[based on Sevag Gharibian's Lecture Notes]

← deterministic TM   quantum TM, circuit model, ...

Know from TCS: P, NP

Goal ("Quantum Quest") of this seminar: Find quantum analogue of P, NP, ... !

↑ quantum computation "inherently" (?) probabilistic

Goal today: "From BPP to BQP" OR understanding the following joke:

What do you call a quantum ghost that computes efficiently?

A BooQP! (It's Halloween, you know!)

→ I "promise" that you will understand this joke after this talk ☺ and this wordplay

← randomized analogue of P

I Bounded-error probabilistic polynomial-time (BPP)

"Monte Carlo" Algoith

Def (BPP) A language $L \subseteq \{0,1\}^*$ is in BPP, if there exists
- (deterministic) TM M
- fixed polynomials $s_L, t_L : \mathbb{N} \to \mathbb{R}^+$ ("string length", "time")

such that for any input $x \in \{0,1\}^n$, M takes in (additional) string $y \in \{0,1\}^{s_L(n)}$, halts in at most $\mathcal{O}(t_L(n))$ steps and
- (Completeness) If $x \in L$, then M accepts for at least $\frac{3}{4}$ of the choices of $y \in \{0,1\}^{s_L(n)}$
- (Soundness) If $x \notin L$, ——— " ——— most $\frac{1}{4}$ ——— " ———

Remarks

1) BPP vs NP: In NP y is the "witness"; $x \in L \to M$ accepts some $y \in \{0,1\}^{s_L(n)}$
$x \notin L \to M$ accepts no $y \in \{0,1\}^{s_L(n)}$

⇝ "more robust"

2) How do you choose y?
↳ can interpret y as uniformly random string over $\{0,1\}^{s_L(n)}$ ⇝ $x \in L \Rightarrow M$ accepts w/ prob $\geq \frac{3}{4}$
$x \notin L \Rightarrow M$ ——— $\leq \frac{1}{4}$

there has to be an inverse-polynomial gap

3) constants $\frac{3}{4}, \frac{1}{4}$ arbitrary ⇝ amplify probability / constants / error reduction by repeating many times in parallel; accept if majority of runs accept (using Chernoff)

Thm (Error reduction) If $L \in$ BPP, $k \in \mathbb{N}$, there exists TM M' s.th
(a) $x \in L \Rightarrow M'$ accepts for $\geq 1 - \frac{1}{2^{|x|^k}}$ strings
(b) $x \notin L \Rightarrow$ $\leq \frac{1}{2^{|x|^k}}$ strings

can be reduced arbitrarily close to 0/1 even exponentially fast

[Lecture Notes - CCT, Zenner]

Chernoff bound If $X_1, \dots, X_n$ IID over $\{0,1\}$ (reject, accept) s.th. $\Pr[X_i = 1] \leq \frac{1}{4}$ $(\forall i)$, then

$$\Pr\left[\sum_{i=1}^{n} X_i \geq \frac{n}{2}\right] \leq e^{-\frac{1}{12}n}$$

Pf. * simulate M independently $24|x|^k$ times on input x
* Accept iff $\geq 12|x|^k$ accepts

⇝ poly-time

(b) $\Pr[X_i = 1] \leq \frac{1}{4}$ $\forall i \in [24|x|^k]$

$$\Pr\left[\sum_{i=1}^{24|x|^k} X_i \geq 12|x|^k\right] \leq e^{-2|x|^k} \leq 2^{-|x|^k}$$

(a) analogous

4) Open Question: $P \stackrel{?}{=} BPP$ ↙ follows under "derandomization" conjectures

strong & subtle property: for input x

5) decision problem, but large set of ships has to be "good", which is not easy to check
↳ BPP is <u>semantic class</u> ← syntactic class: "easy to check" e.g. P, NP

<u>Why problematic?</u>

remember TCS: $enc(q) := 0^{num(q)}1$ (state), $enc(\sigma) := 0^{num(\sigma)}1$ (symbol), $enc(d) := 0^{num(d)}1$ (direction); $enc(q,\sigma) := 1\, enc(q)\, enc(\sigma)\, enc(q')\, enc(\sigma')\, enc(d)$; $enc(M) :=$ concenate $enc(q,\sigma)$ lexicographically

e.g. $L = \{ \text{Encoding}(M, x) \mid M \text{ P-TM which accepts } x \in \{0,1\}^* \} \in P$

$L' = \{ \text{Encoding}(M, x, 1^t) \mid M \text{ BPP-TM which accepts } x \in \{0,1\}^* \text{ in } \leq t \text{ steps} \} \stackrel{?}{\in} BPP$ "semantic class" → probably not

↙ L' is #P-complete ← set of all functions $f : \Sigma^* \to \mathbb{N}$ for which $\exists$ poly-TM w/ add. input, poly p s.t. $\forall x \in \Sigma^*$ $f(x) = \#_{M,p(x)}$

To decide whether M has the property that on all inputs, M accepts or rejects wp $\geq \frac{3}{4}$ undecidable (Rice's Thm)

<u>Solution</u>: We "promise" that M is BPP-TM. ← if promise is broken M can behave arbitrarily

<u>Def</u> (Promise Problem) A promise problem $\mathcal{A}$ is partition into three sets $A_{yes}, A_{no}, A_{\perp}$

<u>Def</u> (Promise BPP) A promise problem $\mathcal{A} = (\mathcal{A}_{yes}, \mathcal{A}_{no}, \mathcal{A}_{\perp})$ is in Promise BQP, if there exists
- (deterministic) TM M
- fixed polynomials $s_{\mathcal{A}}, t_{\mathcal{A}} : \mathbb{N} \to \mathbb{R}^+$

such that for any input $x \in \{0,1\}^n$, M takes in (additional) string $y \in \{0,1\}^{s_{\mathcal{A}}(n)}$, halts in at most $\Theta(t_A(n))$ steps and
- (Completeness) If $x \in \mathcal{A}_{yes}$, then M accepts for at least $\frac{3}{4}$ of the choices of y.
- (Soundness) If $x \in \mathcal{A}_{no}$, most $\frac{1}{4}$
- (Invalid) If $x \in \mathcal{A}_{\perp}$, M may accept or reject arbitrarily.

↖ we don't have to check if M is "BPP" machine anymore

$L' \in$ Promise BPP

Q: Why introduce BPP when we talk about Promise BPP?
A: What community calls BQP is in reality Promise BQP. ⇝ We write and say BQP but actually mean Promise BQP
↳ Also: Promise BQP has complete problems (which Jan will talk about) whereas there are no known complete problems for BQP.

II (Promise) BQP

$\boxed{Q1}$ classically: TM ⇝ quantumly: ?
↳ QTM exist, but we will use circuit model (somewhat natural for us)

$\boxed{Q2}$ How to compute with circuits?
↳ (finite) universal gate set → "approximate" unitary
↳ norms

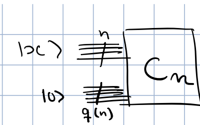
$\boxed{Q3}$ How do errors propagate in quantum (gate sequence / computation)? How are measurements affected by such errors?

A 1

$|x_1| \cdots |x_n| \cdots$

↖ variable input size

$\rightsquigarrow$



← fixed size

↳ P-uniform circuit family

Def A family of quantum circuits $\{C_n\}$ is called P-uniform if there exists a polynomial-time TM M which given input 1^n, outputs a classical description of $\{C_n\}$.

unary so that time poly in n :)
"binary ⇝ poly (log n) :(

Instead of "trick or treat" its "operator or trace"

A 2

Norms: * operator norm $\|M\|_\infty := \max_{\text{unit } |\psi\rangle \in \mathbb{C}^d} \| M|\psi\rangle\|$ (or largest singular value)

* trace norm / 1-norm $\|M\|_1 := \mathrm{tr}\left[\sqrt{M^\dagger M}\right]$ (or sum of singular values)

Properties: * Hölder ineq: $\left|\mathrm{tr}\left[A^\dagger B\right]\right| \leq \|A\|_\infty \|B\|_1$

* submultiplicativity: $\|AB\| \leq \|A\| \|B\|$

* Invariance under unitaries: $\forall\, U, V$ unitaries $\|UMV\| = \|M\|$

↖ operator / trace norm of M is the same as ∞/1-norm applied to vector of singular values of M, U, V leave singular values invariant

Uncountably many unitaries :(

Classically: NAND universal

Quantumly: $\mathcal{U} \in \mathcal{U}\left((\mathbb{C}^2)^{\otimes n}\right)$

CNOT + 1-qubit gates

$H, P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

exactly by $\Theta(n^2 4^n)$ gates

not bad. In general exponential

[see Nielsen Chuang]

Solovay-Kitaev: see https://alexkulpe.github.io/files/Solovay-Kitaev.pdf

approximated by $\Theta(\log^c(\frac{1}{\varepsilon}))$ gates within ε additive error (wrt norm)

↳ small inverse-polynomial additive error w/ poly-logarithmic overhead in gate count

A3

WANT: $\mathcal{U} = \mathcal{U}_m \cdots \mathcal{U}_1$

HAVE: $\mathcal{U}' = \mathcal{U}_m' \cdots \mathcal{U}_1'$ w/ $\|\mathcal{U}_i - \mathcal{U}_i'\| \leq \varepsilon$ ← unitarily invariant

Q: $\|\mathcal{U} - \mathcal{U}'\| = ?$

↳ **Lemma** $\|\cdot\| \in \{\|\cdot\|_\infty, \|\cdot\|_1\}$. $\mathcal{U} = \mathcal{U}_m \cdots \mathcal{U}_1$, $\mathcal{U}' = \mathcal{U}_m' \cdots \mathcal{U}_1'$ quantum circuits for unitaries $\mathcal{U}_i, \mathcal{U}_i'$ satisfying $\|\mathcal{U}_i - \mathcal{U}_i'\| \leq \varepsilon$ $\forall i \in [m]$. Then $\|\mathcal{U} - \mathcal{U}'\| \leq m \cdot \varepsilon$

Pf. by induction. $m = 1$ ✓

Let $V := \mathcal{U}_{m-1} \cdots \mathcal{U}_1$, $V' := \mathcal{U}_{m-1}' \cdots \mathcal{U}_1'$

$$
\begin{aligned}
\|\mathcal{U} - \mathcal{U}'\| &= \|\mathcal{U}_m V - \mathcal{U}_m' V' + \mathcal{U}_m V' - \mathcal{U}_m V'\| \\
&= \|\mathcal{U}_m (V - V') + (\mathcal{U}_m - \mathcal{U}_m') V'\| \\
&\overset{\Delta\text{-ineq}}{\leq} \|\mathcal{U}_m (V - V')\| + \|(\mathcal{U}_m - \mathcal{U}_m') V'\| \\
&= \|V - V'\| + \|\mathcal{U}_m - \mathcal{U}_m'\| \\
&\leq (m-1)\varepsilon + \varepsilon \\
&= m\varepsilon
\end{aligned}
$$

□

⇒ error propagates linearly

What about measurements?

<u>Lemma</u> Let $\rho \in D(\mathbb{C}^d)$ be a quantum state, $\Pi \in Pos(\mathbb{C}^d)$ projector, and $U, V \in \mathcal{U}(\mathbb{C}^d)$ s.th. $\|U - V\|_1 \leq \varepsilon$. Then

$$\left| tr\left[\Pi U \rho U^\dagger\right] - tr\left[\Pi V \rho V^\dagger\right] \right| \leq 2\varepsilon$$

Pf.

$$\begin{aligned}
\left| tr\left[\Pi^\dagger (U\rho U^\dagger - V\rho V^\dagger)\right]\right| &\overset{\text{Hölder}}{\leq} \|\Pi\|_\infty \, \|U\rho U^\dagger - V\rho V^\dagger\|_1 \\
&\leq \|U\rho U^\dagger - V\rho V^\dagger + V\rho U^\dagger - V\rho U^\dagger\| \\
&= \|(U - V)\rho U^\dagger + V\rho(U^\dagger - V^\dagger)\| \\
&\overset{\Delta}{\leq} \|(U-V)\rho U^\dagger\| + \|V\rho(U^\dagger - V^\dagger)\| \\
&\overset{\text{submultiplicativity, } \|\rho\|=1, \|U\|=1}{\leq} 2\|U - V\|_1 \\
&\leq 2\varepsilon
\end{aligned}$$

□

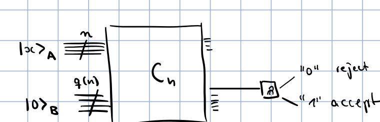
$\Longrightarrow$ small inverse polynomial additive error :)

WLOG: P-unifo TM only needs to pick gates from $\{CNOT, H, P\}$

<u>Def (BQP)</u> A promise problem $\mathcal{A} = \{\mathcal{A}_{yes}, \mathcal{A}_{no}, \mathcal{A}_\perp\} \in BQP$ if $\exists$ P-uniform q. circuit family $\{C_n\}$ and polynomial $q: \mathbb{N} \longrightarrow \mathbb{N}$ satisfying:

$\forall$ input $x \in \{0,1\}^n$, C_n takes in $n + q(n)$ qubits, consisting of x in register A, and $q(n)$ ancillae initialized to $|0\rangle$ in register B.

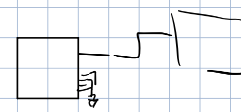
If 1^{st} qubit of B gets measured (in std basis) after applying C_n, then
- (Completeness) If $x \in \mathcal{A}_{yes}$, then C_n accepts wp $\geq \frac{3}{4}$
- (Soundness) If $x \in \mathcal{A}_{no}$, $\leq \frac{1}{4}$
- (Invalid) If $x \in \mathcal{A}_\perp$, C_n may accept or reject arbitrarily



OPTIONAL: DEPENDING ON TIME

maybe first IV then III

III BQP subroutine problem



Classically, can use circuit as subroutine. Quantumly?

$$C\,|x\rangle|0^m\rangle = \sqrt{\tfrac{1}{4}}\;|0\rangle|\psi_0'\rangle + \sqrt{\tfrac{3}{4}}\;|1\rangle|\Psi_1'\rangle$$

output qubit potentially highly entangled w/ rest of qubits

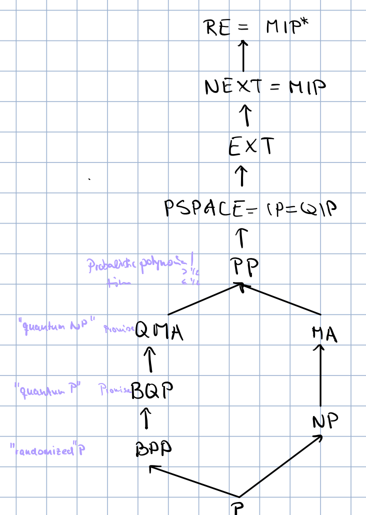
① Discard other qubits as garbage ↯ highly mixed state after tracing out

⟹ Reduce error of C via error reduction (as in BPP)

$$C\,|x\rangle|0^m\rangle = \sqrt{\tfrac{1}{2^n}}\;|0\rangle|\Psi_0\rangle + \sqrt{1-\tfrac{1}{2^n}}\;|1\rangle|\Psi_1'\rangle$$

⇝ tracing out only leads to exp. small error. exp small for poly steps → negligible

IV Relationship to other classes



Now: BQP ⊆ PSPACE

Def (PSPACE) A language $L \subseteq \{0,1\}^*$ is in PSPACE if there exists
- TM M
- fixed polynomials $s_L : \mathbb{N} \to \mathbb{R}^*$

s.th. for any input $x \in \{0,1\}^n$, M uses at most $O(s_L(n))$ cells on its work tape, and
- (Completeness) If $x \in L$, M accepts
- (Soundness) If $x \notin L$, M rejects

Proof. * Let $x \in \mathcal{A} = (\mathcal{A}_{yes}, \mathcal{A}_{no}, \mathcal{A}_1)$ with $|x| = n$ and $\mathcal{A}$ BQP promise problem.

* Then, ∃ poly-time TM M which given $|x|$, outputs quantum circuit $Q_n = U_m \cdots U_1$. (1, 2-qubit gates)

Measuring output qubit in std basis: $x \in \mathcal{A}_{yes} \Rightarrow$ "1" w.p. $\geq \frac{3}{4}$

$x \in \mathcal{A}_{no} \Rightarrow$ "1" w.p. $\leq \frac{1}{4}$

↳ Idea: Estimate probability of outputting 1

* $\Pi_1 = |1\rangle\langle 1|$ projection. $|\psi\rangle = Q_n\,|x\rangle|0^{q(n)}\rangle$

$$\Pr[\text{output } 1] = \langle \psi | \Pi_1 | \psi \rangle$$

more formally $\mathrm{tr}\left[\Pi_1\, \mathrm{tr}_{2,\dots,n+q(n)}\left[|\Psi\rangle\langle\Psi|\right]\right]$

$$= \langle x|\langle 0^{q(n)}|\; U_1^\dagger \cdots U_m^\dagger\, \Pi\, U_m \cdots U_1\; |x\rangle|0^{q(n)}\rangle$$

Feynman path integral trick

$$I = \sum_{x \in \{0,1\}^{n+q(n)}} |x\rangle\langle x|$$

add identities

$$= \langle x| \langle 0^{q(n)}| \, I \, U_1^\dagger \, I \cdots I \, U_m^\dagger \, I \, \Pi_1 \, I \, U_m \, I \cdots I \cdot U_1 \, I \, |x\rangle |0^{q(n)}\rangle$$

$$= \underbrace{\sum_{\substack{x_1,\dots,x_{2m+2} \\ \in \{0,1\}^{n+q(n)}}}}_{\text{exponential sum but we just keep one variable for result and add to it for every summand}} \underbrace{\underbrace{\left(\langle x|\langle 0^{q(n)}|\right)|x_1\rangle}_{\in \mathbb{C}} \underbrace{\langle x_1| U_1^\dagger |x_2\rangle}_{\in \mathbb{C}} \cdots \underbrace{\langle x_{2m+1}| U_1 |x_{2m+2}\rangle}_{\in \mathbb{C},\ \text{matrix entry row } x_{2m+1},\ \text{col } x_{2m+2}} \underbrace{\langle x_{2m+2}| \left(|x\rangle|0^{q(n)}\rangle\right)}_{}}_{\text{product of } 2m+3 \text{ complex numbers} \in \text{poly time}}$$

efficient:

$$\langle x_1| U^\dagger_{(i,j)} \otimes \mathbb{1}_{[n+q(n)]\setminus\{i,j\}} |x_2\rangle$$

$$\ldots = \langle x_{1i} x_{1j}| U^\dagger_{(i,j)} |x_{2i} x_{2j}\rangle \otimes \langle x_{1} x \ldots | I | \ldots\rangle$$

summands $\left(2^{n+q(n)}\right)^{2m+2}$

final value = acceptance prob of Q_n

Caveat: Precision for U, products of complex numbers etc., …

matrix entries $\to 0, 1, \frac{1}{\sqrt{2}}$, $e^{i\pi/8}$

$\frac{1}{\sqrt{2}} \to 1/2$

↗ high precision possible

↳ approximate entries using poly(n) many bits

↳ p large enough ⇝ exponentially small error ☺