Limitations of Quantum Walks and Randomized Algorithms

Jevgēnijs Vihrovs

Sc. Advisor: Dr. Comp. Sci., Prof. Andris Ambainis

Faculty of Computing, University of Latvia

6th September, 2019

Outline

Motivation: Computational Complexity

What is the power of

deterministic, probabilistic, quantum

models of computation?

Check $n \times n$ matrix multiplication $AB = C$:

- Deterministic: $O(n^{2.37})$ [LG14b].
- Randomized: $O(n^2)$ (Freivalds's algorithm) [Fre77].

Integer factorization:

- Randomized: sub-exponential time [LL93].
- Quantum: polynomial time (Shor's algorithm) [Sho97].

Goals: Quantum Walks

- Quantum walks generalize classical random walks.
- Applications in quantum query algorithms:
  - Element distinctness: determine if n numbers are distinct.

    $$O(n^{2/3}) \quad \text{[Amb04]}$$

  - Triangle finding: does a graph on n vertices contain a triangle?

    $$\widetilde{O}(n^{5/4}) \quad \text{[LG14a]}$$

  - Find a marked element in a 2-dimensional $\sqrt{n} \times \sqrt{n}$ grid:

    $$O(\sqrt{n \log n}) \quad \text{[ABN}^{+}\text{13]}$$

- What are the limits of quantum walk possibilities?

Goals: Query Complexity

- A clear mathematical model of computation.
- Applications:
  - Many standard algorithms also work in the query model:
    Binary Search, Sorting, etc.
  - A large variety of quantum query algorithms:
    Element Distinctness, Triangle Finding, Grover's Search, etc.
  - Lower bounds on the running time of the algorithms.

    $$\mathrm{D}(\textsc{Sorting}), \mathrm{R}(\textsc{Sorting}), \mathrm{Q}(\textsc{Sorting}) = \Omega(n \log n). \quad \text{[HNS02]}$$

  - Comparison of the power of computational models.

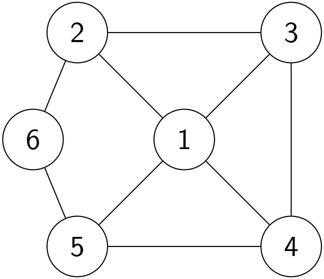
    $$\mathrm{D}(f) = O(\mathrm{R}(f)^3) \qquad \mathrm{D}(f) = O(\mathrm{Q}(f)^6) \qquad \mathrm{R}(f) = O(\mathrm{Q}(f)^6).$$

- What are the best lower bound methods?
  What are the limits of known lower bounds?
  What are the actual relationships between $\mathrm{D}(f), \mathrm{R}(f), \mathrm{Q}(f)$?

Outline

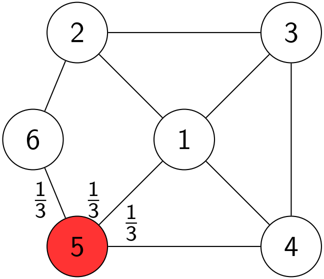
Classical Random Walks

- We walk on an N vertex graph G.



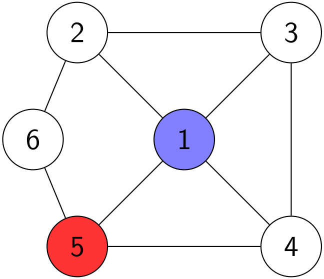
Classical Random Walks

- We walk on an N vertex graph G.



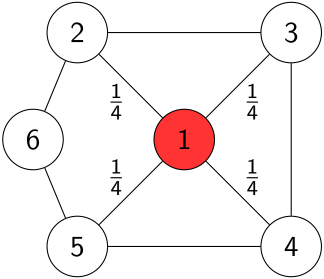
Classical Random Walks

- We walk on an N vertex graph G.



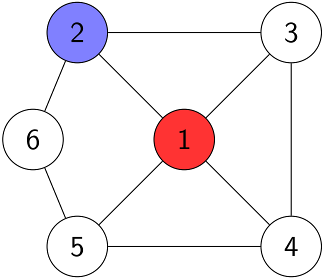
Classical Random Walks

- We walk on an N vertex graph G.



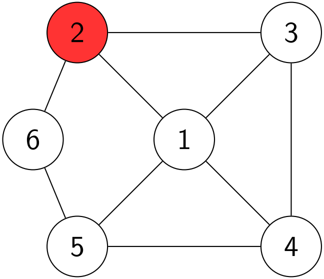
Classical Random Walks

- We walk on an N vertex graph G.



Classical Random Walks

- We walk on an N vertex graph G.



Classical Random Walks

- Applications of random walks:
  - Design of algorithms.
  - Motion of physical particles.
  - Gambling processes.
  - Economics.
  - Social network analysis.
  - ...
- Quantum walks:
  - Discrete-time / Continuous-time.
  - Design of even faster quantum algorithms.
  - Simulation of quantum physical processes.

Grover's Quantum Walk

- $G = (V, E)$ is a graph on N vertices.
- For each edge $\{u, v\}$, there are quantum states $|uv\rangle$ and $|vu\rangle$.
- The state of the quantum walk is

$$\sum_{u \to v} \alpha_{uv} |uv\rangle ,$$

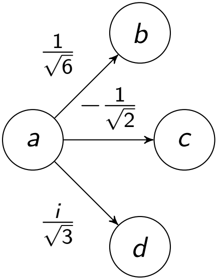
  where α_{uv} are complex amplitudes and $\sum_{u \to v} |\alpha_{uv}|^2 = 1$.
- Measurement: the probability of obtaining $|uv\rangle$ is $|\alpha_{uv}|^2$.

Grover's Quantum Walk

- $|\psi\rangle = \frac{1}{\sqrt{6}}|ab\rangle - \frac{1}{\sqrt{2}}|ac\rangle + \frac{i}{\sqrt{3}}|ad\rangle$.
- The walk is at:

$|ab\rangle$ with prob. $|1/\sqrt{6}|^2 = 1/6$;
$|ac\rangle$ with prob. $|-1/\sqrt{2}|^2 = 1/2$;
$|ad\rangle$ with prob. $|i/\sqrt{3}|^2 = 1/3$.

At vertex a with probability 1.



Grover's Quantum Walk

- $U = SC$ [AKR05].

- C – the "coin" operator. Disperses the amplitudes among the directions within a single vertex.

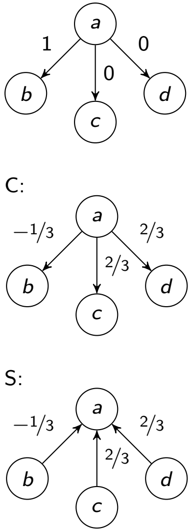
  As C we use Grover's diffusion:

$$C\,|uv\rangle = -\,|uv\rangle + \frac{2}{\deg(u)} \sum_{u \to w} |uw\rangle\,.$$

- S – the "shift" operator. Moves the amplitudes along the edges of the graph.

  As S we use the "flip-flop" shift:

$$S\,|uv\rangle = |vu\rangle\,.$$



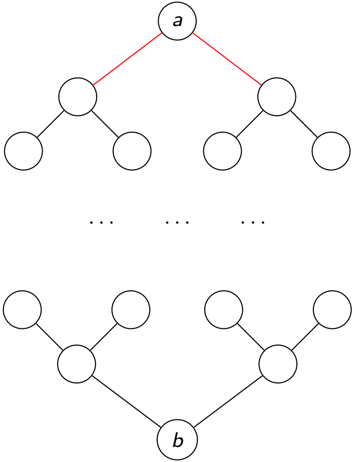
Grover's Quantum Walk

To reach b from a:

1. Prepare the starting state, the uniform superposition

$$|\psi_0\rangle = \frac{1}{\sqrt{\deg(a)}} \sum_{v \sim a} |av\rangle \, .$$

2. Apply T steps of U for some choice of T, $|\psi_T\rangle = U^T |\psi_0\rangle$.
3. Measure the state $|\psi_T\rangle$ and obtain some edge state $|uv\rangle$.
4. Check whether u is equal to b.



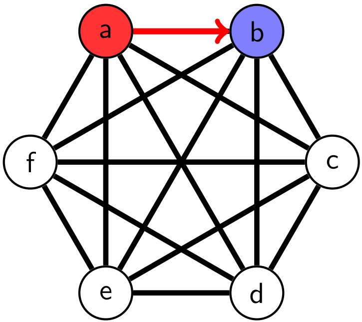
Classically: $\Theta(2^d)$.
Quantumly: $\Theta(d^2)$ [CFG02].

Oscillatory Localization

- Andris Ambainis, Krišjānis Prūsis, Jevgēnijs Vihrovs, and Thomas G. Wong.
  Oscillatory localization of quantum walks analyzed by classical electric circuits.
  Phys. Rev. A, 94:062324, 2016
- *Localization* – the walk remains close to the starting position $|\psi_0\rangle$ with high probability.
- A phenomenon unique to quantum walks.
- Potential applications:
  - Quantum algorithms.
  - Quantum optics.

Oscillatory Localization

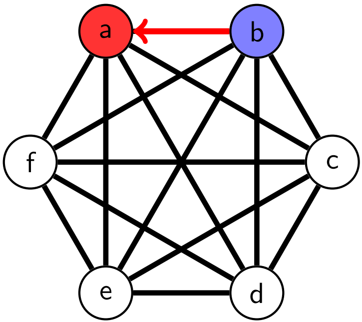
- The complete graph K_N.
- Starting in $|\psi_0\rangle = |ab\rangle$, it localizes.



$t = 0$

Oscillatory Localization

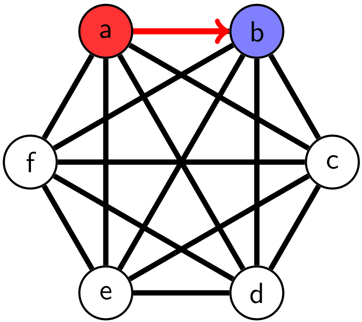
- The complete graph K_N.
- Starting in $|\psi_0\rangle = |ab\rangle$, it localizes.



$t = 1$

Oscillatory Localization

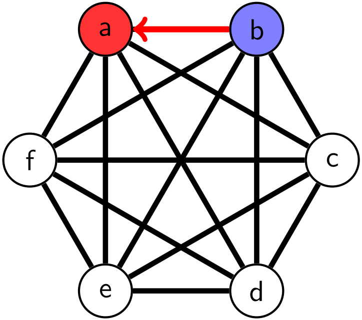
- The complete graph K_N.
- Starting in $|\psi_0\rangle = |ab\rangle$, it localizes.



$t = 2$

Oscillatory Localization

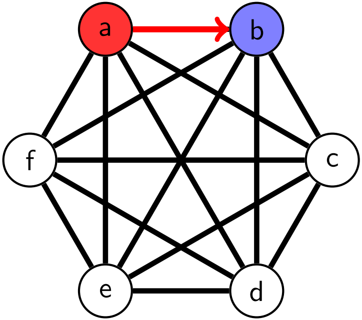
- The complete graph K_N.
- Starting in $|\psi_0\rangle = |ab\rangle$, it localizes.



$t = 3$

Oscillatory Localization

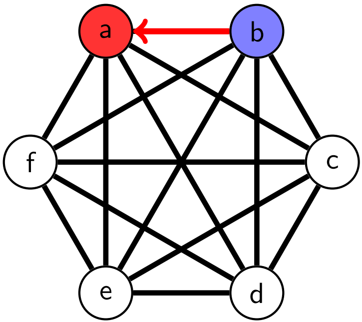
- The complete graph K_N.
- Starting in $|\psi_0\rangle = |ab\rangle$, it localizes.



$t = 4$

Oscillatory Localization

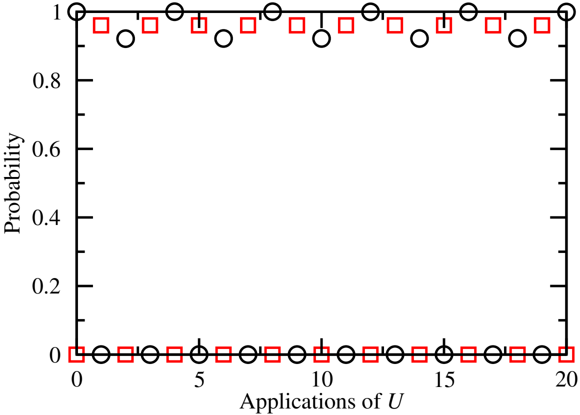
- The complete graph K_N.
- Starting in $|\psi_0\rangle = |ab\rangle$, it localizes.



$t = 5$

Oscillatory Localization

- Example for $N = 16$, black circles are probability at $|ab\rangle$, red squares are probability at $|ba\rangle$.



Oscillatory Localization

- In fact, we can look at the 1-eigenvectors $|\psi\rangle$ of U^2:

$$U^2 |\psi\rangle = |\psi\rangle .$$

- The walk oscillates locally if the starting state is close to these:

$$|\psi_0\rangle \approx |\psi\rangle .$$

- We give a complete description of such eigenvectors.

Oscillatory Localization

Theorem (informal)

- *There are only two types of such eigenvectors*

$$|\psi\rangle = \sum_{u \to v} \alpha_{uv} |uv\rangle .$$

- *The uniform state:*

$$\forall |uv\rangle : \qquad \alpha_{uv} = \frac{1}{\sqrt{2|E|}}.$$

- *Flip states:*

$$\forall u \in V : \qquad \sum_{u \to v} \alpha_{uv} = 0, \qquad \sum_{u \leftarrow v} \alpha_{vu} = 0.$$

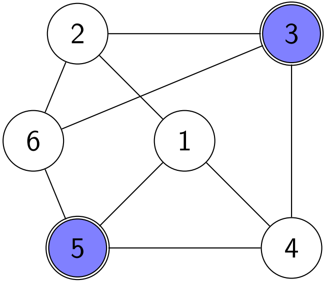
Oscillatory Localization

- We develop several criteria to determine if the walk will localize, given the starting state $|\psi_0\rangle$.
- If the specific electrical network constructed from G and $|\psi_0\rangle$ has low electrical resistance, then localization occurs.
- If the given graph G has high connectivity, then localization occurs.
- As a consequence, $|\psi_0\rangle = |ab\rangle$ localizes in various graphs:
  - d-dimensional grid.
  - Boolean hypercube.
  - Edge-transitive graphs.
  - ...

Outline

Quantum Search

- We walk on an N vertex graph, where some vertices are marked.



Quantum Search

- We start in a uniform superposition over all edges:

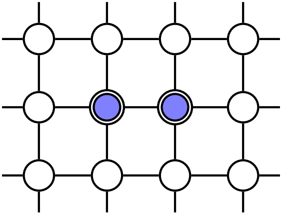
$$|\psi_0\rangle = \frac{1}{\sqrt{2|E|}} \sum_{u \in V} \sum_{u \to v} |uv\rangle .$$

- $U = SCQ$.

$$Q|uv\rangle = \begin{cases} |uv\rangle & u \text{ is not marked;} \\ -|uv\rangle & u \text{ is marked.} \end{cases}$$

Quantum Search

- Single marked element:
  Complete graph: $O(\sqrt{N})$ steps.
  $\sqrt{N} \times \sqrt{N}$ 2D periodic grid:
  $O(\sqrt{N \log N})$ steps [ABN+13].
- Does the same algorithm find any of $2, 3, \ldots, k$ marked elements as efficiently?
- Not always! [NR16] The quantum walk does not evolve.



Stationary States

- What are the configurations of marked vertices when the quantum walk does not evolve?
- In this case, we look at the 1-eigenvectors $|\psi\rangle$ of $U = SCQ$ (stationary states).
- The search remains stationary if the uniform starting state

$$|\psi_0\rangle = \frac{1}{\sqrt{2|E|}} \sum_{u \to v} |uv\rangle .$$

is close to some stationary state $|\psi\rangle \approx |\psi_0\rangle$.

Stationary States

- Krišjānis Prūsis, Jevgēnijs Vihrovs, and Thomas G. Wong. Stationary states in quantum walk search.

  Phys. Rev. A, 94:032334, 2016

- We completely characterize the stationary states:

Theorem

The stationary state $|\psi\rangle$ closest to the uniform starting state $|\psi_0\rangle$ satisfies:

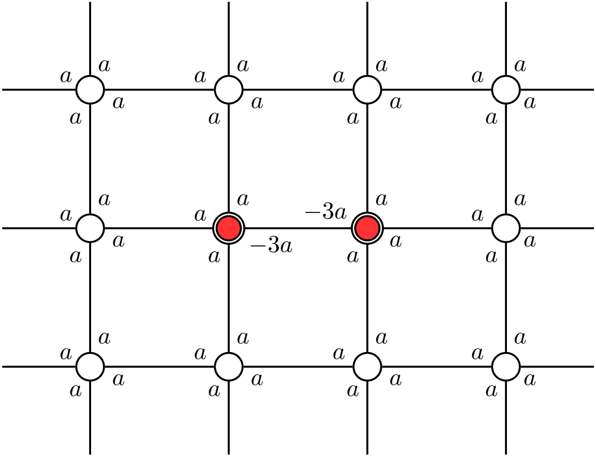
- *For every two adjacent u, v: $\alpha_{uv} = \alpha_{vu}$.*
- *If u is marked,*

$$\sum_{u \to v} \alpha_{uv} = 0.$$

- *If u is not marked,*

α_{uv} is the same for all neighbours v of u.

Stationary States



Stationary States

- The description of such states has been given earlier [NR16]. The previous theorem shows that they are optimal.

- We also describe necessary and sufficient conditions on the existence of stationary states if the marked vertex form a connected component M:

Theorem

- *A stationary state always exists if M is non-bipartite.*
- *If M is bipartite, then a stationary state exists iff the total degrees of both partite sets are equal.*

Outline

Query Model

- An algorithm has to compute $f : S \to H$, where $S \subseteq G^n$, given an input $x \in S$.

- The input $x = (x_1, x_2, \ldots, x_n)$ is a black box: with a single *query* we can obtain the value of one x_i.

- The cost of the computation is the number of queries made when the algorithm returns an output.

Query Model

- The query complexity of f is the minimal worst-case cost of an algorithm computing f.
- Deterministic: $\mathrm{D}(f)$, decision tree complexity.
- Randomized: $\mathrm{R}(f)$, randomness is allowed, the algorithm should be correct on any input with probability at least $2/3$.
- Quantum: $\mathrm{Q}(f)$, the queries are made in superposition, correct with probability $2/3$.

Query Model

- Example: ordered search.
- Input: $\underbrace{0\ldots0}_{\ell}\underbrace{1\ldots1}_{n-\ell}$. The goal: find ℓ.

0	0	0	1	1	1	1	1	1	1

- $\mathrm{D}(\textsc{Ordered Search}) = O(\log n)$.
- Can we do better? Randomly? Quantumly?

Outline

Adversary Bounds

- Quantum adversary lower bound $\mathrm{Adv}(f)$: for all f,

$$Q(f) = \Omega(\mathrm{Adv}(f)). \quad \text{[Amb00]}$$

- Let $f : S \to H$ be any function, where $S \subseteq G^n$. Let $R : S \times S \to \mathbb{R}_{\geq 0}$ be a real-valued function such that $R(x, y) = R(y, x)$ for all $x, y \in S$ and $R(x, y) = 0$ whenever $f(x) = f(y)$. Then for $x \in S$ and an index i, let

$$\theta(x, i) = \frac{\sum_{y \in S} R(x, y)}{\sum_{y \in S : x_i \neq y_i} R(x, y)},$$

  Define

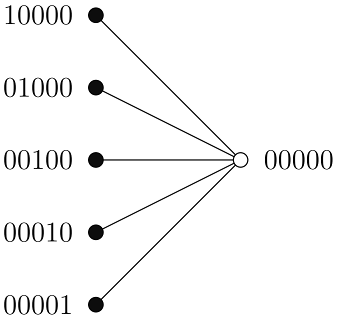
$$\mathrm{Adv}(f) = \max_{R} \min_{\substack{x, y \in S, i \in [n]: \\ R(x,y) > 0, x_i \neq y_i}} \sqrt{\theta(x, i)\theta(y, i)}.$$

- $\mathrm{Adv}(\textsc{Ordered Search}) = \Theta(\log n)$. [LM04].

Adversary Bounds

$$\mathrm{Adv}(f) = \max_R \min_{\substack{x,y \in S, i \in [n]: \\ R(x,y)>0, x_i \neq y_i}} \sqrt{\theta(x,i)\theta(y,i)}.$$

- $\textsc{Or}(x_1, \ldots, x_n)$.
- $R(x,y) = 1$ if $|x| = 1$ and $y = 0^n$.
- If $x_i = 1$, then $\theta(x,i) = 1/1$.
- For all i, $\theta(0^n, i) = n/1$.
- $\mathrm{Adv}(\textsc{Or}) = \sqrt{\theta(x,i)\theta(0^n,i)} = \sqrt{n}$.



Adversary Bounds

- Very powerful lower bound (OR, ORDERED SEARCH, SORTING, AND-OR, GRAPH CONNECTIVITY, etc.).
- Various quantum adversary bounds:
  - Weighted adversary bound.
  - Spectral adversary bound.
  - Kolmogorov adversary bound.
  - Minimax adversary bound.
- Špalek and Szegedy showed that all above are equivalent! [ŠS06].

Adversary Bounds

- Classical (randomized) adversary bound:

$$\mathrm{R}(f) = \Omega(\mathrm{CRA}(f)) \quad [\text{Aar06}].$$

- Define

$$\mathrm{CRA}(f) = \max_{R} \min_{\substack{x,y \in S, i \in [n]: \\ R(x,y) > 0, x_i \neq y_i}} \max\{\theta(x,i), \theta(y,i)\}.$$

- For $\textsc{Or}$,

$$\mathrm{CRA}(\textsc{Or}) = \max\{1, n\} = n.$$

Adversary Bounds

Applications:

- Given a permutation $\pi(1), \ldots, \pi(n)$, check if $\pi^{-1}(1) \leq n/2$.

$$\mathsf{CRA}(\textsc{Permutation Inversion}) = \Omega(n).$$

- Given query access to $F : \{0,1\}^n \to \mathbb{N}$, find x such that $F(x) \leq F(x^i)$ for all $i \in [n]$.

$$\mathsf{CRA}(\textsc{Local Search}) = \Omega(2^{n/2}\sqrt{n}).$$

Adversary Bounds

Other randomized lower bounds:

- Kolmogorov adversary bound $\mathrm{CKA}(f)$.
- Minimax adversary bound $\mathrm{CMM}(f)$.
- Fractional block sensitivity $\mathrm{fbs}(f)$.

Are they also equivalent as the quantum adversary bounds?

Adversary Bounds

- Main result: all are equivalent for total functions f!

Theorem

For any f,

$$\mathrm{fbs}(f) \leq \mathrm{CRA}(f) \leq \mathrm{CKA}(f) = \Theta(\mathrm{CMM}(f)).$$

If f is total, then

$$\mathrm{CMM}(f) \leq \mathrm{fbs}(f).$$

- Andris Ambainis, Martins Kokainis, Krišjānis Prūsis, and Jevgēnijs Vihrovs. All Classical Adversary Methods are Equivalent for Total Functions. In *35th Symposium on Theoretical Aspects of Computer Science (STACS 2018)*, volume 96 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 8:1–8:14, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik

Adversary Bounds

- We also introduce rank-1 adversary bound $\mathrm{CRA}_1(f)$.
- Additional requirement: there must exist $u, v : S \to \mathbb{R}_{\geq 0}$ such that $R(x, y) = u(x)v(y)$ for all $x, y \in S$.
- In general,

$$\mathrm{fbs}(f) \leq \mathrm{CRA}_1(f) \leq \mathrm{CRA}(f).$$

- For total functions,

$$\mathrm{CRA}_1(f) = \mathrm{CRA}(f).$$

- $\mathrm{CRA}_1(f)$ has a simpler formulation.

Adversary Bounds

- For partial functions, the adversary bounds can give different estimates.
- Inputs have a single 1: 000000100.
  $\textsc{Gth}(f) = 1$ iff $x_i = 1$ for $i > n/2$. Then

$$\mathrm{fbs}(\textsc{Gth}) = O(1), \quad \mathrm{CMM}(\textsc{Gth}), \mathrm{CRA}(\textsc{Gth}) = \Omega(n).$$

- Binary sorted inputs: 000111111.
  $\textsc{Osp}(f) = 1$ iff $x_{i-1} = 0$ and $x_i = 1$ for even i. Then

$$\mathrm{CRA}(\textsc{Osp}) = O(1), \quad \mathrm{CMM}(\textsc{Osp}) = \Omega(\log n).$$

Outline

Conclusion

- *Oscillatory Localization*:
    - Developed a mathematical characterization of localization.
    - Provided the tools to estimate the amount of localization.
- *Stationary States*:
    - Developed a mathematical characterization of stationary states.
    - Provided the conditions on the existence of the stationary states.
- *Open question*: Algorithmic applications using stationary states? In fact, localization has been used to give quantum algorithms for electrical network analysis [Wan17].

Conclusion

- *Adversary Bounds*:
    - Proved the equivalence between the classical adversary bounds for total functions.
    - Showed separation examples for partial functions.
- *Block Sensitivity*:
    - Showed optimal separation between block sensitivity and fractional block sensitivity for partial functions.
- *Open questions*:
    - Relationship between classical and quantum adversary bounds?
    - Optimal separation between $\text{bs}(f)$ and $\text{fbs}(f)$ for total functions?

Thanks to my co-authors

Andris Ambainis,
Krišjānis Prūsis,
Thomas Wong,
Mārtiņš Kokainis.

Questions?

Scott Aaronson.
Lower bounds for local search by quantum arguments.
SIAM Journal on Computing, 35(4):804–824, 2006.

Andris Ambainis, Artūrs Bačkurs, Nikolajs Nahimovs, Raitis Ozols, and Alexander Rivosh.
Search by quantum walks on two-dimensional grid without amplitude amplification.
In *Theory of Quantum Computation, Communication, and Cryptography*, pages 87–97, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

Andris Ambainis, Martins Kokainis, Krišjānis Prūsis, and Jevgēnijs Vihrovs.
All Classical Adversary Methods are Equivalent for Total Functions.
In *35th Symposium on Theoretical Aspects of Computer Science (STACS 2018)*, volume 96 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 8:1–8:14, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

Andris Ambainis, Julia Kempe, and Alexander Rivosh.
Coins make quantum walks faster.
In *Proceedings of the 16th Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '05, pages 1099–1108, Philadelphia, PA, USA, 2005. SIAM.

Andris Ambainis.
Quantum lower bounds by quantum arguments.
In *Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing*, STOC'00, pages 636–643, New York, NY, USA, 2000. ACM.