Random circuits have no shortcuts

Quantum information

Random circuits have no shortcuts

Lorenzo Piroli

Philippe Meyer Institute, Physics Department, École Normale Supérieure (ENS), Université PSL, 24 rue Lhomond, F-75231 Paris, France

Email : lorenzo.piroli@phys.ens.fr

Theoretical physicists studying black holes have produced a conjecture that random quantum circuits cannot be simplified. Now, a minimal version of this conjecture has been proven, reaching a milestone in quantum-circuit complexity theory.

Take a collection of qubits initialized in a simple state and consider applying a sequence of random two-qubit gates. One may ask whether the same output state can be prepared using a substantially shorter sequence of judiciously chosen operations. Surprisingly, this question has arisen in the holographic description of black-hole physics, in which the growth of a wormhole's size has been proposed to correspond to the growth of complexity in quantum dynamics. This idea implies the conjecture that the answer is no, a random sequence of gates cannot be shortened unless its length approaches a value that is exponentially large in the number of qubits. Now, writing in Nature Physics,[1] Jonas Haferkamp and collaborators report an unexpectedly simple proof of this conjecture.

The complexity of a computation is a measure of the resources needed to perform it. For instance, the complexity of a classical Boolean function may be defined as the minimal number of elementary operations such as AND or NOT gates needed to evaluate it. This notion extends to the quantum domain, where it can be defined in different ways, depending on the context. Quantum circuits, which are sequences of elementary reversible operations (quantum gates) acting on pairs of qubits, provide a simple and intuitive way to do so: The quantum-circuit complexity of a unitary transformation or quantum state is the number of gates in the shortest quantum circuit that implements the unitary operation or prepares the state.

This notion of quantum-circuit complexity has recently risen to prominence due to connections with the description of eternal black holes, in the context of the anti-de-Sitter-space/conformal-field-theory (AdS/CFT) 'holographic' correspondence, which states that a gravitational theory defined on the anti-de Sitter space is equivalent to a conformal quantum field theory which can be defined at its boundary, with a 'dictionary' for translating calculations between the two theories. Eternal black holes are a special solution to Einstein's equations of gravity, partitioning the space-time into distinct regions connected by a wormhole. Calculations of the wormhole volume show that it grows linearly until it reaches a maximum size that is an exponential function of the black hole's entropy.

Within the AdS/CFT correspondence, the wormhole size should therefore be dual to some quantity in the boundary conformal field theory. Like the wormhole, this quantity should reach an equilibrium value only after a time which is exponentially large in the number of degrees of freedom. However, all local observables are known to reach equilibrium values much faster than this, so they cannot be dual to the wormhole size – a conundrum known as the wormhole-growth paradox. As a possible resolution, it was put forward[2–5] that the wormhole volume is dual to the

quantum complexity of the boundary state. The AdS/CFT correspondence then produces a natural conjecture that the growth of quantum complexity in sufficiently chaotic unitary dynamics should, like the wormhole volume, grow linearly for a time which is exponentially large in the number of degrees of freedom[5,6].

In general it is difficult to analyze the evolution of large quantum systems but the conjecture can be stated in an elementary way using an idealized 'random circuit' toy model for chaotic black-hole dynamics (Fig. 1). Consider using a sequence of random two-qubit gates to construct a large, complicated quantum operator acting on a collection of qubits. The arrangement of the gates is immaterial to the asymptotic behaviour, provided that the circuit displays some minimal connectivity. Brown and Susskind[5,6] conjectured that the complexity of the final state grows linearly with the number of random gates in the circuit, saturating after exponentially many time steps.

While this conjecture has been supported by simple counting arguments,[4,7] obtaining a rigorous proof appeared to be quite challenging. The core difficulty is that the gates performed early in a circuit may partially reverse gates performed later and therefore one can rarely rule out the existence of a smaller 'shortcut' circuit that generates the same unitary operator.

In their work, Haferkamp and colleagues achieved an unexpectedly short, rigorous proof of this conjecture, using an innovative combination of techniques from differential topology and elementary algebraic geometry. On a high-level, the proof shows that random circuits of a given size realize an ensemble of unitary operators that is too random to consist mostly of shorter circuits. They introduced a characterization of the unitary operators that can be generated with a fixed arrangement of gates, and showed that it serves as a good proxy for quantum complexity. By deriving strong lower bounds on this complexity measure, the authors were ultimately able to prove the conjecture.

The main theorem is stated in terms of an explicit lower bound on the complexities of random unitary operators and states. The bound is linear in the number of gates, with a coefficient depending on the specific arrangement of the gates in the circuit. This theorem complements another rigorous insight achieved in an independent work by Brandão and collaborators,[8] focusing on a more operational notion of complexity, for which linear growth could be proven in a limit where the gates act on high-dimensional quantum systems.

Several questions remain open. Most prominently, an outstanding problem is to extend the result to typical, non-random time-independent Hamiltonian evolution, which would prove the strongest version of the conjecture by Brown and Susskind. While this problem is considerably more complicated, significant evidence suggests that the conjecture remains true.[9,10] Overall, our comprehension of quantum complexity in high-energy and many-body physics is still in its infancy. Still, the work by Haferkamp and colleagues represents a very important step towards establishing its physical significance, substantiating the evidence that studying quantum-circuit complexity is the right approach to resolve the wormhole-growth paradox.

The author declares no competing interests

References

1 J. Haferkamp, P. Faist, N. B. T. Kothakonda, J. Eisert, and N. Y. Halpern, *Linear Growth of Quantum Circuit Complexity*, ArXiv:2106.05305 (2021).

2 L. Susskind. *Computational complexity and black hole horizons*. Fort. Phys., 64, 24 (2016).

3 D. Stanford and L. Susskind, *Complexity and Shock Wave Geometries*, Phys. Rev. D 90, 126007 (2014).
4 A. R. Brown, D. A. Roberts, L. Susskind, B. Swingle, and Y. Zhao, *Holographic Complexity Equals Bulk Action?*, Phys. Rev. Lett. 116, 191301 (2016).
5 A. R. Brown and L. Susskind, *Second Law of Quantum Complexity*, Phys. Rev. D 97, 086015 (2018).
6 L. Susskind, *Black Holes and Complexity Classes*, arXiv:1802.02175 (2018).
7 D. A. Roberts and B. Yoshida, *Chaos and Complexity by Design*, J. High Energ. Phys. (2017) 121.
8 F. G. S. L. Brandão, W. Chemissany, N. Hunter-Jones, R. Kueng, and J. Preskill, *Models of Quantum Complexity Growth*, PRX Quantum 2, 030316 (2021).
9 S. Aaronson, *The Complexity of Quantum States and Transformations: From Quantum Money to Black Holes*, ArXiv:1607.05256 (2016)
10 V. Balasubramanian, M. DeCross, A. Kar, and O. Parrikar, *Quantum Complexity of Time Evolution with Chaotic Hamiltonians*, J. High Energ. Phys. (2020), 134.

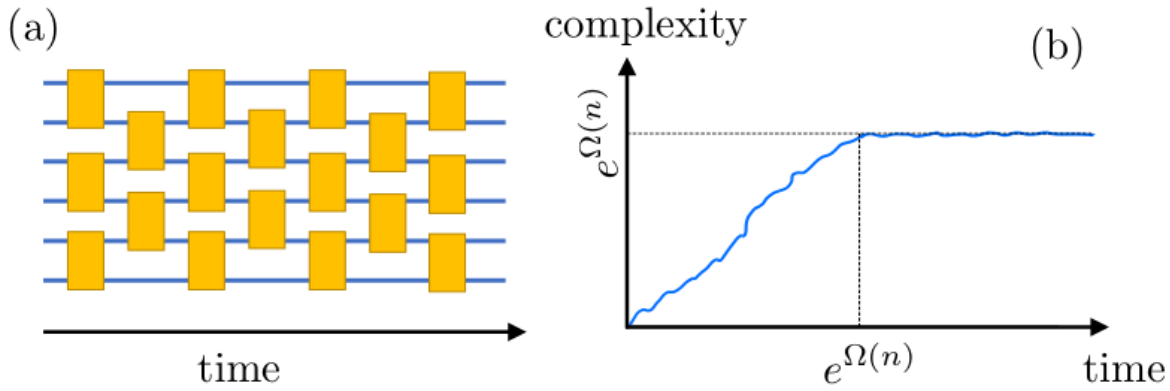

Figure 1: **A quantum circuit made by random two-qubit gates** (a) A random quantum circuit is a sequence of two-qubit gates (light rectangles) arranged to form a composite operation acting on many qubits. The gates need not to act on neighboring qubits, but the architecture must satisfy some minimal connectivity requirement. Each gate is drawn randomly from a uniform probability distribution in the space of two-qubit unitary operators. The size of a given circuit is the number of gates it contains. (b) For a system of n qubits, Haferkamp and collaborators proved that the complexity grows linearly under random quantum-circuit evolution until times exponential in the number n of qubits.