An introductory lecture on quantum computation

Zohreh Davoudi

May 2019

PHYS402 May 8, 2019

In this lecture, we'll learn about:
- ☐ Qubit(s)
- ☐ Single and multi qubit gates
- ☐ Quantum algorithms (Deutsch's and Deutsch-Jozsa's)

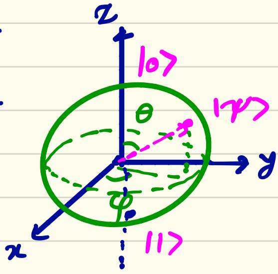
☐ Qubit: A qubit is one unit of storage in quantum computing. Despite a classical bit that can take the values of either 0 or 1, a qubit can in principle store infinite amount of information: A qubit is a quantum state: a superposition of two states, say $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are any complex number. Since the wave-function is normalized, the number of independent real parameters to parametrize $|\psi\rangle$ is 3. Also since the phase of the state doesn't matter, two real numbers do the job. A nice parametrization is:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

which gives the state a geometric representations. All vectors with unit length ending up on the sphere in the right can correspond to one of the possible values of $|\psi\rangle$. This is called the Bloch sphere representation of a qubit. Later we'll see how a gate operates on qubit and can visualize it in terms of an operation on the Bloch vector.

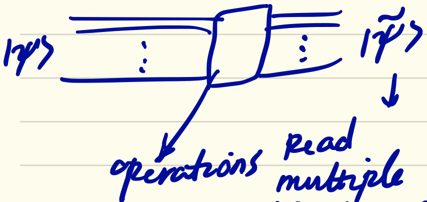


Infinite number of points on Bloch sphere

→ Infinite amount of information in a qubit

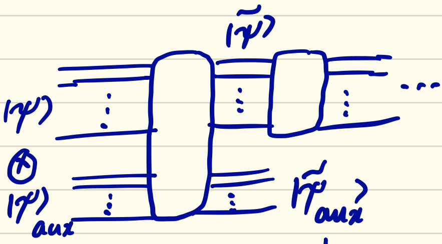
Can we access this infinite information? Unfortunately not. Measuring the qubit leaves us in either $|0\rangle$ or $|1\rangle$. So the outcome looks like if qubit was a classical bit. need a lot of measurements to determine α, β, which are probabilities to be in state $|0\rangle$ or $|1\rangle$, respectively. The power of quantum computing is to keep the huge amount of information in state, manipulate it strongly in parallel with other qubits, and only read off information when massive parallel computation is done and stored in the final state.

There are two possibilities:



Read multiple times, construct the amplitudes

Done with $|\tilde{\psi}\rangle$. Have destroyed it, should start over!



Read $|\tilde{\psi}\rangle_{aux}$, deduce $|\tilde{\psi}\rangle$ given correlations, move on operating on $|\tilde{\psi}\rangle$ without destroying it!

• multiple qubits: The state vector is a direct product of the state of each qubit. For two qubits:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \left[\equiv \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle + \delta|\underset{\nearrow}{3}\rangle\right] \quad 2^n - 1$$

with $|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2=1$. If we make a measurement on the second qubit, we are going to get $|0\rangle$ with a probability of $|\alpha|^2+|\gamma|^2$ and $|1\rangle$ with probability of $|\beta|^2+|\delta|^2$.

$\downarrow$ Ending up in $|\psi'\rangle \propto \alpha|00\rangle + \gamma|10\rangle$

$\downarrow$ Ending up in $|\psi''\rangle \propto \beta|01\rangle + \delta|11\rangle$

□ Gates: operations on state are done through gates.

A gate is a unitary transformation — any unitary tran.!

- Single-qubit gates: In classical computing, NOT is the only non-trivial single-bit gate:

$$0 \to 1, \quad 1 \to 0$$

In quantum computing, there are infinite non-trivial gates since there are infinite 2×2 unitary transformation. To write down its most general form, we take $\underline{4}$ real parameters and find U_1, U_2, U_3, U_4 such that: $U^+U = 1$, with $U = \begin{pmatrix} U_1 & U_2 \\ U_3 & U_4 \end{pmatrix}$.

$$\begin{cases} U_1^+U_1 + U_3^+U_3 = 1 \\ U_1^+U_2 + U_3^+U_4 = 0 \\ U_2^+U_1 + U_4^+U_3 = 0 \\ U_2^+U_2 + U_4^+U_4 = 1 \end{cases} \Rightarrow U_1, U_4 \sim \cos\gamma/2,\ U_2, U_3 \sim \sin\gamma/2$$

Then besides an overall phase, $e^{i\alpha}$, there remains two more independent phase for each to fix, subject to conditions above. These could be taken as $\beta/2 \pm \delta/2$:

$$U = e^{i\alpha}\begin{pmatrix} e^{-i(\beta/2+\delta/2)}\cos\gamma/2 & e^{i(-\beta/2+\delta/2)}\sin\gamma/2 \\ e^{-i(-\beta/2+\delta/2)}\sin\gamma/2 & e^{i(\beta/2+\delta/2)}\cos\gamma/2 \end{pmatrix}$$

$$= e^{i\alpha}\begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix}\begin{pmatrix} \cos\gamma/2 & \sin\gamma/2 \\ \sin\gamma/2 & \cos\gamma/2 \end{pmatrix}\begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}$$

$$= e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

So any unitary transformation on one qubit can be built out of rotations about y and z axis generated by the corresponding pauli matrices, Y and Z, and an overall phase. So the elementry 1-qubit gates are:

$$\begin{cases} X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & [X|\psi\rangle = X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle] \\ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{cases}$$

An additional important 1-qubit gate is the Hadamard gate, acting as: $\begin{cases} H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$, so has the matrix form: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Also have:

$$\begin{cases} -\boxed{S}- \equiv \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} : \text{phase gate} \\ -\boxed{T}- \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} : \pi/8 \text{ gate} \end{cases}$$

Exercise: What does H do to the Bloch sphere?

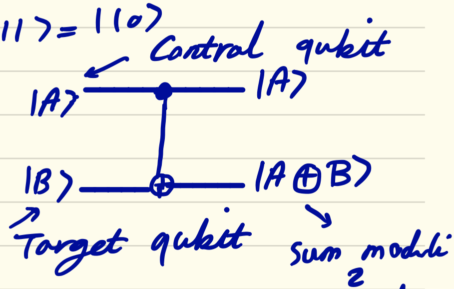
[Answer: Rotating it by 90° around the $\hat{y}$ axis and then by 180° around the $\hat{z}$ axis.]

-multiple qubit gates: It can be shown that with a few single qubit gates and only 1 two-qubit gate, every unitary transform acting on n-qubit can be constructed. This important two_qubit gate is a controled_NOT or CNOT gate, acting as:

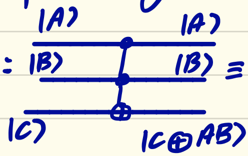
$$\begin{cases} \hat{CNOT}\,|00\rangle = |00\rangle \\ \hat{CNOT}\,|01\rangle = |01\rangle \\ \hat{CNOT}\,|10\rangle = |11\rangle \\ \hat{CNOT}\,|11\rangle = |10\rangle \end{cases}$$

. In matrix form:

$$\hat{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



The most important three-qubit gate is called Toffoli gate, acting with:



$$\equiv \begin{pmatrix} 1 & 0 & & & & & & \\ 0 & 1 & & & & & & \\ & & 1 & 0 & & & & \\ & & 0 & 1 & & & & \\ & & & & 1 & 0 & & \\ & & & & 0 & 1 & & \\ & & & & & & 0 & 1 \\ & & & & & & 1 & 0 \end{pmatrix}$$

Exercise: Try to implement a Toffoli action by using only 1,2-qubit gates. This is an example of how n-qubit gates with $n > 2$ can be constructed using the universal set of gates.

Exercise: Is there a universal cloning operation that can copy the state of any qubit?

$$U_{copy}(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \text{ for all } |\psi\rangle ?$$

U_{copy}: unitary transformation; $|\psi\rangle$: Target State; $|s\rangle$: Auxiliary state

[The answer is no unless $|\psi\rangle, |\psi'\rangle$ are orthogonal. This is called no-cloning theorem.]

One last point to keep in mind is that all quantum operations via gates are reversible as U^{-1} is also a unitary transformation, so the effect of U can be reversed by applying U^{-1} subsequently. This is not true for some of the classical logical gates.

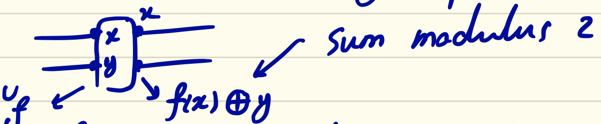
□ Quantum algorithms:

Let's look at a few simple algorithms that demonstrate the potential power of quantum computation through quantum parallelism.

- First an example to demonestrate where parallelism come from in a quantum computian:

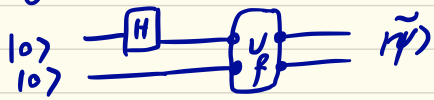
Consider a simple function $f(x)$ that maps $\{0,1\}$ to $\{0,1\}$. Consider a circut made of $\underline{2}$ qubits that implements f through a unitary operation $U_f(x)$

as shown:



Now with the following initial state: $|\psi\rangle = |0\rangle \otimes |0\rangle$ and

operations shown:



where given the property of U_f: $|\tilde{\psi}\rangle = \dfrac{|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle}{\sqrt{2}}$

so by only one evaluation of U_f, both values of $f(x)$ are incoded in the final wavefunction! However, this doesn't mean we can access $f(0)$ and $f(1)$ at the same time! Once we make a measurement on the second qubit, we either get $|0\rangle$ or $|1\rangle$!

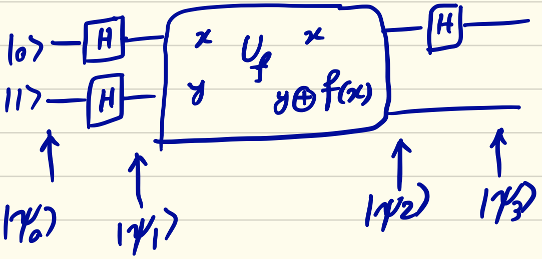
Such parallelism can be still useful to gain global information about the function with only $\underline{1}$ evaluation and $\underline{1}$ measurement. This is Deutch's algorithm.

- Deutch's algorithm:

Find the simplest quantum circuit that evaluates

$f(0)+f(1)$ by only $\underline{1}$ evaluation of the corresponding unitary transformation of function f, where f is a simple function mapping $\{0,1\}$ to $\{0,1\}$.

The circuit that implements this task is the following:



where U_f is some unitary implementation that implements $x, y \to x, y \oplus f(x)$

Example: Find the unitary transformation corresponding to $x,y \to x, y\oplus f(x)$ with $f(x)=x$, $\{0,1\}\to\{0,1\}$.

Since the transformation makes:

$$\underset{|00\rangle}{\begin{pmatrix}1\\0\\0\\0\end{pmatrix}} \to \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad \underset{|01\rangle}{\begin{pmatrix}0\\1\\0\\0\end{pmatrix}} \to \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \quad \underset{|10\rangle}{\begin{pmatrix}0\\0\\1\\0\end{pmatrix}} \to \begin{pmatrix}0\\0\\0\\1\end{pmatrix}, \quad \underset{|11\rangle}{\begin{pmatrix}0\\0\\0\\1\end{pmatrix}} \to \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$

The corresponding U_f is: $U_f = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$

which is a CNOT gate!

Now let's see what this circuit actually does:

$|\psi_0\rangle = |01\rangle$

$|\psi_1\rangle = H^{(1)}|0\rangle H^{(2)}|1\rangle = \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$

$$|\psi_2\rangle = U_f|\psi_1\rangle = \begin{cases} \pm\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)=f(1) \\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)\neq f(1) \end{cases}$$

note that: $\begin{cases} U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle = |x\rangle|0\rangle \text{ or } |x\rangle|1\rangle \\ U_f|x\rangle|1\rangle = |x\rangle|1\oplus f(x)\rangle = |x\rangle|1\rangle \text{ or } |x\rangle|0\rangle \end{cases}$

So the action of U_f on $|x\rangle H^{(2)}|1\rangle$ is:

$$U_f|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] = (-1)^{f(x)}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

And therefore if $f(0)=f(1)$, U_f acting on $|\psi_1\rangle$ does not change the relative sign between $|0\rangle$ and $|1\rangle$ in the first qubit, and it does so if $f(0)\neq f(1)$, hence relation above for $U_f|\psi_1\rangle$.

$$|\psi_3\rangle = H^{(1)}U_f|\psi_1\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)=f(1) \\ \pm|1\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)\neq f(1) \end{cases}$$

Now it is obvious that by measuring only once the first qubit, we read off the value of $f(0) \oplus f(1)$ as if $\begin{cases} f(0)=f(1), & f(0) \oplus f(1) = 0 \\ f(0) \neq f(1), & f(0) \oplus f(1) = 1 \end{cases}$! Note

that classically, we needed two operations that evaluate the value of f at each 0, 1 separately, but quantum mechanically, only one operation of gate U_f was required (well could argue that the state prep. and meas. (Hadamard gates) should be considered as the cost of the operation, but the whole point of this simple example is that if $f(x)$ was truely complicated such that the cost of its evaluation surpasses that of state prep. and meas., then the quantum algorithm would've given some speed up. Still in that case, it might be that a complicated f require many simple unitary operations and in the end one doesn't

gain anything. These are all legitimate concerns.
In fact, it is known that quantum number factoring algorithm by P. Shore is the only quantum algorithm in market with true exponential speed up compared with classical algorithms.

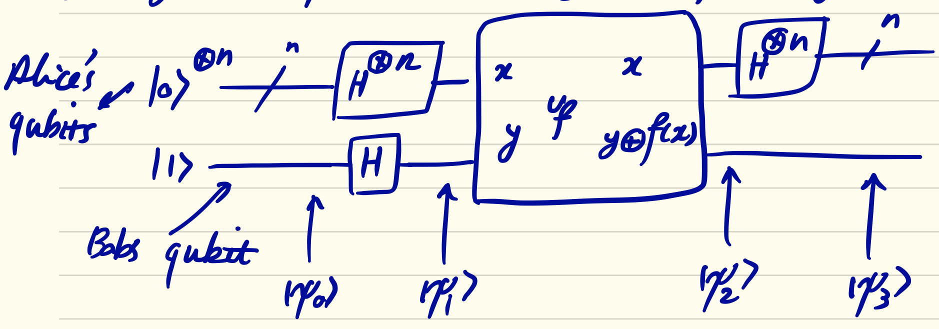
- The Deutsch-Jozsa algorithm

This is another algorithm related to Deutsch's algorithm that we talk about last time that signifies the quantum parallelism.

Consider Alice in London and Bob in DC. Alice mails in a letter a number from 0 to 2^n-1. Bob take the number he recieves from Alice, evaluates the function $f(x)$, $\{0, \dots, 2^{n-1}\} \to \{0,1\}$ at that x value and mails back the result to Alice. Bob only uses one of these functions:
$$\begin{cases} f(x) = \text{Const.} \\ f(x)=0 \text{ for half of } x \text{ values}, f(x)=1 \text{ for other half (Balanced)} \end{cases}$$

Find a quantum circuit that allows Alice to infer whether f is const. or balanced with only one communication with Bob!!

Let's see what is possible classically. Here, Alice needs to send at least $2^n/2+1$ distinct x to Bob to say with certainty if f is constant or balance. For example she can get $2^n/2$ zeros before getting 1, proving that f was not constant after all (the worst case scenario). Quantum mechanically such information can be inferred by only one operation through the following circuit:



Let's see what these gates do on the initial state:

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$$

$$|\psi_1\rangle = H^{\otimes n}|\psi_0\rangle H|1\rangle = \sum_{x=0}^{2^n-1} \frac{|x\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Note that: $H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

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

$$\vdots$$

So $H^{\otimes n}$ makes an equal superposition of all the basis vector of an n qubit system when acted on state $|0\rangle^{\otimes n}$: $H^{\otimes n}|0\rangle^{\otimes n} = \sum_{x=0}^{2^n-1} \frac{|x\rangle}{\sqrt{2^n}}$.

$$|\psi_2\rangle = U_f|\psi_1\rangle = \sum_{x=0}^{2^{n-1}} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|\psi_3\rangle = H^{\otimes n}|\psi_2\rangle = \sum_{z,x} \frac{(-1)^{x\cdot z + f(x)}}{2^n}|z\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

This comes from the following relation:

$$H^{\otimes n}|x\rangle \equiv H^{\otimes}|x_1 x_2 \cdots x_n\rangle = \sum_{z} \frac{(-1)^{z_1x_1 + \cdots + z_nx_n}}{\sqrt{2^n}}|z_1 z_2 \cdots z_n\rangle$$

$\downarrow$

Binary notation: $x_i = 0$ or 1

which is easy to verify by induction. Note that the notation we have used $x \cdot x$ means the inner product of the two vector in their binary representation.

$|\psi_3\rangle$ is a really interesting state. At this point Alice performs a measurement to find out what the state of her n-qubit system is. The cool thing is that if she find her qubits to be in $|00\cdots0\rangle \equiv |0\rangle$ state, she'll know Bob has used a constant function and if she measures anything but $|00\cdots0\rangle$, she'll know Bob has used a balanced function!! The reason is that according to $|\psi_3\rangle$ form, the probability amplitude for Alice's qubits to be in state $|00\cdots0\rangle$ is : $\sum_{x=0}^{2^n-1} \frac{(-1)^{f(x)}}{2^n}$. So with maximum probability (1), Alice's qubits end up in state $|00\cdots0\rangle$ if $f(x)$

always return 0 or 1. Since this probability is exhausted for state $|00\cdots0\rangle$, if Alice measures anything but $|00\cdots0\rangle$, she knows the function could've not been a constant as there would have remained no possibility for her qubits to end up anything else. So this is another example that the qubit correlations can keep information about the global properties of a function as all the function values are evaluated at once and in parallel!

If you are intrigued enough to learn more about quantum computation, here are a few possibilities offered by a quantum computer:

1) Cryptography : The key idea is in exponential speed up in quantum FT, and subsequent application in Shor's algorithm for factoring

numbers.

2) Quantum teleportation: Again the key idea is is the possibility of teleporting information in a parallel manner using quantum entanglement.

3) Quantum simulation of physical systems: Quantum many-body problem is a computationally complex problem as the Hilbert space grows exponentially (or faster) with the number of particles. Since there are 2^n amplitudes to store info about the wavefunction with only n qubits, certain quantum many-body problems can be sped up with QCs.

4) Quantum optimization: There are adiabatic and non-adiabatic algorithms that allows minimum of a cost function ("energy") to be found more efficiently.

And many more topics, including theoretical aspects of quantum information theory.

Finally, if you are truly intrigued, and want to get your hands dirty, don't wait! There are quantum cloud services you can log into, write your own quantum circuits and have it run on an actual quantum computer! Check out for example "IBM Quantum Experience".