Algorithmique quantique :
Des fondements aux dernières applications

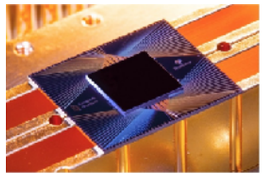
Frédéric Magniez

INSTITUT
DE RECHERCHE
EN INFORMATIQUE
FONDAMENTALE

Université Paris Cité

cnrs

Suprématie quantique



2019-2021

Stratégie nationale

4 janvier 2022

Quelle accélération ?

Thèse de Church-Turing

- Calculabilité

  Ce qui est calculable est indépendant des machines actuelles et futures

  Les progrès technologiques permettent d'augmenter uniquement vitesse et quantité de ressources (mémoire, processeurs, …)

- Non remise en cause par l'ordinateur quantique

Variante quantitative

- Complexité

  Les accélérations sont au plus

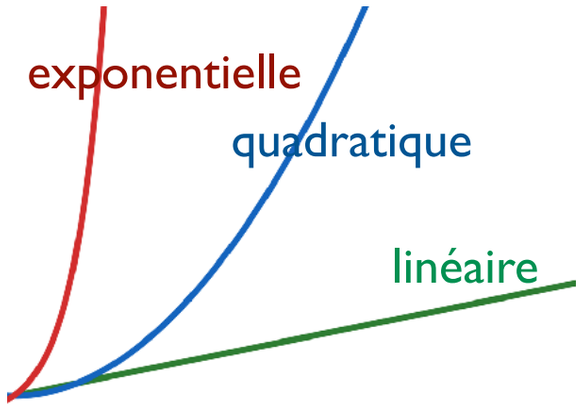
  linéaires : $t \mapsto t/1000$

  quadratiques : $t \mapsto \sqrt{t}, \quad t^2 \mapsto t$

  polynomiales : $t^{1000} \mapsto t$

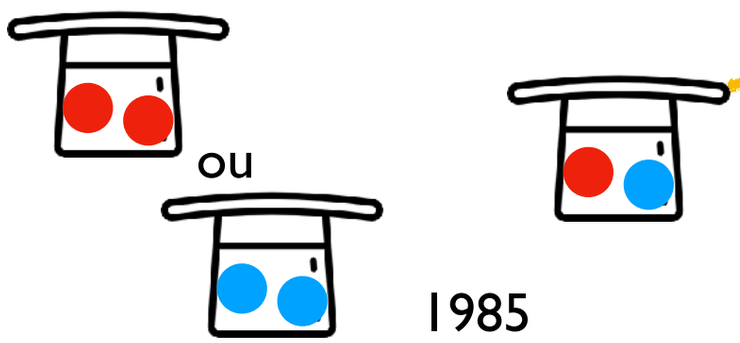
  mais pas exponentielles : $2^t \mapsto t$

- Thèse "contredite" par l'ordinateur quantique



Pourquoi de nouveaux algorithmes ?

Des algorithmes découverts sans ordinateur



1985

QUANTUM

~~1940~~ 1994 - …

1996 - …

$$\begin{cases} 2x + 3x - z = 6 \\ x - z + 7z = 4 \\ -x + 2z + 3z = 2 \end{cases}$$

2009 - …

2013 - …

Information quantique

Etat quantique

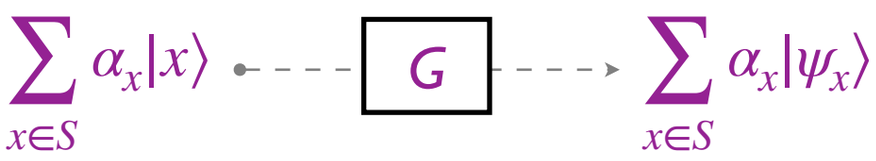
Superposition

- S ensemble d'états classiques
- Vecteur unitaire à |S| coordonnées complexes $(\alpha_x)_{x\in S}$

$$|\psi\rangle = \sum_{x\in S} \alpha_x |x\rangle, \quad \text{avec} \sum_{x\in S} |\alpha_x|^2 = 1$$

Mesure

Transformation unitaire

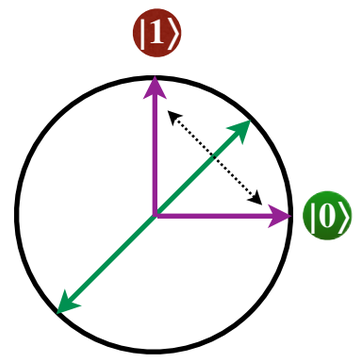


Exemples de transformation

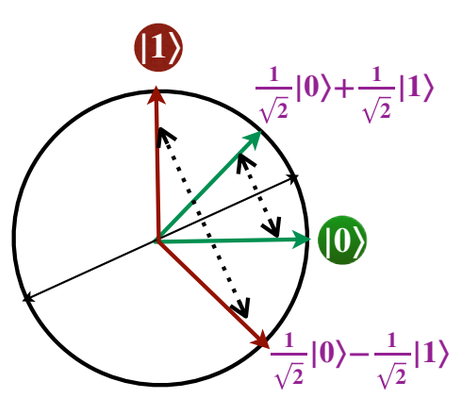
Transformations sur 1-qubit

- Identité : “rien”

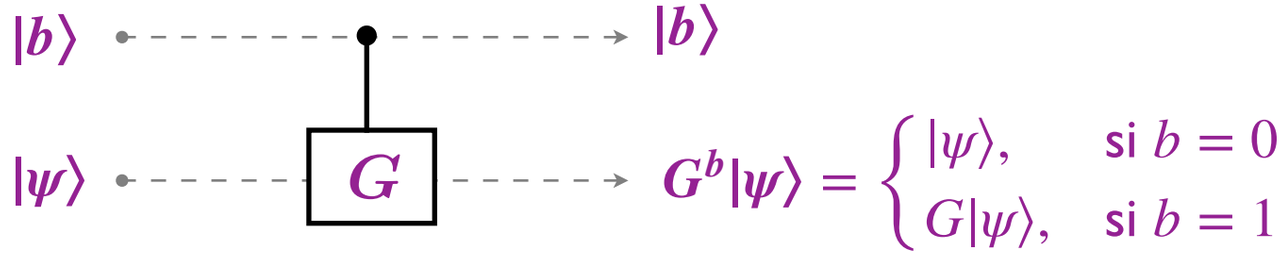
- Négation : symétrie à $\pi/4$ (45°)



- Porte de Hadamard : symétrie à $\pi/8$ (22,5°)



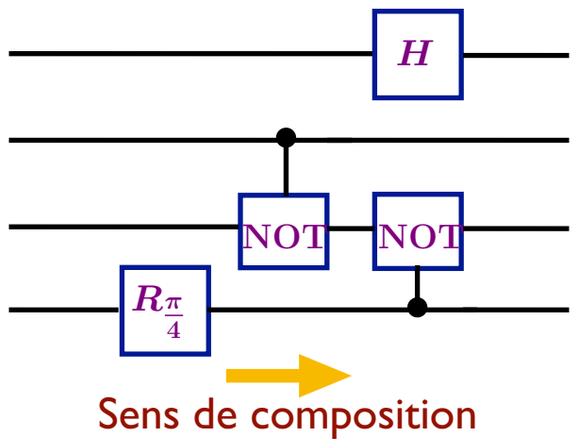
“IF-THEN-ELSE” quantique



Algorithmes quantiques ?

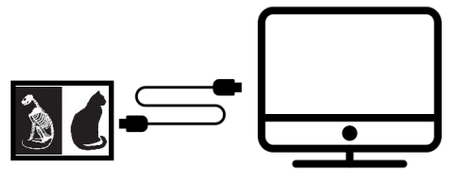
Circuits quantiques

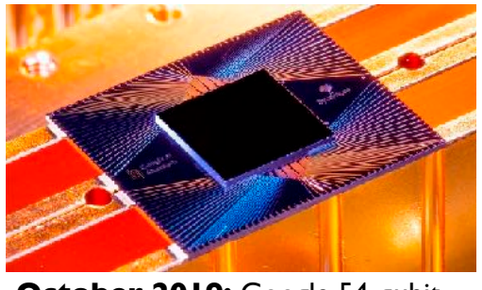
- Une porte quantique est une transformation unitaire sur au plus 3 qubits
- Un circuit quantique est la composition de portes
- Complexités : taille (nb de portes) et profondeur



Programmation de circuits quantiques

- Description à la charge d'un algorithme classique
- Interactions possibles entre algorithme et circuit
- Modèle proche de certaines expériences





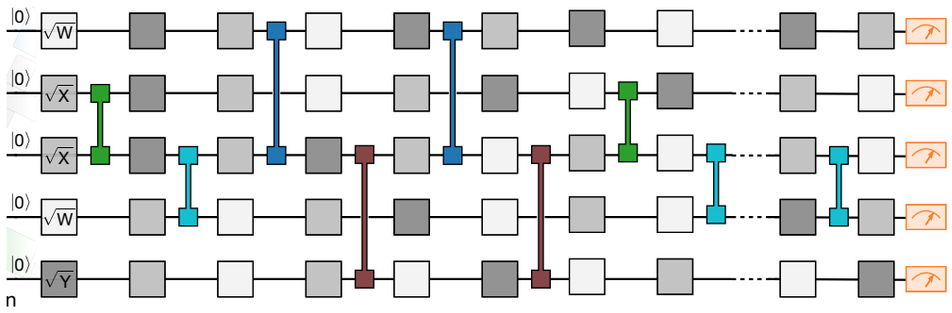
October 2019: Google 54-qubit processor, named "Sycamore"

December 2020: An IBM Quantum Hummingbird r2 Processor (65 qubits).

Quelle était cette prouesse de Google ?

L'expérience de Google 2019 puis de USTC 2021

- Un gigantesque dé non équilibré
- Un dé simulant un circuit quantique



Quelle difficulté ?

- Plusieurs milliers d'années sur nos ordinateurs dès 50 qubits
- Instantané pour la machine quantique de Google / USTC
- MAIS

  Difficile à vérifier

  Avec des imperfections : plus facile à réaliser avec nos ordinateurs

  Suprématie nécessite 70-80 qubits ou une meilleure précision

Dans quel but ?

Premiers algorithmes

Problème de Deutsch - 1985

Problème à Oracle

- L'oracle possède

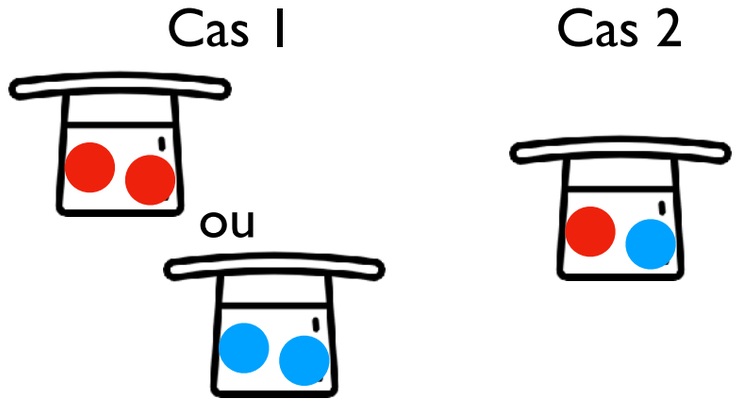
  $f : \{0,1\} \rightarrow \{0,1\}$

- Question possible

  Que vaut $f(0)$? $f(1)$?

- Tâche

  Décider si $f(0)=f(1)$



Classiquement

- 2 questions sont nécessaires

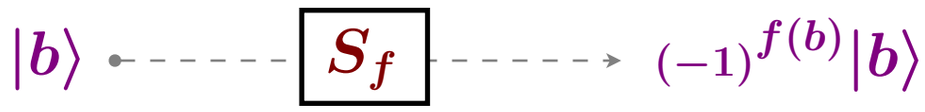
Quantiquement

- 1 seule question en superposition suffit

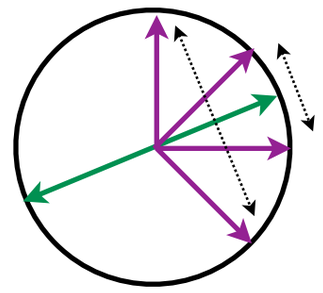
Solution quantique

$x \mapsto f(x)$ peut ne pas être réversible !

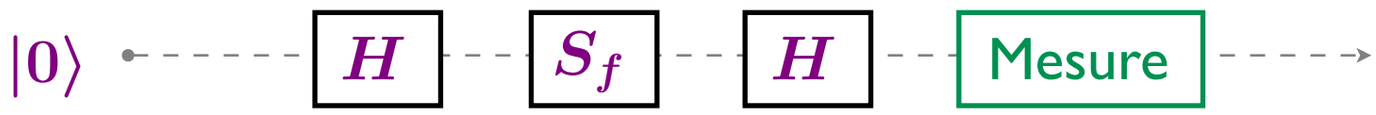
Implémentation quantique de *f*



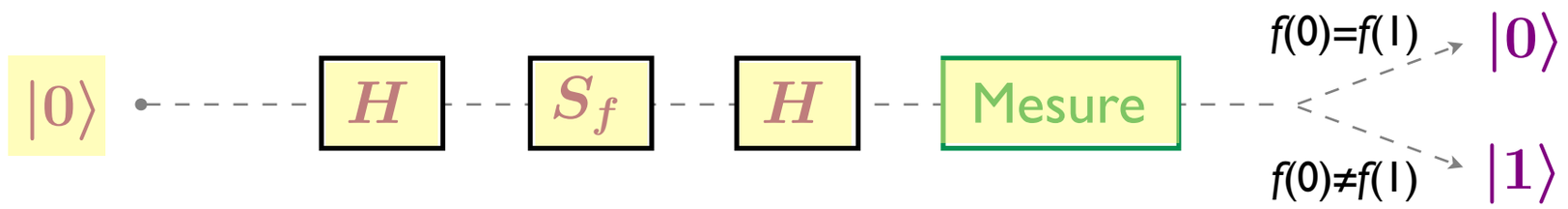
Porte de Hadamard



Circuit quantique



Analyse



Initialisation : $|0\rangle$

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

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

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

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

Problème de Deutsch-Jozsa 1992

Problème à Oracle

- L'oracle possède

  $f : \{0,1\}^n \to \{0,1\}$ constante ou équilibrée

- Question possible

  Que vaut f(x) ?

- Tâche

  Décider si *f* est constante ou équilibrée

Solutions

- $1 + 2^{n-1}$ questions classiques sont nécessaires
- 1 question quantique en superposition suffit

  mais il faut *n* bits quantiques…

- Mais $\log(1/\varepsilon)$ questions probabilistes suffisent pour garantir une erreur d'au plus ε

Exemple : $n = 4$

$f(0000) \stackrel{?}{=} 0$
$f(0001) \stackrel{?}{=} 0$
$f(0010) \stackrel{?}{=} 1$
$f(0011) \stackrel{?}{=} 0$
$f(0100) \stackrel{?}{=} 1$
$f(0101) \stackrel{?}{=} 1$
$f(0110) \stackrel{?}{=} 1$
$f(0111) \stackrel{?}{=} 0$
$f(1000) \stackrel{?}{=} 0$
$f(1001) \stackrel{?}{=} 1$
$f(1010) \stackrel{?}{=} 0$
$f(1011) \stackrel{?}{=} 1$
$f(1100) \stackrel{?}{=} 1$
$f(1101) \stackrel{?}{=} 0$
$f(1110) \stackrel{?}{=} 1$
$f(1111) \stackrel{?}{=} 0$

Bernstein-Vazirani 1993

Problème

- Oracle : $f : \{0,1\}^n \to \{0,1\}$ une fonction

  telle que $f(x) = a \cdot x = \sum_i a_i x_i \mod 2$

  pour une valeur $a \in \{0,1\}^n$ fixée mais inconnue
- Sortie : a

Solutions

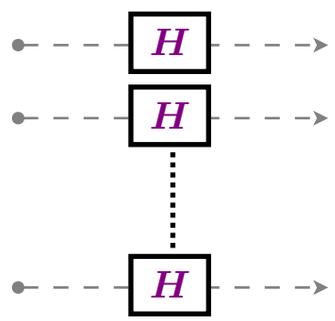
- Probabiliste : n

  Requêtes $f(0^{i-1}10^{n-i}) = a_i$, pour i=1,2,...,n
- Quantique : 1
- Application : Calcul de gradient en une étape au lieu d'un nombre linéaire en la dimension en classique [Jordan 2005]

Solution quantique

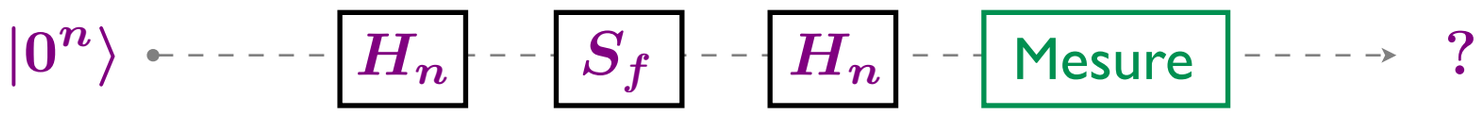
Transformée de Fourier quantique (mod 2)

$H_n =$

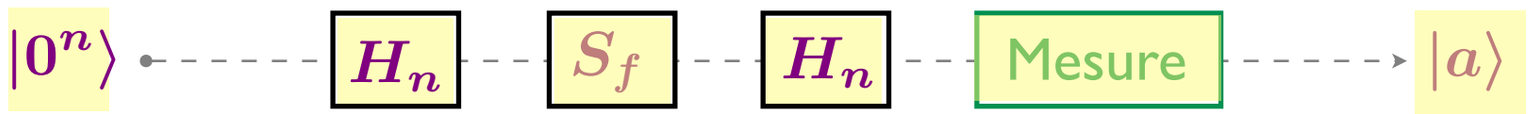


$$H_n|x\rangle = \frac{1}{2^{n/2}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle \qquad \text{où} \quad x\cdot y = \sum_{i=1}^{n} x_i y_i$$

Circuit quantique



Analyse



Initialisation : $|00\ldots0\rangle$

Parallélisation : $\frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle$

Evaluation de f : $\frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} (-1)^{a\cdot x}|x\rangle = H_n|a\rangle$

Interférences : $(H_n)^2|a\rangle$

Etat final : $|a\rangle$

Des applications

Traquer la période

Daniel Simon, 1994

- Trouver la période d'une fonction $f : \{0,1\}^n \to \{0,1\}^n$
- Classique : nombre exponentiel de questions
- Quantique : nombre linéaire de questions

  Ingrédient : Transformée de Fourier quantique (mod 2)
- Article d'abord refusé, mais…

Peter Shor, 1994

- Trouver la période d'une fonction $f : \mathbb{Z} \to \mathbb{Z}_N$
- Applications (sans oracle)

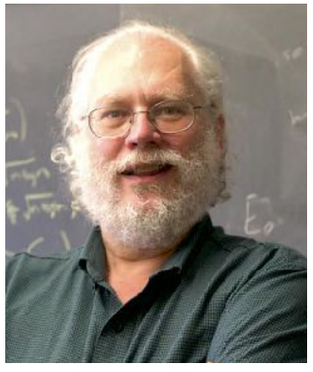
  Factorisation, calcul log discret

  Cryptographie post-quantique
- Ingrédients

  Construction explicite d'une fonction

  Transformée de Fourier quantique (mod *N*)

  Estimation de phase quantique



Peter Shor

Estimation de phase

Problème

- Entrée

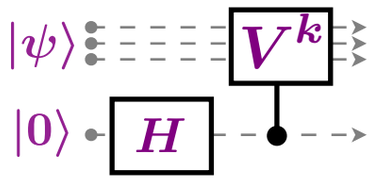
  Transformation unitaire V avec ses "portes" c-V^k pour $k=1,2,\ldots,2^{m-1}$

  Un état quantique $|\psi\rangle$ tel que $V|\psi\rangle = e^{i\alpha}|\psi\rangle$

- Sortie

  La valeur de $\alpha/(2\pi)$ à m bits de précision près

Circuit quantique [Kitaev'95] [Cleve, Ekert, Macchiavello, Mosca'98]



$$\frac{1}{\sqrt{2}}(|\psi\rangle|0\rangle + V^k|\psi\rangle|1\rangle) = \frac{1}{\sqrt{2}}(|\psi\rangle|0\rangle + e^{ik\alpha}|\psi\rangle|1\rangle) = |\psi\rangle\frac{1}{\sqrt{2}}(|0\rangle + e^{ik\alpha}|1\rangle)$$

Estimation de phase

Problème

- Entrée

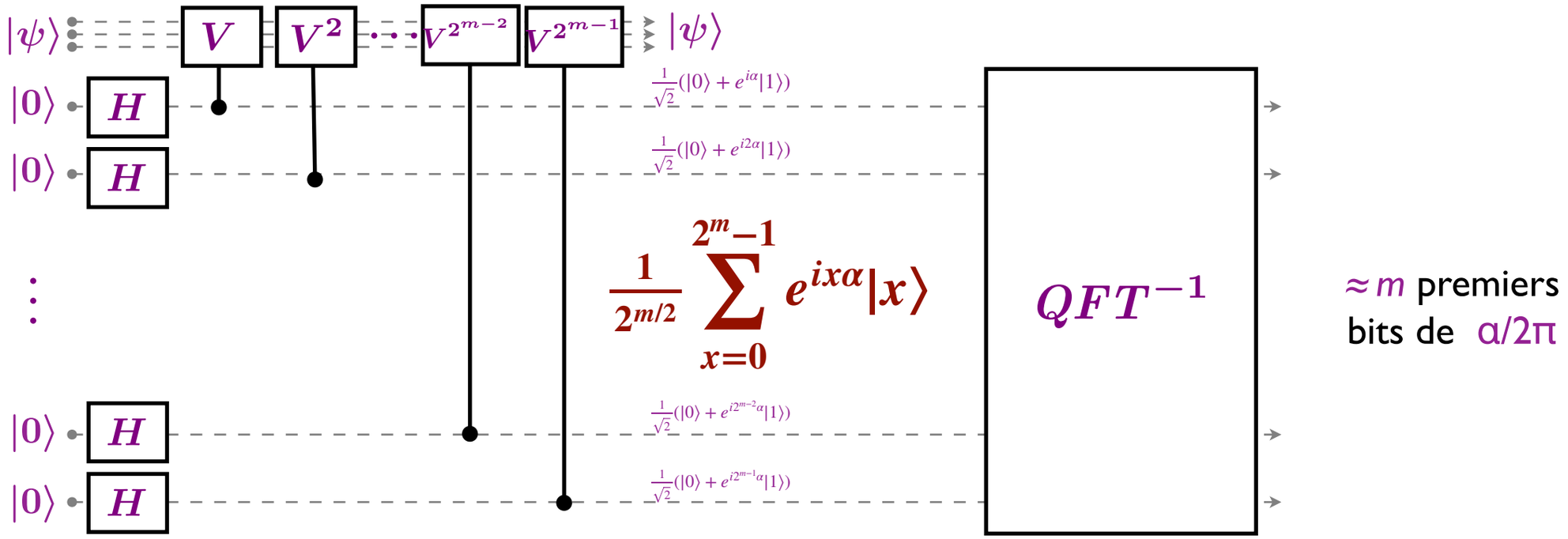
  Transformation unitaire V avec ses "portes" c-V^k pour $k=1,2,\ldots,2^{m-1}$

  Un état quantique $|\psi\rangle$ tel que $V|\psi\rangle = e^{i\alpha}|\psi\rangle$

- Sortie

  La valeur de $\alpha/(2\pi)$ à m bits de précision près

Circuit quantique [Kitaev'95] [Cleve, Ekert, Macchiavello, Mosca'98]



≈ m premiers bits de α/2π

Application : Systèmes linéaires

Système linéaire (quantique)

$$\begin{cases} a_{11}x_1 + a_{12}x_1 + \ldots + a_{1N}x_N = b_1 \\ a_{21}x_1 + a_{22}x_1 + \ldots + a_{1N}x_N = b_2 \\ \vdots \qquad\qquad\qquad\qquad\quad = \vdots \\ a_{N1}x_1 + a_{N2}x_1 + \ldots + a_{NN}x_N = b_N \end{cases}$$

- Entrée

  Un état quantique $|b\rangle$ sur n qubits

  Un circuit réalisant une matrice A unitaire de taille $2^n \times 2^n$

- Sortie

  Un état quantique (proche de) $|x\rangle$ solution de $A|x\rangle = |b\rangle$

- Algorithme pour A^{-1} i.e. tq $|\psi\rangle \mapsto e^{-i\alpha}|\psi\rangle$ lorsque $A|\psi\rangle = e^{+i\alpha}|\psi\rangle$

  Estimation de phase : $|\psi\rangle|0\rangle \mapsto |\psi\rangle|\alpha\rangle$

  Inversion de phase: $|\psi\rangle|0\rangle \mapsto e^{-i\alpha}|\psi\rangle|\alpha\rangle$

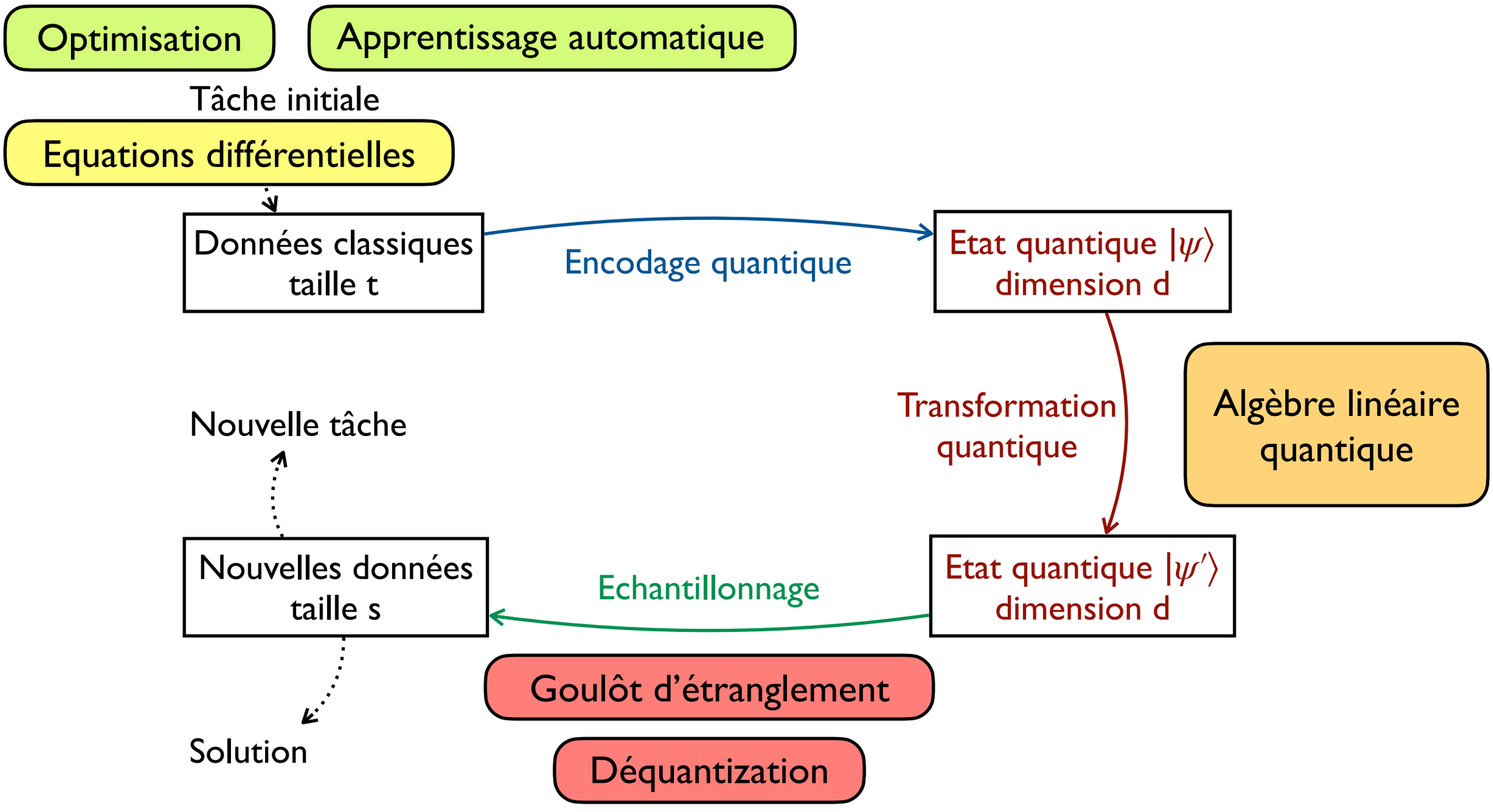
  Estimation de phase inversée : $e^{-i\alpha}|\psi\rangle|\alpha\rangle \mapsto e^{-i\alpha}|\psi\rangle|0\rangle$

Avantages

- Exponentiel en n
- Exponentiel en l'approximation
- Mais… que faire de $|x\rangle$?

  Echantillonnage / Tomographie : mais déquantization possible !

Structure d'un algorithme quantique



Simulation hamiltionienne

Simulation quantique

Equation de Schrödinger

$$i\frac{d|\psi(t)\rangle}{dt} = H|\psi(t)\rangle \qquad \text{(convention } \hbar = 1\text{)}$$

admet pour solution $|\psi(t)\rangle = e^{-itH}|\psi(0)\rangle$ (e^{-itH} est unitaire)

Objectif

- Entrée
  - Système physique régit par un Hamiltonien H
  - Etat initial $|\psi(0)\rangle$
- Simuler l'évolution du système après un temps t : $|\psi(t)\rangle = e^{-itH}|\psi(0)\rangle$

Enjeux

- Simuler un système physique sur un autre
- Préparer des états, mesurer l'énergie…
- Applications : chimie, matériaux, physique des particules, …

Pourquoi est-ce difficile ? 1/2

Ordinateur quantique

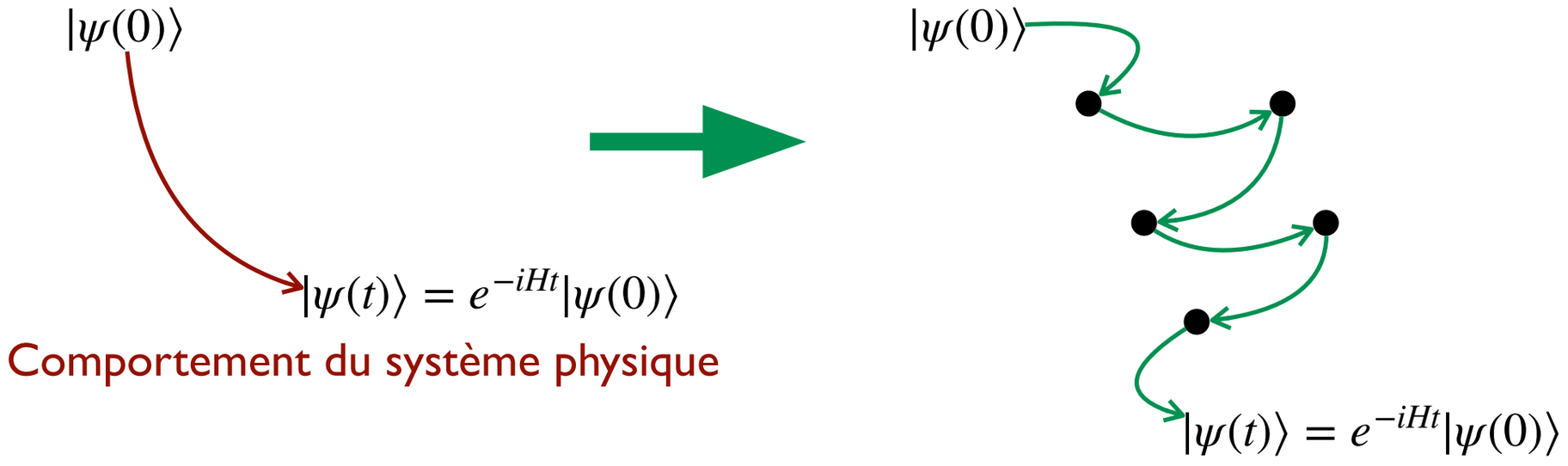
- Pourquoi ne pas construire directement un calculateur quantique qui suit l'hamiltonien à simuler ?

  C'est toute la différence entre un calculateur et un ordinateur

- Objectif :

  Construire un algorithme quantique qui simule tout hamiltonien !

Simulation non directe



Pourquoi est-ce difficile ? 2/2

Difficulté calculatoire

- Même si H possède une représentation simple
- En général $U = e^{-iH}$ n'a plus de telle représentation

$$e^{-iH} = \mathrm{Id} - iH + \frac{1}{2}H^2 + \ldots + \frac{(-i)^j}{j!}H^j + \ldots$$

Approche

- Hypothèse : $H = \sum_{j=1}^{m} H_j$ sur n qubits avec

  e^{-itH_j} facilement réalisable (circuit de taille poly(n))

  Somme de taille raisonnable (m = poly(n))
- Cas commutatif : $H_iH_j = H_jH_i$ alors $e^{-itH} = (e^{-iH_1} \times e^{-iH_2} \times \ldots e^{-iH_m})^t$

  Il suffit de composer les circuits pour chaque e^{-itH_j}
- Cas général : Plusieurs approches

  Formules produit de Lie-Suzuki-Trotter [Lloyd 1996]

  Marches quantiques [Berry, Childs 2012]

  …

  Quantum signal processing [Low, Chuang 2016]

Chimie quantique

Problème

- Calculer l'énergie minimale d'un Hamiltonien H (de description compacte)

$$E_0 = \min_{|\psi\rangle} \langle\psi|H|\psi\rangle$$

- Trop difficile, même pour un ordinateur quantique

Simplification

- Calculer E_0 connaissant un état quantique $|\psi\rangle$ *proche*

  d'un état d'énergie minimale $|\psi_0\rangle$

- Difficile pour un ordinateur classique avec bonne précision [arXiv:2111.09079]
- Facile pour un ordinateur quantique avec même précision

Solution

- Estimation de phase avec $V = e^{iH}$ et $|\psi\rangle$ [Abrams, Lloyd 1999]
- Réitérer plusieurs fois et garder la plus petite valeur

  Après quelques essais E_0 est mesuré
- Alternative :Variational Quantum Algorithms [arXiv:2012.09265]

Optimisation

Optimisation par amplification

Algorithme de Grover et extensions

- Recherche/optimisation par essais successifs [1995,2000]
- Recherche/optimisation par marches aléatoires [2007-…]

  T essais/étapes probabilistes $\rightarrow \sqrt{T}$ essais/étapes quantiques

Heuristiques

- Parcours arborescents [2017-…]

  Type Branch and bound, Backtracking éventuellement stochastique

  T étapes probabilistes $\rightarrow \sqrt{T}$ étapes quantiques
- Applications : SAT solver, Voyageur de commerce, …

Monte Carlo

- Utilisation d'estimateurs statistiques [2015-…]

  T échantillons probabilistes $\rightarrow \sqrt{T}$ échantillons quantiques

Optimisation continue [2004,2016-…]

- Convexe, descente de gradient, programmation linéaire, semi-définie

  Gain polynomial

Programmation dynamique

Principe

1. Décomposer un problème algorithmique en sous-problèmes,
2. Puis résoudre les sous-problèmes, des plus petits aux plus grands en stockant les résultats intermédiaires.

Version quantique [Ambainis et al 2019]

- Principe

  1. Précalculer des solutions pour une partie des sous-ensembles à l'aide de la programmation dynamique

  2. Puis utiliser la recherche de Grover sur le reste des sous-ensembles pour trouver la réponse au problème.

- Voyageur de commerce : calculer un plus court circuit qui passe une et une seule fois par n villes

  Temps quantique $\tilde{O}(1.728^n)$ vs $\tilde{O}(2^n)$ en classique

- Autres applications : Minimum Set Cover, Feedback Arc Set, …

Sparsification

Motivation

- Goulot d'étranglement : données massives
- Idée : Peut-on la compresser ?

  En général non

  Sauf avec perte d'informations

Cas des graphes

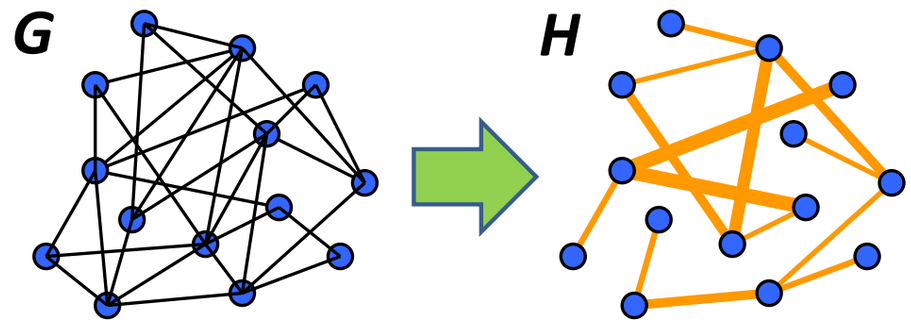
- Chaque graphe G à n nœuds et m arêtes

  peut être compresser en un graphe H à $O(n/\varepsilon^2)$ arêtes

  en temps $O(m)$
- Utilité :

  Algorithmes d'approximation

  Résolution de systèmes laplaciens

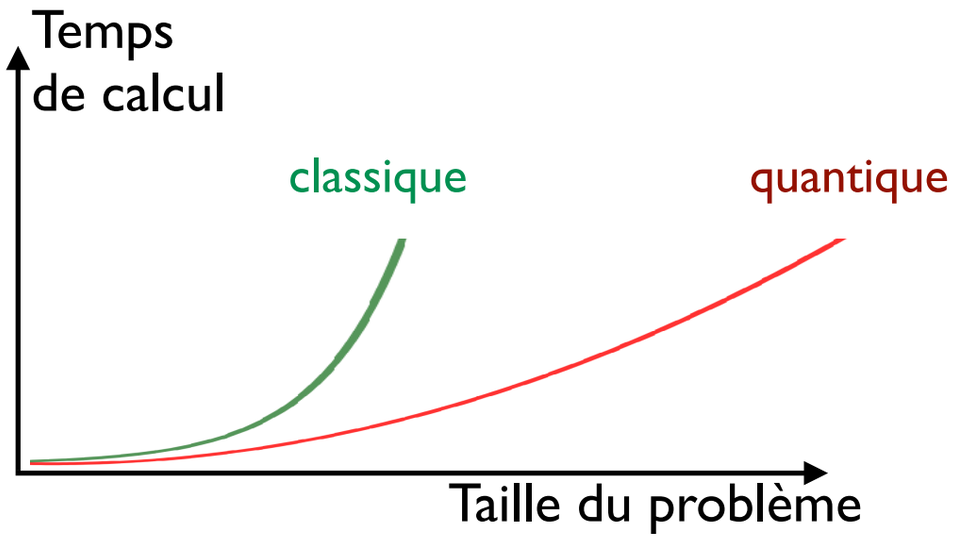


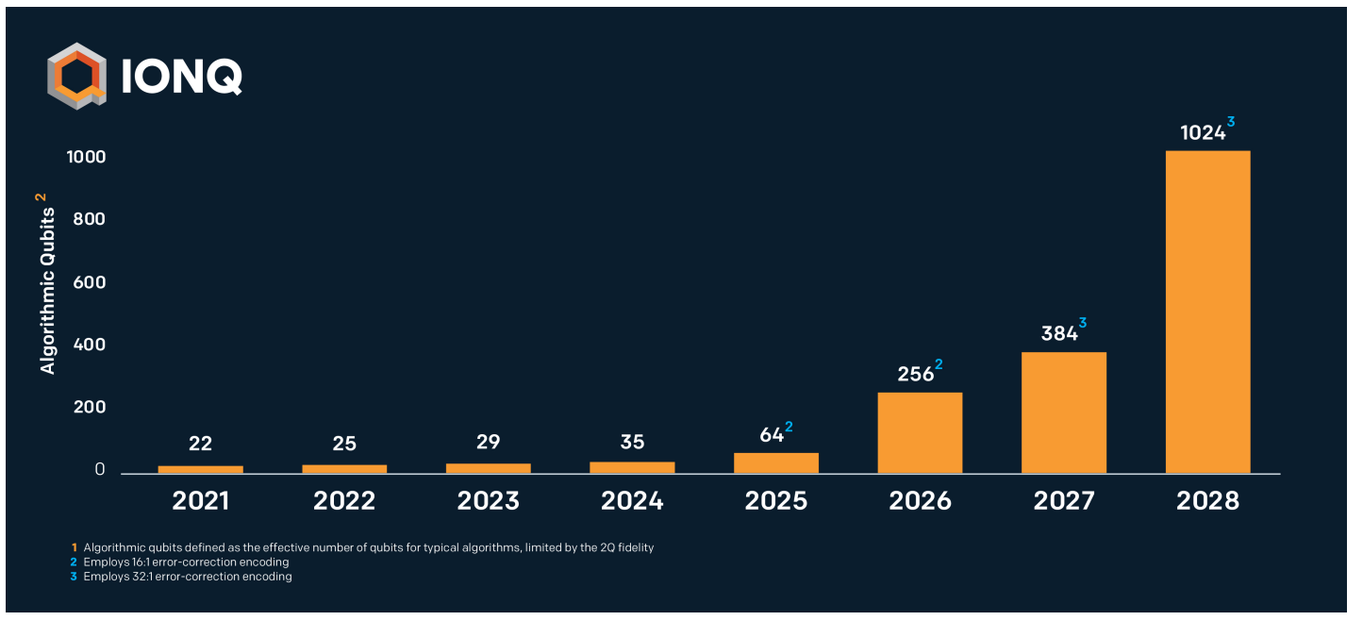
Accélération quantique

- Sparsification en temps $O(\sqrt{mn}/\varepsilon)$ [Apers, de Wolf 2020]

Conclusion
Perspectives

A quand l'accélération ?

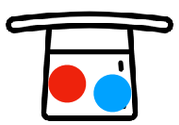


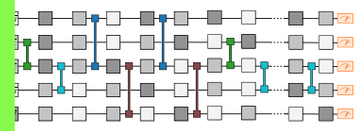


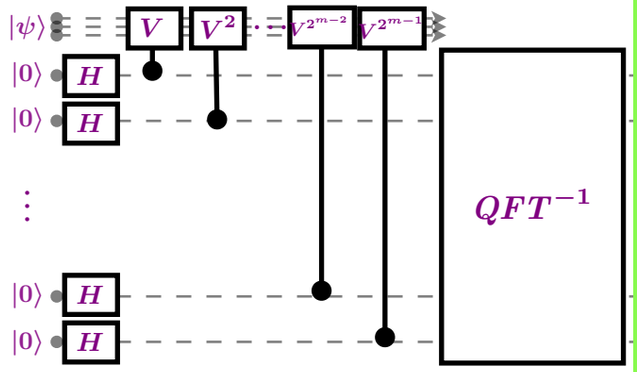
Perspectives

Algorithmes

Technologies







Algorithmes
avec avantage prouvé

Pas d'architecture
pour les programmer

Nouveau courant de pensée
Cryptographie post-quantique
Algorithmes quantum-inspired
Théorie de l'information quantique
Preuves quantiques

Nouvelles technologies quantiques
Communications
Capteurs
Horloges atomiques

Pas d'algorithmes
pour les utiliser

Heuristiques
Utiliser moins de ressources
Prouver un avantage utile

Apprentissage + Simulation

Classical shadow
[arXiv:2012.09265]

Passage à l'échelle
Calcul tolérant aux fautes
Architectures résistantes aux erreurs