S. KIMMEL

Today/Thursday - Computational Complexity
(Quantum) complexity Classes
Complete problem for quantum NP
Containment of Quantum Classes

What Questions is complexity theory interesting in? $\Rightarrow$

Difficult	Problems		Resources	More Power
$\uparrow$	Problem A	$\longleftrightarrow$		$\uparrow$
	Problem B	$\longleftrightarrow$	Quantum	
$\downarrow$	Problem C	$\longleftrightarrow$	Classical	$\downarrow$
Easy				Less Power

In order to compare problems & resources, we need a common language to describe problems.

Language: $L \subseteq \{0,1\}^*$ (a language is a subset of the set of all binary strings)

$\boxed{\text{ex}}$ Let $f = \{f_n\}_{n=1}^{\infty}$ be a family of Boolean formulas $f_n : \{0,1\}^n \to \{0,1\}$. Then $x \in L_f$ if $f_n(x) = 1$ for $x \in \{0,1\}^n$

$\boxed{\text{ex:}}$ $x \in L_{\text{factoring}, K}$ if x has a factor $\leq K$

Questions?

What is a language that corresponds to the problem of eigenvalue estimation?

Divide input x into 2 halves $\rightarrow$ [description of a circuit that creates a unitary U | description of a circuit that creates a state $|\psi\rangle$] (x) then $x \in L_{\text{phase},K}$ if $U|\psi\rangle = e^{2\pi i \omega}|\psi\rangle$ with $\omega < K$

S.KIMMEL

Complexity Class: a set of languages.

def: $L \in P$ if for any input $x \in \{0,1\}^*$, $\exists$ a polynomial time classical algorithm A s.t. $A(x)$ accepts iff $x \in L$.

If input x has length n, the time $< C_0 n^{C_1}$ for constants c_0, c_1.

$P \sim$ polynomial time

def

$L \in NP$ if for any input $x \in \{0,1\}^*$, $\exists$ a polynomial time classical algorithm A s.t.

- If $x \in L$ $\exists$ a string y s.t. $A(x,y)$ accepts
- If $x \notin L$ for all strings y, $A(x,y)$ rejects

"witness"

$NP \sim$ non-deterministic polynomial time

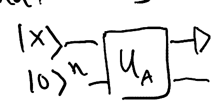
Quantum version of P:

def $L \in BQP$ if for any input $x \in \{0,1\}^*$ $\exists$ a polynomial time quantum algorithm A:

- If $x \in L$, $A(|x\rangle)$ accepts w/prob $> \frac{2}{3}$
- If $x \notin L$, $A(|x\rangle)$ accepts w/prob $< \frac{1}{3}$

$BQP \sim$ bounded error quantum polynomial time

$|x\rangle$ is computational basis state. Circuit:



Questions

What is the quantum version of NP?

S. KIMMEL

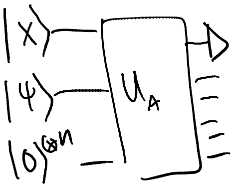
def $L \in$ QMA if for any $x \in \{0,1\}^*$ $\exists$ a polynomial-time quantum algorithm A s.t.

- If $x \in L$, $\exists$ a state $|\psi\rangle$ s.t.

  $A(|x\rangle, |\psi\rangle)$ accepts w/prob $\geq \boxed{\frac{2}{3}}$

- If $x \notin L$, $\forall$ states $|\psi\rangle$,

  $A(|x\rangle, |\psi\rangle)$ accepts w/prob $< 1/3$



QMA ~ quantum merlin Arthur
(merlin sends $|\psi\rangle$ to Arthur, who has a quantum computer)

Class	Input State	Success Prob
QMA	$\lvert\psi\rangle$	$2/3$
QCMA	$\lvert y\rangle$ (standard basis state)	$2/3$
QMA_1	$\lvert\psi\rangle$	1
QMA(2)	$\lvert\psi_1\rangle\lvert\psi_2\rangle$	$2/3$
$QCMA_1$	$\lvert y\rangle$ (standard basis state)	1

S.KIMMEL

(Comparing difficulty of problems)

Complete Problems:

def: A language L is complete for a complexity class C if $L \in C$ and also L is C-hard.

def: L is C-hard if for every $L' \in C$, $\exists$ a polynomial time algorithm to convert input $x' \to$ string x s.t. $x \in L$ iff $x' \in L'$.

Why are complete problems important? Allow us to relate a specific problem to a specific resource.

$\boxed{\text{ex:}}$ Let $x \in \{0,1\}^*$ describe a classical circuit A_x

Let $x \in L_A$ if $A_x(0\ldots0)$ accepts.

A.L.

L_A is P-Complete

(If familiar with complexity, try to think of a complete problem for BQP)

$\Rightarrow$ $L_A \in P$

$\Leftarrow$ L_A is P-hard b/c any other language in P has a poly time circuit to decide it, so encode that circuit as A, with pre-circuit to encode input x.

S.KIMMEL

Thm: k-local Hamiltonian problem is QMA-Complete [Kitaev]

A Hamiltonian H has form $\sum \lambda_i |\psi_i\rangle\langle\psi_i|$.

real eigenvalues — orthonormal basis

H defines an energy landscape.

$|\psi_i\rangle$ s.t. $\lambda_i \leq \lambda_j \ \forall j$ is called "groundstate"

def: [k-local Hamiltonian problem] Let a Hamiltonian $H = \sum_j H_j$ act on n qubits, where H_j are Hamiltonians acting non-trivially on at most K qubits. Let λ be the smallest eigenvalue of H, and let $a, b \in \mathbb{R}$: $a < b$, $b - a > \frac{1}{\text{poly}(n)}$.

Then the problem is to determine if $\lambda \leq a$ ("accept") or $\lambda > b$, promised one is the case.