour factoriser efficacement un produit $N = P \cdot Q$ de grands nombres premiers P et Q.

Plus précisément, si P et Q ont chacun n chiffres, alors l'algorithme effectue de l'ordre de n^3 opérations, tandis que le meilleur algorithme classique connu effectue de l'ordre de $\exp(n^{1/3})$ opérations.

Et une note pour finir

Les ordinateurs quantiques, non seulement ça existe,
mais tout le monde peut y avoir accès “gratuitement” :

IBM Quantum : `https://quantum-computing.ibm.com/`