Q. Complexity

P poly time deterministic

eg. determinant, shortest path

BPP poly time randomized
$\Pr[\text{correct}] \geq 2/3$

$\cong \Pr[\text{correct}] \geq \frac{1}{2} + \frac{1}{n^c}$ or $1 - \exp(-n^c)$

e.g. volume estimation

NP $\exists$ poly time algo A s.t.
$x \in L \Rightarrow \exists y \quad |y| \leq |x|^c, \; A(x,y) = 1$
$x \notin L \Rightarrow \forall y \quad |y| \leq |x|^c, \; A(x,y) = 0$

3-SAT $\phi(y) = (y_2 \vee \overline{y_5} \vee y_6) \wedge (\overline{y_1} \vee y_5 \vee y_7) \wedge \ldots$

MA $\exists$ randomized p time A s.t
$x \in L$ - - - $\Pr(A=1) \geq 2/3$
$x \notin L$ $\forall y$ $\Pr(A(x,y)=1) \leq 1/3$

AM $x \in L \Rightarrow \mathop{\mathbb{E}}_{r} \mathop{V}_{y} A(x,r,y) \geq 2/3$

$\leq 1/3$

approx county 3-SAT solutions

BQP poly time q algo

factoring, H simulation

QMA can verify answer with a q computer

amplification using multiple copies of witness

Complete problems

A (ptime) reduction from L to M means an algorithm for L that uses an M-solver as a subroutine

example can reduce det to finding evalues

$$\det A = \prod_i \lambda_i$$

L is NP-hard if $\forall M \in NP$ M is ptime reducible to L

$$NP\text{-complete} = NP \cap NP\text{-hard}$$

Circuit-SAT is NP-complete

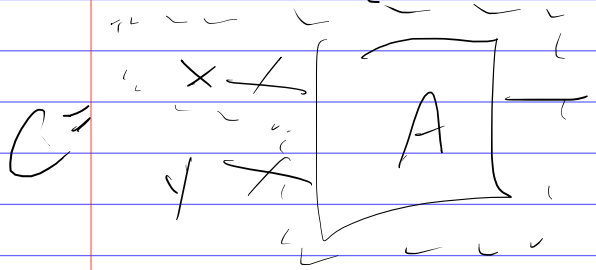
$$= \{ C \text{ a circuit s.t. } \exists x,\ C(x) = 1 \}$$

In NP: witness is x

$\forall L \in NP$, say Hamiltonian cycle
$\exists$ a ptime verifier A

$$x \in L \iff \exists y \text{ s.t. } A(x,y) = 1$$

Turn A into a circuit.
hardwire x inputs



Local Hamiltonian is QMA-complete

Schr eq. $\frac{d}{dt}|\psi\rangle = \frac{H}{i\hbar}|\psi\rangle$ $H = H^\dagger$ Hamiltonian

k-qubit gate $\cong$ k-qubit term

time evolution e^{-iHt}

thermal state $\frac{e^{-H/T}}{\mathrm{Tr}\, e^{-H/T}} \to |g\rangle\langle g|$ as $T \to 0$

lowest energy state. $H|g\rangle = E_0|g\rangle$

can we find it?

$x_1 \vee \bar{x}_2 \vee \bar{x}_3 \iff |011\rangle\langle 011|$

E_0 = min # violated clauses

can also have non-commuting terms

e.g. TFIM $-\sum_{(i,j)\in E} Z_i Z_j - g\sum_i X_i$

Local Hamiltonian problem

given H, estimate E_0

more precisely given H, a, b s.t. $a > b + \frac{1}{\mathrm{poly}(n)}$

determine if $E_0 \geq a$ or $E_0 \leq b$

"promise problem"

In QMA

witness is $|\psi\rangle$

do e^{-iHt} and phase estimation

QMA-complete

verification circuit is $U_1, \ldots, U_T$, measure 1st qubit

$$H = \sum_{t=1}^{T} -|t\rangle\langle t-1| \otimes U_t - |t-1\rangle\langle t| \otimes U_t^\dagger + |T\rangle\langle T| \otimes |0\rangle\langle 0| \otimes I$$

we can't find g states in general

⇒ approximations, special cases, heuristics

Beware: complexity theory has stronger evidence for worst-case hardness than average case.
Leaves room for successful algos for many distributions over NP- or QMA-hard problems.

Post-selection
can output 0, 1, or ?
Post BPP we solve a problem if
$\frac{Pr[0]}{Pr[1]} \geq \frac{2}{3}/\frac{1}{3} = 2$ and $Pr[?] < 1$
$\frac{Pr[0]}{Pr[1]} \leq \frac{1}{3}/\frac{2}{3} = 1/2$
similar for PostBQP

Counting
$\phi(x) = 0$ (unsatisfied) or 1 (satisfied)

$$COUNT(\phi) = \sum_{x \in \{0,1\}^n} \phi(x)$$

NP: COUNT $= 0$ or ≥ 1
Approx counting COUNT $\leq T$ or $\geq 2T$
exact counting compute COUNT. called #P
or $\leq T$ vs $\geq T+1$ called PP

PostBPP $\subseteq$ approx counting
input x, random seed $r \in [R]$
$\phi_{x,0}(r)$ $\phi_{x,1}(r)$
estimate $\frac{COUNT(\phi_{x,0})}{COUNT(\phi_{x,1})}$

Note $COUNT(\phi^{\otimes k}) = COUNT(\phi)^k$
error $2 \to 2^{1/k}$

Approx counting $\subseteq$ PostBPP
Suppose COUNT $\leq T$ or $\geq 4T$
$1 \to 1$
$0 \to ?$
add $2T$ 0's

$\leq T$	$\geq 2^n - T$	$2T$

vs

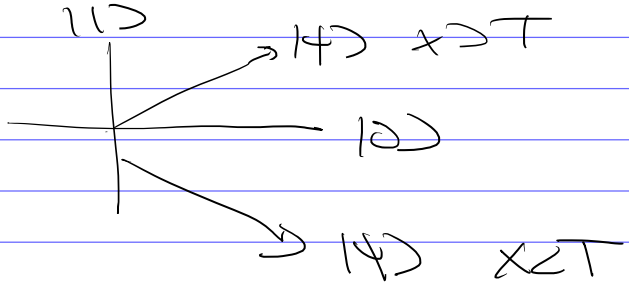
$\geq 4T$	$\leq 2^n - 4T$	$2T$

PostBQP = PP

PostBQP replace $U(2^n)$ with $GL(2^n)$

rotate $(2^{-T}|0\rangle + T|1\rangle)$ to $|0\rangle$

$|\psi\rangle = (2^n x)|0\rangle + x|1\rangle$



Amplify 1 state using $\begin{pmatrix} 1 & \\ 0 & 2 \end{pmatrix}$ repeatedly, i.e. classical postselection

W does this have to do with reality?

simple circuits become universal with postselection

e.g. low-depth linear optics