Polynomial approximations and quantum lower bounds

Yaoyun Shi

University of Michigan
Quantum lower bounds on Collision and Element Distinctness

Yaoyun Shi

University of Michigan
Quantum lower bounds: Why?

Understanding the limitations of quantum computing.

Rule out some approaches for designing efficient quantum algorithms.

E.g.: Lower bound on unstructured search $\implies$ quantum comp. cannot solved NP-complete problems without exploring problem structure.

Results are not necessary disappointing news: existence of cryptography resilient to quantum cryptanalysis.
Quantum lower bounds: What?

Black-box model (Query model/Decision Tree model ...)

- **Oracle function**: $f$.
- **Wants to compute**: $\Gamma(f)$.
- **Complexity**: $\#$ evaluations of $f$.

Decision trees: $f : [N] \rightarrow \{0, 1\}$.

Comparison-based order statistics: sorting, finding minimum,...

Cryptography: $f$: encryption, $\Gamma$: cryptanalysis.

Can prove: classical/quantum lower bounds.
Quantum Computation

State space $\mathcal{H}$: $\mathbb{C}^2$ for 1 quantum bit; $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$ for $n$ qubits.

Computational basis: $\{ | x \rangle : x \in \{0, 1\}^n \}$.

State $| \phi \rangle$: a unit vector in $\mathcal{H}$:

$$| \phi \rangle = \sum_{x \in \{0, 1\}^n} a_x | x \rangle, \quad \alpha_x \in \mathbb{C}, \quad \sum_x |\alpha|^2 = 1.$$  

Operation $U$: unitary operator on $\mathcal{H}$.

Measurement $\mathcal{M}$: on $n$ qubits applied to $| \phi \rangle$:

1. $\forall x \in \{0, 1\}^n$, $\text{Prob}[\text{Observing outcome } x] = |\alpha_x|^2$,

2. If the outcome is $x$, the state becomes $|x\rangle$. 

Quantum black-box computation

Oracle: \( f : [N] \to [M] \).

State space: \( \mathcal{H} := \mathbb{C}^N \otimes \mathbb{C}^M \otimes \mathbb{C}^L \).

Computational basis:
\[
\{ |i, j, a\rangle : i \in [N], j \in [M], a \in [L] \}. 
\]

Query: \( \forall i \in [N], j \in [M], a \in [L], \)
\[
O_f |i, j, a\rangle = |i, j + f(i), a\rangle. 
\]

Algorithm:
(1) Start with a constant vector \( |\phi_0\rangle \in \mathcal{H} \).
(2) Apply
\[
U_0 \to O_f \to U_1 \to \cdots \to O_f \to U_T; 
\]
(3) Measure and output \( \Gamma(f) \) (with high probability).

Quantum complexity \( Q(\Gamma) \): minimum \# queries.
Quantum lower bounds: How?

**Adversary argument:** [Bennett, Bernstein, Brassard, Vazirani '97; Ambainis '00; Høyer, Neerbeck, Shi '01; …]

**Idea:** hard to distinguish similar inputs in one query.

**Successful** on almost all problems, except for...

**Polynomial method:** [Beals, Buhrman, Cleve, Mosca, de Wolf ’98]
Collision and Element Distinctness

Given $f : [N] \rightarrow [M]$ as an oracle.

Def: A collision is $(i, j)$, $i \neq j$, s.t. $f(i) = f(j)$.

Element Distinctness: Is there a collision? Well studied in classical (algebraic) decision trees.

2→1 Collision: $f$ is 2→1. Find a collision.

2→1/1→1: $f$ is either 2→1 or 1→1. Distinguish these two cases.

Cryptanalysis: finding collision
Random 2-to-1 functions: models collision intractable hash functions.
What do we know about them?

Collision classically: $\Theta(\sqrt{N})$ evaluations.

Quantum upper bound: $O(N^{1/3})$ [Brassard, Høyer, Tapp '97].

1. Choose random $k = \Theta(N^{1/3})$;
2. Do Grover’s search $\sqrt{N/k} = \Theta(N^{1/3})$.

Quantum lower bound: $\Omega(N^{1/5})$ [Aaronson '02]

Reduction from 2→1/1→1 to E.D.:

1. Pick a random $\Theta(\sqrt{N})$-subset,
2. Run E.D. algorithm.

$O(N^\alpha)$ for E.D. $\Rightarrow O(N^{\alpha/2})$ for 2→1/1→1.
Results

**Thm 1:** Any quantum algorithm for $2 \rightarrow 1/1 \rightarrow 1$ for $f : [N] \rightarrow [M]$, where $M \geq 3 \frac{N}{2}$, requires $\Omega(N^{1/3})$ evaluations.

**Thm 2:** Any quantum algorithm for $2 \rightarrow 1/1 \rightarrow 1$ for $f : [N] \rightarrow [N]$ requires $\Omega(N^{1/4})$ evaluations.

**Col:** Any quantum algorithm for **Element Distinctness** of $N$ numbers requires $\Omega(N^{2/3})$ queries to the numbers.
Polynomial method

**Def:** Given $f$, $\forall i \in [N]$, and $j \in [M]$:

$$
\delta_{i,j} = \begin{cases} 
1 & \text{if } f(i) = j \\
0 & \text{otherwise.}
\end{cases}
$$

**Observation:** $O_f$ is a linear function of $\delta_{i,j}$:

$$
O_f |i, j, a\rangle = \sum_{j'=1}^{M} \delta_{i,j'} |i, j'+j, a\rangle.
$$

**Lm:**[BBCMW, A] $AccProb(f) = \text{Polynomial of deg } \leq 2T \text{ over } \{\delta_{i,j}\}$.

Problem becomes lower bounding polynomial degree of any $P(f)[\delta_{1,1}, \delta_{1,2}, \cdots, \delta_{N,M}]$ such that

1. For all $f$, $P(f) \in [0, 1]$;
2. If $f$ is $1\rightarrow1$, $P(f) \approx 1$;
3. If $f$ is $2\rightarrow1$, $P(f) \approx 0$. 
How to lower bound polynomial degrees?

**Def:** A polynomial $g[x_1, x_2, \cdots, x_N]$ approximates $f : \{0, 1\}^N \rightarrow \{0, 1\}$ if $\forall x = x_1x_2\cdots x_N \in \{0, 1\}^N$,

$$|g(x) - f(x)| \leq 1/3.$$

**Def:** Approximation degree of $f$,

$$\tilde{\deg}(f) := \min \{ \deg(g) : g \text{ approx. } f \}.$$

All known method: Multivariate $\Rightarrow$ uni-variate. Apply Markov Inequality or Bernstein Inequality
Polynomial \( h : \mathbb{R} \to \mathbb{R}, \|h\|_{[-1,1]} = 1. \)

**Markov’s Inequality:**

\[ \|h'\| \leq (\text{deg}(h))^2. \]

**Bernstein’s Inequality:**

\[ |h'(x)| \leq \frac{\text{deg}(h)}{\sqrt{1-x^2}}, \quad \forall x \in (-1, 1). \]
Discrete version:[Paturi ’94] If
(1) \(|h(i)| \leq c\), for all \(i \in [0...N]\);
(2) \(|h(\lceil \xi - 1 \rceil) - h(\xi)| \geq c'\), for some \(\xi \in (0, N]\).

Then

\[
deg(h) = \Omega(\sqrt{\xi \cdot (N + 1 - \xi)}).
\]

In particular

\[
deg(h) = \Omega(\sqrt{N}).
\]

Example: symmetric functions:
(1) **symmetrization**: \(g(i) = E_{x:|x|=i} [f(x)]\)
uni-variate; \(deg(g) \leq deg(f)\).
(2) If \(g(i) \neq g(i + 1)\),

\[
\tilde{deg}(f) = \Omega(\sqrt{(i + 1) \cdot (N - i + 1)}).
\]
Aaronson’s Averaging approach.

Ideally:

1. Run algorithm on a random $g \rightarrow 1$ function $f_g$, $g = 1, 2, \ldots, N'$.
2. Prove
   $$P(g) := E \left[ \text{AccProb}(f_g) \right].$$
   is a polynomial of deg $O(T)$.
3. Apply Markov’s Inequ. on $P(g)$.

Problem:

1. $g \nmid N$, for most $g$;
2. $P(g)$ not a polynomial (but closed to one);
3. The range of $g$, $N'$, is small
   $\implies$ week lower bound.
$\Omega(N^{1/4})$ lower bound

**Idea:** Run algorithm on partial functions.

**Def:** $(m, g)$ is valid if $m \in [0..N]$, $g \in [1..N]$, and $g | N$.

**Def:** A $(m, g)$ function is a partial function $f : [N] \rightarrow [N]$, such that $f$ is $g\rightarrow 1$ on $m$ inputs, and not defined elsewhere.

**Modify Algorithm:** If $f(i)$ not defined, Reject!

How do you know $f(i)$ is not defined?

What I meant is: Evaluate $AccProb(G_f)$. 
Proof for \( \Omega(N^{1/4}) \)

\[ P(m,g) := E_{f_m,g}[AccProb(f_{m,g})] \]

is a poly. of deg \( \leq 2T \): counting subgraphs.

**Case 1.** If \( |P(N,g)| \leq 2 \), for \( g \in [1..\sqrt{N}] \).

**Case 2.** \( \exists g_0 \leq \sqrt{N}, \ |P(N,g_0)| > 2 \). Consider \( P(m,g_0) \).
The $\Omega(N^{1/3})$ lower bound:
Use Bernstein’s Inequality

Suppose we have $P(m, g)$ s.t.

$$0 \leq P(m, g) \leq 1 \quad \forall (m, g) \text{ valid},$$

$$P\left(\frac{N}{2}, 1\right) \approx 1, \quad \text{and,} \quad P\left(\frac{N}{2}, 2\right) \approx 0.$$

$\implies \Omega(N^{1/3}).$

**Case 1:** $\forall g \in [0...N^{2/3}]$, $|P\left(\frac{N}{2}, g\right)| \leq 1$.
Apply Markov $\implies \Omega(N^{1/3}).$

**Case 2:** $|P\left(\frac{N}{2}, g_0\right)| > 2$ for some $g_0 \leq N^{2/3}$.
Consider $P(m, g_0)$, $m = 0, g_0, 2g_0, \ldots, \lfloor N/g_0 \rfloor \cdot g_0$. Apply Bernstein Inequality.
**Def:** $\frac{1}{2}$-2→1 v.s. 2→1 Problem.

**Oracle:** $f : [N] \rightarrow [N]$.

**Promise:** $f$ is

1. 2→1 mapped to $[\frac{N}{2} + 1...N]$ on half inputs;
2. Either 1→1 or 2→1 mapped to $[\frac{N}{2}]$ on the other half.

**Distinguish** these two cases.

Algorithm $\mathcal{A}$ for $\frac{1}{2}$-2→1/2→1 $\Rightarrow$ Algorithm $\mathcal{A}'$ for 2→1/1→1.

$\tilde{\mathcal{A}}$: Symmetrize $\mathcal{A}$.

Randomly choose permutations $\sigma$ on $[N]$ and $\tau$ on $[M]$.

Replace query $i$ by $\sigma(i)$;
Replace answer $j$ by $\tau(j)$.

Run $\tilde{\mathcal{A}}$ on any instance

$\Rightarrow$ AccProb = Average AccProb.
$A$ works $\iff$

$$p_{1 \rightarrow 1} := E_{f:1 \rightarrow 1}[AccProb(f)] \approx 1,$$

$$p_{2 \rightarrow 1} := E_{f:2 \rightarrow 1}[AccProb(f)] \approx 0.$$ 

Consider

$$p_{\frac{1}{2} \rightarrow 2 \rightarrow 1} := E_{f:\frac{1}{2} \rightarrow 2 \rightarrow 1}[AccProb(f)].$$

**Case 1:** If $p_{\frac{1}{2} \rightarrow 2 \rightarrow 1} \geq 1/2$.

**Done:** $\tilde{A}$ is good.
Case 2: \( p_{\frac{1}{2}}^{-2} \rightarrow 1 < \frac{1}{2} \).

Idea: transform

\[
\frac{1}{2}^{-2} \rightarrow 1 \text{ to } 1 \rightarrow 1 \implies \text{AccProb} \approx 1;
\]

\[
2 \rightarrow 1 \text{ to } \frac{1}{2}^{-2} \rightarrow 1 \implies \text{AccProb} < \frac{1}{2}.
\]

How? UN-collide \( f^{-1}([\frac{N}{2} + 1...N]) \):

“Run” \( \tilde{A} \) on \( \bar{f} \)

\[
\bar{f}(i) = \begin{cases} 
    f(i) & f(i) \in [\frac{N}{2}] \\
    i + \frac{N}{2} & \text{otherwise}.
\end{cases}
\]
\[ \Omega(N^{1/3}) \] for \( \frac{1}{2} \to 2 \to 1/2 \to 1 \)

**Def:** A \((m, g)\)-function \( f \) satisfies:
1) \( f \) is \( g \to 1 \) mapped to \([\frac{N}{2}]\) on \( m \) inputs;
2) On the remaining input, \( f \) is \( 2 \to 1 \) mapped to \([\frac{N}{2} + 1 \ldots N]\).

**Valid \((m, g)\):** \( g \in [N], m \in [0 \ldots N], g|m, 2|N - m. \)

**Lm:** \( P(m, g) := \text{AccProb[random \((m, g)\)-function]} \)

is a polynomial of \( \text{deg} \leq 2T \).

1) \( P(m, g) \in [0, 1] \) for valid \((m, g)\),
2) \( P(\frac{N}{2}, 1) \approx 1, P(\frac{N}{2}, 2) \approx 0. \)
Conclusion

Results:
Matching lower bound for *Collision*; improved lower bound for *Collision with small range*;

Improved lower bound for *Element Distinctness*.

Technique: Extend and refine Aaronson’s averaging approach in proving polynomial degree lower bound.
Open Problems

Is Polynomial Method universal?

• **Cjct:** $Q(f) \approx \tilde{d}eg(f)$.

• **Cjct:** $\tilde{d}eg(\bigvee_{i=1}^N \bigwedge_{j=1}^N x_{i,j}) = \Omega(N)$.

**Known:** $Q(\cdot) = \Omega(N)$, $\tilde{d}eg(\cdot) = \Omega(\sqrt{N \log N})$.

**Set Equality:** Given 1→1 oracles $f, g : [N] \rightarrow [M]$,

Either $f([N]) = g([N])$ or $f([N]) \cap g([N]) = \emptyset$.

Distinguish these two cases. $O(N^{1/3})$ v.s. $\Omega(1)$.

**Quantum Space-Time trade-off:** Does quantum computer run much faster and at the same time save much space? E.D., Collision...