# Quantum Lower Bounds

Ronald de Wolf

CWI and University of Amsterdam

http://www.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. Black-box computation
2. Early lower bounds
3. Two general methods:
   - polynomials
   - quantum adversary
4. Complexity of searching & sorting
5. Open problems

# 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:

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

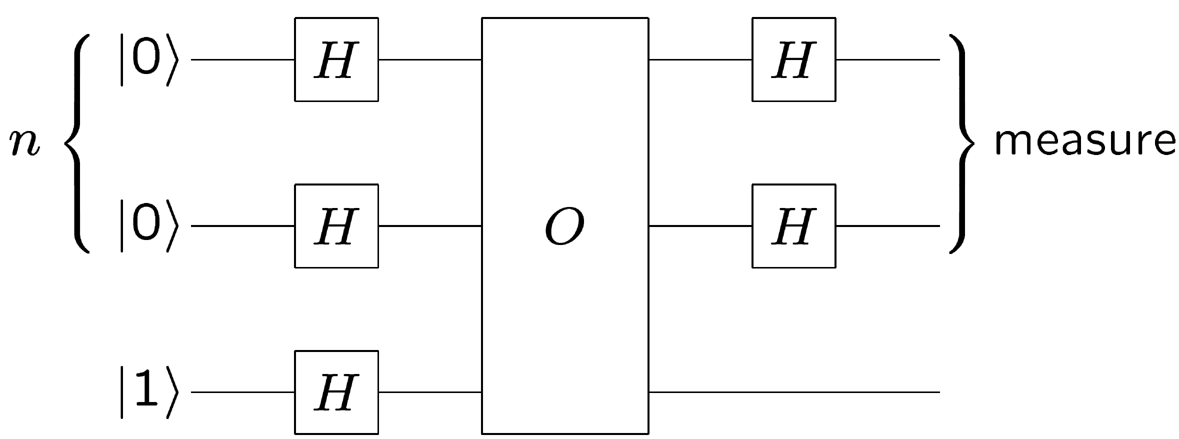
- Minimize the number of queries used

## 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:

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

After query:

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

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 $|j\rangle=|0\ldots0\rangle$ is

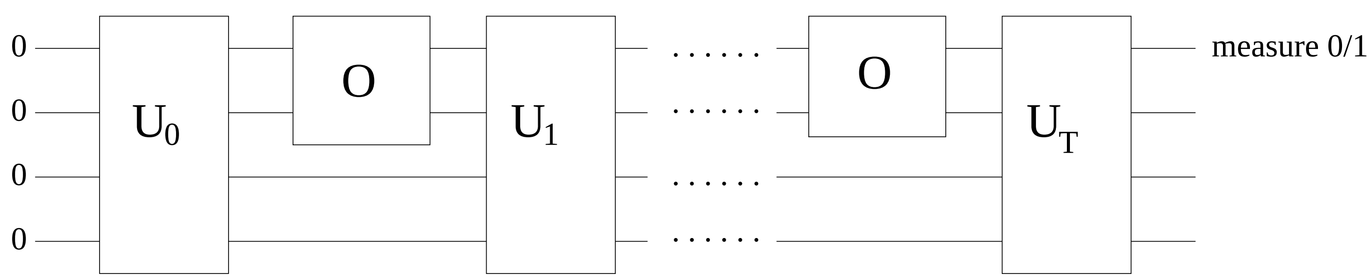
$$\frac{1}{2^n}\sum_{i\in\{0,1\}^n}(-1)^{x_i}=\begin{cases}1 & \text{if constant}\\ 0 & \text{if balanced}\end{cases}$$

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:
  $Q_E(\text{DJ}) = 1$ vs. $D(\text{DJ}) = \frac{N}{2} + 1$

- Shor's period-finding (implies factoring):
  $x = (m(0), \ldots, m(N))$, $\exists r \forall i \; m(i) = m(i + r)$
  $Q_2(\text{find-}r) = O(1)$ 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

## Early Lower Bounds

- Jozsa (91): what is the power of 1 query?
  Answer: not much

- BBBV (93-97): $\sqrt{N}$ lower bound on search
  (pre-dates Grover's algorithm!)

  Their idea (hybrid method):

  Examine $T$-query algo on $x = (0, \ldots, 0)$.
  At most $T^2$ variables influence outcome.
  But all $N$ inputs are relevant
  $\Longrightarrow T^2 \geq N \Longrightarrow T \geq \sqrt{N}$

# Method 1: Polynomials (BBCMW 98)

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

- $p$ 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 $\alpha_k$ 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, $P(x) = f(x)\ \forall x$:

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

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

- For bounded-error: $\dfrac{\widetilde{deg}(f)}{2} \leq Q_2(f)$

## Examples of Degree Lower Bounds

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

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

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

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

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

- Block sensitivity:
  measures influence of changes in $x$ on $f(x)$
  - $\sqrt{bs(f)} \leq \widetilde{deg}(f)$ (Nisan & Szegedy 94)
  - $D(f) \leq bs(f)^3$ for total $f$ (BBCMW 98)
    (i.e., no promise on $N$-bit input)
  - Hence $D(f) \leq Q_2(f)^6$ 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

## Method 2: Adversary (Ambainis)

- Adversary 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 (now incorrect) output on $y$.

- Distinguishing many $(x, y)$-pairs is hard

- Gives good bounds for some problems:
  - $\sqrt{N}$ for quantum search
  - $\sqrt{N}$ for AND-OR tree
  - $\sqrt{N}$ for inverting a permutation

## Idea of the Method

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

- Let $|\psi_x^j\rangle$ be state of the algorithm after $j$ queries on input $x$, then $|\langle\psi_x^T|\psi_y^T\rangle| \leq \frac{1}{2}$ (else measurement can't distinguish them)

- $W_j \stackrel{def}{=} \sum_{x \in X, y \in Y} |\langle\psi_x^j|\psi_y^j\rangle|$

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

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

- If we can show $|W_j - W_{j+1}| \leq B$, then

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

## Example: Search

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

- $W_j \stackrel{def}{=} \sum_{x \in X, y \in Y} |\langle \psi_x^j | \psi_y^j \rangle|$

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

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

- Ambainis: $|W_j - W_{j+1}| \leq \sqrt{N}$, hence

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

# Searching and Sorting

- Searching $N$ unordered elements:

  Quantum, constant error: $\sqrt{N}$ queries
  Error $\varepsilon$: $\sqrt{N \log(1/\varepsilon)}$ queries
  Error 0: $N$ queries

- Searching $N$ ordered elements:

  Classically: $\log N$ queries
  Quantum: $\frac{1}{\pi \log e} \log N \leq Q_E \leq 0.526 \log N$
  (Høyer, Neerbek, Shi, weighted adversary method; upper bound by Farhi et al.)

- Sorting $N$ elements:

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

## Some Open Problems

- Main question is still:

  Which problems admit quantum speed-up?

  (which promises give exponential speed-up?)

- Tighten $D(f) \leq Q_2(f)^6$ bounds

  Conjecture: $D(f) \leq Q_2(f)^2$ (Grover)

- Relation polynomials $\Longleftrightarrow$ adversary?

## 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 2001 (?)

### 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.