IEGULDĪJUMS TAVĀ NĀKOTNĒ

What is the smallest possible quantum query complexity of a Boolean function?

Andris Ambainis
University of Latvia

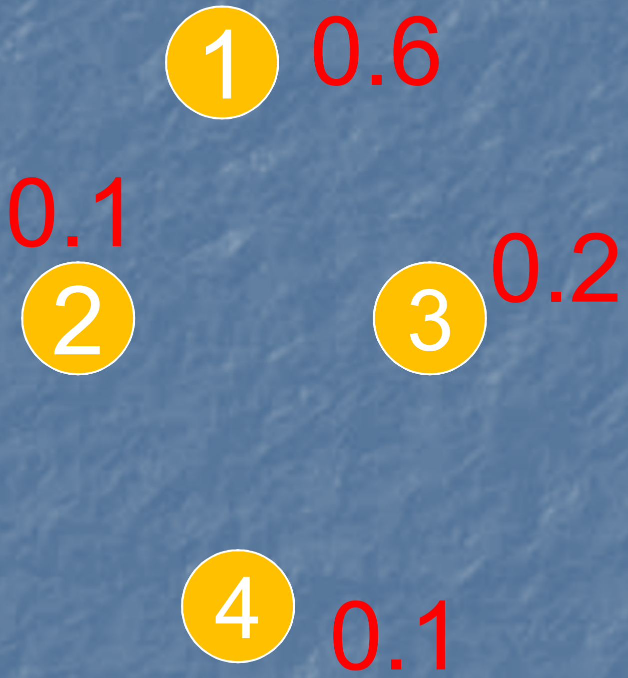
European Social Fund project "Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku" Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

What is quantum computation?

- New model of computing based on quantum mechanics.
- More powerful than conventional models:
  - Factoring: given N=pq, find p and q;
  - Discrete logarithms;
  - Search: given N objects x_i, find an object $i:x_i=1$.

Quantum computation: the model

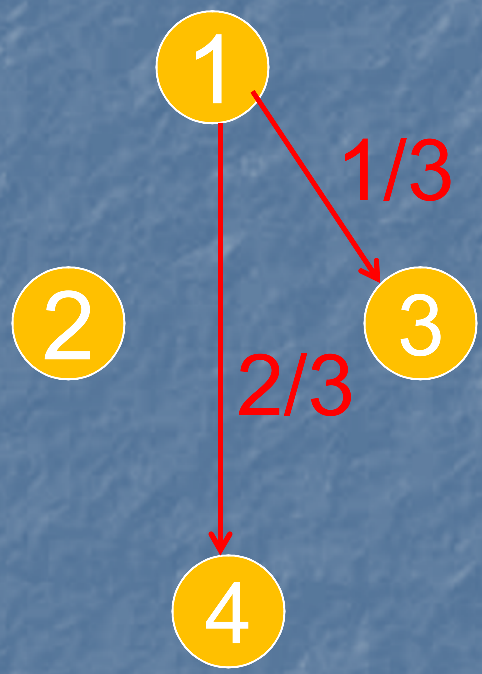
Probabilistic computation



- Probabilistic system with finite state space.
- Current state: probabilities p_i to be in state i.

$$\sum_i p_i = 1$$

Probabilistic computation



- Pick the next state, depending on the current one.
- Transitions: r_{ij} - probabilities to move from i to j.

Probabilistic computation

- Probability vector $(p_1, \ldots, p_N)$.
- Transitions:

$$\begin{pmatrix} p'_1 \\ \cdots \\ p'_N \end{pmatrix} = \begin{pmatrix} r_{11} & \cdots & r_{1N} \\ \cdots & \cdots & \cdots \\ r_{N1} & \cdots & r_{NN} \end{pmatrix} \begin{pmatrix} p_1 \\ \cdots \\ p_N \end{pmatrix}$$

transition probabilities

after the transition

before the transition

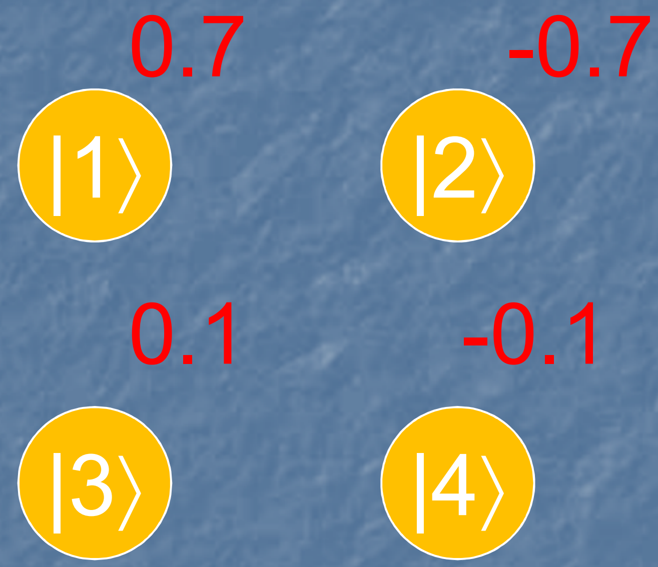
Quantum computation

- Current state: amplitudes α_i to be in state i.

$$\sum_i |\alpha_i|^2 = 1$$

For most purposes, real (possibly negative) amplitudes suffice.

Notation



- Basis states $|1\rangle$, $|2\rangle$, $|3\rangle$, $|4\rangle$.

$$|\Psi\rangle = \begin{pmatrix} 0.7 \\ -0.7 \\ 0.1 \\ -0.1 \end{pmatrix}$$

$$|\Psi\rangle = 0.7\,|1\rangle - 0.7\,|2\rangle + 0.1\,|3\rangle - 0.1\,|4\rangle.$$

Quantum computation

- Amplitude vector $(\alpha_1, \ldots, \alpha_M)$, $\sum_i |\alpha_i|^2 = 1$
- Transitions:

$$\begin{pmatrix} \alpha'_1 \\ \ldots \\ \alpha'_M \end{pmatrix} = \begin{pmatrix} u_{11} & \ldots & u_{1M} \\ \ldots & \ldots & \ldots \\ u_{M1} & \ldots & u_{MM} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \ldots \\ \alpha_M \end{pmatrix}$$

transition matrix

after the transition

before the transition

Measurement

Quantum state:

$$\alpha_1 |1\rangle + \alpha_2 |2\rangle + \ldots + \alpha_N |N\rangle$$

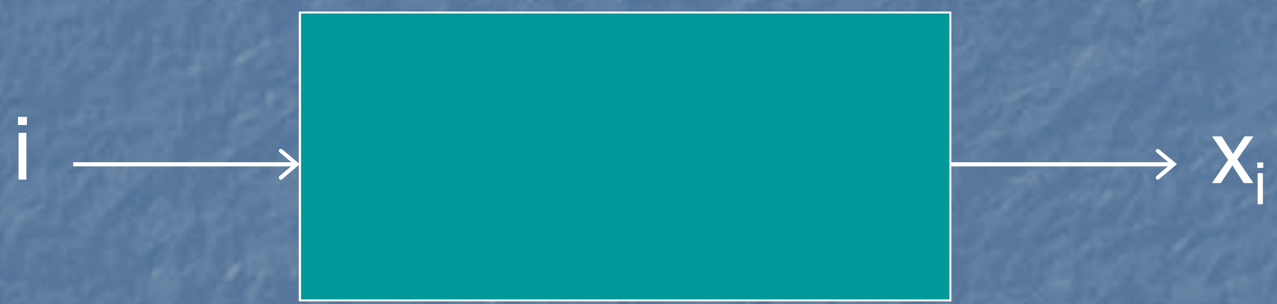
Measurement

	1	2	…	N
prob.	$\|\alpha_1\|^2$	$\|\alpha_2\|^2$		$\|\alpha_N\|^2$

Quantum algorithms in the query model

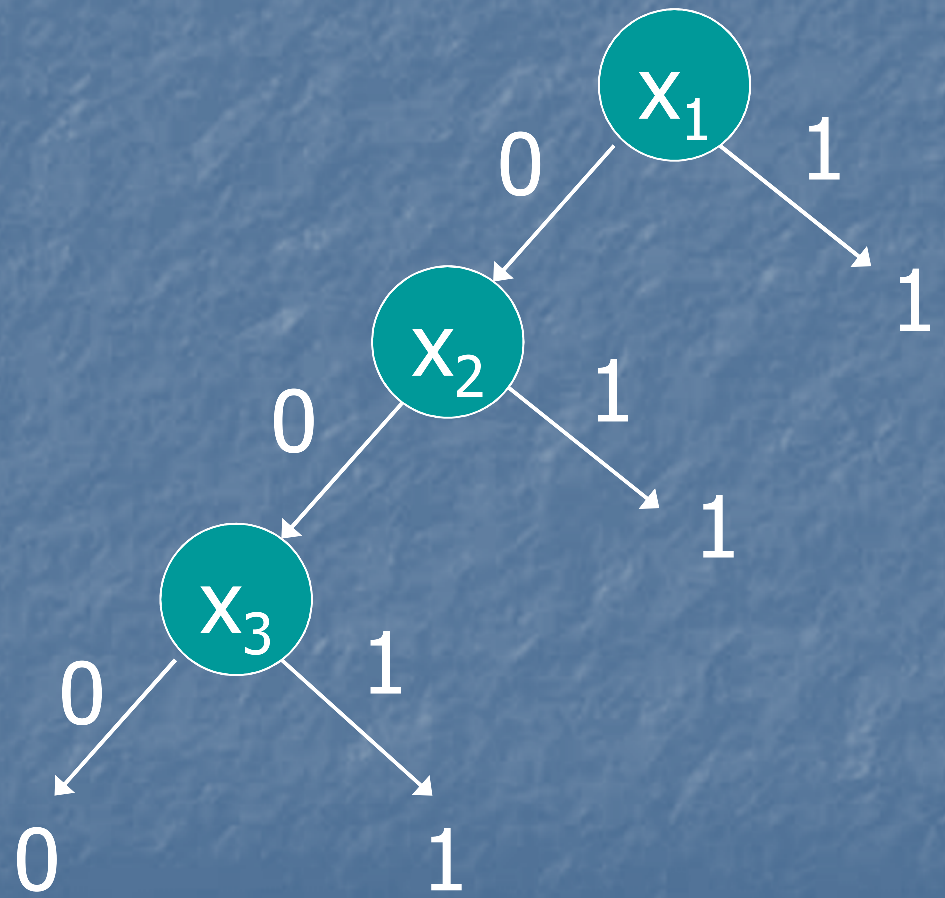
Query model

- Function $f(x_1, ..., x_N)$, $x_i \in \{0,1\}$.
- x_i given by a black box:



What is the smallest number of queries with which one can compute $f(x_1, ..., x_N)$?

Decision trees

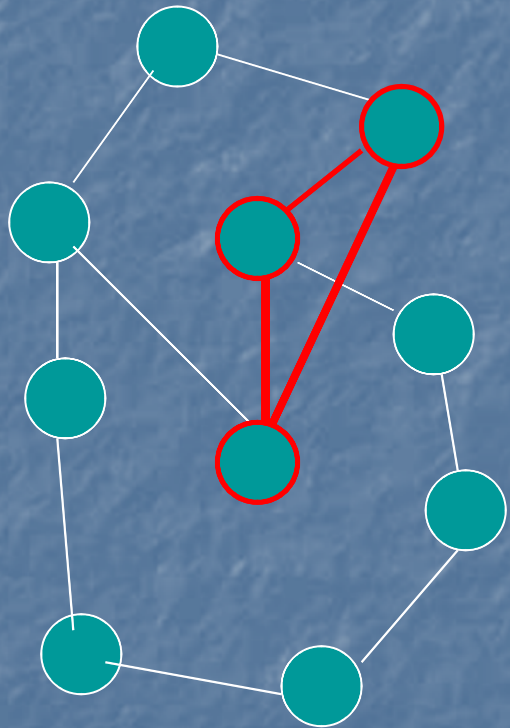


Grover's search

0	1	0	…	0
x_1	x_2	x_3		x_N

- Does there exist $i{:}x_i=1$?
- Queries: ask i, get x_i.
- Classically, N queries required.
- Quantum: $O(\sqrt{N})$ queries [Grover, 1996].

Triangle finding



- Graph G with n vertices.
- n^2 variables x_{ij}; $x_{ij}=1$ if there is an edge (i, j).
- Does G contain a triangle?
- Classically: $O(n^2)$.
- [Lee, et al., 2013] Quantum: $O(n^{9/7})$.

Queries in the quantum world

- Basis states: $|1,1\rangle$, $|1, 2\rangle$, ..., $|N, M\rangle$.
- State:

$$\alpha_{1,1}|1,1\rangle + \alpha_{1,2}|1, 2\rangle + \ldots + \alpha_{N, M}|N, M\rangle.$$

- Query:
  - $|i, j\rangle \rightarrow |i, j\rangle$, if $x_i=0$;
  - $|i, j\rangle \rightarrow -|i, j\rangle$, if $x_i=1$;

Example

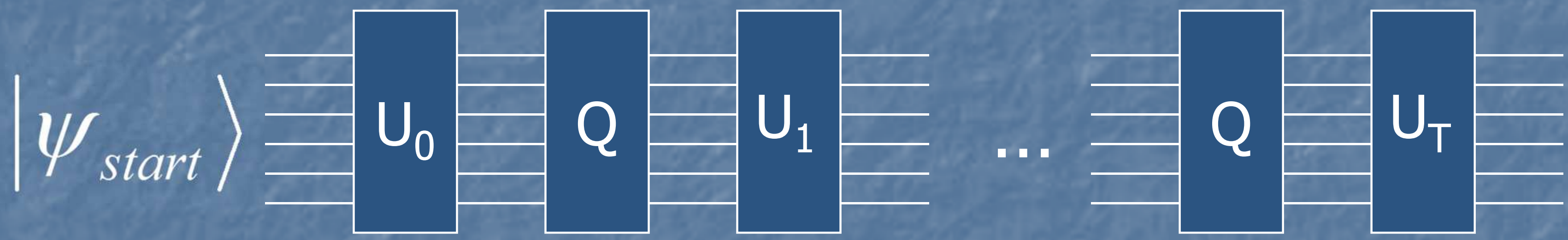
x_1	x_2	x_3
0	1	0

$$\alpha_{1,1}|1, 1\rangle+\alpha_{1,2}|1, 2\rangle+\alpha_{2,1}|2, 1\rangle+\alpha_{3,1}|3,1\rangle$$

$$\Big\downarrow \quad \text{Query}$$

$$\alpha_{1,1}|1, 1\rangle+\alpha_{1,2}|1, 2\rangle- \alpha_{2,1}|2, 1\rangle+\alpha_{3,1}|3,1\rangle$$

Quantum query model



- Fixed starting state.
- U_0, U_1, ..., U_T – independent of x_1, ..., x_N.
- Q – queries.
- Measuring final state gives the result.

Quantum query complexity

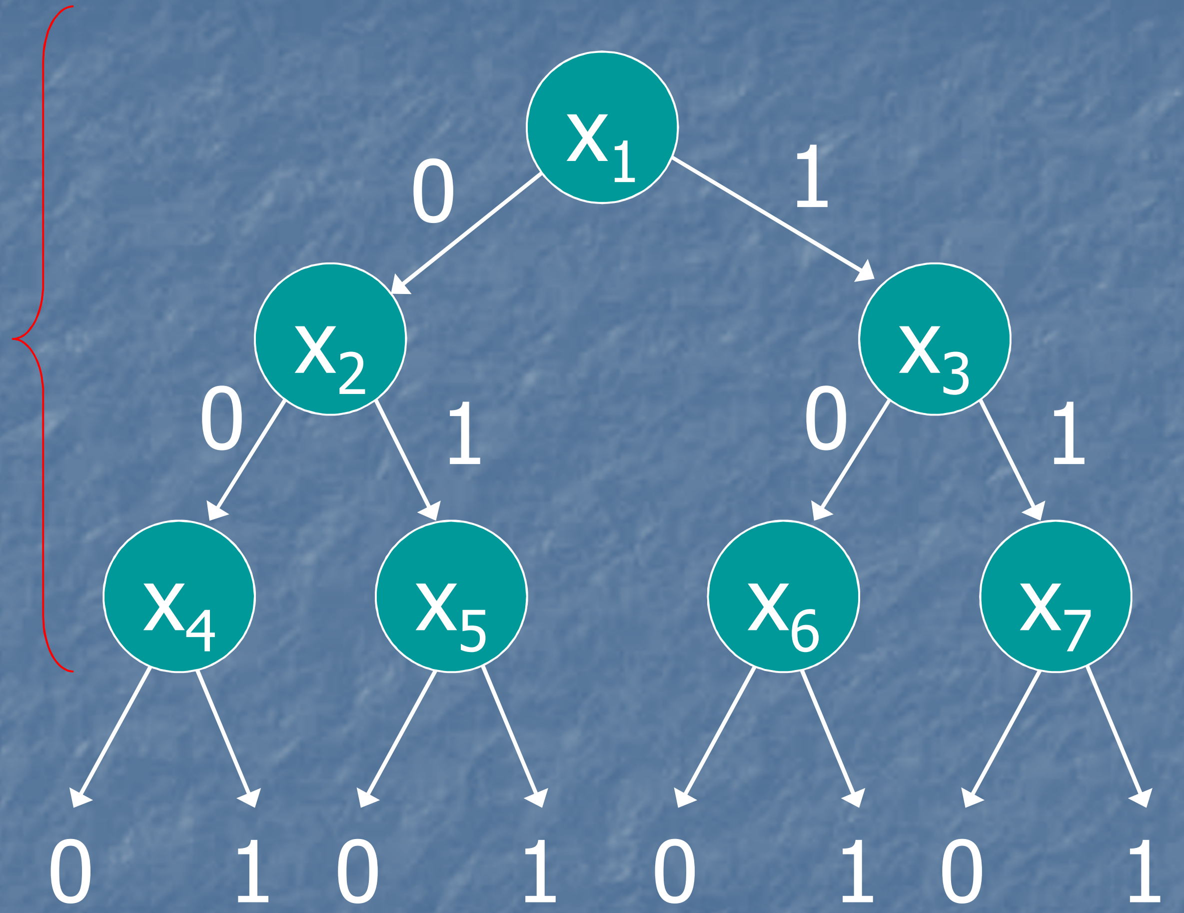
- $Q_E(f)$ – for any $x_1, ..., x_N$, measuring the final state of the algorithm always gives $f(x_1, ..., x_N)$.

- $Q_2(f)$ – for any $x_1, ..., x_N$, measuring the final state of the algorithm gives $f(x_1, ..., x_N)$ with probability $\geq 2/3$.

What is the smallest possible $Q_2(f)$ for $f(x_1, \ldots, x_N)$ that depends on all x_i?

Deterministic algorithms

K levels



2^K-1 variables

$N = 2^K - 1 \Rightarrow K \approx \log N$

Quantum algorithms?

- A quantum algorithm can query $\alpha_{1,1}|1,1\rangle+\alpha_{1,2}|1, 2\rangle+ \ldots +\alpha_{N, M}|N, M\rangle$ in one step.

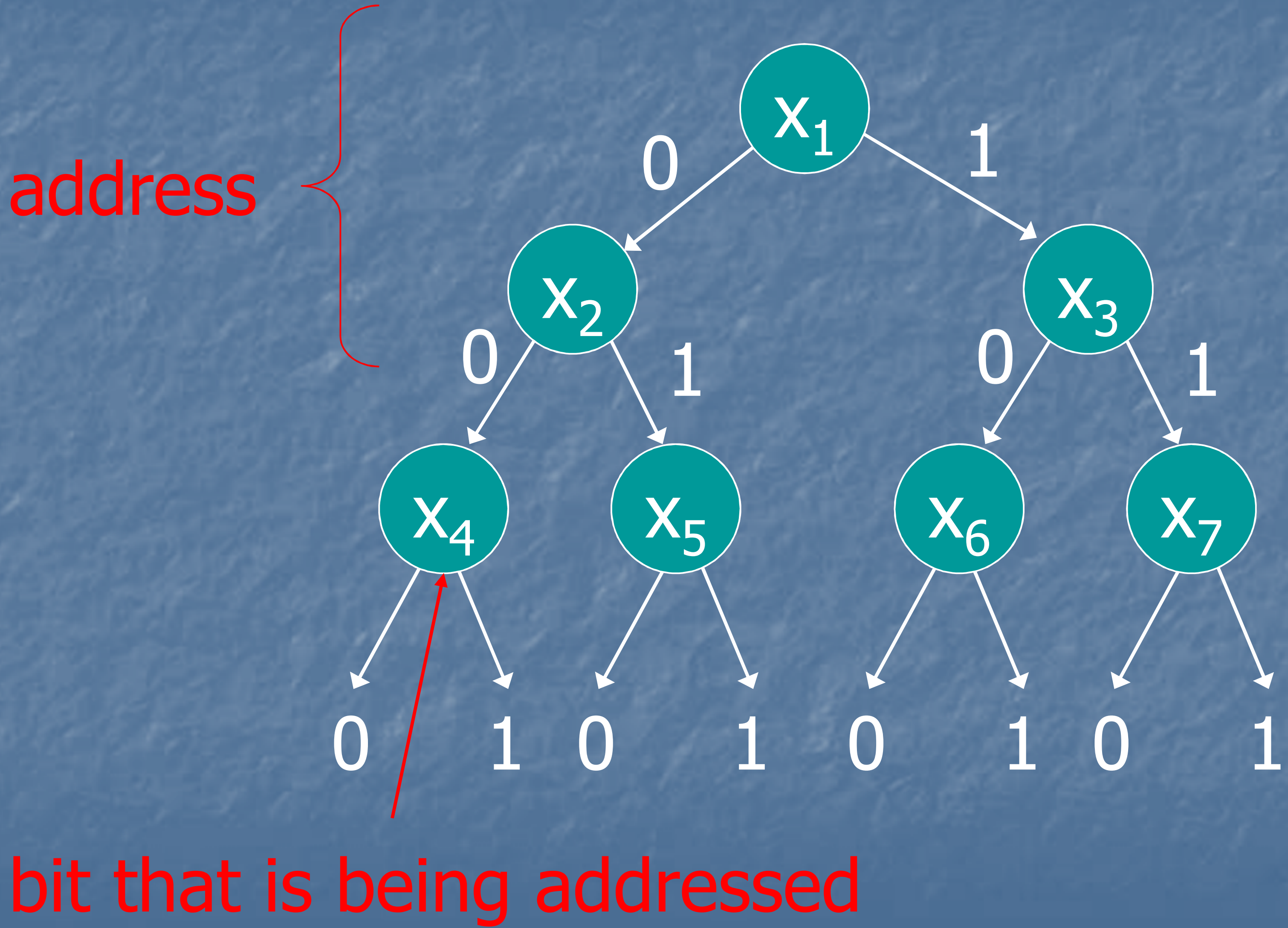
It is not obvious that there is no $f(x_1, ..., x_N)$ that depends on all x_i and is computable with 2 or 3 queries.

Main result

- <u>Theorem</u> (A, de Wolf, 2012):
  - There exists $f(x_1, ..., x_N)$ that depends on all x_i and is computable with $O(\log N / \log \log N)$ queries.
  - Any $f(x_1, ..., x_N)$ that depends on all x_i requires $\Omega(\log N / \log \log N)$ queries.

Part 1: construction

Deterministic algorithms



Addressing schemes

- Addressing scheme: algorithm that makes k queries to $x_1, \ldots, x_N$ and outputs $g(x_1, .. x_N) \in \{1, \ldots, M\}$.

$$f(x_1, \ldots, x_N, y_1, \ldots, y_M) = y_{g(x_1, \ldots, x_N)}$$

N+M variables, k+1 queries

How big can we make M?

Addressing schemes

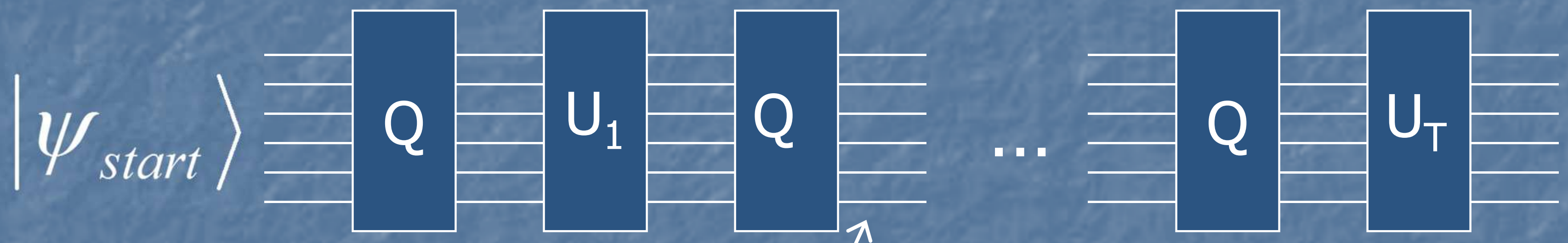
- Classical: k queries => $M = 2^k$ locations.
- Quantum: k queries => $M = k^{ck}$ locations.

Function $f(x_1, ..., x_N, y_1, ..., y_M)$
that depends on $M=k^{ck}$ variables,
is computable with k+1 queries.

$$k+1 = O(\log M/\log \log M)$$

Part 2: lower bound

Analyzing query algorithms



$\alpha_{1,1}|1,1\rangle + \alpha_{1,2}|1, 2\rangle + \dots + \alpha_{N, M}|N, M\rangle$

$\alpha_{1,1}$ is actually $\alpha_{1,1}(x_1, \dots, x_N)$

Polynomials method

- Lemma [Beals et al., 1998] If

$$\sum_{i,j} \alpha_{i,j}(x_1, \ldots, x_N)|i,j\rangle$$

is a state after k queries, then $\alpha_{i,j}(x_1, \ldots, x_N)$ are polynomials in $x_1, \ldots, x_N$ of degree $\leq k$.

Measurement: (i, j) w. probability $|\alpha_{i,j}(x_1, \ldots, x_N)|^2$

Polynomial of degree $\leq 2k$

Implications

- Corollary 1 If f is computable with k quantum queries exactly (no error), there exists p: deg(p)$\leq$2k:

  $f=0 \rightarrow p=0, \quad f=1 \rightarrow p=1.$

- Corollary 2 If f is computable with k quantum queries with prob. $\geq$2/3, there exists p: deg(p)$\leq$2k:

  $f=0 \rightarrow p\in[0, 1/3], \quad f=1 \rightarrow p\in[2/3, 1].$

Results

If $f(x_1, \ldots, x_N)$ depends on all x_i, then

- [Nisan, Szegedy, 1994]

  $\deg(p) = \Omega(\log N)$ for a polynomial p:

  $$f=0 \rightarrow p=0, \quad f=1 \rightarrow p=1.$$

- [A, de Wolf, 2012]

  $\deg(p) = \Omega(\log N / \log\log N)$ for any p:

  $$f=0 \rightarrow p\in[0, 1/3], \quad f=1 \rightarrow p\in[2/3, 1].$$

Influences

- $x=(x_1, \ldots, x_N)$.
- $x^i=(x_1, \ldots, 1-x_i, \ldots, x_N)$.
- Influence of a variable:
  - $\mathrm{Inf}_i(f) = \Pr_x[f(x) \neq f(x^i)]$

Using influences

- $f(x_1, x_2, ..., x_N)$ = polynomial of degree d.
- <u>Lemma 1</u> If f(x) depends on x_i, then $Inf_i(f) \geq \frac{1}{2^d}$
- <u>Lemma 2</u> For any f(x),

$$\frac{N}{2^d} \leq \sum_i Inf_i(f) \leq d$$

$N \leq d\ 2^d$ $\quad$ $d \geq \log N - \log \log N$

Fourier representation of Boolean functions

$S=\{i_1, \ldots, i_k\}$

$$\chi_S(x_1,\ldots,x_N)=\begin{cases} 1 & x_{i_1}+\ldots+x_{i_k} \ even \\ -1 & x_{i_1}+\ldots+x_{i_k} \ odd \end{cases}$$

$$\chi_S(x_1,\ldots,x_N)=(-1)^{x_{i_1}+\ldots+x_{i_k}}$$

Theorem For any $f(x_1, \ldots, x_N)$,

$$f(x_1,\ldots,x_N)=\sum_S \alpha_S \chi_S(x_1,\ldots,x_N)$$

Properties of Fourier coefficients

$$f(x_1,\ldots,x_N)=\sum_S \alpha_S \chi_S(x_1,\ldots,x_N)$$

1) deg(f) = d $\Rightarrow$ α_S=0 for S:|S|>d

2) $\sum_S \alpha_S^2 \le 1$ 3) $\sum_{i\in S} \alpha_S^2 = Inf_i(S)$

$$\sum_i Inf_i(S) = \sum_i \sum_{i\in S} \alpha_S^2 = \sum_S |S|\,\alpha_S^2 \le d$$

Conclusion

- The smallest number of quantum queries to compute $f(x_1, \ldots, x_N)$ that depends on all x_i is $\Theta(\log N / \log \log N)$.
- Uses connection between quantum algorithms and polynomials.