Quantum Complexity Theory

A – Quantum Interactive Proofs

BQP, QMA and QIP :

- Definitions
- Complete problems
- Elementary properties

B – The complexity-theoretic basis for demonstrating a quantum advantage :

- The Google RCS experiment
- The Meyer et al. test of quantumness.

A - Quantum Interactive Proofs

Def: A promise language $L = (L_{yes}, L_{no})$ is in BQP iff there exists a polytime Turing Machine $T : 1^n \to Q_n$ s.t.

$$\forall x \in \{0,1\}^n, \quad x \in L_{yes} \Rightarrow \Pr(Q_{|x|} \text{ accepts } x) \geq \tfrac{2}{3}$$
$$x \in L_{no} \Rightarrow \Pr(Q_{|x|} \text{ accepts } x) \leq \tfrac{1}{3}.$$

Upper bounds :

Def
- A function $f : \{0,1\}^n \to \mathbb{Z}$ is in GapP iff there exists a polynomial time non-deterministic TM M st
$$\forall x \in \{0,1\}^n, \quad f(x) = \#Acc(M,x) - \#Rej(M,x)$$
- $L = (L_{yes}, L_{no})$ is in PP iff there exists $f \in$ GapP s.t.
$$\forall x \in \{0,1\}^n, \quad x \in L_{yes} \Rightarrow f(x) > 0$$
$$x \in L_{no} \Rightarrow f(x) < 0$$

Thm $BQP \subseteq PP$

|

Def: A promise language $L = (L_{yes}, L_{no})$ is in QMA iff there exists a polytime Turing Machine $T : 1^n \to Q_n$ s.t.

$\forall x \in \{0,1\}^n$, $x \in L_{yes} \Rightarrow \exists |\psi\rangle, \Pr(Q_{|x|} \text{ acc. } x, |\psi\rangle) \geq \frac{2}{3}$

$x \in L_{no} \Rightarrow \forall |\psi\rangle, \Pr(Q_{|x|} \text{ acc. } x, |\psi\rangle) \leq \frac{1}{3}$

Complete problems:

- The Local Hamiltonian (LH) problem

  Input: explicit description of LH $H = H_1 + \cdots + H_m$ on $p(n)$ qubits

Answer: "YES" if $\exists |\psi\rangle$: $\langle\psi|H|\psi\rangle \leq -1$
"NO" if $\forall |\psi\rangle$: $\langle\psi|H|\psi\rangle \geq 1$

Thm (Kitaev) The LH problem is complete for QMA.

Thm (Kitaev) The LH problem is complete for QMA.

- Consistency of Local Density Matrices (CLDM)

  Input: Explicit description of density matrices $\rho_1, \dots, \rho_m$, each on at most k out of n qubits

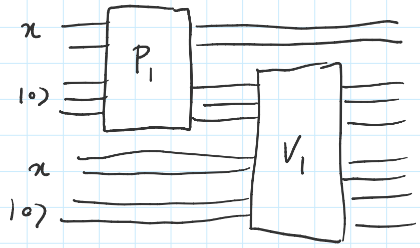
  Answer: "YES" if $\exists \rho$ on $p(n)$ qubits s.t. $\forall i$, $\|\mathrm{Tr}_{\bar{S}_i}(\rho) - \rho_i\|_{tr} \leq \frac{1}{q(n)}$

  "NO" if $\forall \rho$ on $p(n)$ qubits, $\exists i$: $\|\mathrm{Tr}_{\bar{S}_i}(\rho) - \rho_i\|_{tr} \geq \frac{100}{q(n)}$

  Thm (Liu, Broadbent-Grilo)
  The CLDM problem is complete for QMA

Some open questions about QMA:

Interactive Proofs



Def: A promise language $L = (L_{yes}, L_{no})$ in in QIP iff there exists a polytime Turing Machine $T : 1^n \to (V_1, \dots, V_k)$ s.t

$\forall x \in \{0,1\}^n$, $\quad x \in L_{yes} \Rightarrow \exists\, (P_1, \dots, P_k)$: $\Pr(Q_{|x|}$ acc. $x, P_1, \dots, P_k) \geq \frac{2}{3}$

$\quad x \in L_{no} \Rightarrow \forall\, (P_1, \dots, P_k)$: $\Pr(Q_{|x|}$ acc. $x, P_1, \dots, P_k) \leq \frac{1}{3}$

Thm: (Jain, Ji, Upadhyay, Watrous) $\quad$ QIP = PSPACE

Complete problem: Quantum Circuit Distinguishability

Input: Quantum circuits Q_0 and Q_1 on same nb of qubits

Answer: "YES" if $\frac{1}{2} \| Q_0 - Q_1 \|_\diamond \geq \frac{2}{3}$

"NO" if $\frac{1}{2} \| Q_0 - Q_1 \|_\diamond \leq \frac{1}{3}$

B- The complexity-theoretic basis for demonstrating a quantum advantage

Goals:

1- Random Circuit Sampling (RCS)

Experiment:
- Fix a 2D architecture: $\sqrt{n} \times \sqrt{n}$ grid of qubits, nearest-neighbor gates
- Select gates uniformly at random $\rightarrow$ circuit C
- Run C T times. Collect outcomes $x_1, \dots, x_T \in \{0,1\}^{\sqrt{n}}$
- Return $\text{Score}(x) = \frac{1}{T} \sum_{t=1}^{T} \log \frac{1}{P_{\text{ideal}}(x)}$

Complexity-theoretic basis:

Def
- A function $f : \{0,1\}^n \rightarrow \mathbb{Z}$ is in GapP iff there exists a polynomial time non-deterministic TM M st $\forall x \in \{0,1\}^n$, $f(x) = \#\text{Acc}(M,x) - \#\text{Rej}(M,x)$
- A function $f : \{0,1\}^n \rightarrow \mathbb{Z}$ is in $\#P$ iff there exists a polynomial time non-deterministic TM M st $\forall x \in \{0,1\}^n$, $f(x) = \#\text{Acc}(M,x)$

Rk:

Def A c-mult. approx to f is z s.t. $(1-c)\sum_x f(x) \leq z \leq (1+c)\sum_x f(x)$

Observations: • $P^{\frac{1}{\text{poly}}\text{-approx GapP}} = P^{\text{GapP}}$

Observations:

- $P^{\frac{1}{\text{poly}}\text{-approx GapP}} = P^{\text{GapP}}$
- $P^{\frac{1}{\text{poly}}\text{-approx } \#P} \subseteq BPP^{NP}$
- $P^{\text{GapP}} = BPP^{NP} \Rightarrow PH$ collapses.

(Terhal-DiVicenzo, Bremner-Jozsa-Shepherd, Aaronson-Arkhipov):
Suppose that for every quantum circuit C there is a rand-algorithm $\mathcal{A}$ that exactly samples $x \sim |\langle 0|C|x\rangle|^2$
Then A gives an approximation of a GapP function by a #P function

Rk: • Widely applicable:

• Limitations:

Goal: No average-case, approximate sampler

Thm (Bouland, Fefferman, Nirkhe, Vazirani)
If there exists an average-case approximate sampler for RCS
Then there is a $BPP^{NP^{S}}$ algorithm for approximating $|\langle 0|C|z\rangle|^2$ $(\pm \frac{\varepsilon}{2^n})$
with high probability over the choice of C and z.

Conjecture: There is no such algorithm.

Thm: There is no BPP^{NP} algorithm for exactly computing $|\langle 0|C|z\rangle|^2$
with high probability over the choice of C and z.

Thm: There is no BPP algorithm for exactly computing $|\langle 0|C|z\rangle|$ with high probability over the choice of C and z.

2- Interactive test of quantumness based on cryptographic assumption

Kahanamoku-Meyer, Soonwon Choi, Umesh Vazirani, Norman Yao.

Experiment: Repeat T times:

Verifier		Prover
public parameters	$\longrightarrow$	prepare quant. state
	$\xleftarrow{y}$	partial meas.
challenge 1	$\xrightarrow{c_1}$	unitary + partial meas
	$\xleftarrow{r_1}$	
challenge 2	$\xrightarrow{c_2}$	unitary + partial meas.
	$\xleftarrow{r_2}$	
accept/reject.		

Result: Assume the existence of a family of trapdoor claw-free functions. Then:

(a) $\exists$ quantum polytime prover, succeeds w.p. $\sim 85\%$

(b) $\forall$ classical polytime prover succeeds w.p. $\leq 75\%$

Definition: A family $\{f_{pk(\lambda)} : \{0,1\}^{n(\lambda)} \to \{0,1\}^{n(\lambda)}\}_\lambda$ is trapdoor claw-free (TCF)
iff $\exists$ GEN: $1^\lambda \to pk(\lambda), td(\lambda)$ s.t.:

- Given pk, f_{pk} is 2-to-1 and can be efficiently evaluated
- f_{pk} is claw free: hard to find (x,y) s.t. $f_{pk}(x) = f_{pk}(y)$
- Trapdoor: Given td it is easy to recover both preimages of any point.

- Trapdoor: Given t_d it is easy to recover both preimages of any point.

<u>Ex</u>: $f_N(x) = x^2 \mod N \qquad N = q \qquad p, q$ primes

The protocol:

Verifier — **Prover**

Select parameters $\xrightarrow{pk}$ Prepare $\sum_x |x\rangle |f(x)\rangle$

$\hookrightarrow$ meas: y

$\xleftarrow{y}$ $\qquad \rightarrow \frac{1}{\sqrt{2}}(|x_0\rangle + |x_1\rangle)$

Option 1 $\left\{ \begin{array}{l} \xrightarrow{\text{"preimage"}} \quad \text{Measure} \rightarrow x_b \\ \xleftarrow{x_b} \end{array} \right.$

Option 2 $\left\{ \begin{array}{l} \text{random } r \in \{0,1\}^n \xrightarrow{r} \quad \text{Compute } \frac{1}{\sqrt{2}}(|x_0\rangle |r \cdot x_0\rangle + |x_1\rangle |r \cdot x_1\rangle) \\ \xleftarrow{d} \quad \text{Measure } x \text{ in } H^{\otimes n} \rightarrow d \\ \qquad \rightarrow |0\rangle, |1\rangle, |+\rangle, |-\rangle \\ \text{random } m \in \{\pm 1\} \xrightarrow{m} \quad \text{Measure in } \{|m\frac{\pi}{8}\rangle, |m\frac{\pi}{8} + \frac{\pi}{2}\rangle\} \\ \xleftarrow{b} \quad \rightarrow \text{outcome } b \end{array} \right.$

(a) Quantum prover succeeds w.p. 85%

(b) Classical prover succeeds wp $\leq 75\%$

Further directions:

- Verification for quantum supremacy proposals
- Average-case approximate hardness for supremacy proposals
- Test of quantumness:
  - low depth implementation
  - Certified randomness, delegated computation: other assumptions?

- - low depth implementation
  - certified randomness, delegated computation: other assumptions?

Verification for restricted classes of circuits