Quantum Systems

(Lecture 2: Computing with qubits. The Deutsch algorithm)

Luís Soares Barbosa

Universidade do Minho

Computing with qubits

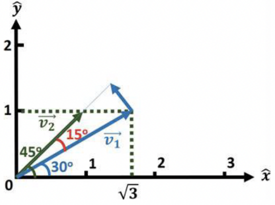
Quantum State: A unit vector of (complex) amplitudes in $\mathcal{C}^n$

- (why unit? why complex amplitudes?)
- ... whose general 'format' is a superposition of ortonormal base vectors, e.g. $|0\rangle, |1\rangle$

This means that a quantum state 'lives' in a complex vector space with a inner product

Recall: what is a inner product?

From a linear algebra textbook: for $\vec{v_1} = \sqrt{3}\,\widehat{x} + \widehat{y}$ and $\vec{v_2} = \widehat{x} + \widehat{y}$, the inner (or dot, or scalar) product is



$$\langle \vec{v_1}, \vec{v_2} \rangle \;=\; |\vec{v_1}||\vec{v_2}|\cos 15 \;\approx\; 2.732$$

i.e. the product of the (magnitudes of) $\vec{v_2}$ by $\vec{v_1}$ projected in the direction of $\vec{v_2}$.

The inner product defines how much the two vectors have in common after scaled by their magnitudes, where magnitudes are computed through the Pythagorean theorem.

Recall: what is a inner product?

If the basis vectors are orthonormal, this can be computed as

$$\langle \vec{v_1}, \vec{v_2} \rangle \; = \; \vec{v_1}^{\dagger} \vec{v_2}$$

where $x^{\dagger}$ is the complex conjugate transpose of x. Thus,

$$\begin{bmatrix} \sqrt{3} & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \approx 2.732$$

Computing with qubits

Quantum State: A unit vector of (complex) amplitudes in $\mathcal{C}^n$

Quantum Operators:

- measurements (destructive!)
- unitary transformations: vector rotations preserving the inner products, ie. the geometry, and consequently, norms:

$$\| v \rangle | \mathrel{\widehat{=}} \sqrt{\langle v, v \rangle}$$

... such operators are reversible.

Some operators

The X gate

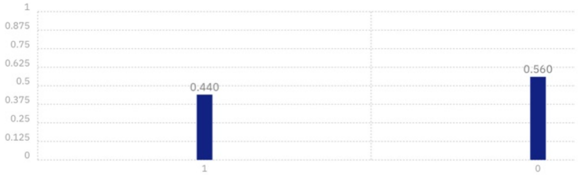
e.g.

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |1\rangle$$

$$X(\alpha|0\rangle + \beta|1\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

Some operators

The H gate



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

The H gate creates superpositions:

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix} = |+\rangle$$

My first quantum algorithm

The Deutsch problem

Decide whether

$$f : \mathbf{2} \longrightarrow \mathbf{2}$$

is constant or not, with a single evaluation of f?

- Classically, to determine which case $f(1) = f(0)$ or $f(1) \neq f(0)$ holds requires running f twice
- Resorting to quantum computation, however, it suffices to run f once . . . due to two quantum effects superposition and interference

Turning f into a quantum operation

$f : \mathbf{2} \longrightarrow \mathbf{2}$ extends to a linear map $\mathbb{C}^2 \to \mathbb{C}^2$

... but not necessarily to a unitary transformation.

proof

The extended f does not preserve norms: Actually, when f is constant on 0 we obtain $f|0\rangle = |0\rangle$ and $f|1\rangle = |0\rangle$.
Thus,

$$\left| \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right| = 1$$

However,

$$\left| f\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right) \right| = \left| \frac{1}{\sqrt{2}}(|0\rangle + |0\rangle) \right| = \left| \frac{2}{\sqrt{2}}|0\rangle \right| = \frac{2}{\sqrt{2}}$$

Turning f into a quantum operation

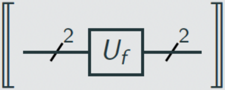
Intuition

f potentially loses information whereas pure quantum operations are reversible [Charles Bennett, 1973]

Actually, a unitary transformation is always injective so if a map loses information it cannot be unitary.

Turning f into a quantum operation

Proposed Solution



$$= |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle$$

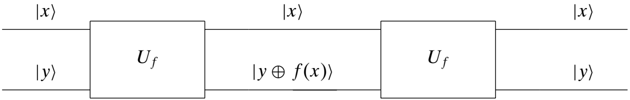
Addition modulo 2

- The oracle takes input $|x\rangle|y\rangle$ to $|x\rangle|y \oplus f(x)\rangle$
- Fixing $y = 0$ it encodes f:

$$U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |0 \oplus f(x)\rangle = |x\rangle \otimes |f(x)\rangle$$

Turning f into a quantum operation

- U_f is a unitary, i.e. a reversible gate



$$|x\rangle|(y \oplus f(x)) \oplus f(x)\rangle \;=\; |x\rangle|y \oplus (f(x) \oplus f(x))\rangle \;=\; |x\rangle|y \oplus 0\rangle \;=\; |x\rangle|y\rangle$$

Exploiting quantum parallelism

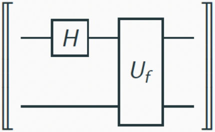
Key message!

- Through superposition one can perform a transformation on multiple basis states at the same time!
- ... but accessing the results is another story.

Exploiting quantum parallelism

Can f be evaluated for $|0\rangle$ and $|1\rangle$ in one step?

Consider the following circuit



$$= U_f(H \otimes I)$$

$$
\begin{aligned}
& U_f(H \otimes I)(|0\rangle \otimes |0\rangle) \\
&= U_f\left(\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right) && \{\text{Defn. of } H \text{ and } I\} \\
&= U_f\left(\tfrac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) && \{\otimes \text{ distributes over } +\} \\
&= \tfrac{1}{\sqrt{2}}(|0\rangle|0 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle) && \{\text{Defn. of } U_f\} \\
&= \underbrace{\tfrac{1}{\sqrt{2}}(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle)}_{f(0) \text{ and } f(1) \text{ in a single run}} && \{0 \oplus x = x\}
\end{aligned}
$$

Are we done?

$$U_f(H \otimes I)(|0\rangle \otimes |0\rangle) \; = \; \underbrace{\frac{1}{\sqrt{2}}(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle)}_{f(0) \text{ and } f(1) \text{ in a single run}}$$

NO

Although both values have been computed simultaneously, only one of them is retrieved upon measurement in the computational basis: Actually, 0 or 1 will be retrieved with identical probability (why?).

YES

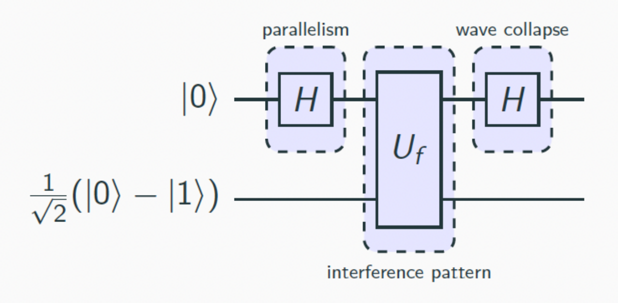
The Deutsch problem is not interested on the concrete values f may take, but on a global property of f: whether it is constant or not, technically on the value of

$$f(0) \oplus f(1)$$

Exploiting quantum parallelism and interference

Actually, the Deutsch algorithm explores another quantum resource — interference — to obtain that global information on f

Let us create an interference pattern dependent on this property, and resort to wave collapse to prepare for the expected result:



Exploiting quantum parallelism and interference

Let us start with a simple, auxiliary computation:

$$
\begin{aligned}
& U_f\,(|x\rangle \otimes (|0\rangle - |1\rangle)) \\
&= U_f\,(|x\rangle|0\rangle - |x\rangle|1\rangle) && \{\otimes \text{ distributes over } + \} \\
&= |x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle && \{\text{Defn. of } f\} \\
&= |x\rangle|f(x)\rangle - |x\rangle|\neg f(x)\rangle && \{0 \oplus x = x, 1 \oplus x = \neg x\} \\
&= |x\rangle \otimes (|f(x)\rangle - |\neg f(x)\rangle) && \{\otimes \text{ distributes over } +\} \\
&= \begin{cases} |x\rangle \otimes (|0\rangle - |1\rangle) & \text{if } f(x) = 0 \\ |x\rangle \otimes (|1\rangle - |0\rangle) & \text{if } f(x) = 1 \end{cases} && \{\text{case distinction}\}
\end{aligned}
$$

leading to

$$
U_f\,(|x\rangle \otimes (|0\rangle - |1\rangle)) \;=\; (-1)^{f(x)}|x\rangle \otimes (|0\rangle - |1\rangle)
$$

Exploiting quantum parallelism and interference

$$
\begin{aligned}
&(H \otimes I)U_f(H \otimes I)\,(|0\rangle \otimes |-\rangle)\\
&= (H \otimes I)U_f\,(|+\rangle \otimes |-\rangle)\\
&= \tfrac{1}{\sqrt{2}}(H \otimes I)U_f\,((|0\rangle + |1\rangle) \otimes |-\rangle)\\
&= \tfrac{1}{\sqrt{2}}(H \otimes I)\,(U_f|0\rangle \otimes |-\rangle + U_f|1\rangle \otimes |-\rangle)\\
&= \tfrac{1}{\sqrt{2}}(H \otimes I)\left((-1)^{f(0)}|0\rangle \otimes |-\rangle + (-1)^{f(1)}|1\rangle \otimes |-\rangle\right) \qquad \{\text{Previous slide}\}\\
&= \begin{cases} (H \otimes I)(\pm 1)|+\rangle \otimes |-\rangle & \text{if } f(0) = f(1)\\ (H \otimes I)(\pm 1)|-\rangle \otimes |-\rangle & \text{if } f(0) \neq f(1)\end{cases}\\
&= \begin{cases} (\pm 1)|0\rangle \otimes |-\rangle & \text{if } f(0) = f(1)\\ (\pm 1)|1\rangle \otimes |-\rangle & \text{if } f(0) \neq f(1)\end{cases}
\end{aligned}
$$

To answer the original problem is now enough to measure the first qubit: if it is in state $|0\rangle$, then f is constant.

Lessons learnt

- A typical structure fro a quantum algorithm includes three phases:
  1. State preparation
     (fix initial setting)
  2. Transformation
     (combination of unitary transformations)
  3. Measurement
     (projection onto a basis vector associated with a measurement tool)
- This 'toy' algorithm is an illustrative simplification of the first

  algorithm with quantum advantage

  presented in literature [Deutsch, 1985]
- All other quantum algorithms crucially rely on similar ideas of quantum interference

What can be expected from quantum computation?

- The meaning of computable remains the same ...
- ... but the order of complexity may change

$\boxed{\text{Factoring in polynomial time - } \mathcal{O}((ln\, n)^3)}$

Peter Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer* (1994)

Which problems a Quantum Computer can solve?

- 1994: Peter Shor's factorization algorithm (exponential speed-up),
- 1996: Grover's unstructured search (quadratic speed-up),
- 2018: Advances in hash collision search, i.e finding two items identical in a long list — serious threat to the basic building blocks of secure electronic commerce.
- 2019: Google announced to have achieved quantum supermacy

Availability of proof of concept hardware

Explosion of emerging applications in several domains: security, finance, optimization, machine learning, ...

Quantum algorithms: Engineering Nature

No magic ...

- A huge amount of information can be stored and manipulated in the states of a relatively small number of qubits,
- ... but measurement will pick up just one of the computed solutions and colapse the whole (quantum) state

... but engineering:

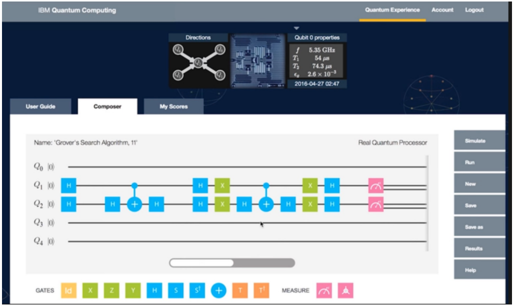
To boost the probability of arriving to a solution by canceling out some computational paths and reinforcing others,

depending on the structure of the problem at hands.

Where exactly do we stand?

NISQ - Noisy Intermediate-Scale Quantum Hybrid machines:

- the quantum device as a coprocessor
- typically accessed as a service over the cloud



Where exactly do we stand?

- Quantum devices have associated decoherence times, which limit the number of quantum operations that can be performed before the results are 'drowned' by noise.
- Each operation performed with quantum gates introduces accuracy errors in the system, which limits the size of quantum circuits that can be executed reliably.