sequential measurements, disturbance, and property testing

Aram Harrow (MIT)
Cedric Lin (Maryland)
Ashley Montanaro (Bristol)

arXiv:1607.03236

QIP 2017

noncommutative probability

union bound: [Gao '14]
measure P_1, ... P_N sequentially.
Pr[any accept] ≤ 4 Σ_i tr[P_i ρ]

also:
Markov's inequality
entropy / compression
relative entropy / hypothesis testing
channel capacities
Lovasz Local Lemma

but what about .... OR?

quantum OR?

given:

measurement operators: $0 \leq A_1, \ldots, A_N \leq I$

goal:

$A_\vee$ "=" $A_1 \vee \ldots \vee A_N$ s.t.
$A_\vee$ accepts iff any A_i accepts

main result

"yes" $\max_i \mathrm{tr}[A_i \rho] \geq 1-\varepsilon \Rightarrow \mathrm{tr}[A_V \rho] \geq (1-\varepsilon)^2 / 4$

"no" $\Sigma_i \mathrm{tr}[A_i \rho] \leq \delta \Rightarrow \mathrm{tr}[A_V \rho] \leq 2\delta$

Constructive, but computational cost is O(N).

Is this tight?

"yes" $\max_i \mathrm{tr}[A_i \rho] \geq 1-\varepsilon$ ➡ $\mathrm{tr}[A_\vee \rho] \geq (1-\varepsilon)^2 / 4$

"no" $\max_i \mathrm{tr}[A_i \rho] \leq \delta$ ➡ $\mathrm{tr}[A_\vee \rho] \leq 2N\delta$

Is the N optimal?

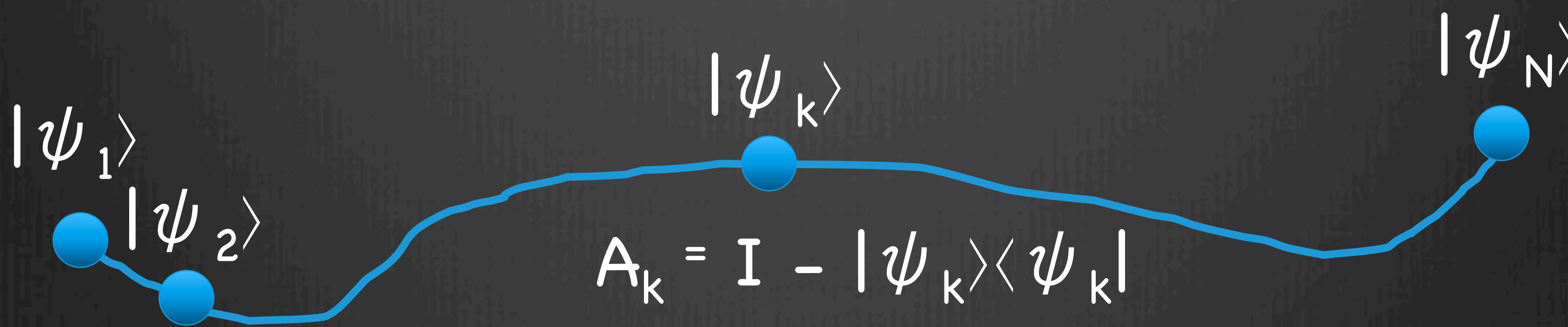
Take $A_i = |i\rangle\langle i|$
"yes": $\rho = |i\rangle\langle i|$ for unknown i
"no": $\rho = I/N$

➡ cannot distinguish

ideas that don't work

1. consecutive measurement

problem: quantum Zeno effect



$A_1 = I - |\psi_1\rangle\langle\psi_1|$

All measurements reject but state changes.

ideas that don't work

2. semidefinite programming

min tr A_V

$A_V \geq A_i$ for all i.

problem: too rigid

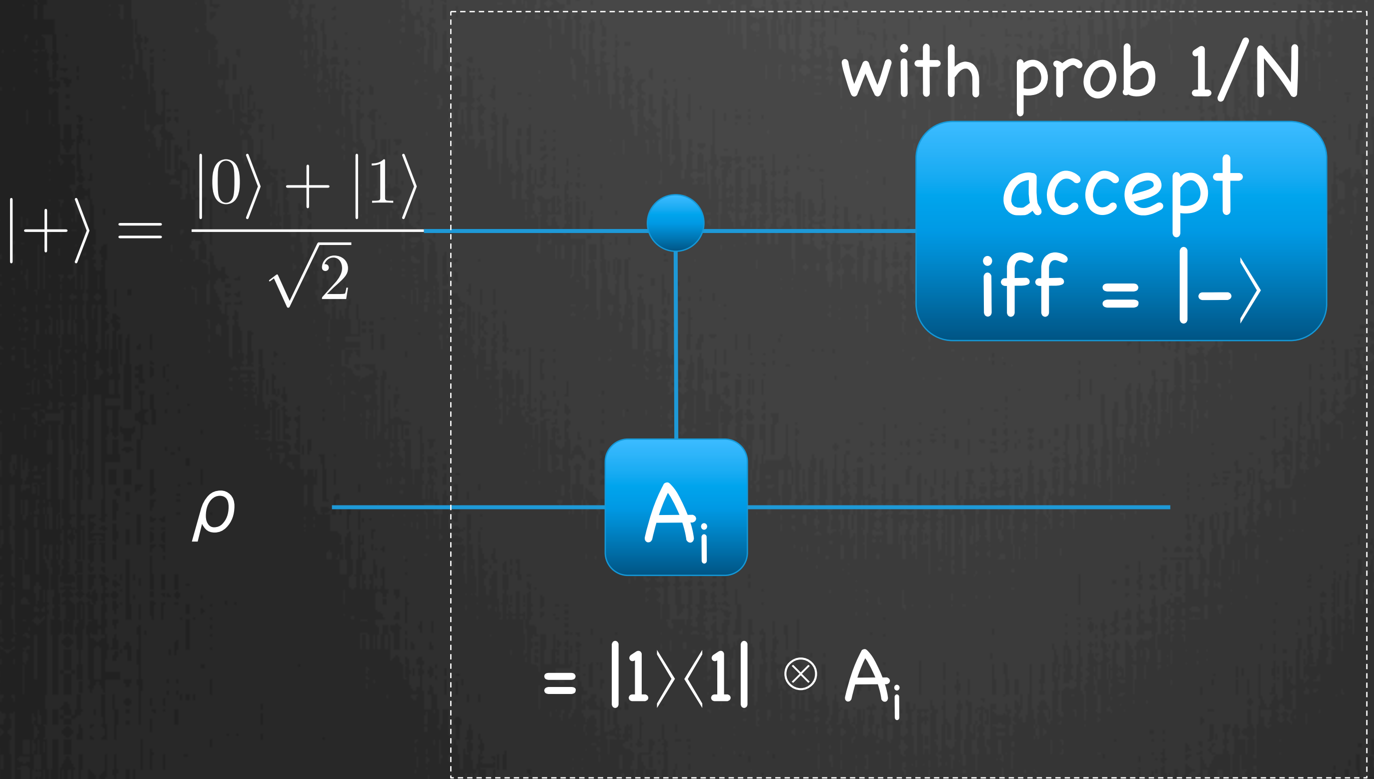
$A_1 = |0\rangle\langle 0|$

$A_2 = |\psi\rangle\langle\psi|$ with $|\psi\rangle = \cos(\varepsilon)|0\rangle + \sin(\varepsilon)|1\rangle$

$A_V = I$ accepts too much

ideas that do work

1. disturbance test



repeat O(N) times

<u>"yes" case</u>

detects either A_i or disturbance

<u>"no" case</u>

nothing happens

ideas that do work

2. modified Marriott-Watrous gap amplification

Strategy: project onto
$P_{\geq}$ = [$\geq$ 1 / 2N eigenspace of $\bar{A} = \frac{\sum_{i=1}^{N} A_i}{N}$]

"no" case: assume tr [$\bar{A}\rho$] $\leq$ δ/N

- $P_{\geq} \leq 2N\bar{A}$
- Pr[accept] = tr [$P_{\geq}\rho$] $\leq$ 2N tr [$\bar{A}\rho$] $\leq$ 2δ

Markov ineq

2. modified Marriott-Watrous gap amplification

Strategy: project onto
$P_\geq$ = [≥ 1 / 2N eigenspace of $\bar{A}$]

$$\bar{A} = \frac{\sum_{i=1}^{N} A_i}{N}$$

"yes" case: tr $\rho A_i \geq 1 - \varepsilon$

$$\sqrt{\operatorname{tr} \rho P_\geq} \geq \left\| \rho - \frac{P_< \rho P_<}{\operatorname{tr} P_< \rho} \right\|_1$$

← gentle measurement

$$\geq \operatorname{tr} \rho A_i - \operatorname{tr} \frac{P_< \rho P_<}{\operatorname{tr} P_< \rho} A_i$$

$$\geq 1 - \epsilon - \frac{1}{2}$$

idea that might work

Perform measurements in a random order [Aaronson '06]

- No proof known
- No counter-example known

Application: property testing

Isomorphism testing [Babai, Chakraborty '10]

$f,g: X \to Y$. $G \subseteq \mathrm{Perm}(X)$

- "yes" case: $\exists \pi$ s.t. $f(\pi x) = g(x)$ $\forall x$
- "no" case: ε-far from any such function
  ($\geq \varepsilon |X|$ disagreements for any π)

Thm: Can test for G-isomorphism with $O((\log |G|)/\varepsilon)$ quantum queries.

Alt proof due to Belov with adversary method.

G-isomorphism testing

suppose $\varepsilon = \Omega(1)$

queries

Problem	G	X	Classical	Quantum
boolean function iso	S_n	$\{0,1\}^n$	$\Omega(2^{n/2})$	$O(n \log n)$
boolean fn linear iso	$GL_n(\mathbb{F}_2)$	$\{0,1\}^n$	$\Omega(2^{n/2})$	$O(n^2)$
graph iso	S_n	$[n] \times [n]$	$\tilde{O}(n^{5/4})$	$O(n \log n)$
hidden subgroup	G	G	$\Omega(\lvert G \rvert^{1/2})$	$O(\log \lvert G \rvert)$

[Alon et al, `13]
[Fischer and Matsliah, `08]
[Friedl et al `09]

- not time efficient
- $\tilde{O}(n^{7/6})$ previously known for g. iso
- HSP result previously known for normal subgroups

property testing with OR

$$|\psi\rangle = \frac{1}{|X|} \sum_{x_1 \in X} |x_1\rangle |f(x_1)\rangle \sum_{x_2 \in X} |x_2\rangle |g(x_2)\rangle$$

$$\Pr[M_\pi \text{ accepts } |\psi\rangle] = \begin{cases} 1 & \text{if } f = g \circ \pi \\ \leq 1 - \varepsilon/2 & \text{if } f \neq g \circ \pi \end{cases}$$

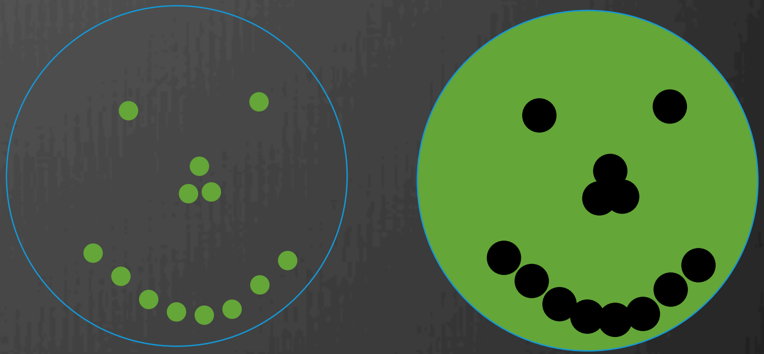
- AND over $O(\log|G|/\varepsilon)$ copies amplifies to 1 vs 1/poly(|G|).
- Use OR test over |G| different choices of π.

quantum property testing

Given finite set $S \subseteq \mathbb{C}^d$

Determine whether $|\psi\rangle \in S$ or is ε-far using $O(\log|S|/\varepsilon)$ copies.

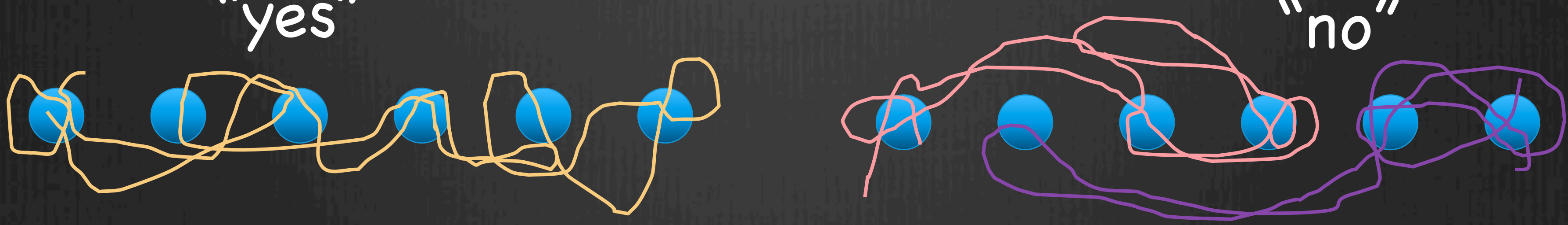
"yes" "no"



[Wang '11]

Genuine n-partite entanglement

"yes" "no"



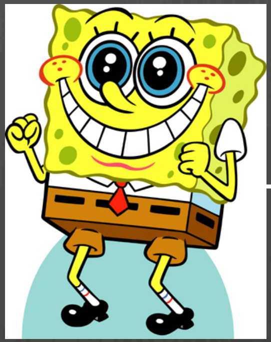
Can test with $O(n/\varepsilon^2)$ copies (vs 2 for product test)

de-Merlinizing

Fixes proof of [Aaronson '06]

x

y



Q qubits

f(x,y)

w untrusted qubits

<u>thm:</u> replace Merlin with O(Q w log(w)) qubits

<u>proof:</u> amplify then OR over all Merlin messages

open questions / thanks

- Time-efficient property testers.
- Quantum OR is not so different from Classical OR in the end. Which primitives carry over and which don't?
- Simultaneous typicality.
- Random ordering or other constructions.

arXiv:1607.03236