Quantum Computing (Introduction)

- Logic gates are operations on bits
  - Classically, these can take any $0 \Leftrightarrow 1$ behavior:
    - + 1 bit gates are
      $I: 0\to 0, 1\to 1$; $NOT: 0\to 1, 1\to 0$; $ZERO: 0\to 0, 1\to 0$;
      $ONE: 0\to 1, 1\to 1$
    - + The simplest multibit gates take 2 bits to 1 bit. These include AND, OR, NAND, NOR

  - Quantum gates are a physical time evolution, so they are unitary operators
    - + ZERO and ONE are not unitary. But there are 2 new possibilities. All 1 qubit gates are

      $I: |0\rangle \to |0\rangle, |1\rangle \to |1\rangle$

      $NOT: |0\rangle \to |1\rangle, |1\rangle \to |0\rangle$

      $R(\phi): |0\rangle \to |0\rangle, |1\rangle \to e^{i\phi}|1\rangle$ "phase rotation"

      $H: |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1\rangle \to 1/\sqrt{2}(|0\rangle - |1\rangle)$ Hadamard
    - + In matrix form with

      $$|0\rangle \doteq \begin{bmatrix}1\\0\end{bmatrix}, \quad |1\rangle \doteq \begin{bmatrix}0\\1\end{bmatrix}$$

      $$I \doteq \begin{bmatrix}1&0\\0&1\end{bmatrix}, \quad NOT \doteq \begin{bmatrix}0&1\\1&0\end{bmatrix}, \quad R(\phi) \doteq \begin{bmatrix}1&0\\0&e^{i\phi}\end{bmatrix}, \quad H \doteq \frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}$$
    - + There cannot be 2 qubit $\to$ 1 qubit gates!
    - + There are 2 qubit $\to$ 2 qubit gates. Take "controlled-NOT" or CNOT as an example. This reverses the 2nd qubit if the 1st is $|1\rangle$ or

      $CNOT: |0\rangle|0\rangle \to |0\rangle|0\rangle, \quad |0\rangle|1\rangle \to |0\rangle|1\rangle$

      $|1\rangle|0\rangle \to |1\rangle|1\rangle, \quad |1\rangle|1\rangle \to |1\rangle|0\rangle$

      You can represent this as addition mod 2

      $$CNOT(|x\rangle|y\rangle) = |x\rangle|x \oplus y\rangle$$
    - + How you actually carry out a quantum gate depends on how you realize a qubit

- No-Cloning Theorem: Can you copy a qubit without measuring it and destroying superpositions?

- Let's suppose we have 2 qubits in state $|\psi\rangle_1 |0\rangle_2$ where $|\psi\rangle$ is an unknown superposition of $|0\rangle + |1\rangle$
  - A "copy" operation C would take
  $$C(|\psi\rangle_1 |0\rangle_2) = |\psi\rangle_1 |\psi\rangle_2 \quad \text{for any } |\psi\rangle$$
  - C must be unitary, so $C^\dagger C = 1$
  - For $|\psi\rangle \neq |\phi\rangle$, consider inner product of $|\alpha\rangle = C(|\psi\rangle_1 |0\rangle_2)$ with $|\beta\rangle = C(|\phi\rangle_1 |0\rangle_2)$. We know $|\alpha\rangle = |\psi\rangle_1 |\psi\rangle_2$ and $|\beta\rangle = |\phi\rangle_1 |\phi\rangle_2$, so $\langle\alpha|\beta\rangle = \langle\psi|\phi\rangle_1 \langle\psi|\phi\rangle_2$ $= (\langle\psi|\phi\rangle)^2$.
  - But also $\langle\alpha|\beta\rangle = (\langle\psi|_1 \langle 0|_2) C^\dagger C (|\phi\rangle_1 |0\rangle_2) = \langle\psi|\phi\rangle_1 \langle 0|0\rangle_2$ $= \langle\psi|\phi\rangle$.
  - This can only be true if $|\psi\rangle = |\phi\rangle$ or $\langle\psi|\phi\rangle = 0$. So C cannot copy all qubits!

— Quantum Teleportation: We can't copy an unknown qubit, but we can send it somewhere else

- Specifically, we have unknown qubit #1 $|\psi\rangle_1 = a|0\rangle_1 + b|1\rangle_1$. We will turn qbit #1 into something else and a different qubit into $|\psi\rangle$
  - To be concrete, let a qubit be an electron spin $|0\rangle = |\downarrow\rangle$, $|1\rangle = |\uparrow\rangle$
  - To prepare the procedure, take qubit $|\psi\rangle_1$ and 2 other electrons in spin state
  $$|S=0\rangle_{2,3} = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_2 |\downarrow\rangle_3 - |\downarrow\rangle_2 |\uparrow\rangle_3\right)$$
  - Keep #2 with #1 and send #3 to receiver. But the state of the system is still
  $$|\Psi\rangle = |\psi\rangle_1 |S=0\rangle_{2,3} = \frac{a}{\sqrt{2}}\left(|\uparrow\rangle_1 |\uparrow\rangle_2 |\downarrow\rangle_3 - |\uparrow\rangle_1 |\downarrow\rangle_2 |\uparrow\rangle_3\right)$$
  $$+ \frac{b}{\sqrt{2}}\left(|\downarrow\rangle_1 |\uparrow\rangle_2 |\downarrow\rangle_3 - |\downarrow\rangle_1 |\downarrow\rangle_2 |\uparrow\rangle_3\right)$$

- Procedure:
  - We still have qubits #1 + #2 and can measure them.
  - We will measure $(S_z^{(tot)})^2$ of these 2 spins. The e'values + e'states are

$S_z^2 = 0 \begin{cases} |1\rangle_{1,2} = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2) \\ |2\rangle_{1,2} = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\downarrow\rangle_2 + |\downarrow\rangle_1|\uparrow\rangle_2) \end{cases}$, $S_z^2 = 1 \begin{cases} |3\rangle_{1,2} = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\uparrow\rangle_2 + |\downarrow\rangle_1|\downarrow\rangle_2) \\ |4\rangle_{1,2} = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\uparrow\rangle_2 - |\downarrow\rangle_1|\downarrow\rangle_2) \end{cases}$

+ So after this measurement, we know qubits #1 + #2 are either in $\{|1\rangle, |2\rangle\}$ if $S_z^2 = 0$ or $\{|3\rangle, |4\rangle\}$ if $S_z^2 = 1$
+ In the 1st case, measure $\vec{S}_{tot}^2$. If $s=0$, state $|1\rangle_{1,2}$, if $s=1$, state $|2\rangle_{1,2}$. In the 2nd case, measure S_x^2 to distinguish $|3\rangle_{1,2}$ from $|4\rangle_{1,2}$

+ We can rewrite the initial total state as

$$|\Psi\rangle = \tfrac{1}{2}\Big[|1\rangle_{1,2}(-a|\uparrow\rangle_3 + b|\downarrow\rangle_3) + |2\rangle_{1,2}(-a|\uparrow\rangle_3 - b|\downarrow\rangle_3) + |3\rangle_{1,2}(a|\downarrow\rangle_3 - b|\uparrow\rangle_3) + |4\rangle_{1,2}(a|\downarrow\rangle_3 + b|\uparrow\rangle_3)\Big]$$

+ After our measurements, $|\Psi\rangle$ has collapsed to one of these 4 terms. Further, by using an appropriately chosen NOT_3 or $R(\pi)_3$, which we can choose by our measurement, the receiver can turn qubit #3 to $|\psi\rangle_3$

- Note again: We start with #2 + #3 entangled. By entangling #1 w/ #2 using our measurements, we disentangle #3. This transfers $|\psi\rangle_1$ to $|\psi\rangle_3$ (Entanglement is a computational resource)

— Deutsch's Algorithm

- Qubits can be superposed so it's possible to do a form of parallel computing on a single qubit. Deutsch's algorithm is a somewhat contrived example but is the 1st to show a speed up vs classical computing

- Suppose we have a function $f: \{0,1\} \to \{0,1\}$
There are 4 possibilities (the 4 classical 1-bit gates)

$\begin{matrix} 0\to0 \\ 1\to0 \end{matrix}$, $\begin{matrix} 0\to1 \\ 1\to0 \end{matrix}$, $\begin{matrix} 0\to0 \\ 1\to1 \end{matrix}$, $\begin{matrix} 0\to1 \\ 1\to1 \end{matrix}$

+ These are in 2 categories: even # of 1s or odd # of 1s
+ Classically, to find which category f is in,
we must evaluate f(0) and f(1).

• Algorithm
+ Implement f on qubits by "f-controlled NOT" f-CNOT
$$f\text{-CNOT}: \left(|x\rangle_1 |y\rangle_2\right) = |x\rangle_1 |f(x)\oplus y\rangle_2$$
+ We start with 2 qubits $|0\rangle_1 |1\rangle_2$ and take $\mathbb{H}_1, \mathbb{H}_2$ to get state
$$|\psi\rangle = \tfrac{1}{2}\left(|0\rangle_1|0\rangle_2 - |0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2 - |1\rangle_1|1\rangle_2\right)$$
+ Act with f-CNOT. This gives

$$f\text{-CNOT}\,|\psi\rangle = \tfrac{1}{2}|0\rangle_1\left(|f(0)\rangle_2 - |f(0)\oplus 1\rangle_2\right) + \tfrac{1}{2}|1\rangle_1\left(|f(1)\rangle_2 - |f(1)\oplus 1\rangle_2\right)$$
+ Now, notice for any f
$$|f\rangle - |f\oplus 1\rangle = \begin{cases} |0\rangle - |1\rangle & (f=0) \\ |1\rangle - |0\rangle & (f=1) \end{cases} = (-1)^f\left(|0\rangle - |1\rangle\right)$$
Therefore
$$f\text{-CNOT}\,|\psi\rangle = (-1)^{f(0)}\left(\tfrac{1}{2}\right)\left(|0\rangle_1 + (-1)^{f(0)+f(1)}|1\rangle_1\right)\left(|0\rangle_2 - |1\rangle_2\right)$$

+ Act again with $\mathbb{H}_1, \mathbb{H}_2$. Since our state is factorized, we just need to know
$$\mathbb{H}_2\left(\tfrac{1}{\sqrt{2}}\left(|0\rangle_2 - |1\rangle_2\right)\right) = |1\rangle_2$$
and
$$\mathbb{H}_1\left(\tfrac{1}{\sqrt{2}}\left(|0\rangle_1 + (-1)^{f(0)+f(1)}|1\rangle_1\right)\right) = \begin{cases} |0\rangle & \text{if } f(0)+f(1) \text{ even} \\ |1\rangle & \text{if odd.} \end{cases}$$
+ Then we just need to measure qubit #1 to get the answer.

• This only requires us to evaluate f once (though we do have to use Hadamard operators). But suppose we have a function $f(x_1, \ldots x_N) = \{0, 1\}$. Classically, we must evaluate a lot but still only once in a quantum computer!

• There are major speed increases for searching (Grover) and prime factorization (Shor) — important for encryption.