Quantum Lower Bounds

Ronald de Wolf

CWI Amsterdam

http://homepages.cwi.nl/~rdewolf

Why Lower Bounds?

- Main question for a computer scientist:

  Which problems admit quantum speed-up?

- Equivalent question:

  Which problems don't?

- We need lower bounds to answer this: provable limits on the power of quantum computers

Overview

1. What can we prove?
2. Black-box model
3. Methods:
   - hybrid
   - polynomials
   - quantum adversary
4. Other stuff, open problems

What Can we Prove?

- Counting argument:
  there are $2^{O(m \log m)}$ m-gate circuits over finite basis, but there are 2^{2^n} different n-bit functions $\Rightarrow$ most f need $m \geq 2^{n/\log(n)}$

- What about explicit functions?

- Even for classical circuits, we can prove only linear lower bounds! (P vs NP)

- We only know how to prove lower bounds in the black-box model

Black-Box Computation

- We want to compute $f : \{0, 1\}^N \rightarrow \{0, 1\}$ of input $x = (x_1, \ldots, x_N)$

- Input can only be accessed via queries:

- Unitary transformation: $\begin{array}{l} O|i, 0\rangle = |i, x_i\rangle \\ O|i, 1\rangle = |i, 1 - x_i\rangle \end{array}$

- QC can query superposition:

$$O\left(\frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i, 0\rangle\right) = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i, x_i\rangle$$

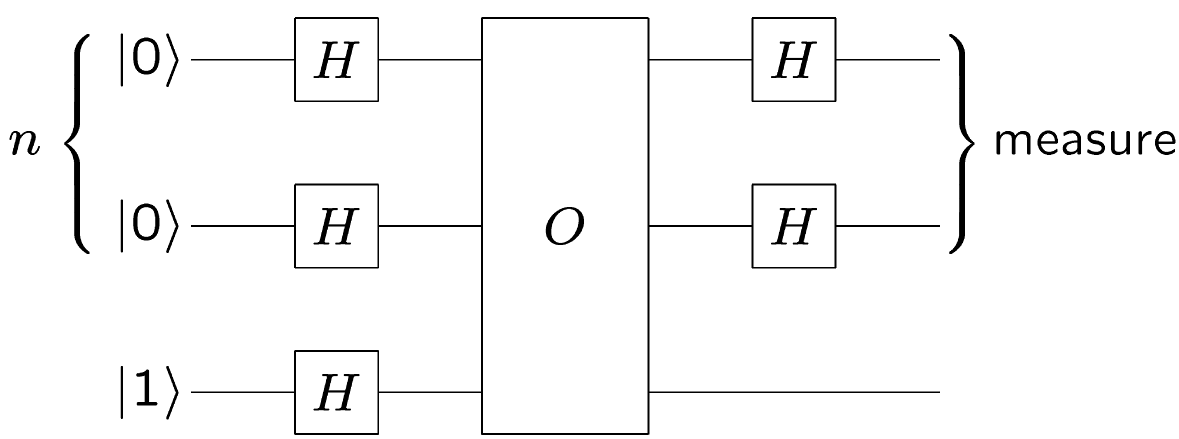
- Minimize the number of queries used

Example: Deutsch-Jozsa

- $x = (x_1, \ldots, x_N)$, $N = 2^n$, either
  (1) all x_i are 0 (constant), or
  (2) exactly half of the x_i are 0 (balanced)

- Classically: $\frac{N}{2} + 1$ queries needed

- Quantum: 1 query suffices



Deutsch-Jozsa (continued)

After first Hadamard:

$$\left(\frac{1}{\sqrt{2^n}}\sum_{i\in\{0,1\}^n}|i\rangle\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

After query:

$$\left(\frac{1}{\sqrt{2^n}}\sum_{i\in\{0,1\}^n}(-1)^{x_i}|i\rangle\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right).$$

After second Hadamard (ignore last qubit):

$$\frac{1}{\sqrt{2^n}}\sum_{i\in\{0,1\}^n}(-1)^{x_i}\frac{1}{\sqrt{2^n}}\sum_{j\in\{0,1\}^n}(-1)^{i\cdot j}|j\rangle.$$

Amplitude of $|j\rangle = |0\ldots 0\rangle$ is

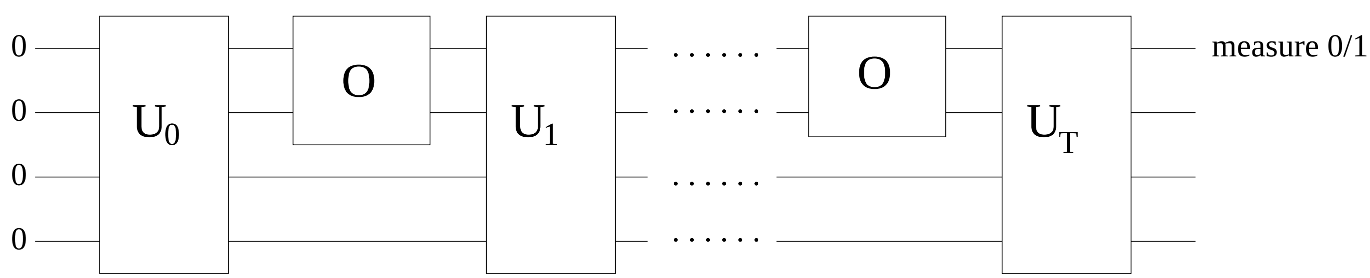
$$\frac{1}{2^n}\sum_{i\in\{0,1\}^n}(-1)^{x_i} = \begin{cases} 1 & \text{if constant} \\ 0 & \text{if balanced} \end{cases}$$

Measurement gives correct answer

Definition of Black-Box Complexities

- $D(f)$: # queries for deterministic algorithm
  $R_2(f)$: # queries for bounded-error algo (error probability $\leq 1/3$ for all x)

- A T-query quantum algorithm:



- $Q_E(f)$: # queries for exact quantum algo
  $Q_2(f)$: # queries for bounded-error quantum algo (error $\leq 1/3$ for all x)

Most Quantum Algorithms are Black-Box

- Deutsch-Jozsa (constant vs. balanced):
  $Q_E(\text{DJ}) = 1$ vs. $D(\text{DJ}) = \frac{N}{2} + 1$

- Shor's period-finding (implies factoring):
  $x = (m(1), \ldots, m(N))$, where m is
  a periodic function with period r
  $Q_2(\text{find-}r) = O(1)$ vs. $R_2(\text{find-}r) \geq N^{1/3}$

- Grover search:
  $x = (x_1, \ldots, x_N)$, find i s.t. $x_i = 1$
  $Q_2(\text{search}) \approx \sqrt{N}$ vs. $R_2(\text{search}) \approx N$

- Also: Simon, counting, ordered search,. . .

- Not: communication complexity, automata

Hybrid Method for Search (BBBV 93)

- Fix a T-query quantum search algorithm
  $|\phi_i^t\rangle$ = state before t-th query, on input e_i
  α_i^t = amplitude on query i in $|\phi_0^t\rangle$
  Compare empty input with all other inputs

- Easy: $\| \phi_0^{t+1} - \phi_i^{t+1} \| \leq \| \phi_0^t - \phi_i^t \| + 2|\alpha_i^t|$,
  so $\frac{1}{2} \leq \| \phi_0^{T+1} - \phi_i^{T+1} \| \leq 2 \sum_{t=1}^{T} |\alpha_i^t|$

- Sum over all i:

$$\frac{N}{2} \leq \sum_{i=1}^{N} 2 \sum_{t=1}^{T} |\alpha_i^t| = 2 \sum_{t=1}^{T} \sum_{i=1}^{N} |\alpha_i^t|$$

$$\overset{\text{CS}}{\leq} 2 \sum_{t=1}^{T} \sqrt{N} \sqrt{\sum_{i=1}^{N} |\alpha_i^t|^2} \leq 2T\sqrt{N}$$

$\Rightarrow \frac{\sqrt{N}}{4} \leq T$

Polynomial Method (BBCMW 98)

- Boolean function $f : \{0,1\}^N \to \{0,1\}$
  polynomial $p : \mathbb{R}^N \to \mathbb{R}$

- p represents f if $f(x) = p(x)\ \forall x$
  $deg(f)$ minimum degree of such p

- p approximates f if $|f(x) - p(x)| \leq 1/3\ \forall x$
  $\widetilde{deg}(f)$ minimum degree of such p

- Example:
  $x_1 + x_2 - x_1 x_2$ represents OR(x_1, x_2)
  $\frac{2}{3}x_1 + \frac{2}{3}x_2$ approximates OR(x_1, x_2)

- Polynomial lower bounds:

$$\frac{deg(f)}{2} \leq Q_E(f) \quad \text{and} \quad \frac{\widetilde{deg}(f)}{2} \leq Q_2(f)$$

Amplitudes Are Polynomials

- Final state after T queries depends on x:

$$|\phi\rangle = \sum_{k \in \{0,1\}^m} \alpha_k(x)|k\rangle$$

- $\alpha_k(x)$ are polynomials of degree $\leq T$, proof:

  1. Initially ($T = 0$) the α_k are constants
  2. O permutes $|i, 0\rangle$ and $|i, 1\rangle$ iff $x_i = 1$:

  $$O\left(\alpha|i,0\rangle + \beta|i,1\rangle\right) =$$

  $$(\alpha(1 - x_i) + \beta x_i)|i,0\rangle + (\alpha x_i + \beta(1 - x_i))|i,1\rangle$$

     thus O adds 1 to the degree

  3. Amplitudes after U_j are linear sums of old amplitudes, cannot increase degree

Lower Bounds from Degrees

- Probability of output 1:

$$P(x) = \sum_{k \text{ starts with } 1} |\alpha_k(x)|^2$$

  $P(x)$ is a polynomial of degree $\leq 2T$

- For exact algorithms, $P(x) = f(x)\ \forall x$:

$$deg(f) \leq \text{degree of } P \leq 2T$$

$$\Rightarrow \frac{deg(f)}{2} \leq Q_E(f)$$

- For bounded-error, $|P(x) - f(x)| \leq 1/3\ \forall x$

$$\Rightarrow \frac{\widetilde{deg}(f)}{2} \leq Q_2(f)$$

Examples of Degree Lower Bounds

- $deg(\text{OR}) = N \Rightarrow Q_E(\text{OR}) \geq N/2$
  No speed-up for error-less search!

- $\widetilde{deg}(\text{OR}) = \sqrt{N} \Rightarrow Q_2(\text{OR}) \geq \sqrt{N}/2$
  BBBV's lower bound on Grover search!

- $\widetilde{deg}(\text{PARITY}) = N \Rightarrow Q_2(\text{PARITY}) \geq N/2$
  No significant speed-up for parity!
  (independently by Farhi ea 98)

- $\widetilde{deg}(f) \approx N$ for most f (Ambainis)
  No significant speed-up for most f!

Tight Bounds for Symmetric f

- f is symmetric if $f(x)$ depends only on Hamming weight $|x|$ of x (OR, PARITY, Threshold,. . .)

- Can "symmetrize" its acceptance probability to single-variate $P(|x|)$ of degree $\leq 2T$

- Paturi 92: $\widetilde{deg}(f) \geq \sqrt{N(N - \Gamma(f) + 1)}$

- Upper bound from quantum counting

$D(f)$ and $Q_2(f)$ Polynomially Related

- Block sensitivity:
  max # disjoint blocks B s.t. $f(x) \neq f(x^B)$
  Measures influence of changes in x on $f(x)$

  1. $\sqrt{bs(f)} \leq \widetilde{deg}(f)$ (Nisan & Szegedy 94)

  2. $D(f) \leq bs(f)^3$ for total f (BBCMW 98)
     (i.e., no promise on N-bit input)

  $\Rightarrow D(f) \leq Q_2(f)^6$ for all total f

- For all total functions in the black-model:

  quantum bounded-error computation
  is at most polynomially better than
  classical deterministic computation

Lower Bound for Collision Problem

- Given $f : [N] \to Z$, either 1-to-1 or r-to-1
  Problem: determine which

- $(N/r)^{1/3}$ quantum queries suffice (BHT 97)

- Aaronson 02 (improved by Shi):

  1. Clever symmetrization gives degree-$2T$ 2-variate polynomial $P(s, m)$ such that $P(1, m) \approx 0$, and $P(s, m) \approx 1$ if $s|m$

  2. This must have high degree

- Gives $N^{2/3}$ bound for element distinctness

Adversary Method (Ambainis 00)

- Generalization of hybrid method
- If A computes f, then it must distinguish inputs x and y whenever $f(x) \neq f(y)$; otherwise correct output of A on x implies the same (incorrect) output on y.
- Distinguishing many (x, y)-pairs is hard
- Need some measure of progress to see how well we're distinguishing all (x, y)-pairs

More Precisely

- Let X and Y be sets of inputs such that $f(x) \neq f(y)$ whenever $x \in X$ and $y \in Y$

- Let $|\phi_x^t\rangle$ be state of the algorithm before t-th query on input x, then $|\langle\phi_x^T|\phi_y^T\rangle| \leq \frac{1}{2}$ (else measurement can't distinguish them)

- $W_t \stackrel{def}{=} \sum_{x\in X, y\in Y} |\langle\phi_x^t|\phi_y^t\rangle|$

- Initially: $W_0 = |X| \cdot |Y|$

- At the end: $W_T \leq \frac{1}{2}|X| \cdot |Y|$

- If we can show $W_t - W_{t+1} \leq \Delta$, then

$$Q_2(f) \geq \frac{W_0 - W_T}{\Delta} \geq \frac{\frac{1}{2}|X| \cdot |Y|}{\Delta}$$

Example: Search

- $X = \{(0, \ldots, 0)\}$
  $Y = \{e_i : 1 \leq i \leq N\}$

- $W_t \stackrel{def}{=} \sum_{x \in X, y \in Y} |\langle \phi_x^t | \phi_y^t \rangle|$

- Initially: $W_0 = |X| \cdot |Y| = N$

- At the end: $W_T \leq \frac{1}{2}|X| \cdot |Y| = \frac{N}{2}$

- Ambainis: $W_t - W_{t+1} \leq \sqrt{N}$, hence

$$Q_2(\text{search}) \geq \frac{W_0 - W_T}{\sqrt{N}} \geq \frac{\sqrt{N}}{2}$$

General Theorem

Consider $f : \{0,1\}^N \to Z$.

If there are sets $X, Y \subseteq \{0,1\}^N$ and relation $R \subseteq X \times Y$ s.t. $f(x) \neq f(y)$ if $x \in X$, $y \in Y$

1. for all $x \in X$ there are at least m different y with $(x,y) \in R$
2. for all $x \in X$ and $i \in [N]$ there are at most ℓ different y with $(x,y) \in R$ and $x_i \neq y_i$
3. for all $y \in Y$ there are at least m' different x with $(x,y) \in R$
4. for all $y \in Y$ and $i \in [N]$ there are at most ℓ' different x with $(x,y) \in R$ and $x_i \neq y_i$

then

$$Q_2(f) \geq \sqrt{\frac{m \cdot m'}{\ell \cdot \ell'}}$$

Other Lower Bounds via Adversary

Very versatile method:

- $\sqrt{N}$ for AND-OR trees
- $\sqrt{N}$ for inverting a permutation $\pi \in S_N$
- $\log N$ for binary search
- $N \log N$ for sorting
- Recent lower bounds on graph algorithms

Searching and Sorting

- Searching N unordered elements:

  Classical: $\approx N$ queries
  Quantum, error ε: $\sqrt{N \log(1/\varepsilon)}$

- Searching N ordered elements:

  Classical: $\log N$ queries
  Quantum: $\frac{1}{\pi \log e} \log N \leq Q_E \leq 0.526 \log N$

  (Høyer-Neerbek-Shi; Farhi ea)

- Sorting N elements:

  Classical: $N \log N + O(N)$ comparisons
  Quantum: $\frac{1}{2\pi \log e} N \log N \leq Q_E \leq 0.526\ N \log N$

Comparison: Polynomials vs Adversary

Cases where polynomial method is stronger:

- Search with small or zero error
- Collision-finding, element distinctness

Cases where adversary method is stronger:

- Iterated base function (Ambainis 03)
- AND-OR tree? ($\widetilde{deg}$ is unknown)

Neither method is optimal. A new semidefinite-programming method by Barnum, Saks, Szegedy is optimal, but very hard to apply

Some Open Problems

- Main question is still:

  Which problems admit quantum speed-up?

  (which promises give exponential speed-up?)

- Tighten general $D(f) \leq Q_2(f)^6$ bound?

- Generalize polynomials and adversary?

- Specific problems, like finding triangle in graph (upper bound $n^{3/2}$, lower bound n)

If You Want to Know More...

Polynomial method:

- Classical: Nisan and Szegedy, *On the degree of Boolean functions as real polynomials*, STOC 92.
- Quantum: Beals, Buhrman, Cleve, Mosca, de Wolf, *Quantum lower bounds by polynomials*, FOCS 98.
- Survey: Buhrman and de Wolf, *Complexity measures and decision tree complexity: A survey*. Theoretical Computer Science 2002
- Collision: Aaronson STOC 02, Shi FOCS 02

Quantum adversary method:

- Original: Ambainis, *Quantum lower bounds by quantum arguments*, STOC 2000.
- Weighted version: Høyer, Neerbek, Shi, *Quantum complexities of ordered searching, sorting, and element distinctness*, ICALP 2001.
- Separation: Ambainis, *Polynomial degree vs. quantum query complexity*, quant-ph/0305028