A Full Characterization of Quantum Advice

Scott Aaronson Andrew Drucker
MIT

June 6, 2010

'Big picture' question

What is the information content of a quantum state?

- This question has fueled a great deal of research in recent decades.
- We give a new way to concisely describe quantum states, with applications in quantum complexity theory.

Quick quantum review

- A quantum state over n qubits is a 'superposition'

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \quad \in \mathbb{C}^{2^n},$$

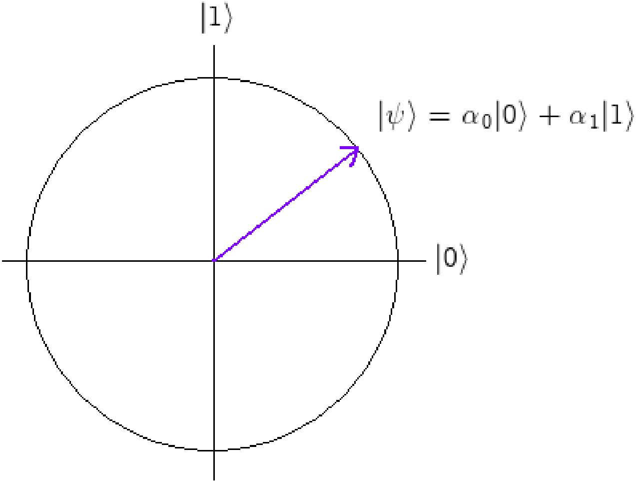
where the values $\{\alpha_x\}$ satisfy

$$\sum_x |\alpha_x|^2 = 1.$$

- If we measure $|\psi\rangle$, it 'collapses' to a classical string: we see outcome $|x\rangle$ with probability $|\alpha_x|^2$.
- More general measurements are allowed: may first apply a unitary linear transformation U to $|\psi\rangle$.

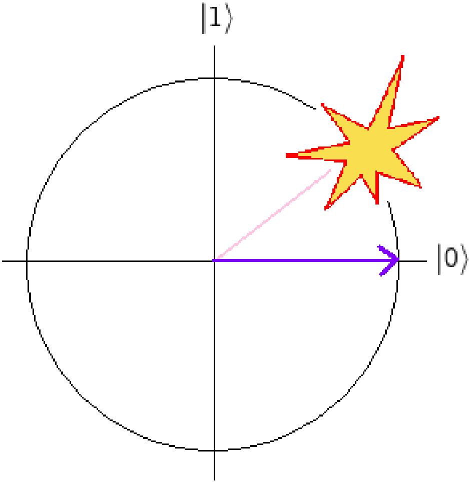
Quantum states are continuous

- Even a single-qubit state $|\psi\rangle$ takes an infinite number of classical bits to specify exactly! However...



Quantum states are continuous

- Most of this information is destroyed upon measurement. We receive only a single-bit outcome.



Qubits vs. bits

- To encode and reliably retrieve m classical bits from a quantum state, we need nearly m qubits **[Hol73]**.
- Quantum states are much less 'spacious' than they first appear!

Qubits vs. bits

- So perhaps concise (approximate) descriptions are possible...
- But, what kind of description is 'good enough'?

Measurement-preserving descriptions

- Suggestion **[Aar04, Aar06]**: given a state $|\psi\rangle$, try to describe a state $|\widetilde{\psi}\rangle$ which is statistically close to $|\psi\rangle$ under every simple, 2-outcome measurement.
- 'Simple' $\leftrightarrow$ 'Performable by a small quantum circuit'.
- Could reflect an assumption about nature, or about our intended uses of the state $|\psi\rangle$.

Simple descriptions for simple measurements

Theorem (Aar04)

Fix $c > 0$, and let $|\psi\rangle$ be an n-qubit state. Using $\mathrm{poly}(n, 1/\varepsilon)$ bits, one can describe a state $|\widetilde{\psi}\rangle$, for which $|\psi\rangle$ and $|\widetilde{\psi}\rangle$ are ε-close in statistical distance under every 2-outcome measurement by quantum circuits of size $\leq n^c$.

Simple descriptions for simple measurements

- Unfortunately, **[Aar04]** gave no efficient way to actually construct the approximating state $|\widetilde{\psi}\rangle$ from its classical description!
- This problem remains open.
- But we can improve substantially on the previous result.

Simple descriptions for simple measurements

Main Theorem

Fix $c > 0$, and let $|\psi\rangle$ be an n-qubit state. There exists a quantum circuit $C_{|\psi\rangle}$ of size $\text{poly}(n, 1/\varepsilon)$ performing a test on an input state $|\phi\rangle$.
Any $|\phi\rangle$ that passes the test can be used to simulate $|\psi\rangle$ to ε accuracy, under every 2-outcome measurement by quantum circuits of size $\le n^c$.

- We can efficiently recognize an encoded copy of $|\psi\rangle$, provided by an untrusted prover!
- ($|\phi\rangle$ is not just a copy of $|\psi\rangle$.)
- Caveat: the mapping $|\psi\rangle \to C_{|\psi\rangle}$ is nonconstructive.

Simple descriptions for simple measurements

Main Theorem

Fix $c > 0$, and let $|\psi\rangle$ be an n-qubit state. There exists a quantum circuit $C_{|\psi\rangle}$ of size $\text{poly}(n, 1/\varepsilon)$ performing a test on an input state $|\phi\rangle$.
Any $|\phi\rangle$ that passes the test can be used to simulate $|\psi\rangle$ to ε accuracy, under every 2-outcome measurement by quantum circuits of size $\leq n^c$.

- We can efficiently recognize an encoded copy of $|\psi\rangle$, provided by an untrusted prover!
- ($|\phi\rangle$ is not just a copy of $|\psi\rangle$.)
- Caveat: the mapping $|\psi\rangle \rightarrow C_{|\psi\rangle}$ is nonconstructive.

Simple descriptions for simple measurements

Main Theorem

Fix $c > 0$, and let $|\psi\rangle$ be an n-qubit state. There exists a quantum circuit $C_{|\psi\rangle}$ of size $\mathrm{poly}(n, 1/\varepsilon)$ *performing a test on an input state $|\phi\rangle$.*
Any $|\phi\rangle$ that passes the test can be used to simulate $|\psi\rangle$ to ε accuracy, under every 2-outcome measurement by quantum circuits of size $\leq n^c$.

- We can efficiently recognize an encoded copy of $|\psi\rangle$, provided by an untrusted prover!
- ($|\phi\rangle$ is not just a copy of $|\psi\rangle$.)
- Caveat: the mapping $|\psi\rangle \rightarrow C_{|\psi\rangle}$ is nonconstructive.

Simple descriptions for simple measurements

Main Theorem

Fix $c > 0$, and let $|\psi\rangle$ be an n-qubit state. There exists a quantum circuit $C_{|\psi\rangle}$ of size $\mathrm{poly}(n, 1/\varepsilon)$ performing a test on an input state $|\phi\rangle$.
Any $|\phi\rangle$ that passes the test can be used to simulate $|\psi\rangle$ to ε accuracy, under every 2-outcome measurement by quantum circuits of size $\leq n^c$.

- We can efficiently recognize an encoded copy of $|\psi\rangle$, provided by an untrusted prover!
- ($|\phi\rangle$ is not just a copy of $|\psi\rangle$.)
- Caveat: the mapping $|\psi\rangle \rightarrow C_{|\psi\rangle}$ is nonconstructive.

Proof sketch (rough)

- Each n-qubit state $|\zeta\rangle$ defines a function

$$F_{|\zeta\rangle} : \{\text{Size-}n^c \text{ quantum circuits}\} \rightarrow [0, 1],$$

by the rule

$$F_{|\zeta\rangle}(C) := \Pr\left[C(|\zeta\rangle) = 1\right].$$

- Let S be the set of all such functions.
- Key known fact: S has low 'fat-shattering dimension' **[Aar06], [ANTV99]**.

Wishful thinking

- Perhaps $F_{|\psi\rangle}$ can be 'singled out' among functions in S, by specifying its values on a small number ($\text{poly}(n, 1/\varepsilon)$) of measurement circuits.
- In this case, say $|\psi\rangle$ is isolatable in S.
- Then, our test $C_{|\psi\rangle}$ could simply request many copies of $|\psi\rangle$, and measure to compare against these values!

Wishful thinking

- Alas, $|\psi\rangle$ may <u>not</u> be isolatable...
- But something almost as good occurs:
- $F_{|\psi\rangle}$ can be 'built' out of a small number of functions in S which <u>are</u> isolatable!

The majority-certificates lemma

Lemma (informal)

For each $F_{|\psi\rangle} \in S$, we can express

$$F_{|\psi\rangle} \approx \frac{1}{k} \sum_{i=1}^{k} F_{|\zeta_i\rangle},$$

where

i) $k = O(\text{poly}(n, 1/\varepsilon))$;

ii) *Each $|\zeta_i\rangle$ is isolatable;*

iii) *The equation above holds to high accuracy on every measurement circuit of size $\leq n^c$.*

The majority-certificates lemma

- Then, to prove our main theorem:
- Our test circuit $C_{|\psi\rangle}$ requests copies of $|\zeta_1\rangle, \ldots, |\zeta_k\rangle$;
- It tests each according to our earlier idea.
- Having accurate copies of $|\zeta_1\rangle, \ldots, |\zeta_k\rangle$ lets us simulate $|\psi\rangle$.

The majority-certificates lemma

- The lemma's proof is a boosting-type argument (using results in learning theory of real-valued functions).
- Our lemma is not specific to quantum, and may find other uses.

Application: Quantum complexity classes

- Our main theorem gives new bounds on the complexity class **BQP/qpoly [NY03]**.
- This class models quantum poly-time computation aided by a non-uniform quantum advice state (on poly(n) qubits), which depends only on the input length.

Theorem

BQP/qpoly $\subseteq$ **QMA/poly**.

- We can replace quantum advice with classical advice, with the help of an untrusted prover.
- Improves on results from **[Aar04], [Aar06]**.

Application: Quantum complexity classes

- In fact, we can exactly characterize **BQP/qpoly** in terms of a quantum class involving only classical nonuniform advice.
- Other applications, and open problems, in the paper...

Thanks!