Sequential measurements, disturbance and property testing

Aram Harrow[1], Cedric Yen-Yu Lin[2] & Ashley Montanaro[3]

[1] Center for Theoretical Physics, MIT
[2] Joint Center for Quantum Information and Computer Science, U of Maryland
[3] School of Mathematics, University of Bristol

18 February 2017


I KNEW WHO I WAS
THIS MORNING
BUT I'VE CHANGED
A FEW TIMES
SINCE THEN

Introduction

In this talk I will describe an algorithm that solves the following problem.

Problem

Given a quantum state and a sequence of accept/reject measurements such that either:

Introduction

In this talk I will describe an algorithm that solves the following problem.

Problem

Given a quantum state and a sequence of accept/reject measurements such that either:

1. At least one of the measurements accepts the state with high probability;

Introduction

In this talk I will describe an algorithm that solves the following problem.

Problem

Given a quantum state and a sequence of accept/reject measurements such that either:

1. At least one of the measurements accepts the state with high probability;
2. All of the measurements accept with low probability,

determine which is the case.

Introduction

In this talk I will describe an algorithm that solves the following problem.

Problem

Given a quantum state and a sequence of accept/reject measurements such that either:

1. At least one of the measurements accepts the state with high probability;
2. All of the measurements accept with low probability,

determine which is the case.

I will then discuss applications to property testing, and in particular an exponential reduction in quantum query complexity for testing isomorphism under group actions.

Quantum mechanics in a nutshell

For the purposes of this talk:

- A state ψ of a quantum system is a unit vector.

Quantum mechanics in a nutshell

For the purposes of this talk:

- A state ψ of a quantum system is a unit vector.
- A two-outcome measurement M is a pair $\{P, I - P\}$ where P is a projector onto a subspace.

Quantum mechanics in a nutshell

For the purposes of this talk:

- A state ψ of a quantum system is a unit vector.
- A two-outcome measurement M is a pair $\{P, I - P\}$ where P is a projector onto a subspace.
- M accepts with probability $\|P\psi\|^2$ and otherwise rejects.

Quantum mechanics in a nutshell

For the purposes of this talk:

- A state ψ of a quantum system is a unit vector.
- A two-outcome measurement M is a pair $\{P, I-P\}$ where P is a projector onto a subspace.
- M accepts with probability $\|P\psi\|^2$ and otherwise rejects.
- If M accepts (resp. rejects), the new state of the system is

$$\frac{P\psi}{\|P\psi\|}, \quad \text{resp.} \quad \frac{(I-P)\psi}{\|(I-P)\psi\|}.$$

The problem

Restating the previous problem mathematically:

Problem

We have a quantum state ψ and a sequence of measurements $M_1, \ldots, M_n$, corresponding to projectors $P_1, \ldots, P_n$.

The problem

Restating the previous problem mathematically:

Problem

We have a quantum state ψ and a sequence of measurements $M_1, \ldots, M_n$, corresponding to projectors $P_1, \ldots, P_n$.
We are promised that either:

1. There exists i such that $\|P_i\psi\|^2 = \Omega(1)$ ("yes" case);

The problem

Restating the previous problem mathematically:

Problem

We have a quantum state ψ and a sequence of measurements $M_1, \ldots, M_n$, corresponding to projectors $P_1, \ldots, P_n$.
We are promised that either:

1. There exists i such that $\|P_i \psi\|^2 = \Omega(1)$ ("yes" case);
2. For all i, $\|P_i \psi\|^2 = o(1/n)$ ("no" case).

The problem

Restating the previous problem mathematically:

Problem

We have a quantum state ψ and a sequence of measurements $M_1, \ldots, M_n$, corresponding to projectors $P_1, \ldots, P_n$.
We are promised that either:

1. There exists i such that $\|P_i\psi\|^2 = \Omega(1)$ ("yes" case);
2. For all i, $\|P_i\psi\|^2 = o(1/n)$ ("no" case).

Our task is to determine which is the case.

The problem

Restating the previous problem mathematically:

Problem

We have a quantum state ψ and a sequence of measurements $M_1, \ldots, M_n$, corresponding to projectors $P_1, \ldots, P_n$.
We are promised that either:

1. There exists i such that $\|P_i \psi\|^2 = \Omega(1)$ ("yes" case);
2. For all i, $\|P_i \psi\|^2 = o(1/n)$ ("no" case).

Our task is to determine which is the case.

This problem can be seen as a quantum version of computing the OR of the measurement outcomes.

The problem

Restating the previous problem mathematically:

Problem

We have a quantum state ψ and a sequence of measurements $M_1, \ldots, M_n$, corresponding to projectors $P_1, \ldots, P_n$.
We are promised that either:

1. There exists i such that $\|P_i\psi\|^2 = \Omega(1)$ ("yes" case);
2. For all i, $\|P_i\psi\|^2 = o(1/n)$ ("no" case).

Our task is to determine which is the case.

This problem can be seen as a quantum version of computing the OR of the measurement outcomes.

Obvious "solution": Try M_1, then M_2, then $\ldots$, then M_n.

The quantum anti-Zeno effect

- Set
$$\psi_k = \left(\cos\left(\frac{\pi k}{2n}\right), \sin\left(\frac{\pi k}{2n}\right)\right)^T$$
and set $M_k = \{I - \psi_k \psi_k^\perp, \psi_k \psi_k^\perp\}$ (first outcome: acceptance, second outcome: rejection).

The quantum anti-Zeno effect

- Set
$$\psi_k = \left(\cos\left(\frac{\pi k}{2n}\right), \sin\left(\frac{\pi k}{2n}\right)\right)^T$$
and set $M_k = \{I - \psi_k\psi_k^{\perp}, \psi_k\psi_k^{\perp}\}$ (first outcome: acceptance, second outcome: rejection).
- If we have ψ_k and apply the measurement M_{k+1}, the probability of rejection is precisely
$$\left(\cos\left(\frac{\pi}{2n}\right)\right)^2 = 1 - O(1/n^2)$$
and the residual state following rejection is ψ_{k+1}.

The quantum anti-Zeno effect

- Set
$$\psi_k = \left(\cos\left(\frac{\pi k}{2n}\right), \sin\left(\frac{\pi k}{2n}\right)\right)^T$$
and set $M_k = \{I - \psi_k \psi_k^\perp, \psi_k \psi_k^\perp\}$ (first outcome: acceptance, second outcome: rejection).
- If we have ψ_k and apply the measurement M_{k+1}, the probability of rejection is precisely
$$\left(\cos\left(\frac{\pi}{2n}\right)\right)^2 = 1 - O(1/n^2)$$
and the residual state following rejection is ψ_{k+1}.
- So if we perform $M_1, \ldots, M_n$ on initial state $\binom{1}{0} = \psi_0$, then Pr[ever accept] $= O(1/n)$.

The quantum anti-Zeno effect

- Set
$$\psi_k = \left(\cos\left(\frac{\pi k}{2n}\right), \sin\left(\frac{\pi k}{2n}\right)\right)^T$$
and set $M_k = \{I - \psi_k \psi_k^\perp, \psi_k \psi_k^\perp\}$ (first outcome: acceptance, second outcome: rejection).
- If we have ψ_k and apply the measurement M_{k+1}, the probability of rejection is precisely
$$\left(\cos\left(\frac{\pi}{2n}\right)\right)^2 = 1 - O(1/n^2)$$
and the residual state following rejection is ψ_{k+1}.
- So if we perform $M_1, \ldots, M_n$ on initial state $\binom{1}{0} = \psi_0$, then $\Pr[\text{ever accept}] = O(1/n)$.
- But if the final measurement M_n were performed on $\binom{1}{0}$, it would accept with certainty.

Combating the quantum anti-Zeno effect

We give two procedures with similar parameters that combat this effect and solve the above problem:

- One procedure is based on Marriott-Watrous gap amplification and has better constants and a more elegant correctness proof.
- The other procedure has more direct intuition and is easier to describe in a talk…

Combating the quantum anti-Zeno effect

We give two procedures with similar parameters that combat this effect and solve the above problem:

- One procedure is based on Marriott-Watrous gap amplification and has better constants and a more elegant correctness proof.
- The other procedure has more direct intuition and is easier to describe in a talk…

The intuition behind the second procedure:

- Testing measurements in order doesn't work if the final state is far away from the initial state.

Combating the quantum anti-Zeno effect

We give two procedures with similar parameters that combat this effect and solve the above problem:

- One procedure is based on Marriott-Watrous gap amplification and has better constants and a more elegant correctness proof.
- The other procedure has more direct intuition and is easier to describe in a talk…

The intuition behind the second procedure:

- Testing measurements in order doesn't work if the final state is far away from the initial state.
- So why not just test for this disturbance?

A quantum OR bound by testing disturbance

Algorithm (informal)

Repeat the following $O(n)$ times:

A quantum OR bound by testing disturbance

Algorithm (informal)

Repeat the following $O(n)$ times:

1. With probability $O(1/n)$, do a disturbance test on the current state and return the result.

A quantum OR bound by testing disturbance

Algorithm (informal)

Repeat the following $O(n)$ times:

1. With probability $O(1/n)$, do a disturbance test on the current state and return the result.
2. Pick k at random and perform measurement M_k. Accept if the measurement accepts.

A quantum OR bound by testing disturbance

Algorithm (informal)

Repeat the following $O(n)$ times:

1. With probability $O(1/n)$, do a disturbance test on the current state and return the result.
2. Pick k at random and perform measurement M_k. Accept if the measurement accepts.

Reject.

A quantum OR bound by testing disturbance

Algorithm (informal)

Repeat the following $O(n)$ times:

1. With probability $O(1/n)$, do a disturbance test on the current state and return the result.
2. Pick k at random and perform measurement M_k. Accept if the measurement accepts.

Reject.

The disturbance test accepts whp if the current state is far from the initial state, and rejects whp if it is close to the initial state.

A quantum OR bound by testing disturbance

Algorithm (informal)

Repeat the following $O(n)$ times:

1. With probability $O(1/n)$, do a disturbance test on the current state and return the result.
2. Pick k at random and perform measurement M_k. Accept if the measurement accepts.

Reject.

The disturbance test accepts whp if the current state is far from the initial state, and rejects whp if it is close to the initial state.

Proof intuition: In a "yes" case, if the current state is close to the initial state, the test in step 2 will accept whp.

A quantum OR bound by testing disturbance

Algorithm (informal)

Repeat the following $O(n)$ times:

1. With probability $O(1/n)$, do a disturbance test on the current state and return the result.
2. Pick k at random and perform measurement M_k. Accept if the measurement accepts.

Reject.

The disturbance test accepts whp if the current state is far from the initial state, and rejects whp if it is close to the initial state.

Proof intuition: In a "yes" case, if the current state is close to the initial state, the test in step 2 will accept whp. Otherwise, the test in step 1 will accept whp.

A quantum OR bound by testing disturbance

Algorithm (informal)

Repeat the following $O(n)$ times:

1. With probability $O(1/n)$, do a disturbance test on the current state and return the result.
2. Pick k at random and perform measurement M_k. Accept if the measurement accepts.

Reject.

The disturbance test accepts whp if the current state is far from the initial state, and rejects whp if it is close to the initial state.

Proof intuition: In a "yes" case, if the current state is close to the initial state, the test in step 2 will accept whp. Otherwise, the test in step 1 will accept whp. So in either case we accept with prob. $\Omega(1/n)$ in each iteration.

Application to property testing

We can apply this test to the problem of testing isomorphism of functions under a group action [Babai & Chakraborty '10].

Application to property testing

We can apply this test to the problem of testing isomorphism of functions under a group action [Babai & Chakraborty '10].

- Let G be a permutation group acting on a finite set X.

Application to property testing

We can apply this test to the problem of testing isomorphism of functions under a group action [Babai & Chakraborty '10].

- Let G be a permutation group acting on a finite set X.
- $f, g : X \to Y$ are isomorphic if there exists $\sigma \in G$ such that

$$g(x) = f(\sigma(x)) \quad \text{for all } \; x \in X.$$

Application to property testing

We can apply this test to the problem of testing isomorphism of functions under a group action [Babai & Chakraborty '10].

- Let G be a permutation group acting on a finite set X.
- $f, g : X \to Y$ are isomorphic if there exists $\sigma \in G$ such that

$$g(x) = f(\sigma(x)) \quad \text{for all } x \in X.$$

- f and g are ϵ-far from isomorphic if, for all $\sigma \in G$,

$$|\{x \in X : g(x) \neq f(\sigma(x))\}| \geqslant \epsilon |X|.$$

Application to property testing

We can apply this test to the problem of testing isomorphism of functions under a group action [Babai & Chakraborty '10].

- Let G be a permutation group acting on a finite set X.
- $f, g : X \to Y$ are isomorphic if there exists $\sigma \in G$ such that

$$g(x) = f(\sigma(x)) \quad \text{for all } \; x \in X.$$

- f and g are ϵ-far from isomorphic if, for all $\sigma \in G$,

$$|\{x \in X : g(x) \neq f(\sigma(x))\}| \geqslant \epsilon |X|.$$

- An algorithm is an ϵ-tester for G-isomorphism if it distinguishes between these two cases with success probability at least $2/3$.

Application to property testing

We can apply this test to the problem of testing isomorphism of functions under a group action [Babai & Chakraborty '10].

- Let G be a permutation group acting on a finite set X.
- $f, g : X \to Y$ are isomorphic if there exists $\sigma \in G$ such that

$$g(x) = f(\sigma(x)) \quad \text{for all } \; x \in X.$$

- f and g are ϵ-far from isomorphic if, for all $\sigma \in G$,

$$|\{x \in X : g(x) \neq f(\sigma(x))\}| \geqslant \epsilon |X|.$$

- An algorithm is an ϵ-tester for G-isomorphism if it distinguishes between these two cases with success probability at least 2/3.

Theorem

For any set of permutations G, there is a quantum ϵ-tester for G-isomorphism which makes $O((\log |G|)/\epsilon)$ queries.

Consequences

Assume $\epsilon = \Omega(1)$. Then we have the following query complexity bounds:

Problem	G	X	Classical	Quantum
Boolean function iso.	S_n	$\{0,1\}^n$	$\widetilde{\Omega}(2^{n/2})$[1]	$\widetilde{O}(n)$
Boolean fn linear iso.	$GL_n(\mathbb{F}_2)$	$\{0,1\}^n$	$\Omega(2^{n/2})$	$O(n^2)$
Graph isomorphism	S_n	$[n] \times [n]$	$\widetilde{O}(n^{5/4})$[2]	$\widetilde{O}(n)$
Hidden subgroup	G	G	$\Omega(\sqrt{\lvert G \rvert})$[3]	$O(\log \lvert G \rvert)$

[1] [Alon et al. '13] [2] [Fischer and Matsliah '08] [3] [Friedl et al. '09]

Consequences

Assume $\epsilon = \Omega(1)$. Then we have the following query complexity bounds:

Problem	G	X	Classical	Quantum
Boolean function iso.	S_n	$\{0,1\}^n$	$\widetilde{\Omega}(2^{n/2})$ [1]	$\widetilde{O}(n)$
Boolean fn linear iso.	$GL_n(\mathbb{F}_2)$	$\{0,1\}^n$	$\Omega(2^{n/2})$	$O(n^2)$
Graph isomorphism	S_n	$[n] \times [n]$	$\widetilde{O}(n^{5/4})$ [2]	$\widetilde{O}(n)$
Hidden subgroup	G	G	$\Omega(\sqrt{\lvert G \rvert})$ [3]	$O(\log \lvert G \rvert)$

[1] [Alon et al. '13] [2] [Fischer and Matsliah '08] [3] [Friedl et al. '09]

- An $\widetilde{O}(n^{7/6})$-query quantum algorithm was previously given by [Chakraborty et al. '10].

Consequences

Assume $\epsilon = \Omega(1)$. Then we have the following query complexity bounds:

Problem	G	X	Classical	Quantum
Boolean function iso.	S_n	$\{0,1\}^n$	$\widetilde{\Omega}(2^{n/2})$[1]	$\widetilde{O}(n)$
Boolean fn linear iso.	$GL_n(\mathbb{F}_2)$	$\{0,1\}^n$	$\Omega(2^{n/2})$	$O(n^2)$
Graph isomorphism	S_n	$[n] \times [n]$	$\widetilde{O}(n^{5/4})$[2]	$\widetilde{O}(n)$
Hidden subgroup	G	G	$\Omega(\sqrt{\lvert G\rvert})$[3]	$O(\log \lvert G\rvert)$

[1] [Alon et al. '13] [2] [Fischer and Matsliah '08] [3] [Friedl et al. '09]

- An $\widetilde{O}(n^{7/6})$-query quantum algorithm was previously given by [Chakraborty et al. '10].
- Note that the quantum algorithms achieving the complexities above are not time-efficient.

Connecting the OR bound to property testing

How can our algorithm be used for testing isomorphism under group actions?

Connecting the OR bound to property testing

How can our algorithm be used for testing isomorphism under group actions?

- With one query to f and g, we can construct a quantum state ψ corresponding to querying f and g on all inputs in superposition.

Connecting the OR bound to property testing

How can our algorithm be used for testing isomorphism under group actions?

- With one query to f and g, we can construct a quantum state ψ corresponding to querying f and g on all inputs in superposition.
- We can also write down a measurement M_h, for $h \in G$, which tests ψ for isomorphism under h with bounded error.

Connecting the OR bound to property testing

How can our algorithm be used for testing isomorphism under group actions?

- With one query to f and g, we can construct a quantum state ψ corresponding to querying f and g on all inputs in superposition.
- We can also write down a measurement M_h, for $h \in G$, which tests ψ for isomorphism under h with bounded error.
- Taking the AND over k copies of ψ reduces the failure prob. of M_h to $O(2^{-k})$.

Connecting the OR bound to property testing

How can our algorithm be used for testing isomorphism under group actions?

- With one query to f and g, we can construct a quantum state ψ corresponding to querying f and g on all inputs in superposition.
- We can also write down a measurement M_h, for $h \in G$, which tests ψ for isomorphism under h with bounded error.
- Taking the AND over k copies of ψ reduces the failure prob. of M_h to $O(2^{-k})$.

So we can apply the quantum algorithm to $k = O(\log |G|)$ copies of ψ and the sequence of measurements $\{M_h\}$.

Other consequences

We obtain some other consequences too, e.g.:

Other consequences

We obtain some other consequences too, e.g.:

- Efficient testing of properties of quantum states. If $\mathcal{P}$ is a finite subset of the unit sphere, there is a quantum ϵ-tester for membership in $\mathcal{P}$ using $O((\log|\mathcal{P}|)/\epsilon^2)$ copies of the input state.

Other consequences

We obtain some other consequences too, e.g.:

- Efficient testing of properties of quantum states. If $\mathcal{P}$ is a finite subset of the unit sphere, there is a quantum ϵ-tester for membership in $\mathcal{P}$ using $O((\log|\mathcal{P}|)/\epsilon^2)$ copies of the input state.
- Testing genuine multipartite entanglement of a state of n systems using $O(n/\epsilon^2)$ copies of the state.

Other consequences

We obtain some other consequences too, e.g.:

- Efficient testing of properties of quantum states. If $\mathcal{P}$ is a finite subset of the unit sphere, there is a quantum ϵ-tester for membership in $\mathcal{P}$ using $O((\log|\mathcal{P}|)/\epsilon^2)$ copies of the input state.
- Testing genuine multipartite entanglement of a state of n systems using $O(n/\epsilon^2)$ copies of the state.
- De-Merlinizing quantum communication protocols, correcting a claimed result of [Aaronson '06].

Summary and further reading

- Given a quantum state and a sequence of measurements, we can test whether one of them accepts whp.
- This has applications to property testing, including exponential reductions in quantum query complexity.

Summary and further reading

- Given a quantum state and a sequence of measurements, we can test whether one of them accepts whp.
- This has applications to property testing, including exponential reductions in quantum query complexity.

Open questions:

- Can we find time-efficient quantum algorithms for these property testing problems?

Summary and further reading

- Given a quantum state and a sequence of measurements, we can test whether one of them accepts whp.
- This has applications to property testing, including exponential reductions in quantum query complexity.

Open questions:

- Can we find time-efficient quantum algorithms for these property testing problems?
- Are there other applications of the quantum OR bound?

Quantum algorithms: an overview, AM, *npj Quantum Information* 2, 2016
www.nature.com/articles/npjqi201523