IEGULDĪJUMS TAVĀ NĀKOTNĒ

# The need for structure in quantum speedups

Andris Ambainis (Latvia)
Scott Aaronson (MIT)

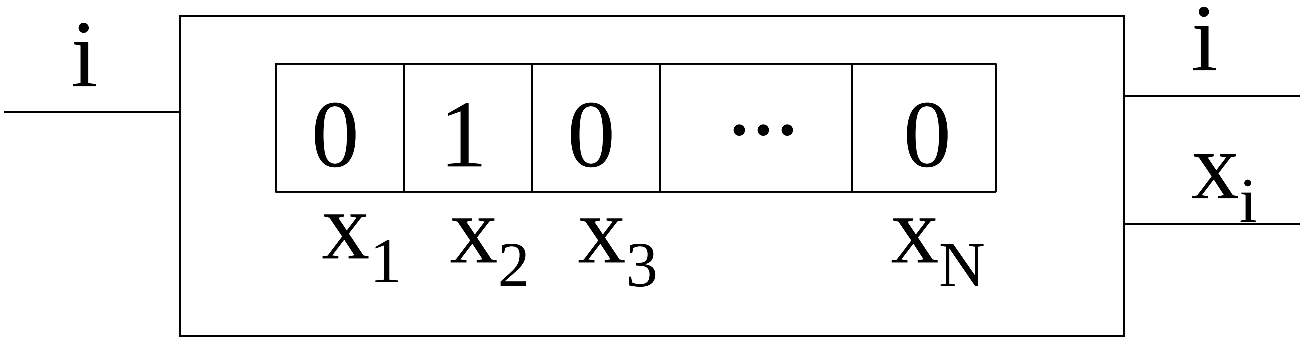
European Social Fund project “Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku” Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

# Main quantum algorithms

- [Shor, 1994] Polynomial time quantum algorithms for factoring and discrete log.
- [Grover, 1996] A quantum algorithm for searching a list of N elements in $O(\sqrt{N})$ steps.

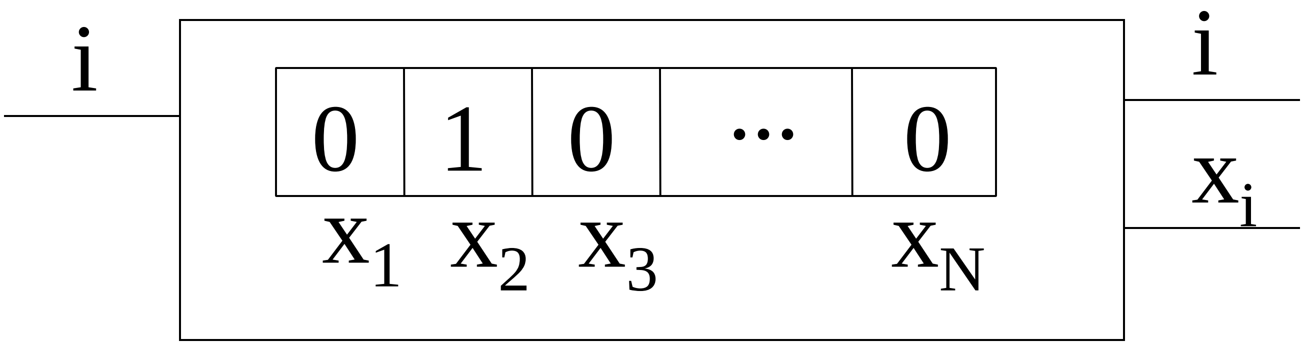
When do we have exponential quantum speedups?

# Query model




- Input $x_1$, …, $x_N$ accessed by queries.
- Complexity = the number of queries.

# Quantum query model




- Quantum query:

$$\sum_i \alpha_i |i\rangle \to \sum_i \alpha_i (-1)^{x_i} |i\rangle$$

# Examples

| | | | | |
|---|---|---|---|---|
| 0 | 1 | 0 | $\cdots$ | 0 |
| $x_1$ | $x_2$ | $x_3$ | | $x_N$ |

- Grover's search:
  - Is there i such that $x_i=1$?
  - N queries classically, $O(\sqrt{N})$ quantumly.
- Quantum counting [BHT00]:
  - Determine the fraction of $i{:}x_i=1$, with precision $\varepsilon$.
  - $O(1/\varepsilon^2)$ queries classically, $O(1/\varepsilon)$ queries quantumly.

# Examples

| | | | | |
|---|---|---|---|---|
| 0 | 1 | 0 | … | 0 |
| $x_1$ | $x_2$ | $x_3$ | | $x_N$ |

- Period-finding:
  - Promise: exists p: $x_{i+p}=x_p$.
  - O(1) queries quantumly*;
  - $\Theta(N^{1/4})$ queries classically.

* with some assumptions on $x_i$.

# Polynomial vs. exponential speedups

- Search: is there $i: x_i=1$?
- Counting: estimate the fraction of $i: x_i=1$.

Symmetric

- Period-finding: find p: $x_i=x_{i+p}$.

Non-symmetric

# Conjecture (Watrous, 2002)

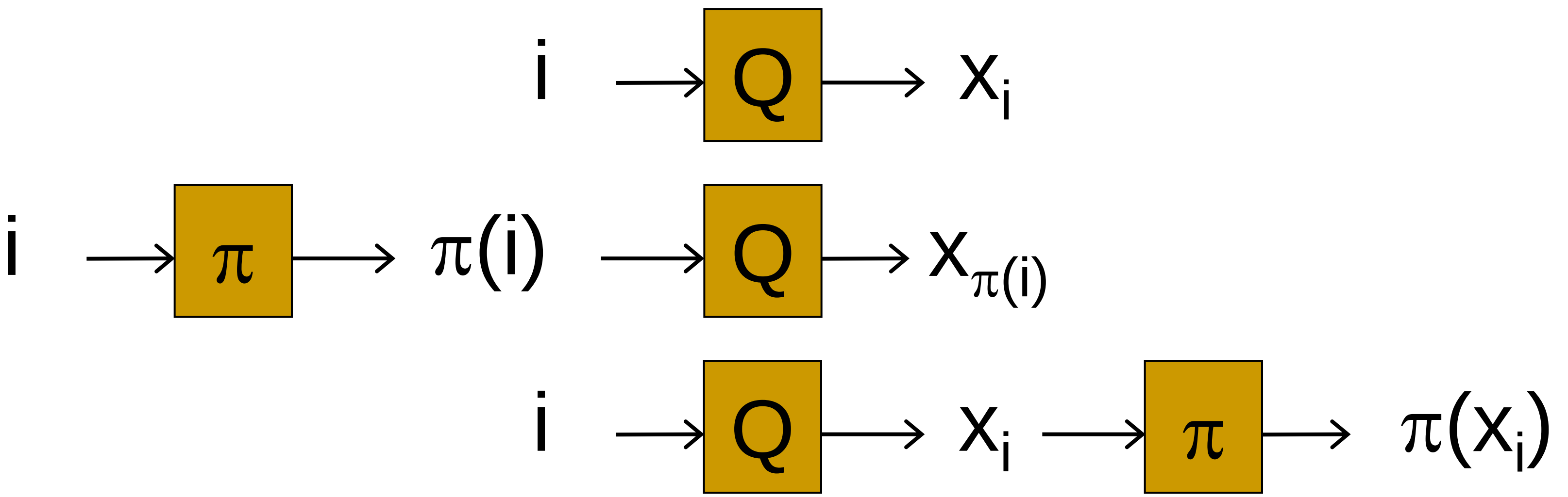
- Conjecture If f – symmetric, then R(f)=O($Q^c$(f)),
  - Q(f) - quantum query complexity of f;
  - R(f) - randomized query complexity of f.

# Folk theorem (easy)

- Theorem For $f(x_1, ..., x_N)$, $x_i \in \{0, 1\}$: $R(f) = O(Q^2(f))$.
- Basic idea: quantum counting is optimal.

Non-boolean $x_i$?

# Two types of symmetries




- Function f is symmetric if

$$f(x_1, \ldots, x_N) = f(x_{\pi(1)}, \ldots, x_{\pi(N)})$$
$$= f(\pi(x_1), \ldots, \pi(x_N)).$$

# Main result

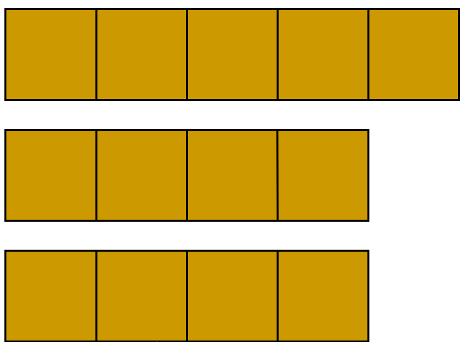
- Theorem If G has both types of symmetries, $R(f)=O^*(Q^9(f))$.

* some log factors are omitted.

- Classical algorithm: random sampling.

# Input types

- Since $G(x_1, \ldots, x_N)$ is symmetric, it only depends on:



$y_1$ the number of $i{:}x_i=1$

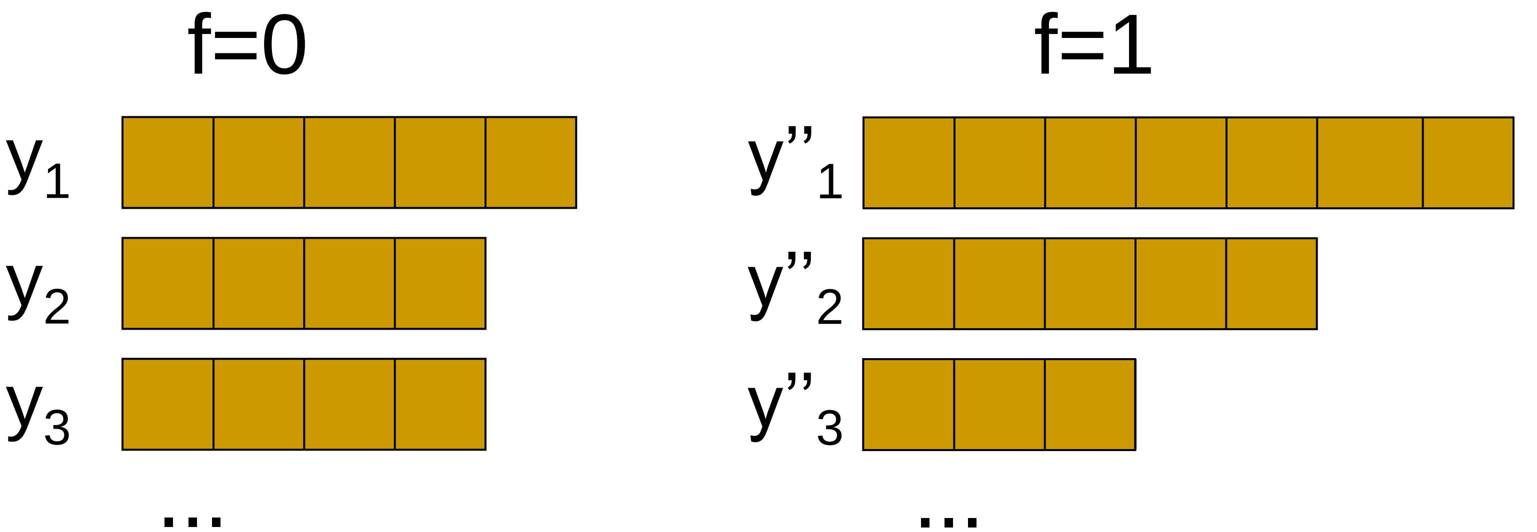
$y_2$ the number of $i{:}x_i=2$

$y_3$ the number of $i{:}x_i=3$

... ...

Can be estimated by random sampling

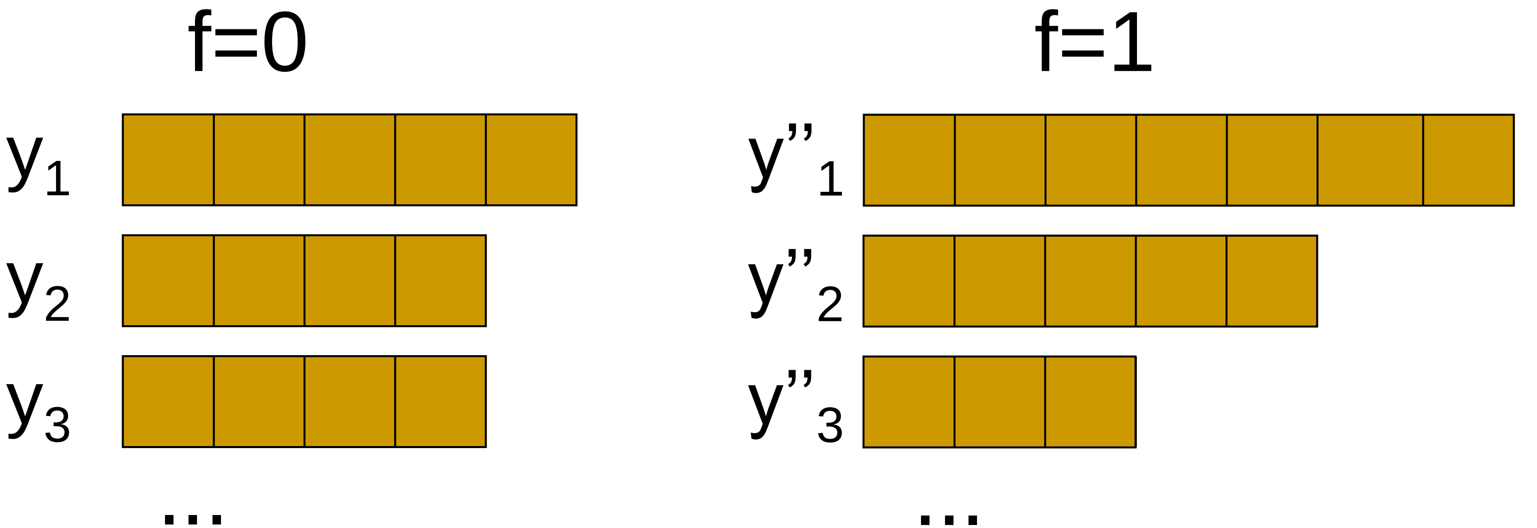
# Distinguishing problem




$y_i$ and $y''_i$ differ by at most $O(N/T)$.

Claim Distinguishing between these two types requires $\Omega(T^{1/7})$ quantum queries.

# Case 1




D – number of different rows

If D small, the types are hard to distinguish.

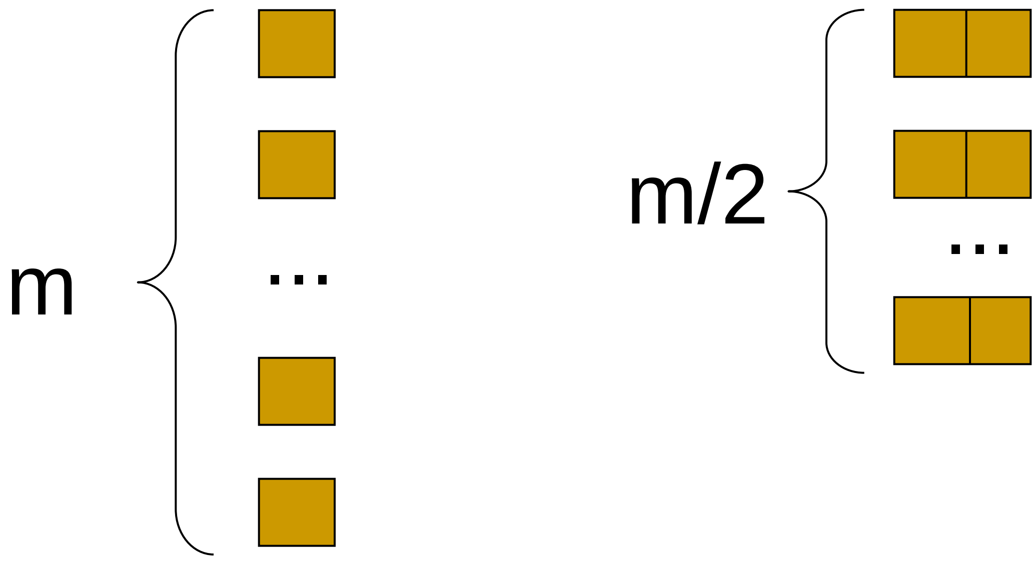
# Folk lemma

- Detecting a difference in $\varepsilon$ fraction of $x_i$'s requires
  - $\Omega(1/\varepsilon)$ queries classically;
  - $\Omega(1/\sqrt{\varepsilon})$ queries quantumly;

  (as long as the $\varepsilon$ fraction of possibly different $x_i$'s is randomly).
- Quantum adversary [A, 2000].

# Case 2

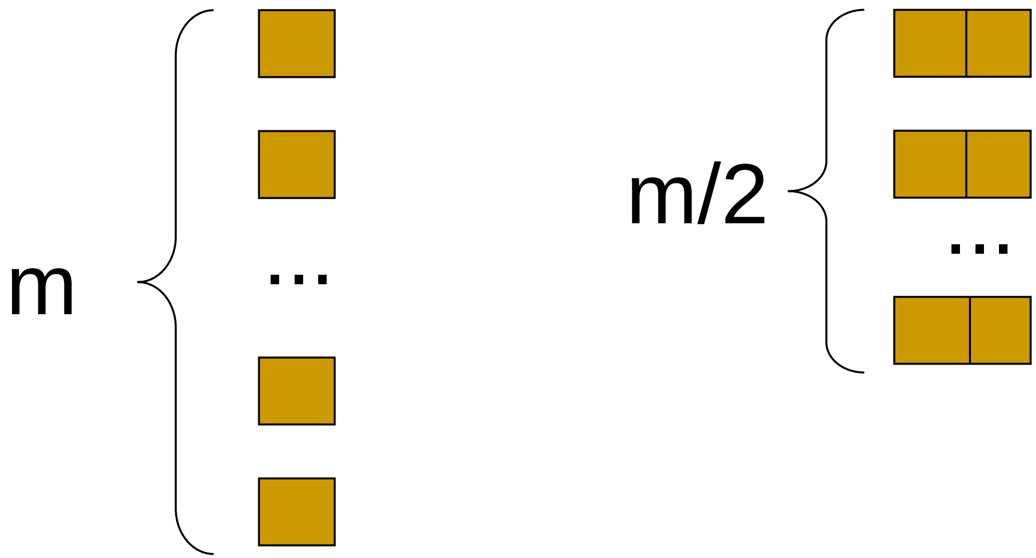
Many different rows.




$\Omega(\sqrt{m})$ queries to distinguish classically.

# Case 2

Many different rows.




[Aaronson, Shi, 2002] $\Omega(m^{1/3})$ queries to distinguish quantumly.

# Open problems

1. Improve the exponent 9 in $R_2(G)=O^*(Q_2^9(G))$.
2. Prove $R_2(G)=O(Q_2^c(G))$ for functions $G(x_1, \ldots, x_N)$ that are only symmetric w. r. t. permuting $x_1, \ldots, x_N$.

# Result 2

# Beals et al., FOCS'1998

- Theorem If $f(x_1, ..., x_N), x_1, ..., x_N \in \{0, 1\}$ is total, then

$$D(f)=O(Q_2^6(f)),$$

  D(f) – deterministic query complexity.

- Incomparable to our first result:
  - [Beals et al.]: total, possibly non-symmetric.

# Folk conjecture (late 1990s)

- Conjecture 1 If $f(x_1, \ldots, x_N), x_1, \ldots, x_N \in \{0, 1\}$ is total, then

$$D_\varepsilon(f)=O(Q_\varepsilon^c(f)),$$

$D_\varepsilon(f)$ and $Q_\varepsilon(f)$ – deterministic and quantum query complexities of computing f correctly on $\geq 1-\varepsilon$ fraction of inputs.

Our result: this follows from Conjecture 2.

# Quantum algorithms => Polynomials

- [Beals et al., 1998] An acceptance probability of a t-query quantum algorithm is a polynomial $p(x_1, ..., x_N)$ of degree 2t.

- [Dinur, et al., 2005] A $p(x_1, ..., x_N)$ of degree t can be $\varepsilon$-approximated by a junta of $2^{O(t/\varepsilon)}$ variables.

$$D_\varepsilon(f) = 2^{O(Q_\delta(f))}$$

# Conjecture 2

- Let $p(x_1, ..., x_N)$ be a polynomial of degree d with the following properties:
  - $0 \leq p(x_1, ..., x_N) \leq 1$;
  - p is $\varepsilon$-far from being a constant.

$$\mathop{E}_{X,Y} |p(X) - p(Y)| \geq \varepsilon$$

# Conjecture 2 (continued)

- Then f has an influential variable: there exists i:

$$\mathop{E}_{X} | p(X) - p(X^i) | \geq \left( \frac{\varepsilon}{d} \right)^{O(1)}$$

- $X^i$ – input X with $x_i$ changed to opposite value.

# Open problem

- Prove Conjecture 2.