Computational Pseudorandomness, the Wormhole Growth Paradox, and Constraints on the AdS/CFT Duality

Adam Bouland
Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, 617 Soda Hall, Berkeley, CA 94720, U.S.A.
abouland@berkeley.edu

Bill Fefferman
Department of Computer Science, University of Chicago, 5730 S Ellis Ave, Chicago, IL 60637, U.S.A.
wjf@uchicago.edu

Umesh Vazirani
Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, 671 Soda Hall, Berkeley, CA 94720, U.S.A.
vazirani@cs.berkeley.edu

Abstract

The AdS/CFT correspondence is central to efforts to reconcile gravity and quantum mechanics, a fundamental goal of physics. It posits a duality between a gravitational theory in Anti de Sitter (AdS) space and a quantum mechanical conformal field theory (CFT), embodied in a map known as the AdS/CFT dictionary mapping states to states and operators to operators. This dictionary map is not well understood and has only been computed on special, structured instances. In this work we introduce cryptographic ideas to the study of AdS/CFT, and provide evidence that either the dictionary must be exponentially hard to compute, or else the quantum Extended Church-Turing thesis must be false in quantum gravity.

Our argument has its origins in a fundamental paradox in the AdS/CFT correspondence known as the wormhole growth paradox. The paradox is that the CFT is believed to be "scrambling" – i.e. the expectation value of local operators equilibrates in polynomial time – whereas the gravity theory is not, because the interiors of certain black holes known as "wormholes" do not equilibrate and instead their volume grows at a linear rate for at least an exponential amount of time. So what could be the CFT dual to wormhole volume? Susskind's proposed resolution was to equate the wormhole volume with the quantum circuit complexity of the CFT state. From a computer science perspective, circuit complexity seems like an unusual choice because it should be difficult to compute, in contrast to physical quantities such as wormhole volume.

We show how to create pseudorandom quantum states in the CFT, thereby arguing that their quantum circuit complexity is not "feelable", in the sense that it cannot be approximated by any efficient experiment. This requires a specialized construction inspired by symmetric block ciphers such as DES and AES, since unfortunately existing constructions based on quantum-resistant one way functions cannot be used in the context of the wormhole growth paradox as only very restricted operations are allowed in the CFT. By contrast we argue that the wormhole volume is "feelable" in some general but non-physical sense. The duality between a "feelable" quantity and an "unfeelable" quantity implies that some aspect of this duality must have exponential complexity. More precisely, it implies that either the dictionary is exponentially complex, or else the quantum gravity theory is exponentially difficult to simulate on a quantum computer.

While at first sight this might seem to justify the discomfort of complexity theorists with equating computational complexity with a physical quantity, a further examination of our arguments shows that any resolution of the wormhole growth paradox must equate wormhole volume to an "unfeelable" quantity, leading to the same conclusions. In other words this discomfort is an inevitable consequence of the paradox.

11th Innovations in Theoretical Computer Science Conference (ITCS 2020).
Editor: Thomas Vidick; Article No. 63; pp. 63:1–63:2
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

2012 ACM Subject Classification Theory of computation → Quantum computation theory; Theory of computation → Pseudorandomness and derandomization; Theory of computation → Quantum complexity theory

Keywords and phrases Quantum complexity theory, pseudorandomness, AdS/CFT correspondence

Digital Object Identifier 10.4230/LIPIcs.ITCS.2020.63

Category Abstract

Related Version A full version of the paper is available at https://arxiv.org/abs/1910.14646v1.

Funding *Adam Bouland*: A.B. was supported in part by ARO Grant W911NF-12-1-0541, NSF Grant CCF-1410022, and a Vannevar Bush faculty fellowship.
Bill Fefferman: B.F. acknowledges support from AFOSR YIP number FA9550-18-1-0148.
Umesh Vazirani: U.V. was supported in part by ARO Grant W911NF-12-1-0541, NSF Grant CCF-1410022, a Vannevar Bush faculty fellowship, and the Miller Institute at U.C. Berkeley through a Miller Professorship.

Acknowledgements We thank Scott Aaronson, Adam Brown, John Preskill, Douglas Stanford, Lenny Susskind, and Brian Swingle for detailed comments. We also thank Chris Akers, Dorit Aharonov, Ahmed Almheiri, Ning Bao, Raphael Bousso, Matt DeCrosse, Helia Kamal, Dan Harlow, Patrick Hayden, Juan Maldacena, Saeed Mehraban, Dominik Neuenfeld, Sepehr Nezami, Fabio Sanches, Jonah Sherman, Jalex Stark, Vincent Su, Michael Walter, and Ying Zhao for helpful discussions.