(A Not So Technical) Introduction to Quantum Computation

What does it take to successfully use quantum computers?

Harold Ollivier

Outline

01

Quantum Computing

What is quantum mechanics?

Definition

Set of axioms used to describe reality (at the microscopic scale)

What is quantum mechanics?

Definition

Set of axioms used to describe reality (at the microscopic scale)

Axioms

1. State of a system is a normalized vector in a complex Hilbert space $\vec{u} \in \mathcal{H}$

What is quantum mechanics?

Definition

Set of axioms used to describe reality (at the microscopic scale)

Axioms

1. State of a system is a normalized vector in a complex Hilbert space $\vec{u} \in \mathcal{H}$
2. Systems can be combined via tensor products $\vec{u}, \vec{v} \rightarrow \vec{u} \otimes \vec{v}$

Definition

Set of axioms used to describe reality (at the microscopic scale)

Axioms

1. State of a system is a normalized vector in a complex Hilbert space $\vec{u} \in \mathcal{H}$
2. Systems can be combined via tensor products $\vec{u}, \vec{v} \rightarrow \vec{u} \otimes \vec{v}$
3. Closed system evolutions are unitaries $\vec{u} \rightarrow U\vec{u},\ U \in \mathcal{U}(\mathcal{H})$

What is quantum mechanics?

Definition

Set of axioms used to describe reality (at the microscopic scale)

Axioms

1. State of a system is a normalized vector in a complex Hilbert space $\vec{u} \in \mathcal{H}$
2. Systems can be combined via tensor products $\vec{u}, \vec{v} \to \vec{u} \otimes \vec{v}$
3. Closed system evolutions are unitaries $\vec{u} \to U\vec{u},\ U \in \mathcal{U}(\mathcal{H})$
4. The probability of measuring $\vec{v}$ when starting $\vec{u}$ is $|(\vec{v}, \vec{u})|^2$

What is quantum mechanics?

Definition

Set of axioms used to describe reality (at the microscopic scale)

Axioms

1. State of a system is a normalized vector in a complex Hilbert space $\vec{u} \in \mathcal{H}$ — Information
2. Systems can be combined via tensor products $\vec{u}, \vec{v} \to \vec{u} \otimes \vec{v}$ — Scaling
3. Closed system evolutions are unitaries $\vec{u} \to U\vec{u}, \ U \in \mathcal{U}(\mathcal{H})$ — Processing
4. The probability of measuring $\vec{v}$ when starting $\vec{u}$ is $|(\vec{v}, \vec{u})|^2$ — Information retrieval

Direct consequences from axioms

Consequences: so what?

- It works! (Lasers, computers, GPS, etc. . .)

Direct consequences from axioms

Consequences: so what?

- It works! (Lasers, computers, GPS, etc. . .)
- Quantum mechanics is linear

Direct consequences from axioms

Consequences: so what?

- It works! (Lasers, computers, GPS, etc. . .)
- Quantum mechanics is linear
- Closed system quantum mechanics is reversible

Direct consequences from axioms

Consequences: so what?

- It works! (Lasers, computers, GPS, etc. . .)
- Quantum mechanics is linear
- Closed system quantum mechanics is reversible

Consequences: that's weird!

- I have superpositions (if $\vec{u}_0$ and $\vec{u}_1$ are valid basis states, so is $\frac{\vec{u}_0+\vec{u}_1}{\sqrt{2}}$ or $\frac{\vec{u}_0-\vec{u}_1}{\sqrt{2}}$)

Direct consequences from axioms

Consequences: so what?

- It works! (Lasers, computers, GPS, etc. . .)
- Quantum mechanics is linear
- Closed system quantum mechanics is reversible

Consequences: that's weird!

- I have superpositions (if $\vec{u}_0$ and $\vec{u}_1$ are valid basis states, so is $\frac{\vec{u}_0+\vec{u}_1}{\sqrt{2}}$ or $\frac{\vec{u}_0-\vec{u}_1}{\sqrt{2}}$)
- I cannot copy information $((\alpha\vec{u}_0 + \beta\vec{u}_1) \otimes (\alpha\vec{u}_0 + \beta\vec{u}_1) \neq \alpha\vec{u}_0 \otimes \vec{u}_0 + \beta\vec{u}_1 \otimes \vec{u}_1)$

Direct consequences from axioms

Consequences: so what?

- It works! (Lasers, computers, GPS, etc. . .)
- Quantum mechanics is linear
- Closed system quantum mechanics is reversible

Consequences: that's weird!

- I have superpositions (if $\vec{u}_0$ and $\vec{u}_1$ are valid basis states, so is $\frac{\vec{u}_0+\vec{u}_1}{\sqrt{2}}$ or $\frac{\vec{u}_0-\vec{u}_1}{\sqrt{2}}$)
- I cannot copy information ($(\alpha\vec{u}_0 + \beta\vec{u}_1) \otimes (\alpha\vec{u}_0 + \beta\vec{u}_1) \neq \alpha\vec{u}_0 \otimes \vec{u}_0 + \beta\vec{u}_1 \otimes \vec{u}_1$)
- I cannot erase information (No unitary U can map $\vec{u}_0$ and $\vec{u}_1$ to $\vec{u}_0$)

Direct consequences from axioms

Consequences: so what?

- It works! (Lasers, computers, GPS, etc. . .)
- Quantum mechanics is linear
- Closed system quantum mechanics is reversible

Consequences: that's weird!

- I have superpositions (if $\vec{u}_0$ and $\vec{u}_1$ are valid basis states, so is $\frac{\vec{u}_0+\vec{u}_1}{\sqrt{2}}$ or $\frac{\vec{u}_0-\vec{u}_1}{\sqrt{2}}$)
- I cannot copy information $((\alpha\vec{u}_0 + \beta\vec{u}_1) \otimes (\alpha\vec{u}_0 + \beta\vec{u}_1) \neq \alpha\vec{u}_0 \otimes \vec{u}_0 + \beta\vec{u}_1 \otimes \vec{u}_1)$
- I cannot erase information (No unitary U can map $\vec{u}_0$ and $\vec{u}_1$ to $\vec{u}_0$)

But it is nonetheless possible to compute

- The classical NAND gate is universal (for classical computations) but not reversible

Consequences: so what?

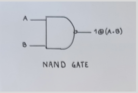
- It works! (Lasers, computers, GPS, etc...)
- Quantum mechanics is linear
- Closed system quantum mechanics is reversible

Consequences: that's weird!

- I have superpositions (if $\vec{u}_0$ and $\vec{u}_1$ are valid basis states, so is $\frac{\vec{u}_0+\vec{u}_1}{\sqrt{2}}$ or $\frac{\vec{u}_0-\vec{u}_1}{\sqrt{2}}$)
- I cannot copy information ($(\alpha\vec{u}_0 + \beta\vec{u}_1) \otimes (\alpha\vec{u}_0 + \beta\vec{u}_1) \neq \alpha\vec{u}_0 \otimes \vec{u}_0 + \beta\vec{u}_1 \otimes \vec{u}_1$)
- I cannot erase information (No unitary U can map $\vec{u}_0$ and $\vec{u}_1$ to $\vec{u}_0$)

But it is nonetheless possible to compute

- The classical NAND gate is universal (for classical computations) but not reversible



Consequences: so what?

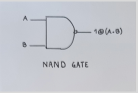
- It works! (Lasers, computers, GPS, etc. . .)
- Quantum mechanics is linear
- Closed system quantum mechanics is reversible

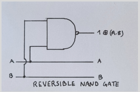
Consequences: that's weird!

- I have superpositions (if $\vec{u}_0$ and $\vec{u}_1$ are valid basis states, so is $\frac{\vec{u}_0+\vec{u}_1}{\sqrt{2}}$ or $\frac{\vec{u}_0-\vec{u}_1}{\sqrt{2}}$)
- I cannot copy information $((\alpha\vec{u}_0+\beta\vec{u}_1)\otimes(\alpha\vec{u}_0+\beta\vec{u}_1)\neq\alpha\vec{u}_0\otimes\vec{u}_0+\beta\vec{u}_1\otimes\vec{u}_1)$
- I cannot erase information (No unitary U can map $\vec{u}_0$ and $\vec{u}_1$ to $\vec{u}_0$)

But it is nonetheless possible to compute

- The classical NAND gate is universal (for classical computations) but not reversible





Direct consequences from axioms

Consequences: so what?

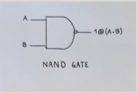
- It works! (Lasers, computers, GPS, etc. . .)
- Quantum mechanics is linear
- Closed system quantum mechanics is reversible

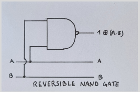
Consequences: that's weird!

- I have superpositions (if $\vec{u}_0$ and $\vec{u}_1$ are valid basis states, so is $\frac{\vec{u}_0+\vec{u}_1}{\sqrt{2}}$ or $\frac{\vec{u}_0-\vec{u}_1}{\sqrt{2}}$)
- I cannot copy information ($(\alpha\vec{u}_0 + \beta\vec{u}_1) \otimes (\alpha\vec{u}_0 + \beta\vec{u}_1) \neq \alpha\vec{u}_0 \otimes \vec{u}_0 + \beta\vec{u}_1 \otimes \vec{u}_1$)
- I cannot erase information (No unitary U can map $\vec{u}_0$ and $\vec{u}_1$ to $\vec{u}_0$)

But it is nonetheless possible to compute

- The classical NAND gate is universal (for classical computations) but not reversible





- The Toffoli matches the NAND gate computation but is reversible

Consequences: so what?

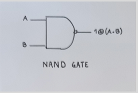
- It works! (Lasers, computers, GPS, etc. . .)
- Quantum mechanics is linear
- Closed system quantum mechanics is reversible

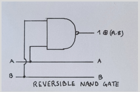
Consequences: that's weird!

- I have superpositions (if $\vec{u}_0$ and $\vec{u}_1$ are valid basis states, so is $\frac{\vec{u}_0+\vec{u}_1}{\sqrt{2}}$ or $\frac{\vec{u}_0-\vec{u}_1}{\sqrt{2}}$)
- I cannot copy information $((\alpha\vec{u}_0 + \beta\vec{u}_1) \otimes (\alpha\vec{u}_0 + \beta\vec{u}_1) \neq \alpha\vec{u}_0 \otimes \vec{u}_0 + \beta\vec{u}_1 \otimes \vec{u}_1)$
- I cannot erase information (No unitary U can map $\vec{u}_0$ and $\vec{u}_1$ to $\vec{u}_0$)

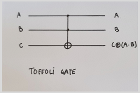
But it is nonetheless possible to compute

- The classical NAND gate is universal (for classical computations) but not reversible





- The Toffoli matches the NAND gate computation but is reversible



Direct consequences from axioms

Consequences: so what?

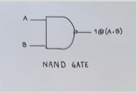
- It works! (Lasers, computers, GPS, etc...)
- Quantum mechanics is linear
- Closed system quantum mechanics is reversible

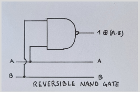
Consequences: that's weird!

- I have superpositions (if $\vec{u}_0$ and $\vec{u}_1$ are valid basis states, so is $\frac{\vec{u}_0+\vec{u}_1}{\sqrt{2}}$ or $\frac{\vec{u}_0-\vec{u}_1}{\sqrt{2}}$)
- I cannot copy information ($(\alpha\vec{u}_0 + \beta\vec{u}_1) \otimes (\alpha\vec{u}_0 + \beta\vec{u}_1) \neq \alpha\vec{u}_0 \otimes \vec{u}_0 + \beta\vec{u}_1 \otimes \vec{u}_1$)
- I cannot erase information (No unitary U can map $\vec{u}_0$ and $\vec{u}_1$ to $\vec{u}_0$)

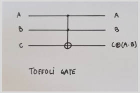
But it is nonetheless possible to compute

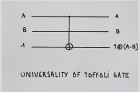
- The classical NAND gate is universal (for classical computations) but not reversible





- The Toffoli matches the NAND gate computation but is reversible





Is that it? Diving into superpositions

The Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Is that it? Diving into superpositions

The Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

H maps basis vectors to equal weight superpositions

$$\vec{u}_0 \to \frac{1}{\sqrt{2}}(\vec{u}_0 + \vec{u}_1) \quad \vec{u}_1 \to \frac{1}{\sqrt{2}}(\vec{u}_0 - \vec{u}_1)$$

Is that it? Diving into superpositions

The Hadamard gate

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

H maps basis vectors to equal weight superpositions

$$\vec{u}_0 \rightarrow \frac{1}{\sqrt{2}}(\vec{u}_0 + \vec{u}_1) \quad \vec{u}_1 \rightarrow \frac{1}{\sqrt{2}}(\vec{u}_0 - \vec{u}_1)$$

One H gate behaves like a random number generator:

- $\Pr(\vec{u}_0|H\vec{u}_0) = \frac{1}{2} = |(\vec{u}_0|H\vec{u}_0)|^2$
- $\Pr(\vec{u}_1|H\vec{u}_0) = \frac{1}{2} = |(\vec{u}_1|H\vec{u}_0)|^2$.
- $\Pr(\vec{u}_0|H\vec{u}_1) = \frac{1}{2} = |(\vec{u}_0|H\vec{u}_1)|^2$
- $\Pr(\vec{u}_1|H\vec{u}_1) = \frac{1}{2} = |(\vec{u}_1|H\vec{u}_1)|^2$.

The Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

H maps basis vectors to equal weight superpositions

$$\vec{u}_0 \to \frac{1}{\sqrt{2}}(\vec{u}_0 + \vec{u}_1) \quad \vec{u}_1 \to \frac{1}{\sqrt{2}}(\vec{u}_0 - \vec{u}_1)$$

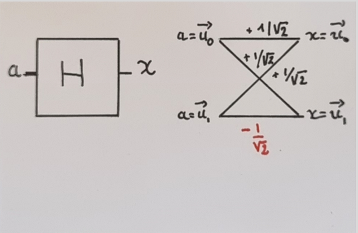
One *H* gate behaves like a random number generator:

- $\Pr(\vec{u}_0|H\vec{u}_0) = \frac{1}{2} = |(\vec{u}_0|H\vec{u}_0)|^2$
- $\Pr(\vec{u}_1|H\vec{u}_0) = \frac{1}{2} = |(\vec{u}_1|H\vec{u}_0)|^2$.
- $\Pr(\vec{u}_0|H\vec{u}_1) = \frac{1}{2} = |(\vec{u}_0|H\vec{u}_1)|^2$
- $\Pr(\vec{u}_1|H\vec{u}_1) = \frac{1}{2} = |(\vec{u}_1|H\vec{u}_1)|^2$.

Two successive *H* gates behave like identity

$$\vec{u}_0 \xrightarrow{H} \frac{1}{\sqrt{2}}(\vec{u}_0 + \vec{u}_1) \xrightarrow{H} \frac{1}{2}(\vec{u}_0 + \vec{u}_1 + \vec{u}_0 - \vec{u}_1) = \vec{u}_0.$$

A different view of the Hadamard gate



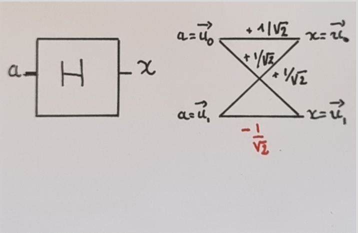
We can compactly represent the computation of amplitudes

	$\mathbf{a}=0$	$\mathbf{a}=1$
$\mathbf{x}=0$	$1/\sqrt{2}$	$1/\sqrt{2}$
$\mathbf{x}=1$	$1/\sqrt{2}$	$-1/\sqrt{2}$

which we can rewrite $(-1)^{\mathbf{a}.\mathbf{x}}/\sqrt{2}$.

Using superpositions

A different view of the Hadamard gate

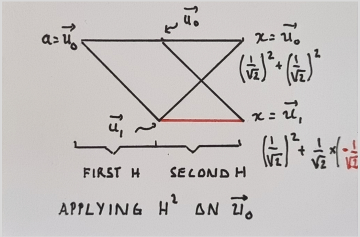


We can compactly represent the computation of amplitudes

	$\mathbf{a} = 0$	$\mathbf{a} = 1$
$\mathbf{x} = 0$	$1/\sqrt{2}$	$1/\sqrt{2}$
$\mathbf{x} = 1$	$1/\sqrt{2}$	$-1/\sqrt{2}$

which we can rewrite $(-1)^{\mathbf{a}.\mathbf{x}}/\sqrt{2}$.

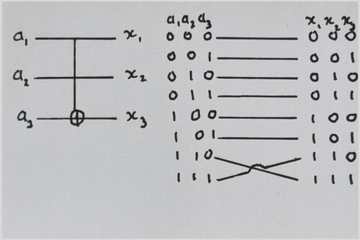
And its power



Because contributions (amplitudes) can be negative,

- Some paths add-up (constructive interference)
- Some paths cancel each other (destructive interference)

Toffoli gate



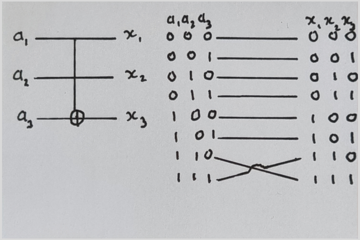
The amplitudes can also be computed in a very compact way:

$$\delta_{x_1,a_1} \times \delta_{x_2,a_2} \times \delta_{x_3,a_3 \oplus (a_1.a_2)}$$

i.e. is 1 when the input-output relation is satisfied, and 0 otherwise

Using superpositions

Toffoli gate

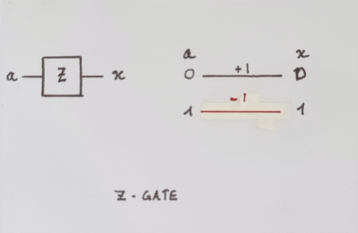


The amplitudes can also be computed in a very compact way:

$$\delta_{x_1, a_1} \times \delta_{x_2, a_2} \times \delta_{x_3, a_3 \oplus (a_1 . a_2)}$$

i.e. is 1 when the input-output relation is satisfied, and 0 otherwise

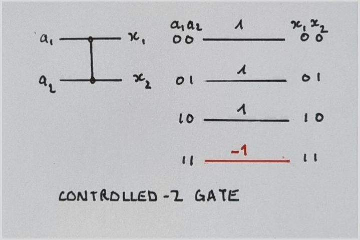
Z gate



The amplitudes are written:

$$\delta_{x,a} \times (-1)^a$$

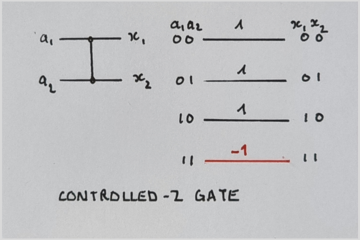
CZ gate



For *CZ* the amplitude is $(-1)^{a_1 \cdot a_2} \delta_{a_1, x_1} \delta_{a_2, x_2}$

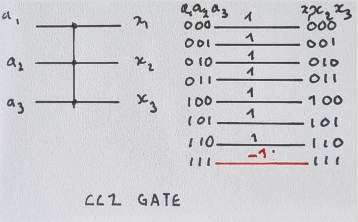
Using superpositions

CZ gate



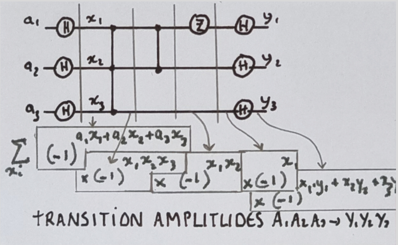
For *CZ* the amplitude is $(-1)^{a_1 \cdot a_2} \delta_{a_1,x_1} \delta_{a_2,x_2}$

CCZ gate



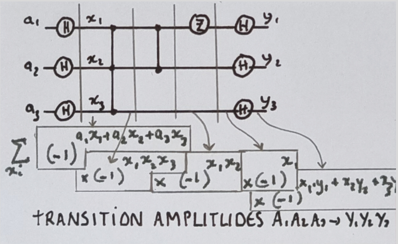
For *CCZ* it is $(-1)^{a_1 \cdot a_2 \cdot a_3} \delta_{a_1,x_1} \delta_{a_2,x_2} \delta_{a_3,x_3}$

Computing amplitudes for small circuits (recursively applying the formulas)



The power of superpositions

Computing amplitudes for small circuits (recursively applying the formulas)



The transition amplitude from $a = \vec{u}_0^{\otimes n}$ to $y = \vec{u}_0^{\otimes n}$ corresponds to:

$$(\vec{u}_0^{\otimes n}, C_P \vec{u}_0^{\otimes n}) = \frac{1}{2^n} \sum_{x=(x_i)_i \in \{0,1\}^n} (-1)^{P(x)} = \frac{1}{2^n} (\#\{x : P(x) = 0\} - \#\{x : P(x) = 1\})$$

The power of superpositions

Quantum computers "compute" transition amplitudes

$$(\vec{u}_0^{\otimes n}, C_P \vec{u}_0^{\otimes n}) = \frac{1}{2^n} \sum_{x=(x_i)_i \in \{0,1\}^n} (-1)^{P(x)} = \frac{1}{2^n} (\#\{x : P(x) = 0\} - \#\{x : P(x) = 1\})$$

Defining $gap(P)$ for P degree-3 polynomial

$$gap(P) = \#\{x : P(x) = 0\} - \#\{x : P(x) = 1\}$$

where $P = \sum \alpha_{i,j,k} x_i.x_j.x_k + \sum \beta_{i,j} x_i.x_j + \sum \gamma_i x_i$, and $\alpha_{i,j,k}, \beta_{i,j}, \gamma_i \in \{0, 1\}$.

The power of superpositions

Quantum computers "compute" transition amplitudes

$$(\vec{u}_0^{\otimes n}, C_P \vec{u}_0^{\otimes n}) = \frac{1}{2^n} \sum_{x=(x_i)_i \in \{0,1\}^n} (-1)^{P(x)} = \frac{1}{2^n}(\#\{x : P(x) = 0\} - \#\{x : P(x) = 1\})$$

Defining $gap(P)$ for P degree-3 polynomial

$$gap(P) = \#\{x : P(x) = 0\} - \#\{x : P(x) = 1\}$$

where $P = \sum \alpha_{i,j,k} x_i.x_j.x_k + \sum \beta_{i,j} x_i.x_j + \sum \gamma_i x_i$, and $\alpha_{i,j,k}, \beta_{i,j}, \gamma_i \in \{0, 1\}$.

Hardness

- Classically computing $gap(P)$ is hard (in $PP \supset NP$)
- Computing $ngap(P) = gap(P)/2^n$ is also hard
- Quantum computers seem to do it with few gates: $ngap(P) = (\vec{u}_0^{\otimes n}, C_P \vec{u}_0^{\otimes n})$

The power of quantum computers is fragile

Exact computation of $ngap(P)$ is hard

But

Quantum computers do not give access to these values with perfect accuracy, but only to samples and, additionnally, they can be noisy

Exact computation of $ngap(P)$ is hard

But

Quantum computers do not give access to these values with perfect accuracy, but only to samples and, additionnally, they can be noisy

- It is still hard to obtain a multiplicative approximation of $ngap(f)$ in the worst case

The power of quantum computers is fragile

Exact computation of $ngap(P)$ is hard

But

Quantum computers do not give access to these values with perfect accuracy, but only to samples and, additionnally, they can be noisy

- It is still hard to obtain a multiplicative approximation of $ngap(f)$ in the worst case
- It is thought to be hard on average

Exact computation of $ngap(P)$ is hard

But

Quantum computers do not give access to these values with perfect accuracy, but only to samples and, additionnally, they can be noisy

- It is still hard to obtain a multiplicative approximation of $ngap(f)$ in the worst case
- It is thought to be hard on average
- It can become easy for additive approximation for classes of functions that remain hard multiplicatively

The power of quantum computers is fragile

Exact computation of $ngap(P)$ is hard

But

Quantum computers do not give access to these values with perfect accuracy, but only to samples and, additionnally, they can be noisy

- It is still hard to obtain a multiplicative approximation of $ngap(f)$ in the worst case
- It is thought to be hard on average
- It can become easy for additive approximation for classes of functions that remain hard multiplicatively
- It can be easy when there is noise

Take home messages

1. QC do computations that correspond to exponentially many parallel computations

Take home messages

1. QC do computations that correspond to exponentially many parallel computations
2. But retrieving the information out of this exponentially many superposed states is tricky

Take home messages

1. QC do computations that correspond to exponentially many parallel computations
2. But retrieving the information out of this exponentially many superposed states is tricky
3. QC will not help in all situations

Take home messages

1. QC do computations that correspond to exponentially many parallel computations
2. But retrieving the information out of this exponentially many superposed states is tricky
3. QC will not help in all situations
4. Useful QC algorithms need to be designed (or checked) on a case-by-case basis: no easy black-box approach

Take home messages

1. QC do computations that correspond to exponentially many parallel computations
2. But retrieving the information out of this exponentially many superposed states is tricky
3. QC will not help in all situations
4. Useful QC algorithms need to be designed (or checked) on a case-by-case basis: no easy black-box approach
5. Keep in mind that we assumed perfect machines (without noise)

02

Current Impacts

Examples of algorithms using coherent QC (large machines, error free)

- Discrete log (exponential)
- Linear algebra with quantum encoded data (possibly exponential, mostly polynomial)
- Search (quadratic)

Examples of algorithms using coherent QC (large machines, error free)

- Discrete log (exponential)
- Linear algebra with quantum encoded data (possibly exponential, mostly polynomial)
- Search (quadratic)

Examples of algorithms using noisy QC (not quite useful with current machines, but getting closer)

- Variational Quantum Eigensolver (VQE): optimization problems recast as minimization of energy / QML
- Quantum Alternating Operator Ansatz (QAOA): combinatorial optimization
- Analog QC: physics simulations, optimization

Some quantum algorithms and more...

Examples of algorithms using coherent QC (large machines, error free)

- Discrete log (exponential)
- Linear algebra with quantum encoded data (possibly exponential, mostly polynomial)
- Search (quadratic)

Examples of algorithms using noisy QC (not quite useful with current machines, but getting closer)

- Variational Quantum Eigensolver (VQE): optimization problems recast as minimization of energy / QML
- Quantum Alternating Operator Ansatz (QAOA): combinatorial optimization
- Analog QC: physics simulations, optimization

Quantum cryptography (QKD)

- Protecting information with statistical security (ie. without hardness asumptions)

On cryptography

- 2016 NIST has started the process of changing the way public key crypto is done to become post-quantum (ie. quantum resistant)
- Calls issued, some protocols are being standardized
- Major impact on all industries (with increased operational risks)

On cryptography

- 2016 NIST has started the process of changing the way public key crypto is done to become post-quantum (ie. quantum resistant)
- Calls issued, some protocols are being standardized
- Major impact on all industries (with increased operational risks)

On computing

- A lot of work is being done to pinpoint possible use-cases
- Assessment of the current power of quantum machines
  - Well chosen problem (hard for classical / easy for quantum): supremacy experiment
  - Useful problem (but brute force classical simulation): latest IBM Nature paper
  - Small scale proof of concept: hard to apprehend the scaling
- Trying to develop a GPU-like approach with HPC coupling

03

Looking into the future

Expected imapcts

Impact your client's businesses

- Need to account for crypto uncertainty
  - People store have long-term valuable documents
  - Need to properly upgrade security of systems before it's too late
- Ensuring that some computations are correct / trusting computations

Expected imapcts

Impact your client's businesses

- Need to account for crypto uncertainty
  - People store have long-term valuable documents
  - Need to properly upgrade security of systems before it's too late
- Ensuring that some computations are correct / trusting computations

Impact on your own business

- Dependent on applications
- Algebra + optim: Quite general

When?

Current HW status

- In the hundred's of qubits non error corrected
- In a zone where there is some battle with classical computing (for well chosen problems)
- Many different architectures where some could potentially arrive faster than expected

When?

Current HW status

- In the hundred's of qubits non error corrected
- In a zone where there is some battle with classical computing (for well chosen problems)
- Many different architectures where some could potentially arrive faster than expected

Bottlenecks

- Assessment of usefulness of QC requires reanalysing the full computational software stack
- Takes time and knowledge to know what you are trying to improve
- Improving over state of the art means you know what it is for your problem

What?

You can (should?) take actions now

- Get an idea with small scale hackathons (to get a first feeling)

What?

You can (should?) take actions now

- Get an idea with small scale hackathons (to get a first feeling)
- Build small teams that try to take one problem and improve it

What?

You can (should?) take actions now

- Get an idea with small scale hackathons (to get a first feeling)
- Build small teams that try to take one problem and improve it
- Look where quantum can help

You can (should?) take actions now

- Get an idea with small scale hackathons (to get a first feeling)
- Build small teams that try to take one problem and improve it
- Look where quantum can help
- Work with private companies (when getting inspiration from others / adapting something described elsewhere)

What?

You can (should?) take actions now

- Get an idea with small scale hackathons (to get a first feeling)
- Build small teams that try to take one problem and improve it
- Look where quantum can help
- Work with private companies (when getting inspiration from others / adapting something described elsewhere)
- Work with academic labs when you want to tackle something that (really) nobody has looked at before

04

Thank you! (time for questions)