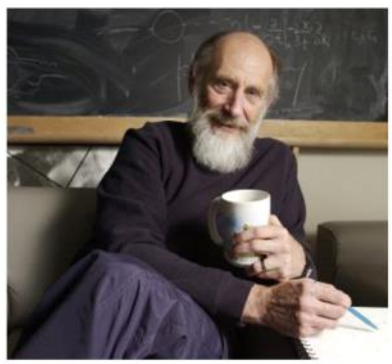
On the Hardness of Detecting Macroscopic Superpositions

Scott Aaronson (UT Austin)

Shoulders of Everett Workshop,
July 9, 2021

Based on a joint paper with Yosi Atia & Leonard Susskind (arXiv:2009.07450)



Background: For the past decade, a bunch of physicists (Susskind, Preskill, Swingle, Harlow...) have been thinking about the black hole information problem, AdS/CFT, and quantum gravity more generally, using the language of qubits, quantum circuits & complexity.

Often they're forced to consider wildly nonlocal changes of basis (e.g., from Hawking radiation to the black hole interior that it "encodes"), or states like

$$\frac{|\text{BlackHole}\rangle + |\text{NoBlackHole}\rangle}{\sqrt{2}},$$

for which it's extremely hard to avoid the question of Everettianism!

Central to their investigations has been the following distance metric on n-qubit states:

$$\boxed{\begin{array}{l} C_\varepsilon(|\psi\rangle, |\varphi\rangle) = \text{minimum \# of} \\ \text{1\&2-qubit gates in any quantum} \\ \text{circuit } C \text{ such that } C|\psi\rangle \approx_\varepsilon |\varphi\rangle. \end{array}}$$

circuit C such that $C|\psi\rangle \approx_\varepsilon |\varphi\rangle$ }

"Relative Circuit Complexity"

This is wildly different from the usual Hilbert space distance! E.g., $|0\ldots00\rangle$ and $|0\ldots01\rangle$ are close in complexity metric yet orthogonal.

If $|Z\rangle$ is Haar-random, then

$$|00\cdots00\rangle \text{ and } \sqrt{0.99}\,|00\cdots00\rangle+\sqrt{0.01}\,|Z\rangle$$

are close in inner product, yet exponentially far in complexity metric (w.h.p. over $|Z\rangle$ and for small enough ε)

In Jan. 2016, Susskind (who uses me as a CS consultant) posed the following problem to me: given two orthogonal "macroscopic" states $|v\rangle$ and $|w\rangle$ (e.g.

geometries' in quantum gravity), give a complexity criterion for when it's "hard" or "easy" to distinguish a superposition

$$\frac{|v\rangle + |w\rangle}{\sqrt{2}}$$

from an incoherent mixture of the two.

<u>Susskind's conjecture</u>: The circuit complexity of this distinguishing task should be <u>characterized</u> by $C_\varepsilon(|v\rangle, |w\rangle)$, the relative circuit complexity of $|v\rangle$ & $|w\rangle$.

<u>What we found</u>: Susskind's conjecture is not quite true (we give an explicit counterexample). <u>But</u>, the complexity of detecting macroscopic coherence is characterized—up to

a factor of 2 — by a closely related measure called "swap complexity":

$$\boxed{S_\varepsilon(|v\rangle,|w\rangle) = \#\text{ of gates in smallest circuit } C \text{ s.t. } \frac{|\langle v|C|w\rangle + \langle w|C|v\rangle|}{2} \geq 1-\varepsilon}$$

I.e., the same circuit C has to map $|v\rangle$ to $|w\rangle$ and $|w\rangle$ to $|v\rangle$, with no relative phase!

Observation: Distinguishing $\frac{|v\rangle+|w\rangle}{\sqrt{2}}$ from $\frac{|v\rangle-|w\rangle}{\sqrt{2}}$ is essentially equivalent to distinguishing either from

$$\frac{|v\rangle\langle v| + |w\rangle\langle w|}{2}$$

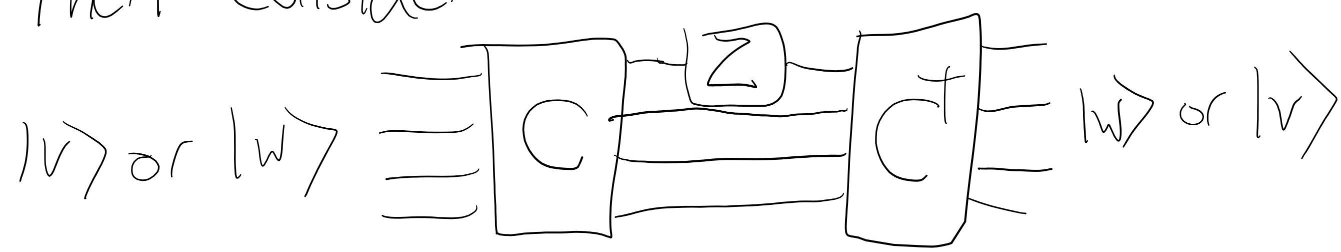
Proof of the Swapping/Distinguishing Connection

(i) Easy distinguishing $\Rightarrow$ easy swapping

Let $|\psi\rangle = \frac{|v\rangle+|w\rangle}{\sqrt{2}}$ & $|\varphi\rangle = \frac{|v\rangle-|w\rangle}{\sqrt{2}}$, So $|v\rangle = \frac{|\psi\rangle + |\varphi\rangle}{\sqrt{2}}$ & $|w\rangle = \frac{|\psi\rangle - |\varphi\rangle}{\sqrt{2}}$.

Suppose $C|\psi\rangle = |0\rangle|\cdots\rangle$ & $C|\varphi\rangle = |1\rangle|\cdots\rangle$.

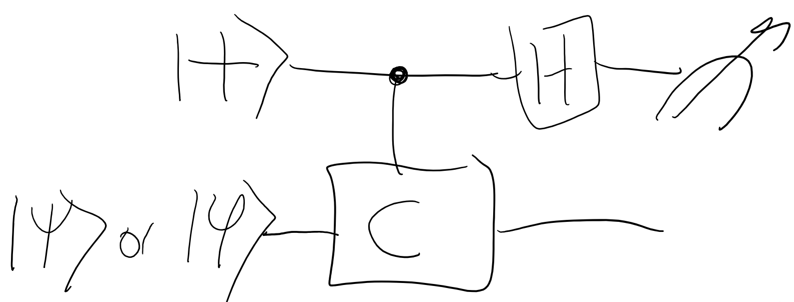
Then consider:



(1') Easy swapping $\Rightarrow$ easy distinguishing

Suppose $C|v\rangle = |w\rangle$ & $C|w\rangle = |v\rangle$.

Then consider



We show that both implications are robust!

<u>Theorem</u>: Suppose we have a circuit C s.t. $\langle u|C|v\rangle = a$ & $\langle v|C|u\rangle = b$.

Using C, we can distinguish $\frac{|u\rangle+|v\rangle}{\sqrt{2}}$ from $\frac{|u\rangle-|v\rangle}{\sqrt{2}}$ with bias $\boxed{\frac{|a+b|}{2}}$.

<u>Theorem</u>: Suppose we can distinguish $\frac{|u\rangle+|v\rangle}{\sqrt{2}}$ from $\frac{|u\rangle-|v\rangle}{\sqrt{2}}$ with bias δ, using a circuit with T gates. Then

$$S_\delta(|u\rangle, |v\rangle) \leq 2T+1.$$

We show that the error parameters in both theorems are tight!

Remarks

Swappability of $|u\rangle$ & $|v\rangle$ is <u>NOT</u> equivalent to distinguishability of $|u\rangle$ & $|v\rangle$!

Let $|z\rangle$ be Haar-random, orthogonal to $|0\cdots0\rangle$.

Then $|0\cdots0\rangle, |z\rangle$: easy to distinguish, hard to swap.

$\frac{|0\cdots0\rangle+|z\rangle}{\sqrt{2}}, \frac{|0\cdots0\rangle-|z\rangle}{\sqrt{2}}$: easy to swap, hard to distinguish.

Distinguishability in one basis is equivalent to swappability in a <u>complementary</u> basis!

Why did we need to use swap complexity rather than relative complexity?

Suppose we have a small circuit C s.t.

$$C|u\rangle = |v\rangle, \quad C|v\rangle = -|u\rangle$$

This <u>need not help at all</u> in distinguishing $\frac{|u\rangle+|v\rangle}{\sqrt{2}}$ from $\frac{|u\rangle-|v\rangle}{\sqrt{2}}$!

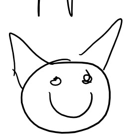
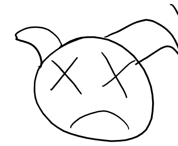
The latter can even remain exponentially hard, e.g. if

$$|u\rangle = \frac{|0\rangle|z\rangle + |1\rangle|0\cdots0\rangle}{\sqrt{2}},$$

$$|v\rangle = \frac{i|0\rangle|z\rangle - i|1\rangle|0\cdots0\rangle}{\sqrt{2}},$$

$|z\rangle$ Haar-random & orthogonal to $|0\cdots0\rangle$.

This won't happen if e.g.

$|u\rangle = |$  $\rangle$, $|v\rangle = |$  $\rangle$,

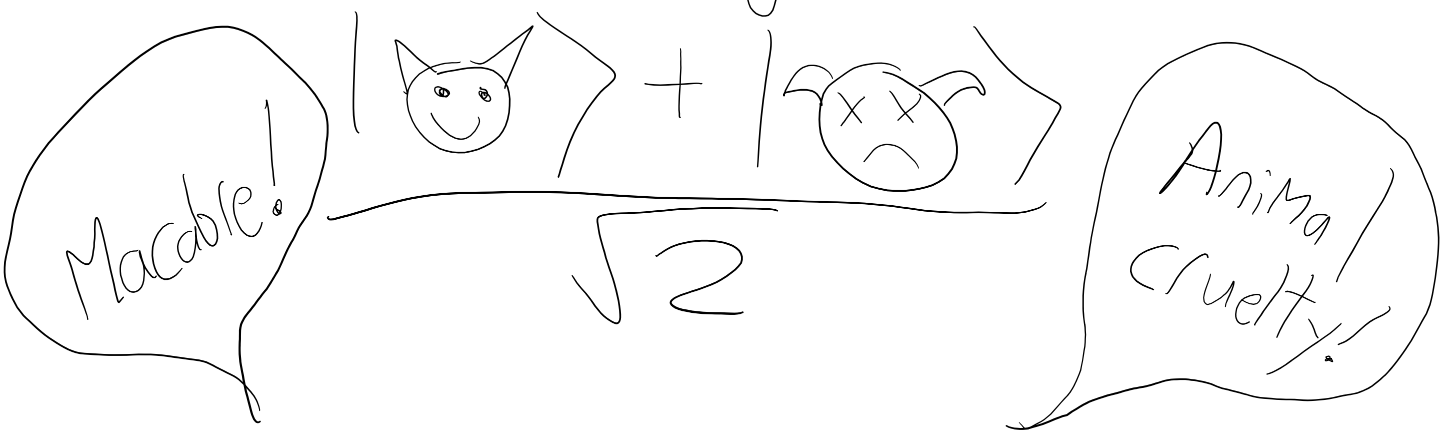
since it's easy to check if a cat is dead & apply a -1 phase if so. But it could happen for $|u\rangle, |v\rangle$ that are hard to distinguish.

Why Should Any of You Care About Any of This?

---

(1) You've been

① You've been fed misinformation about Schrödinger's cat!



THE REALITY: If you had the technological ability (as measured by circuit size) to distinguish a superposition of Alive & Dead from an incoherent mixture, you'd <u>necessarily</u> also have the technological ability to bring a dead cat back to life.

"The Schrödinger's cat experiment is necromancy-hard!"

(& if rotating between $|\text{Alive}\rangle$ & $|\text{Dead}\rangle$ is so easy, was the cat ever "dead" at all?)

People have made related observations before

E.g., Aharonov & Rohrlich 2008: You could revive a dead cat with probability $\frac{1}{2}$

This is weaker than what we show

---

② David Deutsch's thought experiment.

"Testing" the MWI by running an AGI on a QC, and proving it was in a state like

$$\frac{|\text{Perception}_1\rangle + |\text{Perception}_2\rangle}{\sqrt{2}}.$$

<u>My view</u>: Alas, people would keep arguing about MWI even then!

Just like they'd keep arguing about

the Hard Problem of Consciousness — and for similar reasons.

<u>One possible view</u>: Consciousness, at least of any sort we know about from experience, is a phenomenon intimately bound up with the Arrow of Time, the Second Law & irreversibility

If an external agent could rotate you at will from $|\text{Perception}_1\rangle$ to $|\text{Perception}_2\rangle$ and back to $|\text{Perception}_1\rangle$, would your "perceptions" mean anything? Would they even be perceptions at all?

And yet, if that external agent could measure interference between the $|\text{Perception}_1\rangle$ & $|\text{Perception}_2\rangle$ branches, then they'd <u>necessarily</u> have branches, then they'd necessarily have this ability to rotate.

For more, see my "Ghost In The Quantum Turing Machine" essay (arXiv:1306.0159), though it simply accepts as folklore the connection between swapping & detecting interference that this work made more formal.

Discussion Prompts

1. Is quantum circuit complexity a suitable proxy for "difficulty"?
2. Is "difficulty" (e.g., of recohering two branches) ever relevant to quantum foundations?
3. If not, then what's a better,

criterion for two Everett branches to have independent existence?

(4) Does the Everett interpretation <u>require</u> it to be possible, at least in principle, to recohere two different mental states of a conscious being?

(5) Anything else we/I should try to prove that might bear on any of these questions?