2. Quantum Computational Models

ANIMESH DATTA

(warwick.ac.uk/qinfo)

Church-Turing thesis: is a hypothesis about the nature of computable functions.

The heuristic agreement is that all algorithmically computable functions are Turing-computable.

↓

Crudely speaking, this is a classical computer with unlimited memory.

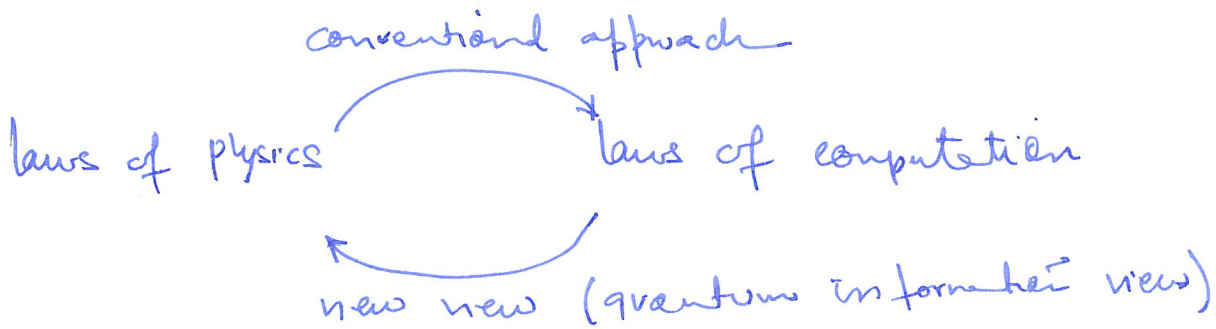
But it addresses and suggests connection to the space and time requirements for computations. It asks fundamental questions such as

1. What is physical computation?
2. What is the potential and limitation of physical computation?
3. What is meant by the universality of computation?

The long-standing open question is its derivation from the laws of physics. A modern, sharper conjecture:

~~Theory~~ Church-Turing-Deutsch Principle:

> Every physical process can be simulated efficiently by a universal computing device.



→ Nature is a massive computing device.

→ The laws of physics (including the undiscovered theories of the future) accomodate the notion of universal computation.

Current Status & observation: Classical Computers do not seem to be able to simulate quantum systems efficiently.

Possible resolutions: ① A quantum Turing machine should be a universal computing model.

② An efficient classical simulation of quantum systems is indeed possible.

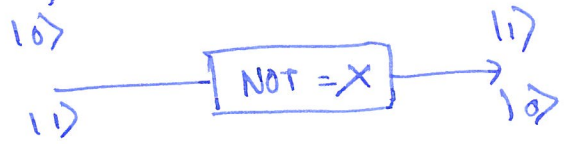
The following models are known to be universal computing devices/systems:

- Quantum Turing machine
- Quantum circuit model → quantum cellular automata
  → Topological computation
  → Holonomic computation
- Quantum adiabatic computation
- Quantum random walk
- Measurement-based quantum computation.
  → teleportation-based
  → Entanglement-based.

Quantum circuits:

bit strings $\longleftrightarrow$ state vectors
gates $\longleftrightarrow$ unitary operations
measurements $\longleftrightarrow$ Born rule for probs.

Since vectors (and operators) need a basis, we will conventionally use the eigenstates of a Pauli-Z operator: $|0\rangle$ and $|1\rangle$.



$$X|a\rangle = |\bar{a}\rangle = |1 \oplus a\rangle$$

← (Eigen states)

Measurement:

$$p_0 = |\langle 0|+\rangle|^2 = 1/2$$
$$p_1 = |\langle 1|+\rangle|^2 = 1/2$$

In general:

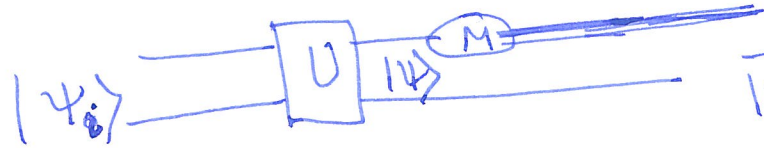
$$= \alpha(U_{11}|0\rangle + U_{21}|1\rangle) + \beta(U_{12}|0\rangle + U_{22}|1\rangle)$$
$$= \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

For the conservation of probabilities:

$$(\alpha^* \beta^*) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = 1$$
$$(\alpha^* \beta^*) U^\dagger U \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = 1$$
$$\Rightarrow U^\dagger U = \mathbb{I} \quad \therefore (U \text{ is unitary})$$

A general measurement:

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$



$$0: p_0 = |c_{00}|^2 + |c_{01}|^2$$
$$1: p_1 = |c_{10}|^2 + |c_{11}|^2$$
$$|\psi_0\rangle = \frac{c_{00}|0\rangle + c_{01}|1\rangle}{\sqrt{p_0}}$$
$$|\psi_1\rangle = \frac{c_{10}|0\rangle + c_{11}|1\rangle}{\sqrt{p_1}}$$

$$p_0 = |\langle 00|U|\psi_i\rangle|^2 + |\langle 01|U|\psi_i\rangle|^2$$

$$= \langle \psi_i|U^\dagger|00\rangle\langle 00|U|\psi_i\rangle + \langle \psi|U^\dagger|01\rangle\langle 01|U|\psi\rangle$$

$$= \langle \psi_i|U^\dagger(P_0 \otimes I)U|\psi_i\rangle$$

where $P_0 = |0\rangle\langle 0| \otimes I$

$= |00\rangle\langle 00| + |01\rangle\langle 01|$.

and the state after the measurement is $\frac{1}{\sqrt{p_0}}(P_0 \otimes I)U|\psi_{in}\rangle$

So, what's going on?

1. An arbitrary classical gate M becomes a linear operator

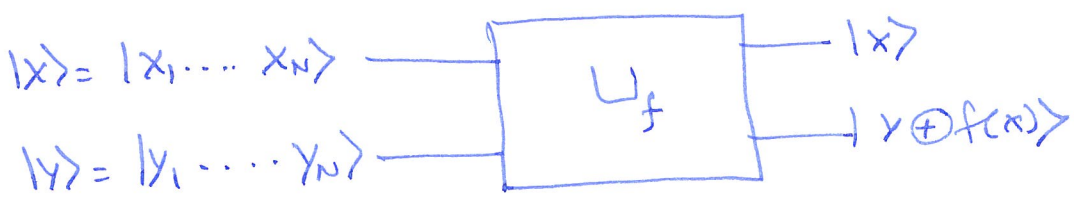
$$A|x\rangle = |M_x\rangle, \quad \langle y|A|x\rangle = \delta_{y,M_x}$$

2. A reversible classical gate becomes a permutation unitary

3. There are many more unitaries than reversible classical gates.

4. Born rule for measurements.

Function evaluation in quantum circuits:



If f is a Boolean function, U_f is a controlled bit-flip op.

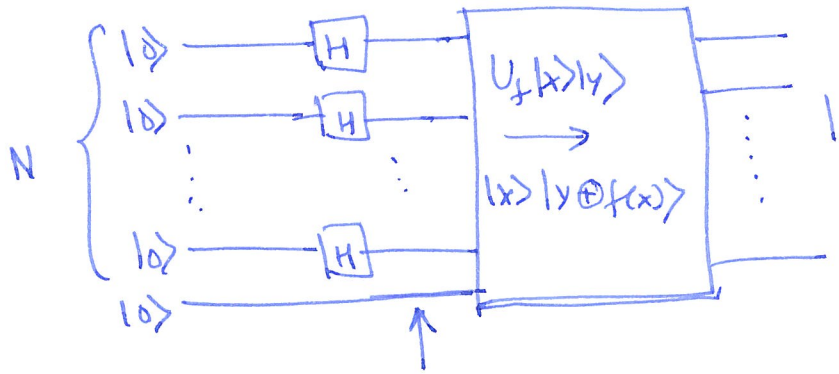
The control qubits are $|x\rangle = |x_1 \cdots x_N\rangle$, the value of the control is determined by $f(x)$.

If $f(x)=0$, the target qubit remains unchanged,

If $f(x)=1$, " " " flips.

$$U_f|x\rangle|y\rangle = |x\rangle|y\oplus f(x)\rangle = |x\rangle \otimes X^{f(x)}|y\rangle.$$

Quantum parallelism: f on an N-bit Boolean function.



$$|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_x |x\rangle|f(x)\rangle$$

All values of $f(x)$ calc. in parallel

$$|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_x |x\rangle|0\rangle$$

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

$$H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

$H^{\otimes N}$ – Walsh-Hadamard transform

$$H^{\otimes N}|0\rangle^{\otimes N} = \left[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right]^{\otimes N} = \frac{1}{\sqrt{2^N}} \sum_x |x\rangle$$

→ all possible bit strings

For any bit b:

$$H|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle) = \frac{1}{\sqrt{2}} \sum_x (-1)^{bx}|x\rangle$$

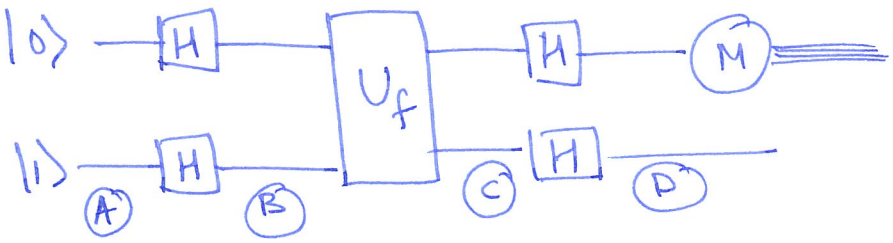
For any bit string s:

$$H^{\otimes N}|s\rangle = \frac{1}{\sqrt{2^N}} \sum_{x_1,\ldots x_N} (-1)^{x_1 s_1 + \cdots x_n s_n} |x_1 \ldots x_N\rangle = \frac{1}{\sqrt{2^N}} \sum_x (-1)^{x\cdot s}|x\rangle$$

Deutsch's algorithm:

$f: \{0,1\} \longrightarrow \{0,1\}$

1-bit Boolean function



One shot determination of parity of f.

(A): $|\psi_A\rangle = |0\rangle \otimes |1\rangle$

(B) $|\psi_B\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$

(C) $|\psi_C\rangle = \frac{1}{2}\left(|0\rangle|f(0)\rangle - |0\rangle|\overline{f(0)}\rangle + |1\rangle|f(1)\rangle - |1\rangle|\overline{f(1)}\rangle\right)$

$$= \begin{cases} \frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle) & : f(0)=f(1)=0 \\ \frac{1}{2}(|0\rangle-|1\rangle)(|0\rangle-|1\rangle) & : f(0)=0,\ f(1)=1 \\ -\frac{1}{2}(|0\rangle-|1\rangle)(|0\rangle-|1\rangle) & : f(0)=1,\ f(1)=1 \\ -\frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle) & : f(0)=f(1)=1 \end{cases}$$

Last two are the same.

$$= \frac{1}{2}(-1)^{f(0)}\left(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right)(|0\rangle - |1\rangle).$$

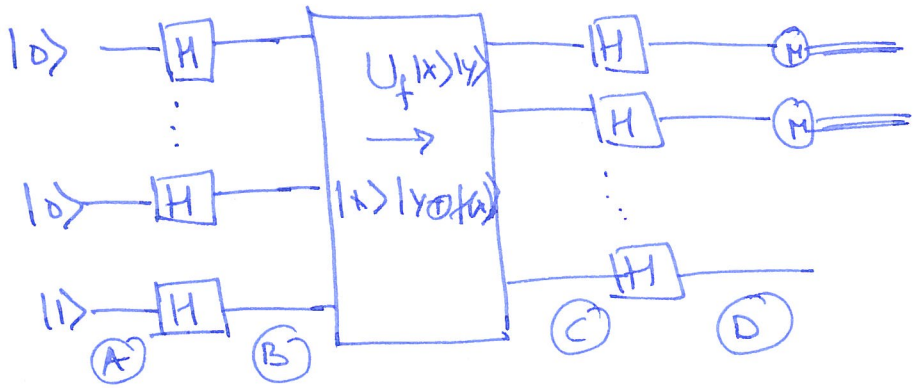
(D) $|\psi_D\rangle = (-1)^{f(0)}\,|f(0)\oplus f(1)\rangle\,|1\rangle$

Any classical algorithm to determine the parity of f, or whether f is constant or balanced, needs two runs. Deutsch does it in one.

Deutsch-Jozsa algorithm: to determine whether

$f : \{0,1\}^N \longrightarrow \{0,1\}$ is constant or balanced.

The number of classical calls to be sure is $\frac{2^N}{2} = 2^{N-1}$.



Quantum strategy needs just one shot.
Exponential adv. but needs an oracle U_f.

(A): $|\psi_A\rangle = |0\rangle^N \otimes |1\rangle$

(B): $|\psi_B\rangle = H^{\otimes N}|0\rangle^{\otimes N} \otimes H|1\rangle$

$$= \frac{1}{\sqrt{2^N}} \sum_x |x\rangle \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

(C) $$|\psi_C\rangle = \frac{1}{\sqrt{2^N}} \sum_x |x\rangle \frac{1}{\sqrt{2}}\left(|f(x)\rangle - |\overline{f(x)}\rangle\right)$$

$$= \left(\frac{1}{\sqrt{2^N}} \sum_x (-1)^{f(x)} |x\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$|\phi\rangle \equiv$ function value in phase — ancilla qubit uncorrelated

$$\langle \phi^{\text{const}} | \phi^{\text{balanced}} \rangle = \pm \sum_x (-1)^{f(x)} = 0$$

(D) $$|\psi_D\rangle = \left(\frac{1}{\sqrt{2^N}} \sum_{x,y} (-1)^{f(x)\oplus x\cdot y} |y\rangle\right)(|1\rangle)$$

$|\chi\rangle$

constant f: $|\chi\rangle = \pm|0\rangle^N$

balanced f:

$$^N\langle 0|\chi\rangle = \frac{1}{2^N} \sum_x (-1)^{f(x)} = 0$$