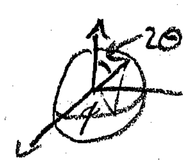
Quantum Computing (+ Information)

- Classical vs Quantum Information + Logic
  - Classical information comes in bits
    - This is the smallest unit of information: yes/no or 0 vs 1. You can also do math by stringing bits as binary numbers
    - We process information (or compute) with operations called logic gates
      - 1 bit gates: $I: 0 \to 0,\ 1 \to 1$ (identity)
        NOT: $0 \to 1,\ 1 \to 0$; ZERO: $0 \to 0,\ 1 \to 0$; ONE: $0 \to 1,\ 1 \to 1$
        You can see these are all 4 possibilities
      - There are of course multi-bit gates.
        The simplest take 2 bits to 1 bit: AND, OR, NAND, NOR
  - Quantum information comes in qubits aka qbits
    - A 1D Hilbert space has only 1 state = no information. Qbits live in 2D Hilbert space
      - Define $0 = |0\rangle$ and $1 = |1\rangle$ as orthonormal basis vectors
        By superposition, one qbit has a continuous amount of info.
      - Specifically, the most general qbit is $|\psi\rangle = \cos\theta|0\rangle + \sin\theta e^{i\phi}|1\rangle$ (up to physically non-meaningful overall phase).
        This can be represented by the Bloch sphere



    - Perform logic operations with Quantum gates
      - To do these physically, you have to allow some kind of quantum evolution $\Rightarrow$ quantum gates are unitary operators
      - Tells us that ZERO and ONE are not valid quantum gates
        However, there are 2 new quantum gates
        "phase rotation" $R: |0\rangle \to |0\rangle,\ |1\rangle \to e^{i\phi}|1\rangle$
        "Hadamard" $H: |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

+ Unitary operation also means there are no 2qbit → 1qbit gates (like the classical AND, OR, NAND, NOR). Instead there are 2qbit → 2qbit gates. We consider the "controlled-NOT" or CNOT gate

$$\text{CNOT}: |0\rangle|0\rangle \to |0\rangle|0\rangle,\ |0\rangle|1\rangle \to |0\rangle|1\rangle,\ |1\rangle|0\rangle \to |1\rangle|1\rangle,$$
$$|1\rangle|1\rangle \to |1\rangle|0\rangle \quad = \text{reverse } 2^{nd} \text{ if } 1^{st} \text{ is } 1.$$

+ CNOT can be represented by addition mod 2

$$\text{CNOT}(|x\rangle|y\rangle) = |x\rangle\,|x\oplus y\rangle \quad \text{where } \oplus = + \text{ mod } 2$$

+ How you do a quantum gate depends on physical realization of qbits.

- No-Cloning Theorem
  - Of course, you can copy + measure classical data easily. We do it all the time.
  - If you measure a qbit, you destroy it by "collapsing the wavefunction." Can you copy it?
  - Trial "copier": We have particle 1 in state $|\psi\rangle$ (unknown) and particle 2 in state $|0\rangle$.
    - Then a "copy" operator $C(|\psi\rangle_1|0\rangle_2) = |\psi\rangle_1|\psi\rangle_2$ for any state $|\psi\rangle$.
    - C must be unitary, so $C^\dagger C = 1$.
    - If $|\psi\rangle \neq |\phi\rangle$, Consider the inner product of $C(|\psi\rangle_1|0\rangle_2)$ with $C(|\phi\rangle_1|0\rangle_2)$

      + $C|\psi\rangle_1|0\rangle_2 = |\psi\rangle_1|\psi\rangle_2$, $C|\phi\rangle_1|0\rangle_2 = |\phi\rangle_1|\phi\rangle_2$

      $$\Rightarrow {}_1\langle\psi|\,{}_2\langle 0|C^\dagger C|\phi\rangle_1|0\rangle_2 = \langle\psi|\phi\rangle_1\langle\psi|\phi\rangle_2 = (\langle\psi|\phi\rangle)^2$$

      + But the inner product also

      $$= ({}_1\langle\psi|\,{}_2\langle 0|)C^\dagger C(|\phi\rangle_1|0\rangle_2) = {}_1\langle\psi|\phi\rangle_1\,{}_2\langle 0|0\rangle_2 = \langle\psi|\phi\rangle$$

      + That's impossible unless $\langle\psi|\phi\rangle = 0$ or $|\psi\rangle = |\phi\rangle$!

      See Griffiths §12.3 for alternate proof.
  - It is not possible to "clone" an unknown qbit.

- Teleportation
  - Suppose you have an <u>unknown</u> qbit $|\psi\rangle = a|0\rangle + b|1\rangle$. You can "send" it to some one at a distance. Specifically, you turn your qbit into something else, while the other qbit becomes $|\psi\rangle$.
    - For concreteness, let each qbit be an electron's spin state with $|0\rangle = |\Downarrow\rangle$ and $|1\rangle = |\Uparrow\rangle$
    - We have the unknown qbit $|\psi\rangle_1$ and 2 electrons in the spin singlet

$$|s=0\rangle_{2,3} = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_2|\downarrow\rangle_3 - |\downarrow\rangle_2|\uparrow\rangle_3\right).$$ We keep electron #2 and send #3 elsewhere.

    - Teleportation "ruins" the state of electron #1 and turns #3 into $|\psi\rangle_3$

  - Procedure:
    - The total state of the system is

$$|\Psi\rangle = |\psi\rangle_1|s=0\rangle_{2,3} = \frac{a}{\sqrt{2}}\left(|\uparrow\rangle_1|\uparrow\rangle_2|\downarrow\rangle_3 - |\uparrow\rangle_1|\downarrow\rangle_2|\uparrow\rangle_3\right) + \frac{b}{\sqrt{2}}\left(|\downarrow\rangle_1|\uparrow\rangle_2|\downarrow\rangle_3 - |\downarrow\rangle_1|\downarrow\rangle_2|\uparrow\rangle_3\right)$$

    - We have control over electrons #1 + #2 + can measure them.
      + The operator $\left(S_z^{(total)}\right)^2$ has eigenvalues and eigenvectors

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

This is not quite the eigenbasis for $S_z^{(tot)}$

      + We can determine which state $|1\rangle, |2\rangle, |3\rangle, |4\rangle$ our electrons are in by measuring $\left(S_z^{(tot)}\right)^2$ then (a) $\left(\vec{S}^{(tot)}\right)^2$ if $S_z^2 = 0$ or (b) $\left(S_x^{(tot)}\right)^2$ if $S_z^2 = 1$
    - The total state can be written

$$|\Psi\rangle = |1\rangle_{1,2}\left(-\frac{a}{2}|\uparrow\rangle_3 + \frac{b}{2}|\downarrow\rangle_3\right) + |2\rangle_{1,2}\left(-\frac{a}{2}|\uparrow\rangle_3 - \frac{b}{2}|\downarrow\rangle_3\right)$$

$$+ |3\rangle_{1,2}\left(\frac{a}{2}|\downarrow\rangle_3 - \frac{b}{2}|\uparrow\rangle_3\right) + |4\rangle_{1,2}\left(\frac{a}{2}|\downarrow\rangle_3 + \frac{b}{2}|\uparrow\rangle_3\right)$$

      + The state of the 3rd particle is determined after our measurement!
      + We can turn any of these states into $|\psi\rangle$ (up to a phase) by a partial spin-flip: exposing the electron to a $\vec{B}$-field in the right direction for the right length of time.

Quantum Algorithms

- Due to superposition, it's possible to do <u>parallel</u> computing on one qbit! We'll study a somewhat contrived example below.
- Consider some function $f: \{0,1\} \to \{0,1\}$. 1 bit/qbit (like
  - There are 4 such functions: $\begin{matrix} 0\to 0 \\ 1\to 0 \end{matrix}$, $\begin{matrix} 0\to 1 \\ 1\to 0 \end{matrix}$, $\begin{matrix} 0\to 0 \\ 1\to 1 \end{matrix}$, $\begin{matrix} 0\to 1 \\ 1\to 1 \end{matrix}$
    - + These equal the 4 classical 1 bit gates
    - + These fall into 2 categories: 50% 1's or 0/100% 1's.
  - Classically, if we want to know which category an unknown function f is in, we must evaluate f twice.
- Deutsch's Algorithm (1st quantum algorithm with a "speed-up")
  - Again, we want to ask if f evaluates to 50% 1's or not.
  - Define the evaluation of f through "f-controlled NOT" or

$$f\text{-CNOT}(|x\rangle|y\rangle) = |x\rangle|f(x)\oplus y\rangle$$ ← a bit like CNOT.

  - Start with 2 qbit state $|0\rangle_1|1\rangle_2$
    - + Act with H on both qbits, so state $\to |\psi\rangle = \frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle)$
    - + Act on $|\psi\rangle$ with f-CNOT. This is

$$\tfrac{1}{2}|0\rangle_1(|f(0)\rangle - |f(0)\oplus 1\rangle)_2 + \tfrac{1}{2}|1\rangle_1(|f(1)\rangle - |f(1)\oplus 1\rangle)_2$$

    - + Note that $|f\rangle - |f\oplus 1\rangle = \left\{ \begin{matrix} |0\rangle - |1\rangle \\ \text{or} \\ |1\rangle - |0\rangle \end{matrix} \right\} = (-1)^f(|0\rangle - |1\rangle)$

so our state is

$$\tfrac{1}{2}\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right]_1(|0\rangle - |1\rangle)_2 = (-1)^{f(0)}\tfrac{1}{2}\left[|0\rangle + (-1)^{f(0)+f(1)}|1\rangle\right]_1 \cdots$$

    - + Act again with H on both states.

$$H\left(\tfrac{1}{\sqrt{2}}(|0\rangle_2 - |1\rangle_2)\right) = |1\rangle_2$$

$$H\left(\tfrac{1}{\sqrt{2}}(|0\rangle_1 + (-1)^{f(0)+f(1)}|1\rangle_1)\right) = |f(0)\oplus f(1)\rangle_1$$

$$= \begin{cases} |0\rangle & \text{if } f \text{ NOT } 50\% \text{ 1's} \\ |1\rangle & \text{if } f \text{ is } 50\% \text{ 1's} \end{cases}$$

  - The H operations reduce the speed-up. BUT it is possible to generalize to $f(x_1, \dots x_N) = \{ {0 \atop 1} \}$ and still only evaluate f once!
  - There are also major speed-ups for searching (Grover) + factorization (Shor), etc