Quantum computation - circuit model

- steps: basic unitary gates acting on qubit lines
- initial state $|i_1\rangle \ldots |i_n\rangle |0\rangle \ldots |0\rangle$ for input $x = i_1 \ldots i_n \in B_n$
- output: measure one (or more) qubits at end
- can allow intermediate measurements (mmts) as steps but adds nothing new - principle of deferred mmts

Universal sets of gates

General U on n qubits - ~~gates~~ parameters, so no finite set of gates can be universal. Ask for approx universality for

for any $\epsilon > 0$ any U on n qubits there is a circuit $\tilde{U}$ s.t.

$$\|U - \tilde{U}\| < \epsilon \quad \text{i.e.} \quad \max_{\langle\psi|\psi\rangle = 1} \|U|\psi\rangle - \tilde{U}|\psi\rangle\| < \epsilon$$

Facts $\{CX, \text{all 1-qubit gates}\}$ infinite set is exactly universal

$\{H, T = P_{\pi/4} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, CX\}$ is approx universal

Complexity class BQP (bounded error quantum poly-time) class of decision problems computable with poly-sized quantum circuits & p_{acc} (ans correct) $> 2/3$.
Can show - BQP independent of choice of approx universal gate set,

- $BPP \subseteq BQP$
- is $BQP \supsetneq BPP$? unproven!

Reversible version of any Boolean $f: B_m \to B_n$

Fact (a) for any classical comp, there is an equivalent comp that uses only reversible (invertible) Boolean gates, with modest (poly) overhead of space/time resources
(b) for any reversible Boolean $f: B_n \to B_n$ (permutation of ~~n~~-bit strings) the linear map on n qubits defined by

$$U: |x\rangle \to |f(x)\rangle \quad , |x\rangle = |i_1\rangle \ldots |i_n\rangle$$

by linear extension to general vector $|v\rangle = \sum_x a_x |x\rangle$ is unitary

Hence, classical comp appears as a special case of quantum comp.

Let $f : B_m \to B_n$, $x \mapsto z_y = f(x)$, $x \in B_m$, $z_y \in B_n$

Consider $\tilde{f} : B_{m+n} \to B_{m+n}$

$(x, y) \longmapsto (x, y \oplus f(x))$

x: input/output register; y: output register

$\oplus$ is bitwise addition of n-bit strings mod 2, i.e. addition in $(\mathbb{Z}_2)^n$ (not $\mathbb{Z}_{2^n}$)

e.g. $\begin{array}{r} 011 \\ 110 \\ \hline 101 \end{array}$ $\oplus$

$f \leftrightarrow \tilde{f}$ each easily given the other

<u>Lemma</u> $\tilde{f}$ always reversible, actually self inverse

note $x \oplus x = 0$ all x, i.e. $x = -x$

then $(x, y) \xrightarrow{\tilde{f}} (x, y \oplus f(x)) \xrightarrow{\tilde{f}} (x, y \oplus \underbrace{f(x) \oplus f(x)}_{=0})$

Next if $g : B_n \to B_n$, $x \mapsto g(x)$ is reversible

then linear map A defined by $A : |x\rangle \longmapsto |g(x)\rangle$ on n qubits is unitary because x^{th} col of matrix of A on vector $A|x\rangle = |g(x)\rangle$ & clearly $|g(x)\rangle$ are all o.n.

Hence for any $f : B_m \to B_n$ get unitary map on $m+n$ qubits denoted U_f

$U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ implementing $\tilde{f}$ on comp bases states.

Computation by quantum parallelism $f : B_m \to B_n$

Have $|x\rangle_m |0 \ldots 0\rangle_n \xrightarrow{U_f} |x\rangle|f(x)\rangle$

so by linearity

$$\left(\frac{1}{\sqrt{2^m}} \sum_{\text{all } x} |x\rangle\right) |0 \ldots 0\rangle \xrightarrow{U_f} \underline{\frac{1}{\sqrt{2^m}} \sum_{\text{all } x} |x\rangle |f(x)\rangle}$$

One run of U_f get $|f\rangle$ that embodies all $|f\rangle$ exponentially many values $f(x)$'s.

Furthermore $|\psi\rangle = \frac{1}{\sqrt{2^m}} \sum_{\text{all } x} |x\rangle$ has exponentially many, but can be made in linear time by n H's $|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ so $|0\rangle \ldots |0\rangle \xrightarrow{\otimes^n H} \frac{1}{\sqrt{2^n}}(|0\rangle+|1\rangle)\ldots(|0\rangle+|1\rangle) = |\psi\rangle$