Pseudorandomness and the AdS/CFT correspondence

Adam Bouland

YITP workshop, March 2021

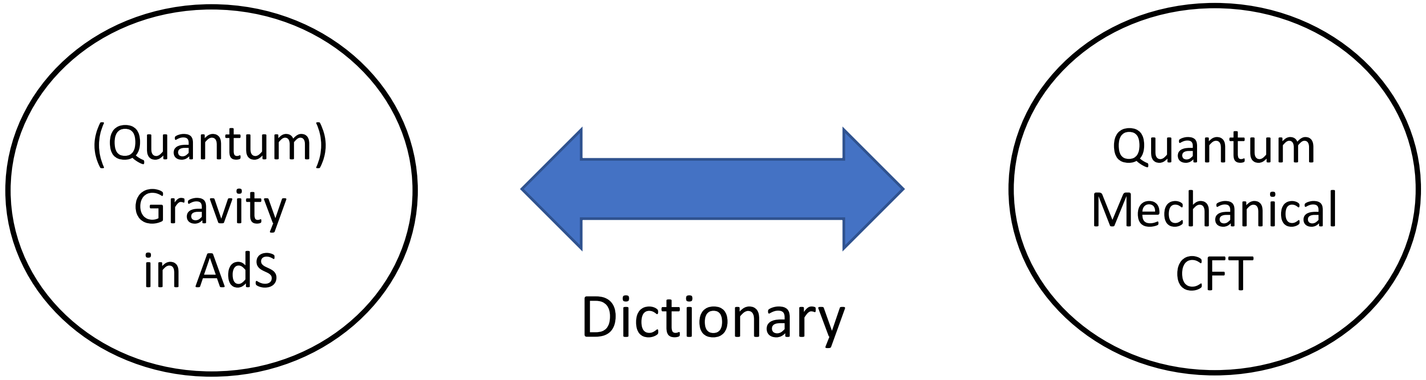
Based on work with Bill Fefferman and Umesh Vazirani

arXiv:1910.14646

Berkeley
UNIVERSITY OF CALIFORNIA

THE UNIVERSITY OF
CHICAGO

AdS/CFT correspondence [Maldacena ‘97]



- “Dictionary” maps states to states, and operators to operators
- You can construct a theory of quantum gravity via studying the dual quantum theory!

Goal: Understand Dictionary

- What is its domain of validity?
- What are its entanglement/error correction properties?
- How useful will this dictionary be?

Quantum Gravity in the Lab:
Teleportation by Size and Traversable Wormholes

Adam R. Brown,[1,2] Hrant Gharibyan,[2,3] Stefan Leichenauer,[1] Henry W. Lin,[1,4] Sepehr Nezami,[1,2] Grant Salton,[3,2] Leonard Susskind,[1,2] Brian Swingle,[5] and Michael Walter[6]

[1] *Google, Mountain View, CA 94043, USA*

[2] *Department of Physics, Stanford University, Stanford, CA 94305, USA*

[3] *Institute for Quantum Information and Matter, Caltech, Pasadena CA 91125, USA*

Our results [B. Fefferman Vazirani'19]

- The dictionary must be **exponentially complex**
  - Or the quantum extended Church-Turing Thesis is false in quantum gravity

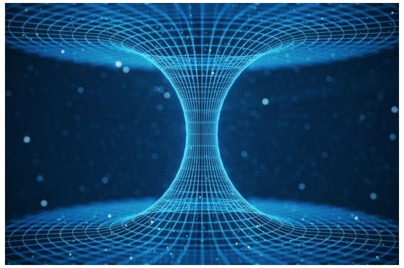
- This arises due to **computational pseudorandomness** in a well-studied subset of CFT states from the wormhole growth paradox
  - Forced to equate "something like complexity" of CFT states with "something like volume" of AdS wormholes

- Might limit utility of dictionary?

Wormhole growth paradox [Susskind’14]

Gravity

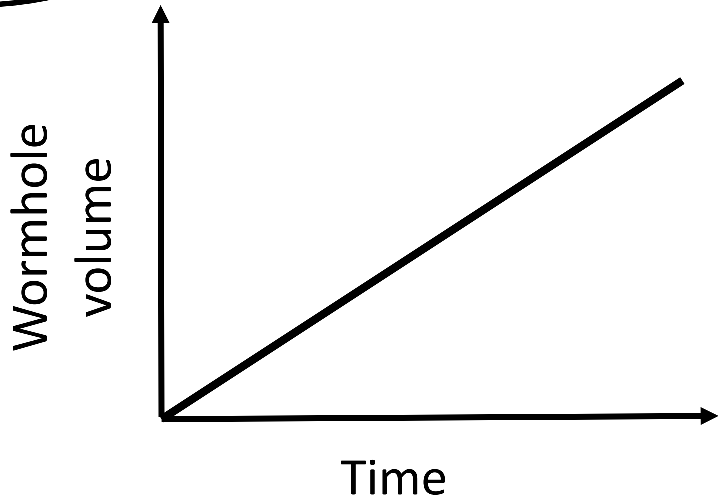
Quantum Mechanics



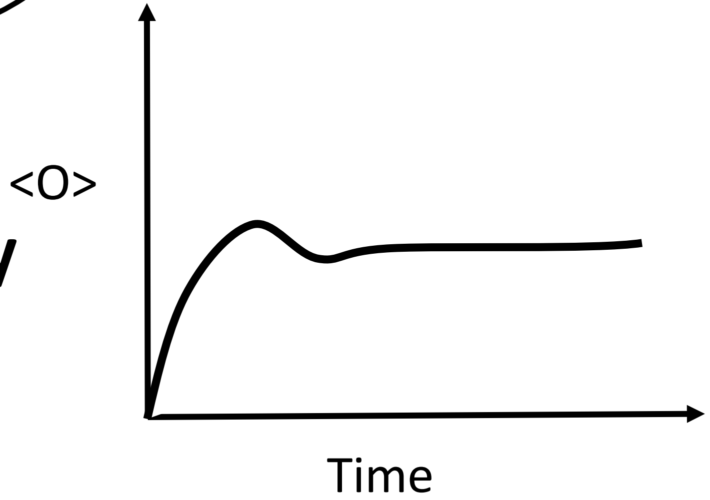
Q: What quantity on RHS corresponds to wormhole volume?

Dual=?

Wormholes: Do not equilibrate for exp time



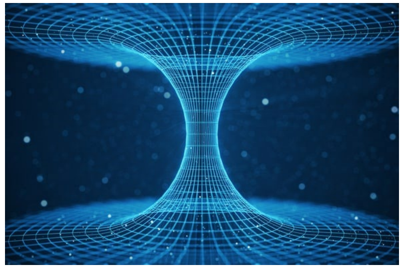
Quantum theory: rapidly equilibrates



Susskind's proposed solution

Gravity

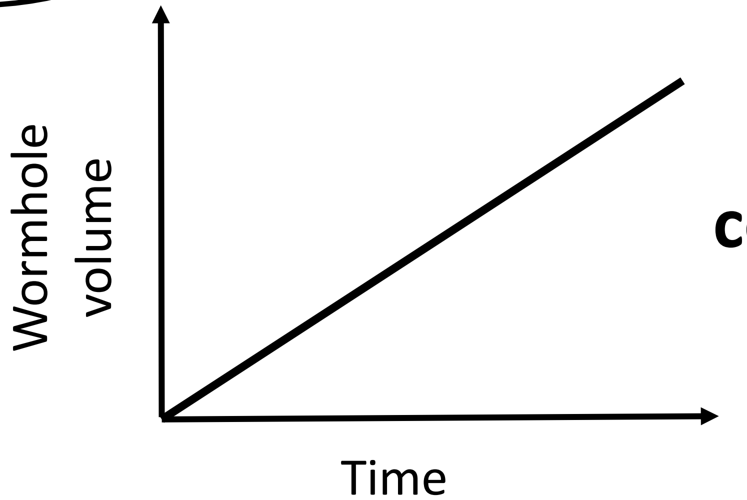
Quantum Mechanics



Q: What quantity on RHS corresponds to wormhole volume?

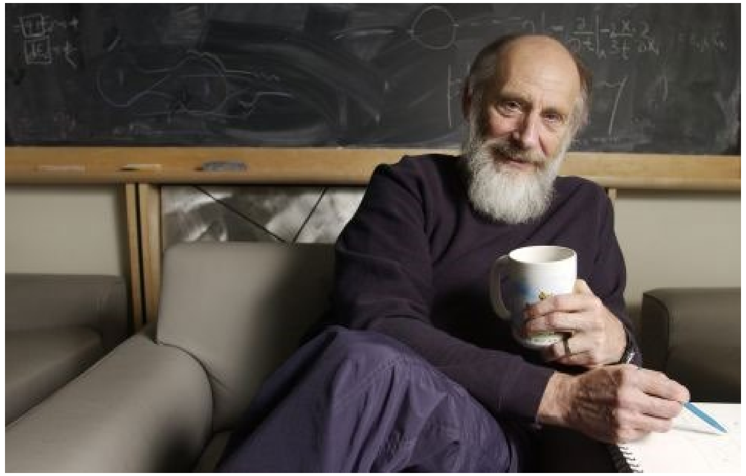
Dual= Circuit complexity

Wormholes: Do not equilibrate for exp time



Susskind'14: Circuit complexity is the dual to wormhole volume "Complexity=Volume"

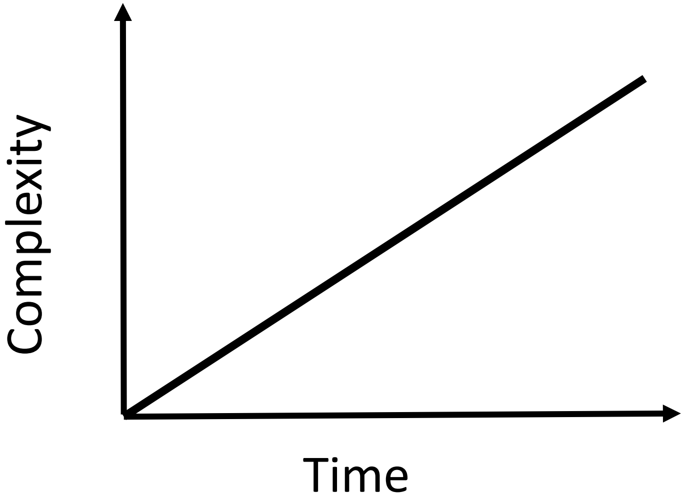
Susskind's resolution: Complexity is physical!



- **Intuition**: Model CFT by n-qubit state (n=entropy). Let U be evolution of the CFT Hamiltonian for a scrambling time.
- The state after t scrambling epochs is given by

$$e^{-iHt}|\psi\rangle \approx UU\ldots UU|\psi\rangle = U^t\,|\psi\rangle$$

The complexity of $e^{-iHt}|\psi\rangle$ (relative to $|\psi\rangle$) should grow linearly with time, because there should be no "shortcuts" to preparing this state



Supporting evidence for Complexity=Volume

- Complexity: Aaronson '17, Brandao Bohdanowicz '18, Balasubramanian et al. '19: linear complexity growth is plausible
- Gravity: Consider perturbing the evolution of the CFT by ℓ << n "shocks"

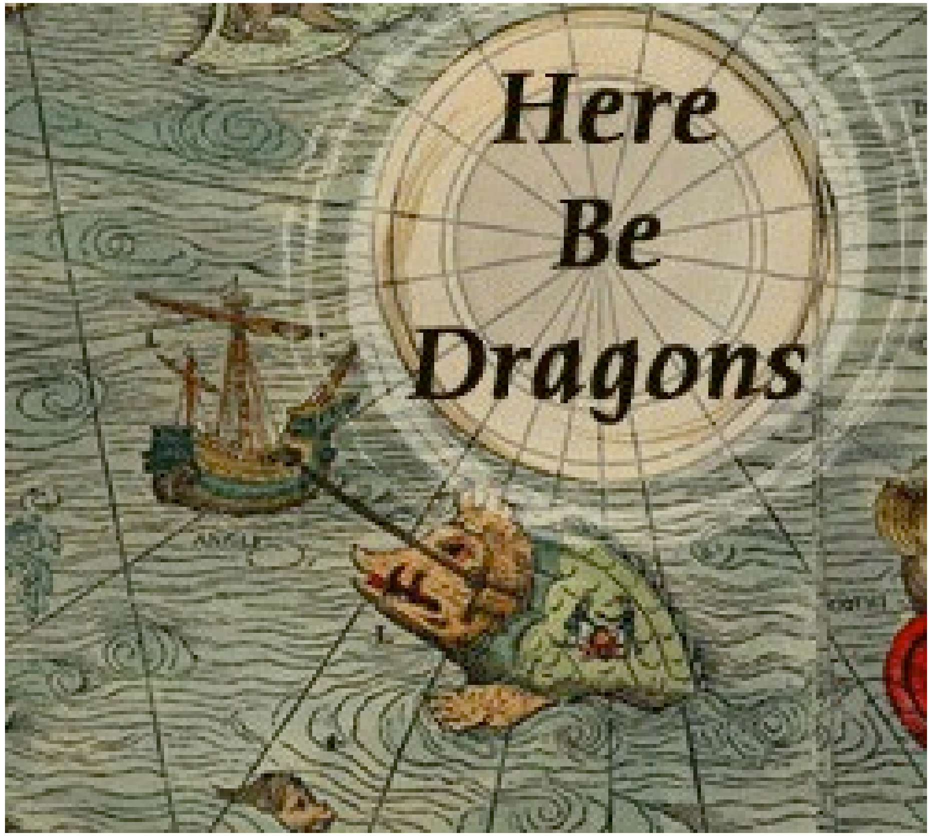
$$U O_\ell U O_{\ell-1} \ldots O_1 \, U|TFD\rangle$$

"Shock states"

  - Gravity side: these "shocks" throw energy into the wormhole
  - Qubit model: correspond to insertion of one-qubit gates

[SS'14]: The changes to the wormhole's volume induced by throwing in shocks matches the changes in complexity of these states under adding operator insertions!

Susskind’s resolution: Complexity is physical!



CS Discomfort: “Type mismatch”

1) Complexity should be difficult to feel or estimate [’90s]

2) Wormhole volume should be easy to estimate

BUT

1) Very special subset of states being considered. Maybe the complexity of “shock” states is easier to estimate? Or maybe complexity is not the dual?

2) No single observer in the black hole can estimate volume -- maybe it is inaccessible?

Can these objections be realized in this model?

If so, what would it mean for AdS/CFT?

First result [**B.**, Fefferman, Vazirani '19]

1) The "shock" states arising in the wormhole growth paradox are **computationally pseudorandom**
    - Given a CFT state with an unknown shockwave pattern, hard to distinguish from a Haar random state
    - Corollary: complexity of these states – or more generally their length of time evolution -- is not "feelable"

Soon: will show why this has major implications for AdS/CFT

Cryptography for quantum gravity theorists

Q: How to encrypt data over the internet?

- Message $x \in \{0,1\}^n$, secret key $k \in \{0,1\}^n$
- First attempt: one-time pad
  - Enc(x) = x XOR k

- Pro: information-theoretic security
- Con: can only use the key once!
  - If messages x_1 x_2 differ by one bit, so do their encodings
  - "Too structured"
  - Want encryption to be more "scrambled"

Better solution: Block ciphers

- Let σ be a fixed, known permutation that is **highly scrambling.**

$$\mathrm{Enc}(x) = \sigma X^k \ldots \sigma X^k \sigma X^k \sigma\, x$$

where X^k applies the secret key k (by XOR) to every bit of the string

Intuition: easy to invert if you know k

Hard to invert even if you are mistaken on a single bit of k due to the "scrambling" nature of the permutation – just looks random

Can prove security in model where σ is totally "unstructured"

Application to quantum gravity

Let U be evolution of CFT for a scrambling time, and let

“s

A quantum block (Bloch?) cipher!

- Consider “shock states”

$$UO_\ell UO_{\ell-1}\ldots O_1 U|TFD\rangle$$

- These are states for which we have evidence for C=V

- Let σ be a fixed but highly scrambling permutation in S_{2n}. Let

$$\mathrm{Enc}(x,k) = \sigma X^k \ldots \sigma X^k \sigma X^k \sigma\ x$$

where X flips the first bit of the string

Consequence: Computational Pseudorandomness [Ji Liu Song '18]

A collection of efficiently preparable states $\{|\psi_k\rangle\}$ on n qubits, k in $\{0,1\}^m$, is a **quantum pseudorandom state ensemble** (**PRS**) if for any polynomial q(n), q(n) copies of $|\psi_k\rangle$ (for a random k) are not BQP-distinguishable from q(n) copies of a Haar random state $|\varphi\rangle$

"Like a t-design, but computational instead of info-theoretic security"

Our result: shock states are a **naturally** pseudorandom, as they are analog of block ciphers

Our Pseudorandomness Construction

$|\psi_k\rangle = U k_\ell \, U k_{\ell-1} \ldots k_1 \, U|TFD\rangle$, k in {I,X,Y,Z}$^\ell$

Key idea: Shocks create "branching points" in the evolution

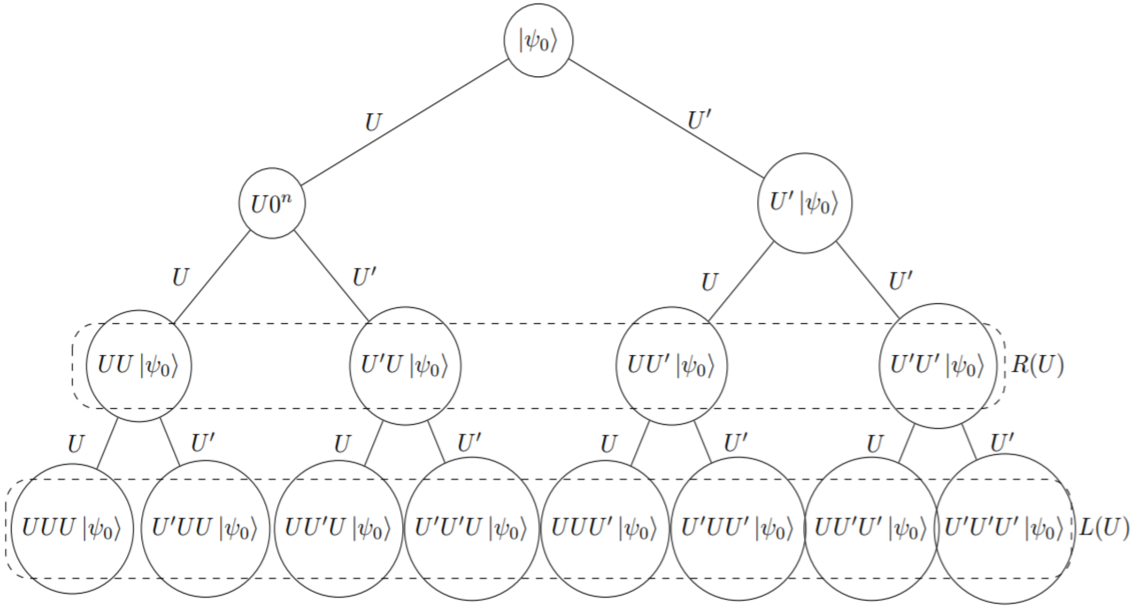


Figure 2: Representation of the tree $T(U)$ for $k = 3$. $R(U)$ denotes the nodes in the second to last row of the tree, and $L(U)$ denotes the leaves of the tree.

If U were Haar-random, then each state in tree would be nearly orthogonal to every over state in tree

Claim: Given an unknown state |φ>, hard to tell if the state is in this tree or not!

Prove in black box model, and conjecture security in white-box model where U is evolution for a scrambling time

Implications of pseudorandomness

- Cannot efficiently tell shock states apart, even those with very different lengths of time evolution/wormhole volume
- Corollary: complexity of these states – or more generally their length of time evolution -- is not “feelable”
  - **Whatever** the dual to volume is, it is difficult to compute
  - ***Must*** be something like complexity!

Second result [**B.**, Fefferman, Vazirani '19]

2) Showed wormhole volume is easy to compute

- We give an efficient **algorithm** which achieves a very rough approximation of the wormhole volume

Dictionary allows you to extract the global metric

Computing volume is a simple calculation

Dictionary only allows reconstruction of experiences of individual observers

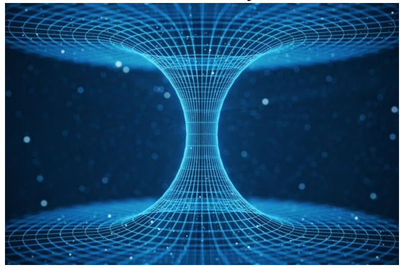
- Consider poly(n) observers in the wormhole, who can meet pairwise or exchange messages to determine if they are close or not.
- Postprocessing their outcomes results in a coarse approximation to the volume.

Implications

Gravity

PERMANENTLY

Quantum Mechanics



Dictionary

?

Result 2: Wormhole volume is easy to compute

Result 1: Whatever ? is, it must be difficult to compute (like complexity)

Conclusion: Dictionary must be exponentially difficult to compute!

What does this mean for AdS/CFT?

The complexity of the dictionary is a **bug**

Limits what one can learn about wormhole interiors from the CFT

Susskind ’20: “Computational Cosmic Censorship”: All violations of the quantum ECT or exponentially complex dictionaries are shielded by horizons

The complexity of the dictionary is a **feature**

Kim Preskill Tang ’20: “Computational protection of causality”:

High complexity prevents someone from modifying wormhole interior via its dual description in the boundary

Alternative: the quantum ECT is false in quantum gravity!

Thanks!

Our result [**B.**, Fefferman, Vazirani '19]

Why is it reasonable to assume postprocessing?

- Algorithm **simulates** the experiences of the different observers, and postprocesses the results

Resulting experiment is not physically implementable –

But is a **computationally efficient** algorithm (assuming qECT)