# Lecture 10 - Quantum computational supremacy (advantage)

Oracle problems - BV, Simon, DJ

Non-oracle problems - Factoring

↳ Shor's alg → Period finding

$f: \{0 \dots d-1\} \to \{0 \dots d-1\}$

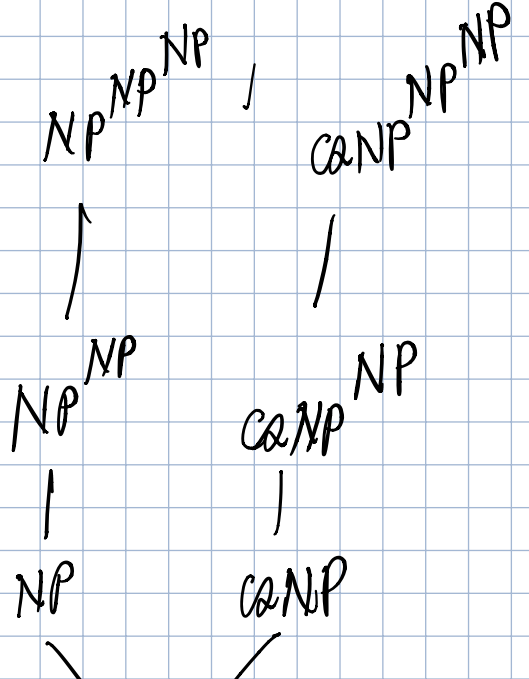
$f(k+x) = f(x)$

$2^{\sqrt[3]{n} \cdots}$

$BPP \stackrel{?}{=} BQP$

$P \neq NP$

PH is infinite



$P$

$\exists$ an oracle $O$ s.t. $BQP^O = BPP^O$ and $PH^O$ is infinite.

Sampling problems

$$in: x \to D_x : \{0,1\}^{m=poly(|x|)} \to [0,1]$$

$$\sum_{y \in \{0,1\}^m} D_x(y) = 1$$

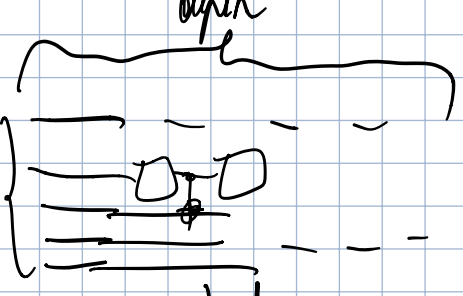
Out: sample from $D_x$

sample $y_n$ s.t $Pr(y) = D_x(y)$

$\{0,1\}^m$

Exact-Circuit-Sampling (ECS)

E.g: in: quantum circuit $C$ on $n$ qubits



Out: $y \in \{0,1\}^n$

st $\Pr(y) = |\langle y|C|\underbrace{0\ldots0}_{0^n}\rangle|^2$

$C = H^{\otimes n}$

$H^{\otimes n}|0\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} |y\rangle$

$\Pr(y) = \frac{1}{2^n}$

Circuits that have gates from $\{H, T, CNOT\}$

Approximate-Circuit-Sampling (ACS)

E.g:

in: quantum circuit $C$ on $n$ qubits

$\varepsilon > 0$

Out: $y \in \{0,1\}^n$

st $\Pr(y) \approx_\varepsilon |\langle y|C|\underbrace{0\ldots0}_{0^n}\rangle|^2$

$$\left| \Pr(y) - \left| \langle y | C | \underbrace{0 \cdots 0}_{0^n} \rangle \right|^2 \right| \leq \varepsilon$$

---

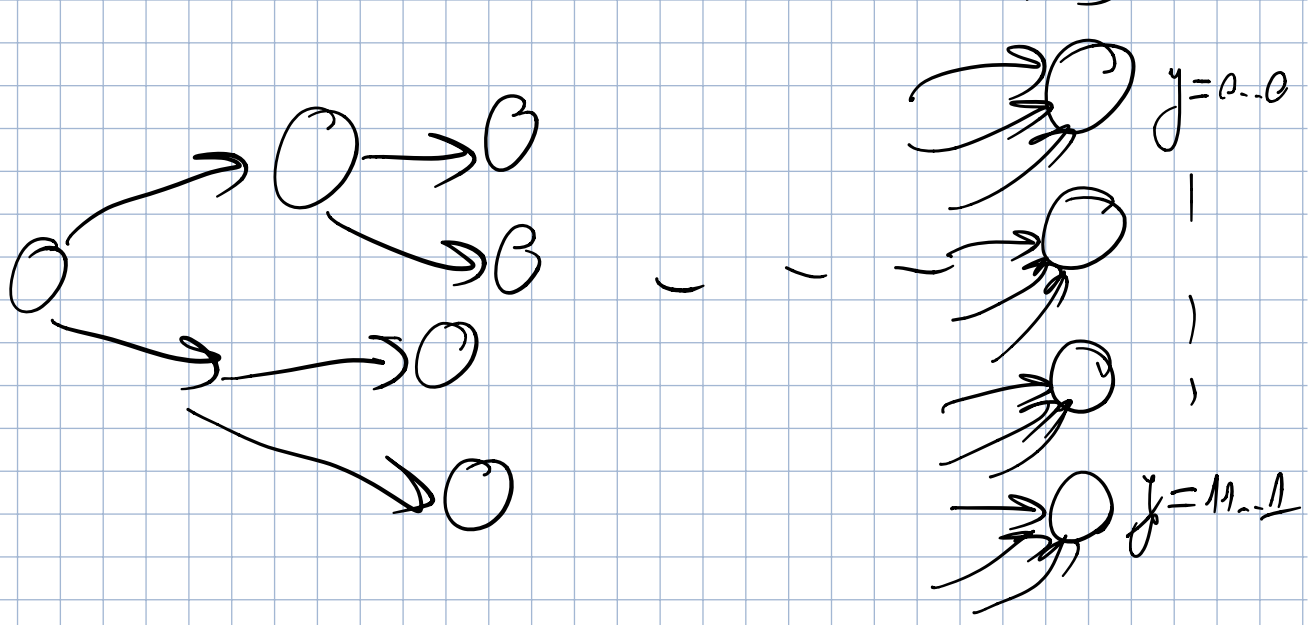
Prob poly-time alg $A(x) \to y$, $y \in \{0,1\}^m$ ($x \in \{0,1\}^n$)

How hard is it to compute the prob that the alg outputs $y$?

$f \in \#P$

$$\Pr(A(x) \text{ outputs } y) = \frac{f(x,y)}{2^{\text{poly}(|x|)}}$$

A poly-time alg for computing $\Rightarrow P = P^{\#P}$ ($P = NP$)




What about estimating $Pr(y)$?

a) Additive estimate

Out a number $E$ s.t

$$|E - Pr(y)| \leq \varepsilon, \quad \varepsilon > 0$$

This can be done in BPP

Run $A$ poly $(|x|)$ many times

$$E = \frac{\#y}{\#_{Tot}} \qquad \varepsilon = \frac{1}{poly(|x|)}$$

if $Pr(y) = 2^{-|x|}$

b) Multiplicative error estimate

Out a number $E$ s.t. $\exists\ g > 1$ s.t.

$$\frac{1}{g} \cdot Pr(y) \leq E \leq g \cdot Pr(y)$$

Stockmeyer approximate method

$\exists$ a $BPP^{NP}$ alg for mult estimating any #P-complete fun $f$. with $g = 1 + \frac{1}{poly(|x|)}$

$BPP \subseteq NP^{NP}$

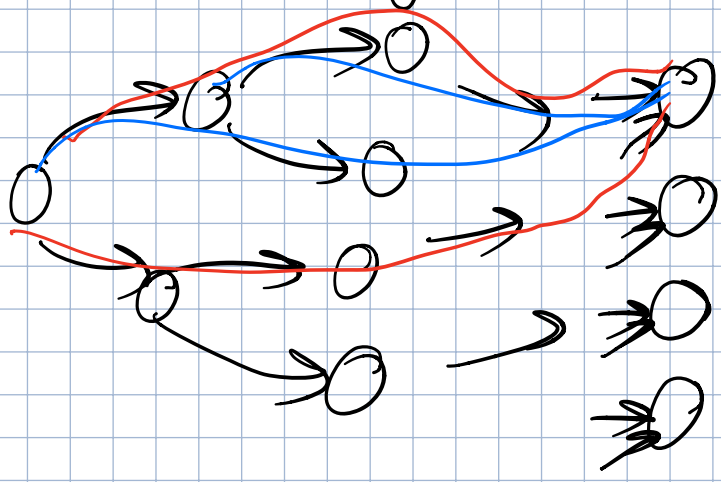
$BPP^{NP} \subseteq NP^{NP^{NP}}$ $\longrightarrow$ collapses at the third level.

Toda's thm: $P^{\#P} \geq PH$

What about estimating $P_A(y)$ when alg is quantum.

a) Exact case

GapP-hard



a) Additive error

Can be done in BQP with $\varepsilon = \frac{1}{poly(|x|)}$

b) Multiplicative error

Also GapP-hard!

---

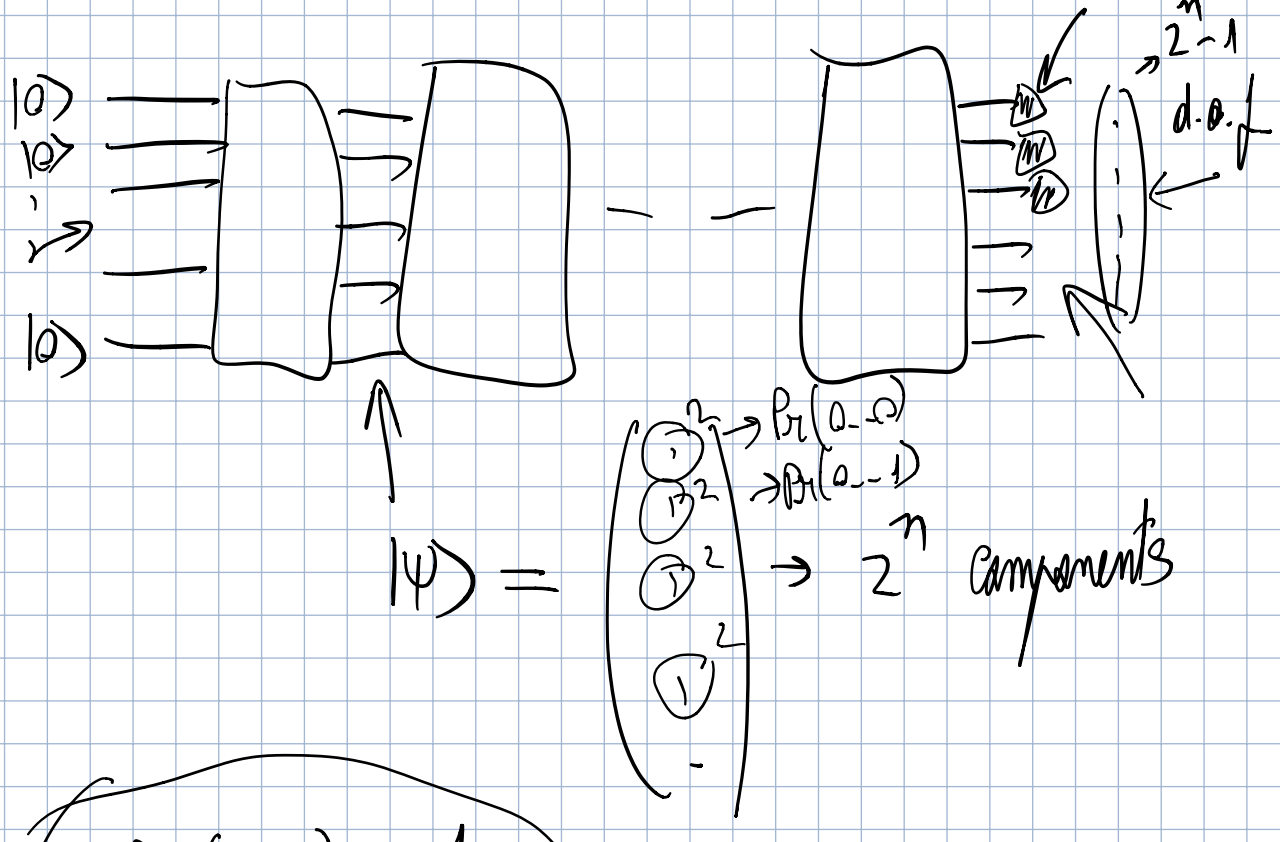
Assume that a poly prob alg A can sample from $|\langle y|C|0^n\rangle|^2$ for any poly-size q.c. C with gates in $\{H, T, CNOT\}$

$\Rightarrow$ From Stockmeyer $|\langle y|C|0^m\rangle|^2$ can be estimated in $BPP^{NP}$ within mult error.

However this is GapP-hard.

$$\Rightarrow BPP^{NP} \geq P^{GapP} = P^{\#P} \geq PH$$

$\Rightarrow$ PH collapses at 3rd level!!!




$Pr(00) = \frac{1}{2}$

$Pr(11) = \frac{1}{2}$

$Pr(01) = Pr(10) = 0$

$\Pr(0) = \frac{1}{2}$ $\Pr(1) = \frac{1}{2}$

Average case hardness of 2 circ. sampling.

Suppose you pick $C$ at random from all 2 circ. on $n$-qubit.

$|\langle y|C|0^n\rangle|^2$ - Gap P hard.

RCS

Pick random $C$

Sample from $|\langle y|C|0^n\rangle|^2$

Additive error sampling from

We don't know ( $\varepsilon = \frac{1}{2^{\#2}} \rightarrow$ Gap P hard)

XHOG

$y_1, y_2 \dots y_k$

$k \ll 2^n$

$2^{depth(C)} < n$

$$S = \frac{1}{k} \sum_{i=1}^{k} Pr(y_i)$$

for uniform $S = \frac{1}{2^n}$

for 2 circ $S \geq \frac{b}{2^n}$ $\quad b > 1$

$1.0006$

$|\langle 0\dots0|C|0\dots0\rangle|^2 \sim Exp(1)$

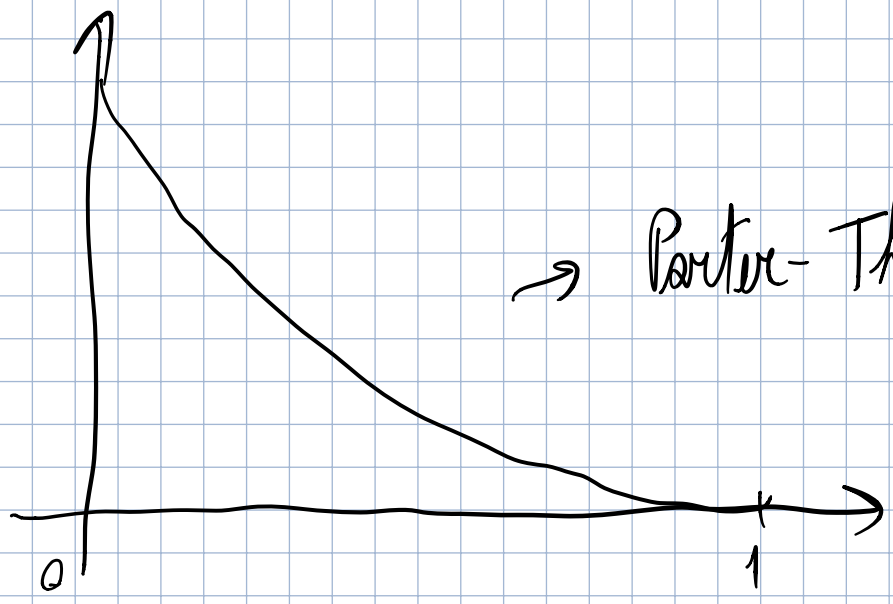
distrib. like a Gaussian (unit circle)

random $C \sim$ random unitaries $U \in U_n$ (Haar meas)

$(SU(N))$ $\quad 2^n$

↓

t designs




→ Porter-Thomas

Quantum chaos