Les promesses de l'ordinateur quantique

Xavier Caruso
Institut de Mathématiques de Bordeaux
xavier.caruso@normalesup.org

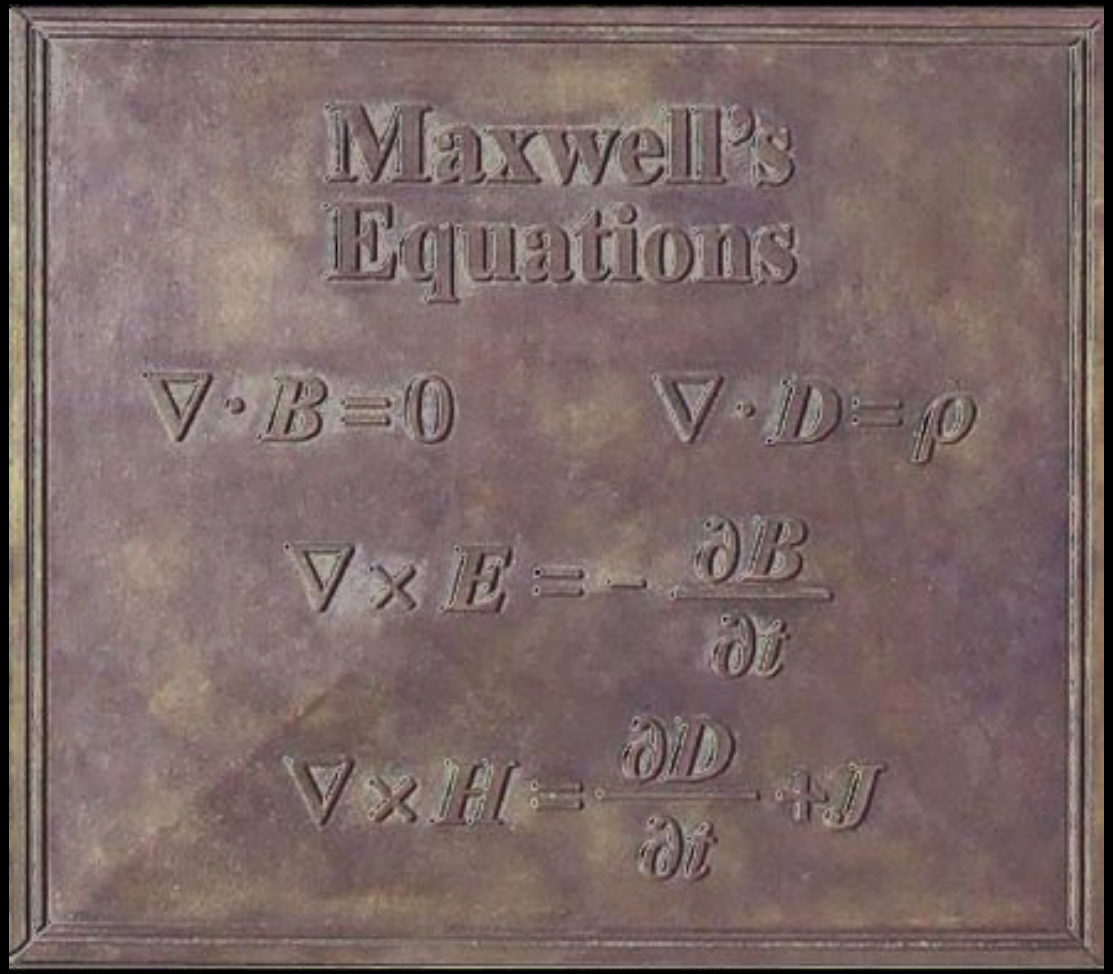
midismath

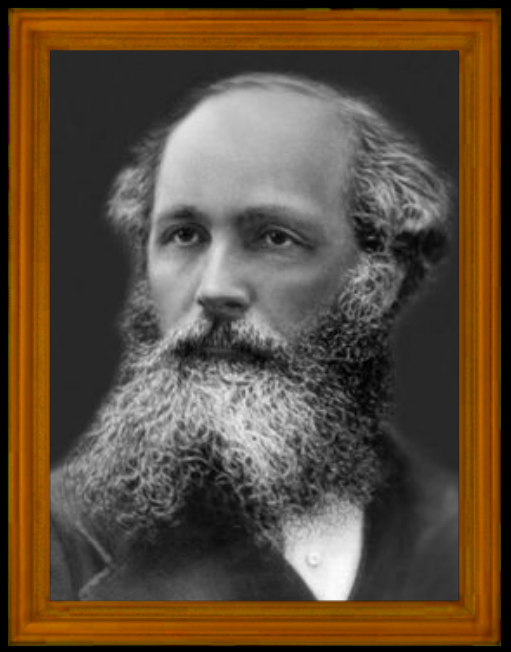
11 avril 2022

1ère partie

Calcul quantique : les origines

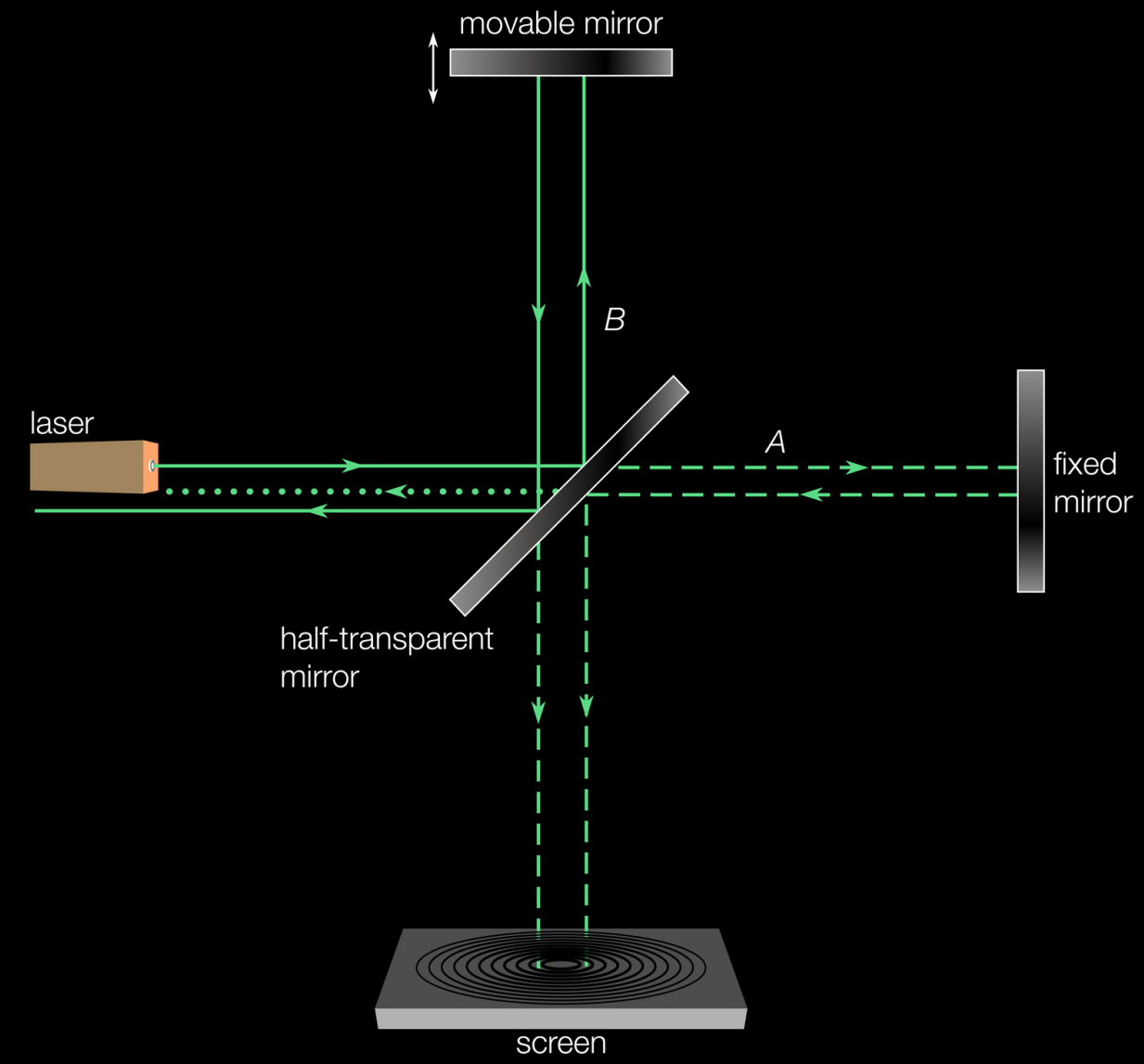
Electromagnétisme



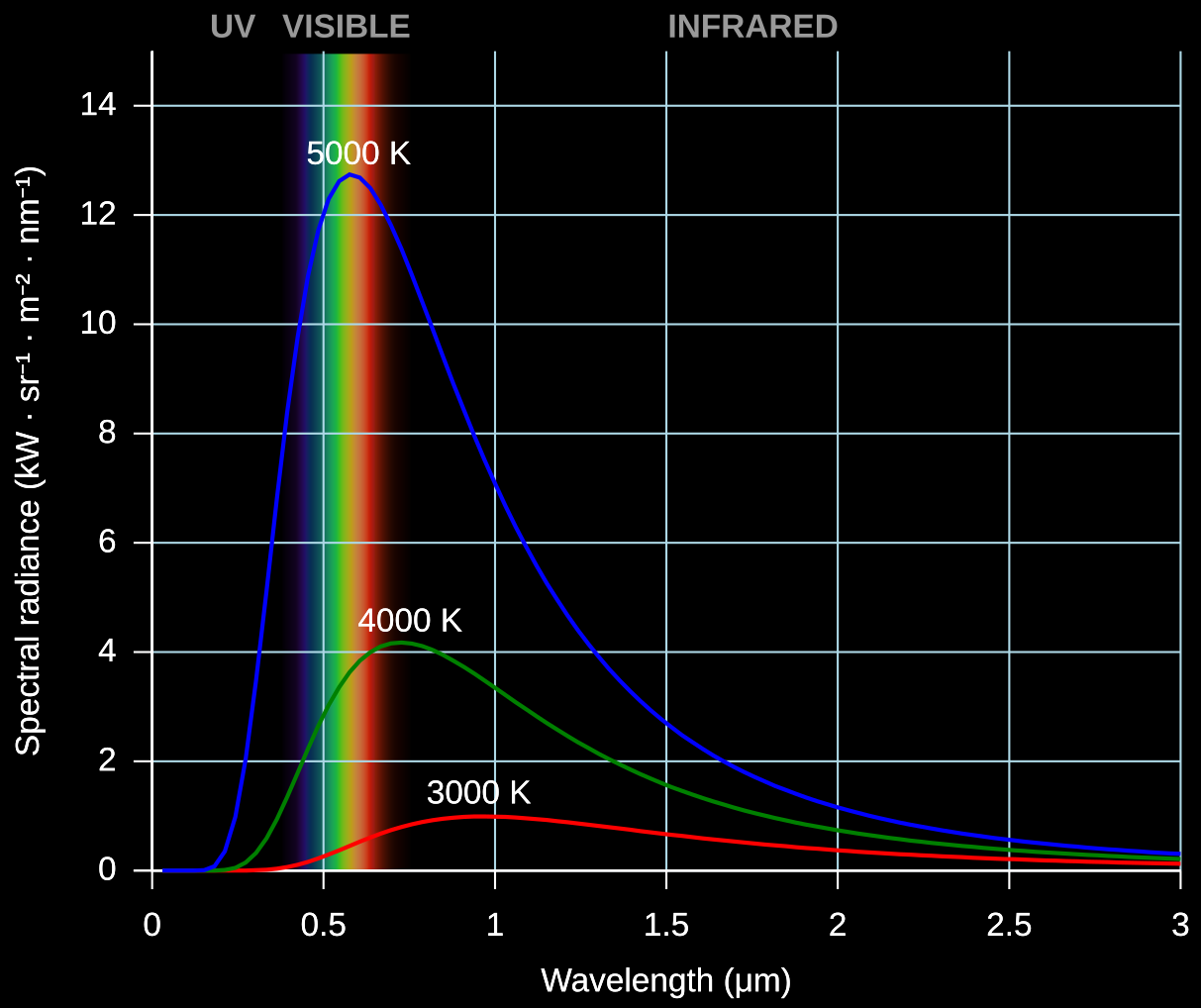


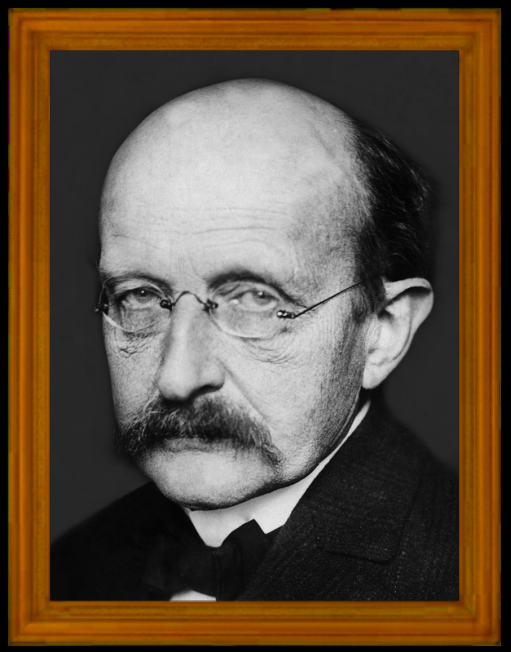
James Clark Maxwell
1831 – 1879

Interféromètre de Michelson-Morley



Radiation du corps noir

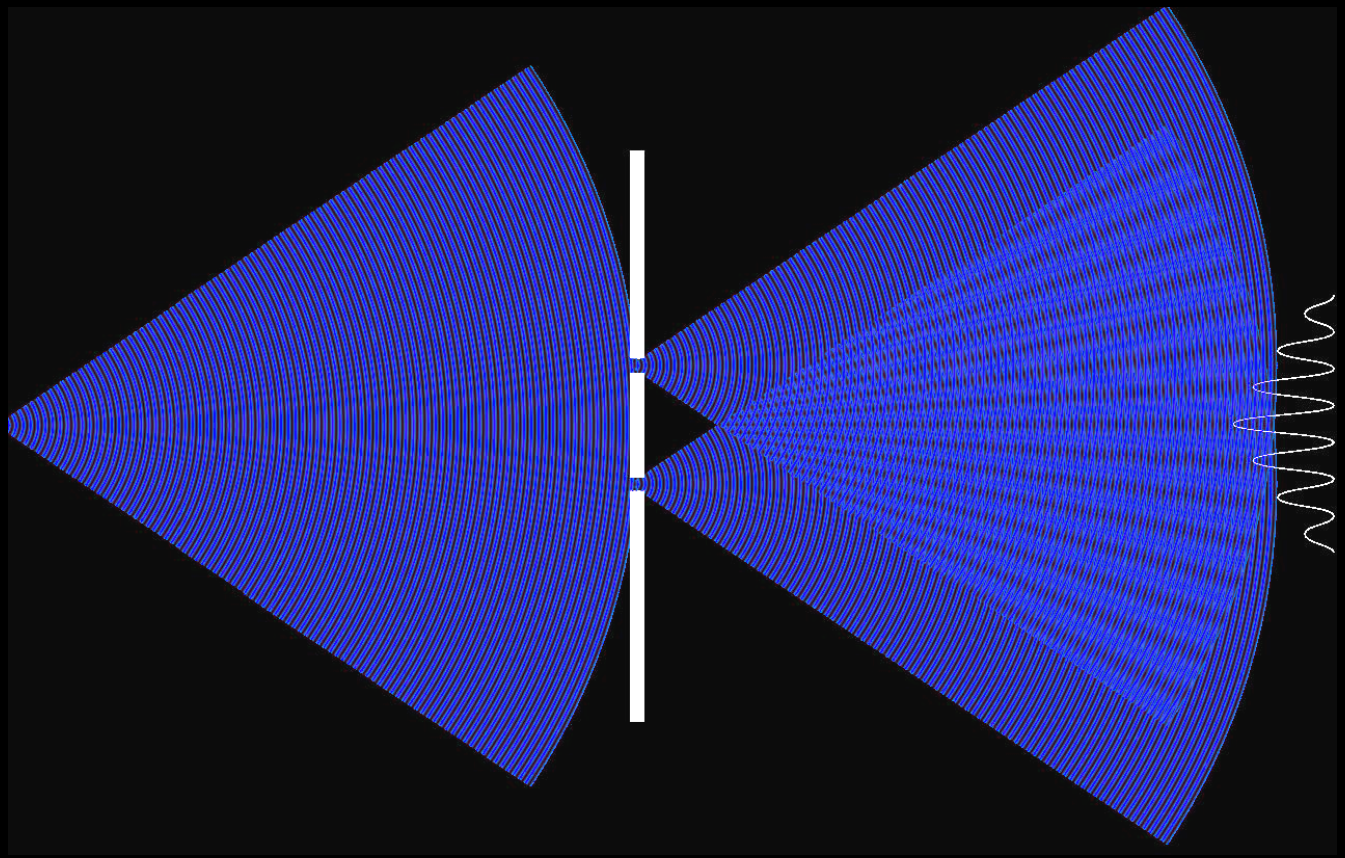




Max Planck

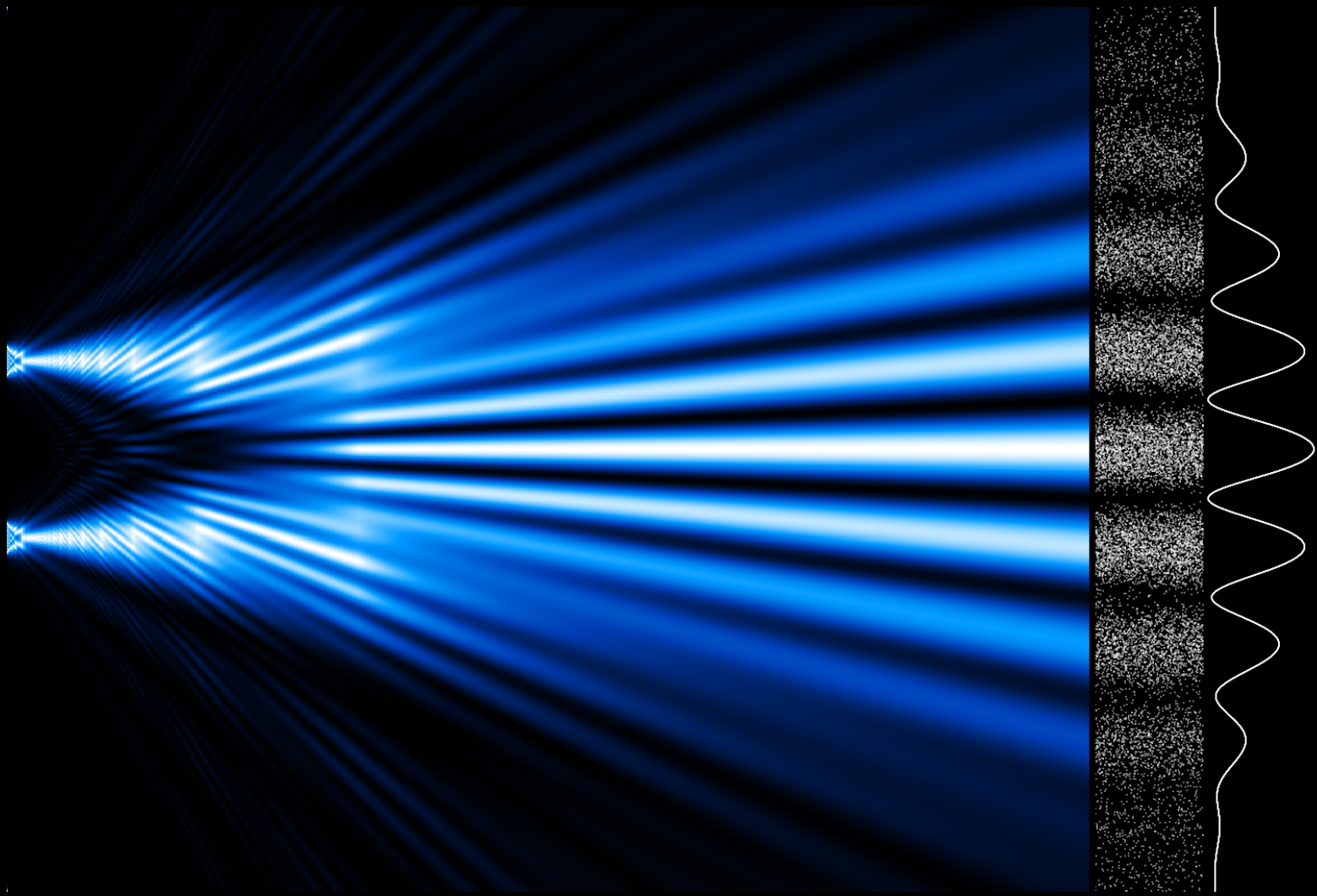
1858 – 1947

L'expérience de Young

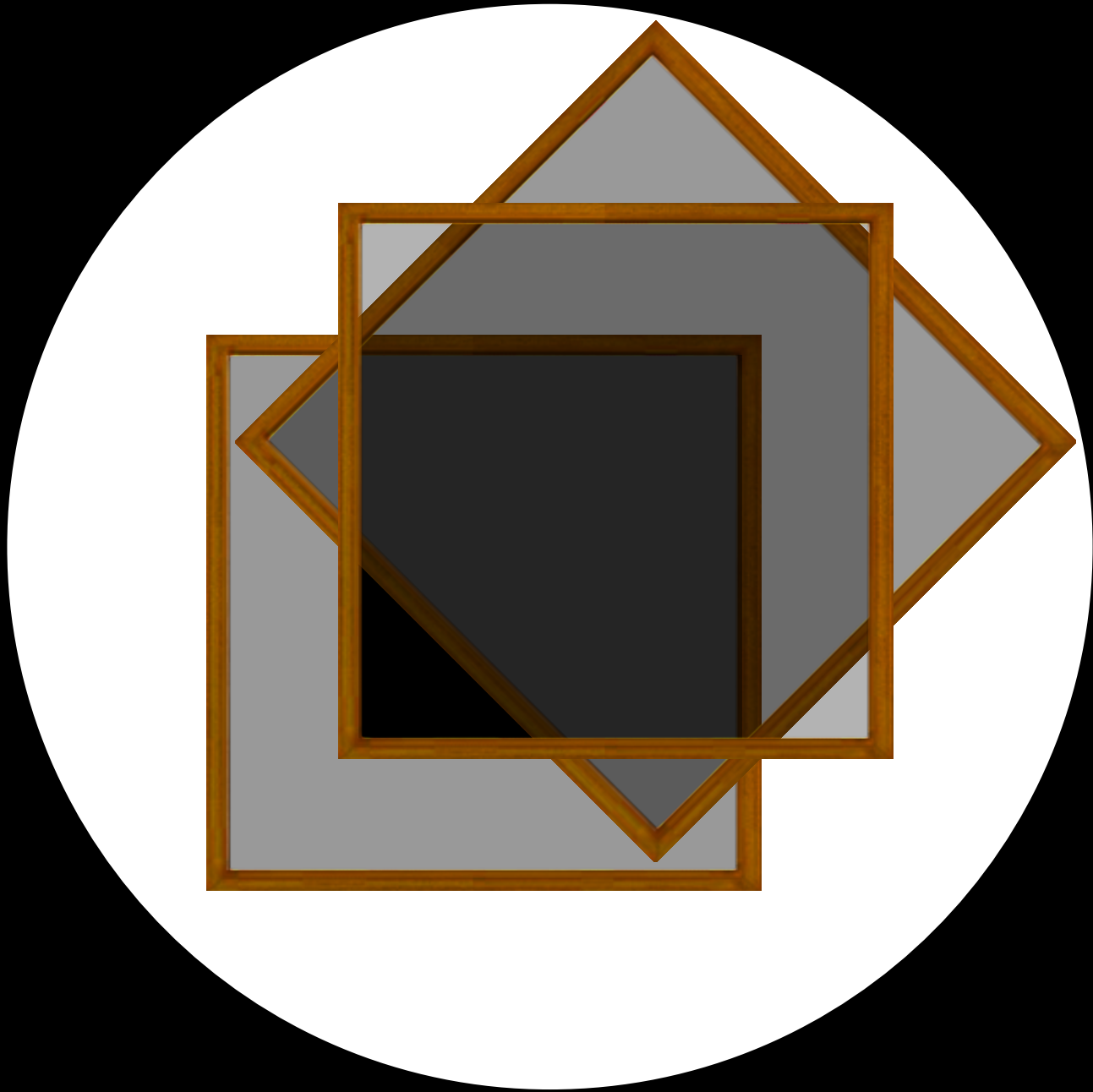


Thomas Young
1773 – 1829

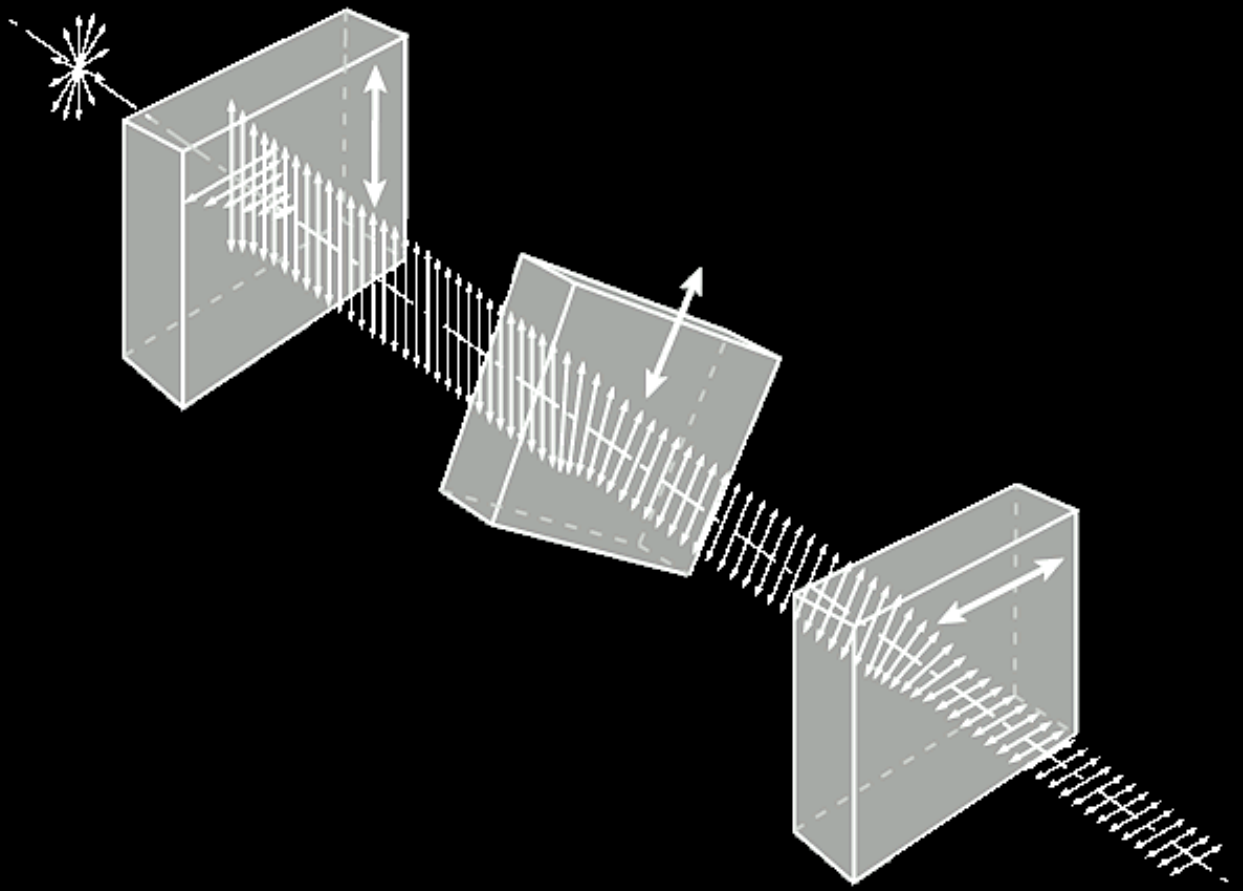
L'expérience de Young

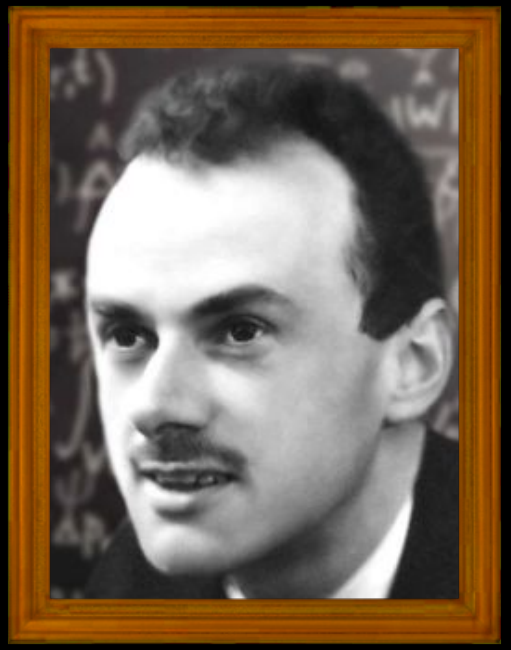


Polarisateurs de Dirac



Polarisateurs de Dirac





Paul Dirac
1902 – 1984

Formalisme de la mécanique quantique

Werner Heisenberg
1901 – 1976

Fonction d'onde

Un système physique est décrit par une fonction d'onde ψ dans un espace de Hilbert

une particule: $\psi : \mathbb{R}^3 \to \mathbb{C}$

polarisation: $\psi = \alpha \,|\uparrow\rangle + \beta \,|\rightarrow\rangle$

Intrication

Les interactions entre systèmes physiques sont modélisées par le produit tensoriel des espaces de Hilbert sous-jacents

particule polarisée: $\psi = \psi_1 \,|\uparrow\rangle + \psi_2 \,|\rightarrow\rangle$

deux particules: $\psi : \mathbb{R}^6 \to \mathbb{C}$

deux polarisations: $\psi = \alpha \,|\uparrow\uparrow\rangle + \beta \,|\uparrow\rightarrow\rangle + \gamma \,|\rightarrow\uparrow\rangle + \delta \,|\rightarrow\rightarrow\rangle$

Le formalisme de la mécanique quantique

Erwin Schrödinger
1887 – 1961

Evolution

L'évolution d'un système physique suit l'équation de Schrödinger:

$$i\hbar \frac{d\psi}{dt} = H\,\psi$$

Mesures

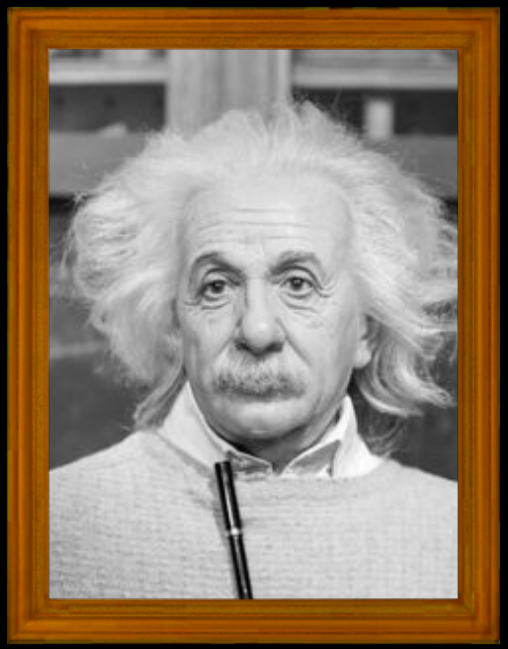
Une mesure est modélisée par un observable
qui est un opérateur auto-adjoint de l'espace de Hilbert sous-jacent

Le résultat de la mesure est une valeur propre de cet opérateur

La probabilité que ce résultat soit observé est la norme de
la projection de la foncteur d'onde sur l'espace propre correspondant

Après la mesure, la foncteur d'onde est remplacée par sa projection

Le paradoxe EPR



Albert Einstein
1879 – 1955

Boris Podolsky
1896 – 1966

Nathan Rosen
1909 – 1995

Le paradoxe EPR

$$\frac{|\uparrow\uparrow\rangle + |\rightarrow\rightarrow\rangle}{\sqrt{2}}$$

2ème partie

Modélisation de l'ordinateur quantique

L'idée de l'ordinateur quantique

Richard Feynman
1918 – 1988

Polarisation d'un photon :

$$\alpha \left| \uparrow \right\rangle + \beta \left| \rightarrow \right\rangle$$

Polarisation de deux photons :

$$\alpha \left| \uparrow \uparrow \right\rangle + \beta \left| \uparrow \rightarrow \right\rangle + \gamma \left| \rightarrow \uparrow \right\rangle + \delta \left| \rightarrow \rightarrow \right\rangle$$

Polarisation de trois photons :

$$\alpha_0 \left| \uparrow \uparrow \uparrow \right\rangle + \alpha_1 \left| \uparrow \uparrow \rightarrow \right\rangle + \alpha_2 \left| \uparrow \rightarrow \uparrow \right\rangle + \alpha_3 \left| \uparrow \rightarrow \rightarrow \right\rangle$$
$$+ \alpha_4 \left| \rightarrow \uparrow \uparrow \right\rangle + \alpha_5 \left| \rightarrow \uparrow \rightarrow \right\rangle + \alpha_6 \left| \rightarrow \rightarrow \uparrow \right\rangle + \alpha_7 \left| \rightarrow \rightarrow \rightarrow \right\rangle$$

Polarisation de *n* photons :

$$\alpha_0 \left| \uparrow \ldots \uparrow \uparrow \right\rangle + \alpha_1 \left| \uparrow \ldots \uparrow \rightarrow \right\rangle + \cdots + \alpha_{2^n-1} \left| \rightarrow \ldots \rightarrow \rightarrow \right\rangle$$

L'idée de l'ordinateur quantique

Richard Feynman
1918 – 1988

1-qubit:

$$\alpha\,|0\rangle + \beta\,|1\rangle$$

2-qubit:

$$\alpha\,|0\;0\rangle + \beta\,|0\;1\rangle + \gamma\,|1\;0\rangle + \delta\,|1\;1\rangle$$

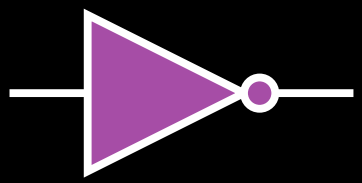
3-qubit:

$$\alpha_0\,|0\;0\;0\rangle + \alpha_1\,|0\;0\;1\rangle + \alpha_2\,|0\;1\;0\rangle + \alpha_3\,|0\;1\;1\rangle + \alpha_4\,|1\;0\;0\rangle + \alpha_5\,|1\;0\;1\rangle + \alpha_6\,|1\;1\;0\rangle + \alpha_7\,|1\;1\;1\rangle$$

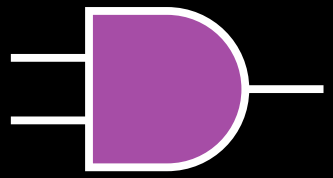
n-qubit:

$$\alpha_0\,|0\;\ldots\;0\;0\rangle + \alpha_1\,|0\;\ldots\;0\;1\rangle + \cdots + \alpha_{2^n-1}\,|1\;\ldots\;1\;1\rangle$$

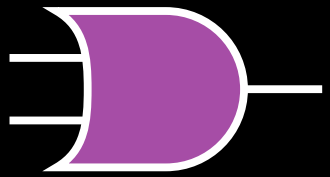
Portes logiques



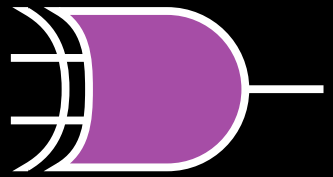
NOT



AND

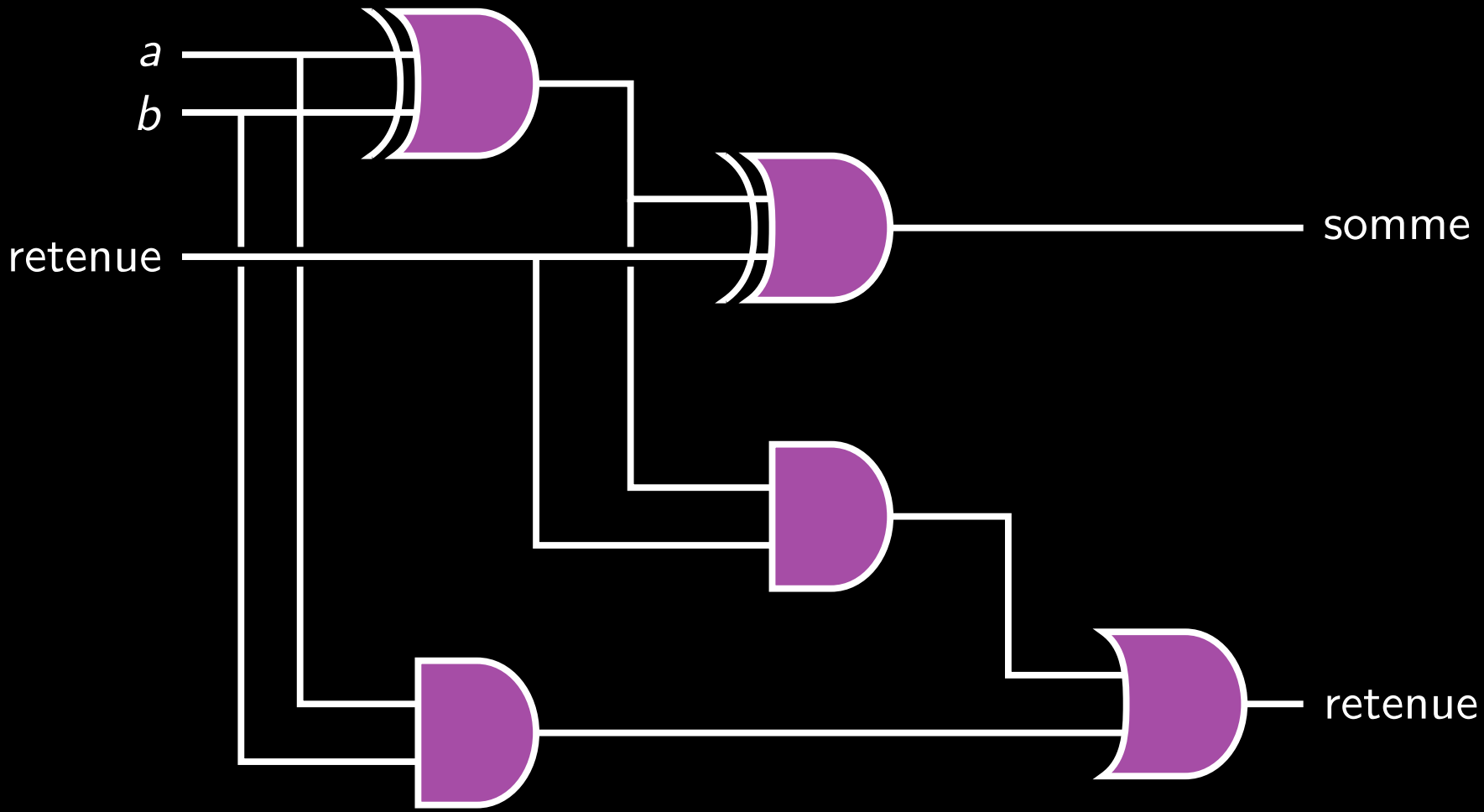


OR



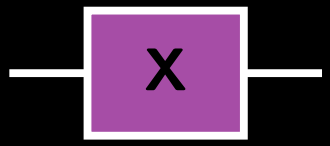
XOR

Circuits



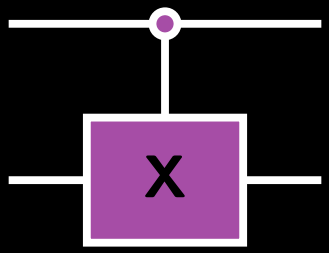
Portes logiques quantiques

NOT



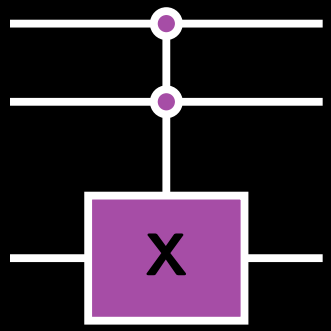
$|0\rangle \mapsto |1\rangle$
$|1\rangle \mapsto |0\rangle$

Controlled-NOT



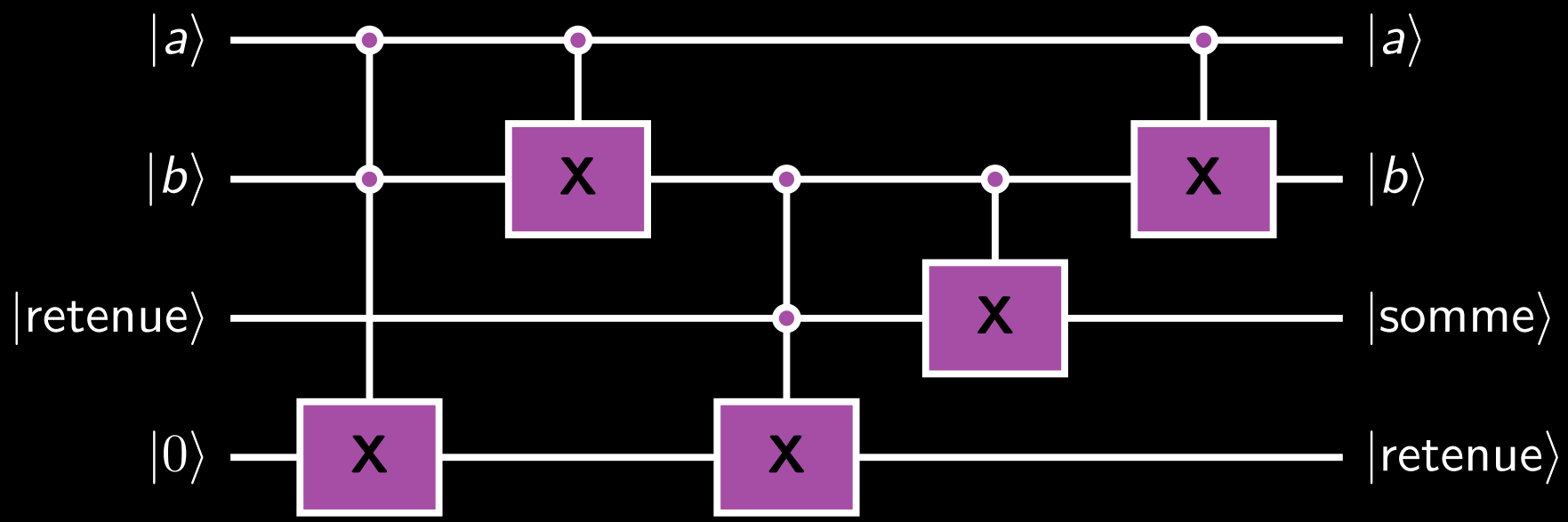
$|00\rangle \mapsto |00\rangle$
$|01\rangle \mapsto |01\rangle$
$|10\rangle \mapsto |11\rangle$
$|11\rangle \mapsto |10\rangle$

Toffoli



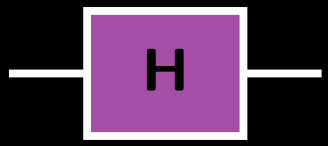
$|000\rangle \mapsto |000\rangle$
$|001\rangle \mapsto |001\rangle$
$|010\rangle \mapsto |010\rangle$
$|011\rangle \mapsto |011\rangle$
$|100\rangle \mapsto |100\rangle$
$|101\rangle \mapsto |101\rangle$
$|110\rangle \mapsto |111\rangle$
$|111\rangle \mapsto |110\rangle$

Circuits quantiques



D'autres portes quantiques

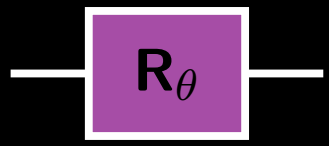
Hadamard



$$|0\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|1\rangle \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

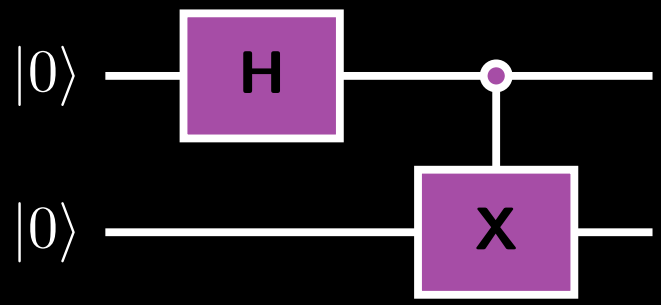
Phase shift



$$|0\rangle \mapsto |0\rangle$$

$$|1\rangle \mapsto e^{i\theta}\,|1\rangle$$

Le circuit EPR



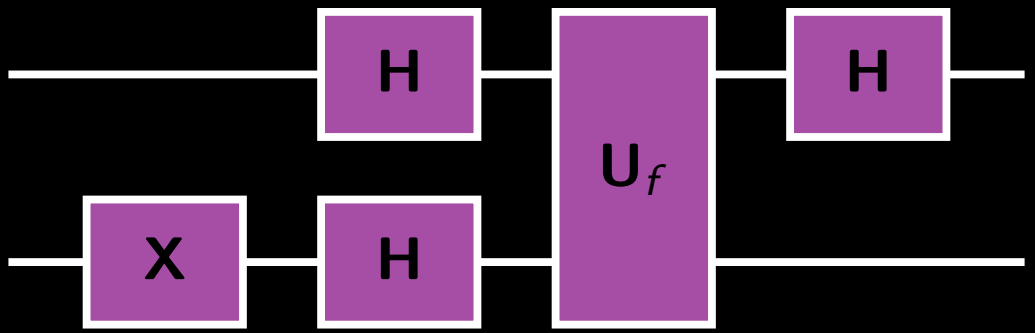
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

L'algorithme de Deutsch

Soit $f : \mathbb{Z} \to X$
Soit $a, b \in \mathbb{Z}$

On peut décider si $f(a) = f(b)$
en évaluant une unique fois la fonction f

David Deutsch
1953 –

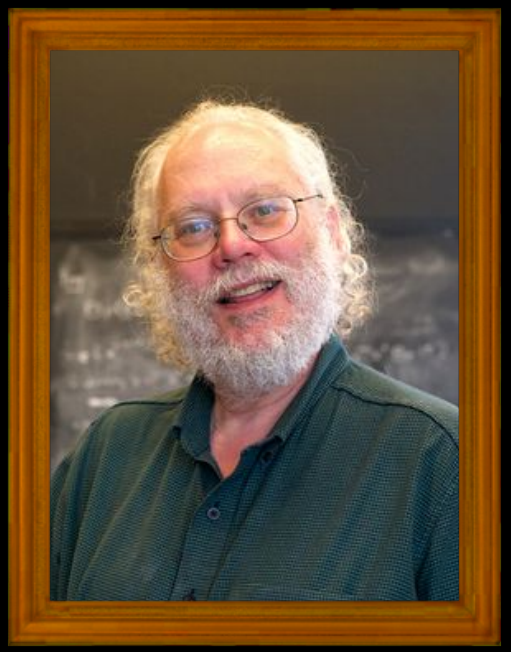


L'algorithme de Shor

Soit $f : \mathbb{Z} \to X$ périodique de période n

On suppose que $f(1), \ldots, f(n)$
sont deux à deux distincts

On peut calculer n en au plus
$O(\log n)$ appels à la fonction f



Peter Shor
1959 –

Applications

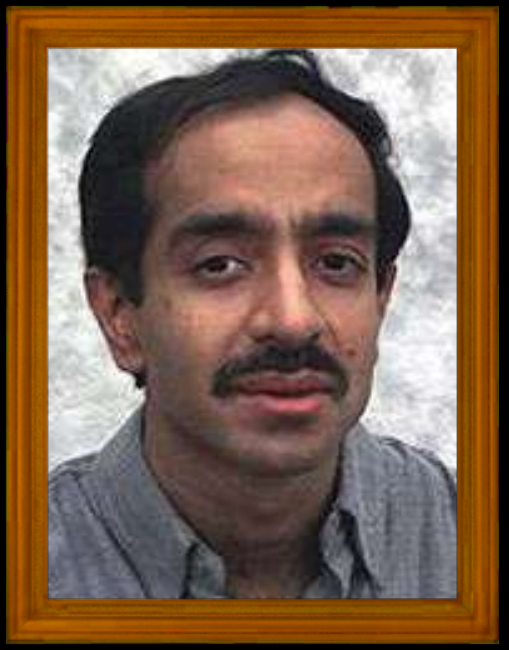
- ☞ Calcul du caridnal d'un groupe commutatif
- ☞ Factorisation des entires
- ☞ Calcul de logarithmes discrets

L'algorithme de Grover

On se donne:

- ✔ un algorithme classique qui résout un problème donné avec probabilité $\varepsilon > 0$
- ✔ un algorithme classique qui vérifie si un certain candidat est solution du problème

Alors, on peut trouver une solution du problème en appelant $O(\varepsilon^{-1/2})$ fois ces routines



Lov Grover
1961 –

Applications

- ☞ Calcul de l'image inverse par une fonction
- ☞ Recherche de collisions

3ème partie

Construction d'un ordinateur quantique

Emulateurs

ProjectQ

```
X | x[0]
measurements = [0] * (2 * n) # will hold the 2n measurement results
ctrl_qubit = eng.allocate_qubit()
for k  in range(2 * n):
    current_a = pow(a, 1 << (2 * n - 1 - k), N)
    # one iteration of 1-qubit QPE
    H | ctrl_qubit
    with Control(eng, ctrl_qubit):
        MultiplyByConstantModN(current_a, N) | x
    # perform inverse QFT -> Rotations conditioned on previous outcomes
    for i in range(k):
        if measurements[i]:
            R(-math.pi / (1 << (k - i))) | ctrl_qubit
H | ctrl_qubit
```

Les difficultés

- ☞ La manipulation de qubits intriqués est difficile

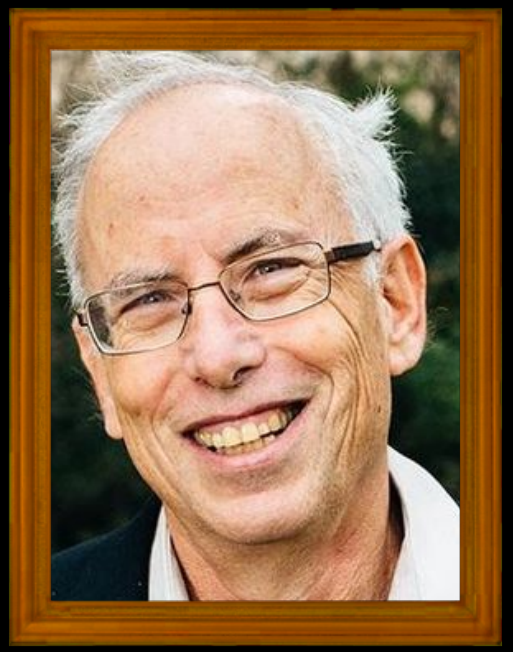
  $\Longrightarrow$ la mémoire est limitée !

- ☞ Garder un système quantique stable pendant un temps prolongé est difficile

  $\Longrightarrow$ la complexité est limitée !

- ☞ Permettre des interactions avec l'environnement semble incompatible avec les axiomes de la mécanique quantique

  $\Longrightarrow$ la programmation est limitée !

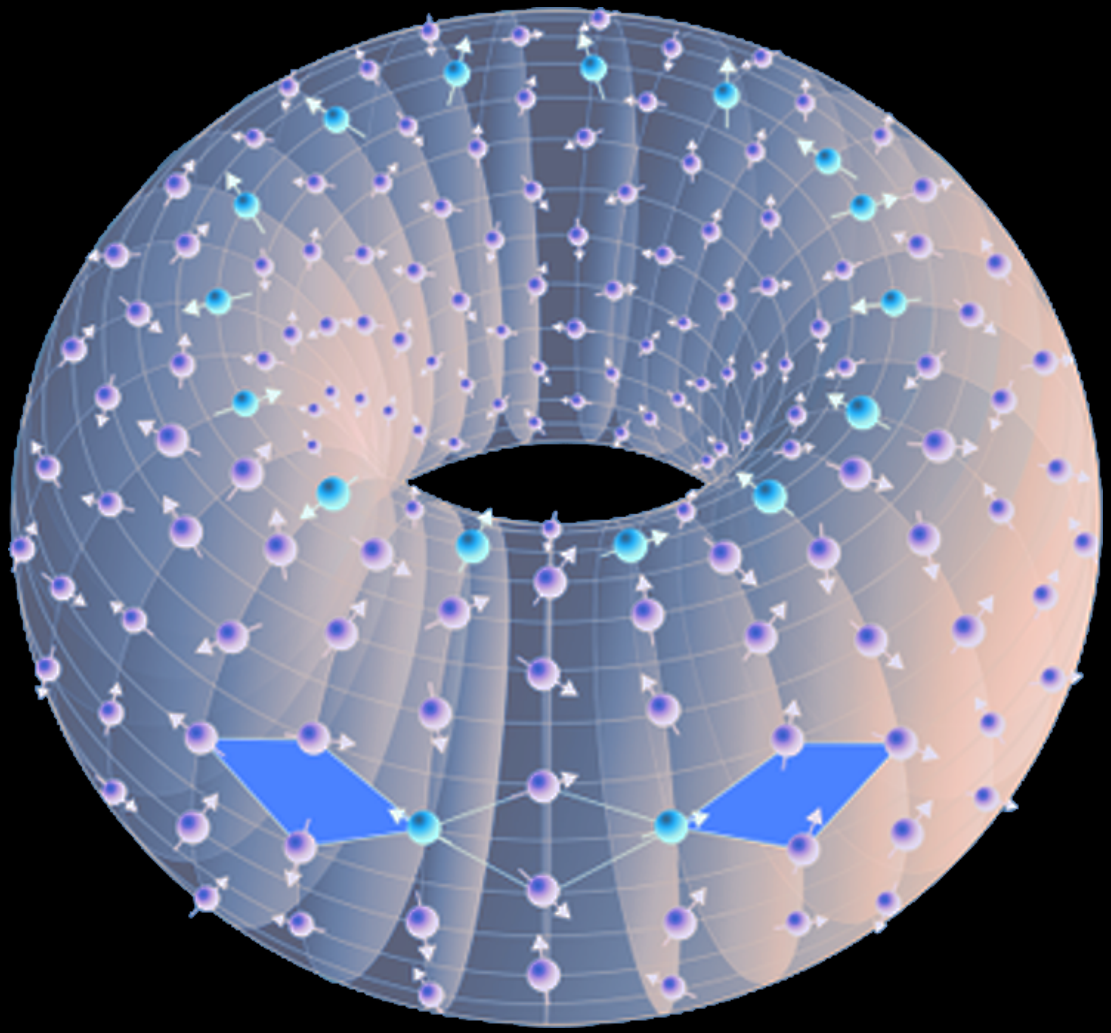


Gil Kalai
1955 –

Est-ce qu'un ordinateur quantique peut résoudre un problème qui est insoluble avec un ordinateur classique ?

[Suprématie quantique]

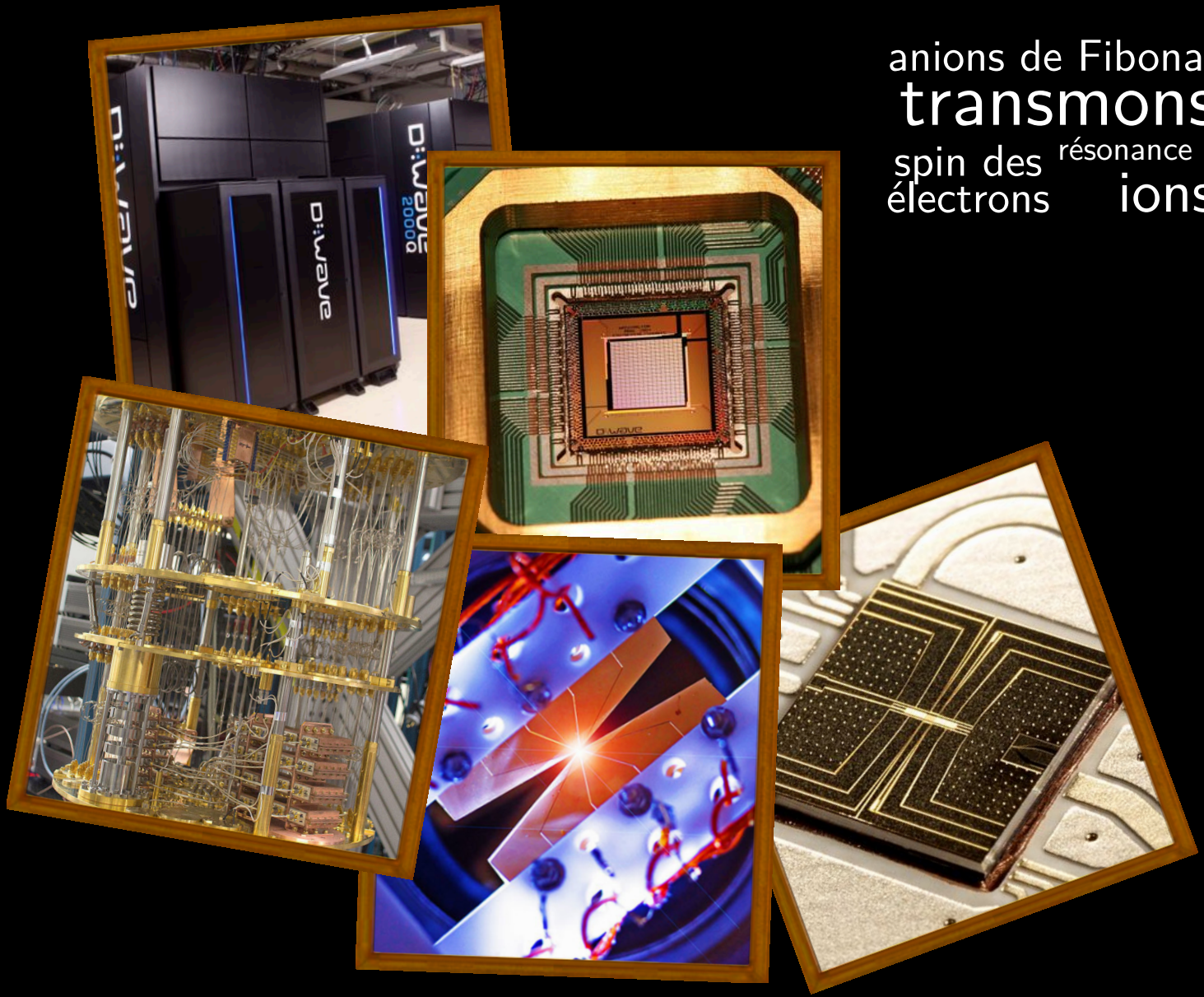
Codes correcteurs d'erreurs quantiques



Alexei Kitaev

1963 –

De nombreux essais



anions de Fibonacci
jonction de Josephson
transmons
spin des électrons
résonance magnétique nucléaire
ions piégés

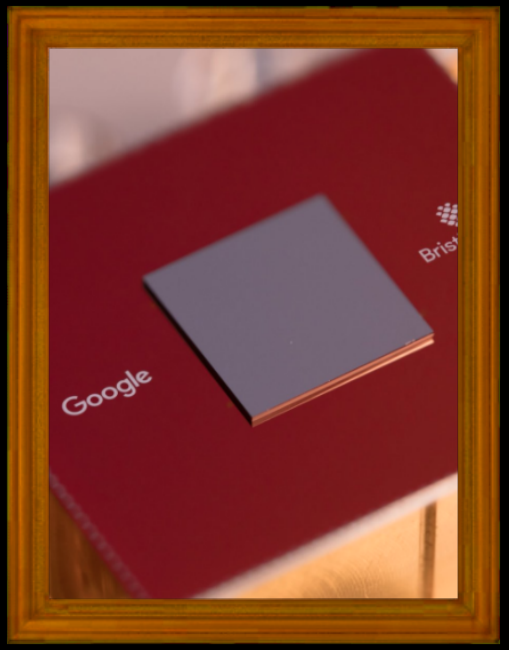
Vers la suprématie quantique

Characteristics

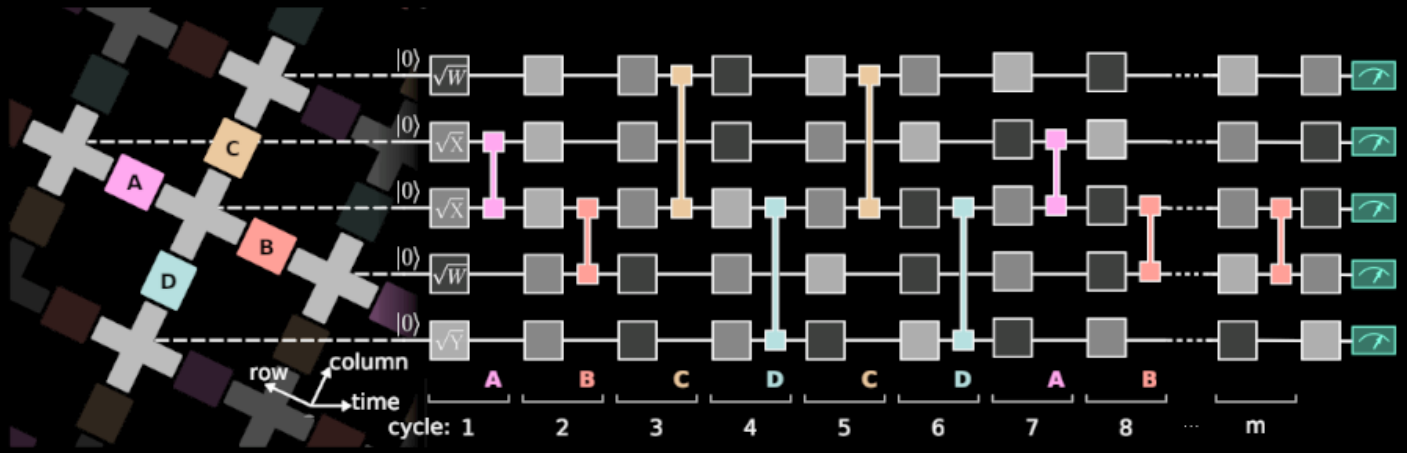
- ☞ 53 qubits
- ☞ 86 couplages

Performances

- ☞ 1113 portes à 1 qubit
- ☞ 430 portes à 2 qubits
- ☞ fiabilité estimée à 0.2%



Sycamore
2019 –



|Merci pour votre attention⟩