Lecturer: Tongyang, scribed by Shuo Zhou
Date: December 15, 2023

Lecture 19

Quantum Computational Complexity

- Solving Linear Systems
- P, BPP, BQP
- BQP-completeness

1 Solving Linear Systems

Lemma 1. The function $f(x) = \frac{1-(1-x^2)^b}{x}$ is ϵ-close to $\frac{1}{x}$ on the domain D_{dk} for any integer $b \geq (kd)^2 \log(kd/\epsilon)$.
2. $f(x)$ can be exactly represented by a linear combination of Chebyshev polynomials of at most $2b-1$:

$$f(x) = \frac{1-(1-x^2)^b}{x} = 4\sum_{j=0}^{b-1}(-1)^j \left[\frac{\sum_{i=j+1}^{b} C_{b+i}^{2b}}{2^{2b}}\right] T_{2j+1}(x).$$

Reference. Lemma 17 and 18 of Childs, Kothari. Somma. SICOMP 2017. arxiv:1511.02306.
The non-unitary LCU part is also adopted from this paper.
Theorem. QLSP can be solved by $O(dk^2 \log^2(dk/\epsilon))$ queries to U_A and $O(k\log(dk/\epsilon))$ queries to U_B.
Algorithm:

1. Implement the quantum walk for the Hamiltonian $H = A/d$, as introduced above.
2. Approximate H^{-1} by $g(H)$, where $g(x) = 4\sum_{j=0}^{j_0}(-1)^j \left[\frac{\sum_{i=j+1}^{b} C_{b+i}^{2b}}{2^{2b}}\right] T_{2j+1}(x)$ with $j_0 = \sqrt{b\log(4b/\epsilon)}$, and use non-unitary LCU.

Correctness: Since $x^{-1} \geq 1 \ \ \forall x \in D_{dk}$, the condition is met in non-unitary LCU.
ϵ-approximation: $f(x)$ is an ϵ-approximation of x^{-1}, and since

$$\frac{1}{2^{2b}}\sum_{i=j+1}^{b} C_{b+1}^{2b} \leq e^{-j^2/b}.$$

We have

$$|f(x)-g(x)| = \left|4\sum_{j=j_0+1}^{b-1}(-1)^j \left[\frac{\sum_{i=j+1}^{b} C_{b+i}^{2b}}{2^{2b}}\right] T_{2j+1}(x)\right| \leq 4\sum_{j=j_0+1}^{b-1} e^{-j^2/b} \leq 4e^{-j^2/b} \leq \epsilon.$$

Cost: Degree $= O(j_0) = O(kd\log(dk/\epsilon))$, $\alpha = \frac{4}{d}\sum_{j=0}^{j_0}(-1)^j \left[\frac{\sum_{i=j+1}^{b} C_{b+i}^{2b}}{2^{2b}}\right] \leq \frac{4j_0}{d} = O(k\log(dk/\epsilon))$.
$\Rightarrow O(k\log(dk/\epsilon))$ calls to U_B, and $O(j_0\alpha) = O(dk^2\log^2(dk/\epsilon))$ calls to O_A.

Remark.

1. Any classical algorithm for solving linear systems takes $\Omega(dN)$ cost in the worst case, whereas quantumly we only have linear dependence in sparsity $\Rightarrow$ exponentially better in dimension. However, the classical output is a whole vector, but quantumly we only have a state.

2. The very first quantum algorithm for $QLSP$ was proposed by Harrow, Hassidim and Lloyd, also known as the HHL algorithm. Complexity: $\text{poly}(d, n, 1//\epsilon, k)$.

3. The k^2 dependence here is actually worse than the classical counterpart k. With more effort, quantumly we can reach linear in k.

Optimal: $\Theta(dk\log(1/\epsilon))$ [Costa-An-Sanders-Su-Babbush-Berry] PRX Quantum, arxiv:2111.08152.

2 Quantum Computational Complexity

Complexity Classes: Formulated as binary strings. An instance of a problem is a string and the problem is cast as recognizing a language, which is a set of strings.

For example: BALANCED $= \{01, 10, 0011, 0110, 1001, 1010, 1100, \ldots\}$ (equal number of $0, 1$)
PRIME$=\{10, 11, 101, 111, \ldots\}$ (binary representation of prime numbers)

We say an algorithm recognizes a language if it accepts a string in the language and reject strings not in the language.

A complexity class is a set of languages recognized by some type of computation.

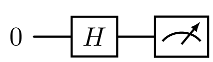
For example: $L \in P$: L can be determined by a poly-time deterministic classical algorithm.
$L \in$ BPP (bounded, probabilistic polynomial) There is a randomized classical algorithm A which runs in polynomial time, such that:

$$\forall x \in \{0,1\}^* : \begin{cases} \forall x \in L : \Pr[A \text{ accepts } x] \geq \frac{2}{3} \\ \forall x \notin L : \Pr[A \text{ rejects } x] \geq \frac{2}{3} \end{cases}$$

What's worth mentioning, $P \subseteq$ åBPP.

$L \in$ BQP: There is a quantum algorithm U which takes polynomial (2-qubit) gats such that:

$$\forall x \in \{0,1\}^* : \begin{cases} \forall x \in L : \Pr[U \text{ accepts } x] \geq \frac{2}{3} \\ \forall x \notin L : \Pr[U \text{ rejects } x] \geq \frac{2}{3} \end{cases}$$


equivalent to flipping a coin $\Rightarrow$BPP $\subseteq$ BQP.

In general, it's difficult to prove that some problem is really hard.

Instead: We show that some problems are "computational equivalent" and appear to be different manifestation of one really hard problem.

Reduction. Problem X reduces (don't confuse with "reduce from") to problem Y if arbitrary instances of problem X can be solved using:

- Polynomial number of calls to an oracle that solves Y, plus

- Polynomial number of standard computation steps.

Notation: $X \leqslant_p Y$ (This is also known as Karp reduction.)

Completeness. For a complexity class C, we say X is a C-complete problem if $X \in C$, and for any problem $Y \in C$, $Y \leqslant_p X$.

Theorem. The problem of solving linear systems is BQP-complete.

Proof. We have proved that $QLSP \in$ BQP.

Now we consider any quantum algorithm Y in BQP, written as $Y = U_T \cdots U_2 U_1$. Here each $U_i \in \mathbb{C}^{2^n \times 2^n}$ acts only nontrivally on two quits. $T = \text{poly}(n)$.

The initial state is $|0\rangle^{\otimes n}$, and the answer is determined by measuring the first qubit of the final state. Formally:

$$\forall y \in \{0,1\}^* : \begin{cases} \forall y \in Y : \text{Prob. of getting 1 when measuring the 1st qubit of } U_T \dots U_1 |0\rangle^{\otimes n} \geq \frac{2}{3} \\ \forall y \notin Y : \text{Prob. of getting 1 when measuring the 1st qubit of } U_T \dots U_1 |0\rangle^{\otimes n} \leq \frac{1}{3} \end{cases}$$

The key technique of making reductions: Clock construction. Consider:

$$U = \sum_{t=1}^{T} |t+1\rangle \langle t | \otimes U_t \ + \ |t+T+1\rangle \langle t+T| \otimes I + |t+2T+1 \bmod 3T\rangle\langle t+2T| \otimes U_{T+1-t}^\dagger.$$

Properties:

1) U has dimension $3T \cdot 2^n \cdot T = \text{poly}(n) \Rightarrow$ can be represented $O(n \log n)$ qubits.

2) U is a unitary. This is because

$$\begin{aligned} U^\dagger U &= \sum_{t=1}^{T} |t\rangle \langle t| \otimes U_t^\dagger U_t + |t+T\rangle \langle t+T| \otimes I + |t+2T\rangle \langle t+2T| \otimes U_{T+1-t} U_{T+1-t}^\dagger \\ &= \sum_{t=1}^{3T} |t\rangle \langle t| \otimes I = I. \end{aligned}$$

3) For t satisfying $T \leq t \leq 2T$, $U^t|1\rangle|\psi\rangle = |t+1\rangle \otimes U_T \dots U_1 |\psi\rangle$ for any n-quit state $|\phi\rangle$.

4) $U^{3T} = I$. This is became for any $t \in [3T]$ and n-qubit state $|\psi\rangle$, $U^{3T} |t\rangle |\psi\rangle = |t\rangle |\psi\rangle$.

Now, we define $A = I - Ue^{-1/T}$.

A is 5-sparse, and $k(A) \leq 4T$.

This is because each U_t is 4-sparse, as it acts nontrivially on 2 quits.

If λ is an eigenvalue of U with eigenvector $|\lambda\rangle$. then $|\lambda\rangle$ is an eigenvector of $I - Ue^{-1/T}$ with eigenvalue $1 - \lambda e^{-1/T}$.

U is unitary $\Rightarrow |\lambda| = 1 \Rightarrow \left|1 - \lambda e^{-1/T}\right| \epsilon \left[1 - e^{-1/T}, 1 + e^{-1/T}\right] \leqslant \left[\frac{1}{2T}, 2\right] \quad (T \geqslant 2)$

$(1-x)^{-1} = 1 + x + x^2 + \cdots \Rightarrow A^{-1} = \sum_{k=0}^{\infty} U^k e^{-k/T}$. Since $U^{3T} = I$. we can assume $0 \leq k \leq 3T - 1$.

Algorithm:

· Run solving linear system algorithm for $A(x) = |b\rangle$, when A is chosen above, and $|b\rangle = |1\rangle \otimes |0\rangle^{\otimes n}$.

For the solution $|x\rangle$, if we meanie the first register and obtain t satisfying $T \leq t \leq 2T$ (this happens with probability $\geqslant e^{-2} / \left(1 + e^{-2} + e^{-4}\right) \geqslant 0.117$).

In this case, the second register is the state $U_T \cdots \cdot U_1 |0^n\rangle$.

Set ε in $QLSP$ to be 0.01 , the above probability $\geqslant 0.117 - 0.01 > 0.1$.

Repeat the above for 20 times, we succeed with prob. $1 - (1 - 0.1)^{20} \geqslant 0.878$. This will make the margin of BQP being $\frac{2}{3} \times 0.878 \geqslant 0.585 > 0.5$.

Note: For BQP, 2/3 can be replaced by any constant $> \frac{1}{2}$.

A is $O(1)$-sparse has a condition number at most polynomial, and $|1\rangle\,|0\rangle^{\otimes n}$ can be trivially prepared. Our quantum algorithm for $QLSP$ runs in polynomial time. $\square$