ARTICLES
https://doi.org/10.1038/s41567-022-01539-6

nature physics

OPEN

Linear growth of quantum circuit complexity

Jonas Haferkamp[1,2] ✉, Philippe Faist[1], Naga B. T. Kothakonda[1,3], Jens Eisert[1,2] and Nicole Yunger Halpern[4,5,6,7,8]

The complexity of quantum states has become a key quantity of interest across various subfields of physics, from quantum computing to the theory of black holes. The evolution of generic quantum systems can be modelled by considering a collection of qubits subjected to sequences of random unitary gates. Here we investigate how the complexity of these random quantum circuits increases by considering how to construct a unitary operation from Haar-random two-qubit quantum gates. Implementing the unitary operation exactly requires a minimal number of gates—this is the operation's exact circuit complexity. We prove a conjecture that this complexity grows linearly, before saturating when the number of applied gates reaches a threshold that grows exponentially with the number of qubits. Our proof overcomes difficulties in establishing lower bounds for the exact circuit complexity by combining differential topology and elementary algebraic geometry with an inductive construction of Clifford circuits.

Complexity is a pervasive concept at the intersection of computer science, quantum computing, quantum many-body systems and black hole physics. In general, complexity quantifies the resources required to implement a computation. For example, the complexity of a Boolean function can be defined as the minimal number of gates, chosen from a given gate set, necessary to evaluate the function. In quantum computing, the circuit model provides a natural measure of complexity for pure states and unitaries: a unitary transformation's quantum circuit complexity is the size, measured with the number of gates, of the smallest circuit that effects the unitary. Similarly, a pure state's quantum circuit complexity definable is the size of the smallest circuit that produces the state from a product state.

Quantum circuit complexity, by quantifying the minimal size of any circuit that implements a given unitary, is closely related to computational notions of complexity. The latter quantify the difficulty of solving a given computational task with a quantum computer and determine quantum complexity classes. Yet quantum circuit complexity can subtly differ from computational notions of quantum complexity: the computational notion depends on the difficulty of finding the circuit. In the following, we refer to quantum circuit complexity as 'quantum complexity' for convenience.

Quantum complexity has risen to prominence recently due to connections between gate complexity and holography in high-energy physics, in the context of the anti-de-Sitter space/conformal field theory (AdS/CFT) correspondence[1–5]. In the bulk theory, a wormhole's volume grows steadily for exponentially long times. By contrast, in boundary quantum theories, local observables tend to thermalize much more quickly. This contrast is known as the 'wormhole-growth paradox'[1]. It appears to contradict the AdS/CFT correspondence, which postulates a mapping of physical operators between the bulk theory and a quantum boundary theory. A resolution has been proposed in the 'complexity equals volume' conjecture: the wormhole's volume is conjectured to be dual not to a local quantum observable, but to the boundary state's quantum complexity[2]. Similarly, the 'complexity equals action' conjecture posits that a holographic state's complexity is dual to a certain space–time region's action[6].

A counting argument reveals that the vast majority of unitaries have near-maximal complexities[7]. Yet lower-bounding the quantum complexity is a long-standing open problem in quantum information theory. The core difficulty is that the gates performed early in a circuit may partially cancel with gates performed later. One can rarely rule out the existence of a 'shortcut', a seemingly unrelated but smaller circuit that generates the same unitary. Consequently, quantum-gate-synthesis algorithms, which decompose a given unitary into gates, run for times exponential in the system size[8]. Approaches to lower-bounding unitaries' quantum complexities include Nielsen's geometric picture[9–13].

A key question in the study of quantum complexity is the following. Consider constructing deeper and deeper circuits for an n-qubit system, by applying random two-qubit gates. At what rate does the circuit complexity increase? Brown and Susskind conjectured that the complexity of quantum circuits generically grows linearly for an exponentially long time[4,14]. Intuitively, the conjecture is that most circuits are fundamentally 'incompressible': no substantially shorter quantum circuit effects the same unitary. Quantum complexity, if it grows linearly with a generic circuit's depth, strongly supports the 'complexity equals volume' conjecture as a proposal to the wormhole-growth paradox[1,2]. The conjecture therefore implies that complexity growth is as generic as thermalization[15,16] and operator growth[17,18] (the spreading of an initially local operator's support in the Heisenberg picture). However, in contrast to easily measurable physical quantities, which thermalize rapidly, complexity grows for an exponentially long time. Brown and Susskind have supported their conjecture using Nielsen's geometric approach (Fig. 1b)[9–12].

Brandão et al.[19] recently proved a key result about the growth of quantum complexity under random circuits. The authors leveraged the mathematical toolbox of t-designs, finite collections of unitaries that approximate completely random unitaries. A t-design is a probability distribution, over unitaries, whose first t moments equal the Haar measure's moments[20–22]. The Haar measure is the unique

[1]Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, Berlin, Germany. [2]Helmholtz-Zentrum Berlin für Materialien und Energie, Berlin, Germany. [3]Institute for Theoretical Physics, University of Cologne, Cologne, Germany. [4]ITAMP, Harvard-Smithsonian Center for Astrophysics, Cambridge, MA, USA. [5]Department of Physics, Harvard University, Cambridge, MA, USA. [6]Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA, USA. [7]Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA, USA. [8]Institute for Physical Science and Technology, University of Maryland, College Park, MD, USA. ✉e-mail: jonas.haferkamp@fu-berlin.de

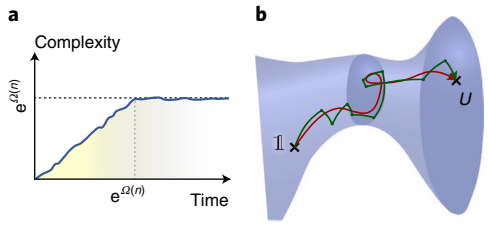

Fig. 1 | The geometric approach to complexity provides a strong intuitive and physical basis for the complexity growth conjecture that we prove. **a**, The complexity has been conjectured to grow linearly under random quantum circuits until times exponential in the number n of qubits[4]. **b**, The blue region depicts part of the space of n-qubit unitaries. A unitary U has a complexity that we define as the minimal number of two-qubit gates necessary to effect U (green jagged path; each path segment represents a gate). Nielsen's complexity[9–12], involved in ref. [4], attributes a high metric cost to directions associated with nonlocal operators. In this geometry, the unitary's complexity is the shortest path that connects $\mathbb{1}$ to U (red line). Nielsen's geometry suggests the toolbox of differential geometry, avoiding circuits' discreteness. The circuit complexity upper-bounds Nielsen's complexity; opposite bounds hold for approximate circuit complexity[12].

unitarily invariant probability measure over a compact group. Reference [19] proved that quantum complexity robustly grows polynomially in a random circuit's size. The complexity's growth was shown to be linear in the circuit's size if the local Hilbert-space dimension is large.

We prove that the complexity of a random circuit grows linearly with time (with the number of gates applied). We consider unitaries constructed from quantum circuits composed of Haar-random two-qubit gates. The focus of our proof is the set of unitaries that can be generated with a fixed arrangement of gates. We show that this set's dimension, which we call accessible dimension, serves as a good proxy for the quantum complexity of almost every unitary in the set. Our bound on the complexity holds for all random circuits described above, with probability 1. Instead of invoking unitary designs[19] or Nielsen's geometric approach[9–12], we employ elementary aspects of differential topology and algebraic geometry, combined with an inductive construction of Clifford circuits. The latter are circuits that transform Pauli strings to Pauli strings up to a phase[23–27].

This work is organized as follows. First, we introduce the set-up and definitions. Second, we present the main result, the complexity's exponentially long linear growth. Third, we present a high-level overview of the proof. The key mathematical steps follow, in the Methods. Two corollaries follow: an extension to random arrangements of gates and an extension to slightly imperfect gates. In the Discussion we compare our results with known results and explain our work's implications for various subfields of quantum physics. Finally, we discuss the opportunities engendered by this work. In Supplementary Appendix A we review the elementary algebraic geometry required for the proof. Proof details are provided in Supplementary Appendix B. We elaborate on states' complexities in Supplementary Appendix C. We prove two corollaries in Supplementary Appendices D and E. Finally, we compare notions of circuit complexity in Supplementary Appendix F.

Preliminaries. This work concerns a system of n qubits. For convenience, we assume that n is even. We simplify tensor-product notation as $|0^k\rangle := |0\rangle^{\otimes k}$, for $k=1,2,\ldots,n$, and $\mathbb{1}_k$ denotes the k-qubit identity operator. Let $U_{j,k}$ denote a unitary gate that operates on qubits j and k. Such gates need not couple the qubits together and need not be geometrically local. An architecture is an arrangement of some fixed number R of gates (Fig. 2a).

Definition 1. (Architecture) *An architecture is a directed acyclic graph that contains $R \in \mathbb{Z}_{>0}$ vertices (gates). Two edges (qubits) enter each vertex, and two edges exit.*

Figure 2b,c illustrates example architectures governed by our results.

- A brickwork is the architecture of any circuit formed as follows. Apply a string of two-qubit gates: $U_{1,2} \otimes U_{3,4} \otimes \ldots \otimes U_{n-1,n}$. Then apply a staggered string of gates, as shown in Fig. 2b. Perform this pair of steps T times in total, using possibly different gates each time.
- A staircase is the architecture of any circuit formed as in Fig. 2c. Apply a stepwise string of two-qubit gates: $U_{n,n-1}U_{n-2,n-1}\ldots U_{2,1}$. Repeat this process T times, using possibly different gates each time.

The total number of gates in the brickwork architecture, as in the staircase architecture, is $R=(n-1)T$. Our results extend to more general architectures, for example, the architecture depicted in Fig. 2a and architectures of non-nearest-neighbour gates. Circuits of a given architecture can be formed randomly.

Definition 2. (Random quantum circuit) *Let A denote an arbitrary architecture. A probability distribution can be induced over the architecture-A circuits as follows: for each vertex in A, draw a gate Haar-randomly from SU(4). Then contract the unitaries along the edges of A. Each circuit so constructed is called a random quantum circuit.*

Implementing a unitary with the optimal gates, in the optimal architecture, concretizes the notion of complexity.

Definition 3. (Exact circuit complexities) Let $U \in \mathrm{SU}(2^n)$ denote an n-qubit unitary. The (exact) circuit complexity $\mathcal{C}_\mathrm{u}(U)$ is the least number of two-qubit gates in any circuit that implements U. Similarly, let $|\psi\rangle$ denote a pure quantum state vector. The (exact) state complexity $\mathcal{C}_\mathrm{state}(|\psi\rangle)$ is the least number r of two-qubit gates $U_1, U_2, \ldots, U_r$, arranged in any architecture, such that $U_1 U_2 \ldots U_r |0^n\rangle = |\psi\rangle$.

We now define a backwards light cone, a concept that helps us focus on sufficiently connected circuits. Consider creating two vertical cuts in a circuit (dashed lines, Fig. 2). The gates between the cuts form a block. We say that a block contains a backwards light cone if some qubit t links to each other qubit t' via a directed path of gates (a path that may be unique to t'). The backwards light cone consists of the gates in the paths.

Main result, linear growth of complexity in random quantum circuits. Our main result is a lower bound on the complexities of random unitaries and states. The bound holds with unit probability.

Theorem 1. (Linear growth of complexity) *Let U denote a unitary implemented by a random quantum circuit in an architecture formed by concatenating T blocks of $\leq L$ gates each, each block containing a backwards light cone. The unitary's circuit complexity is lower-bounded as*

$$\mathcal{C}_\mathrm{u}(U) \geq \frac{R}{9L} - \frac{n}{3}, \tag{1}$$

with unit probability, until the number of gates grows to $T \geq 4^n - 1$. The same bound holds for $\mathcal{C}_\mathrm{state}(U|0^n\rangle)$, until $T \geq 2^{n+1} - 1$.

The theorem governs all architectures that contain enough backwards light cones. The brickwork architecture forms a familiar special case. Let us choose for a brickwork's blocks to contain $2n$ of the columns in Fig. 2b. Each block contains $L=n(n-1)$ gates (in the absence of periodic boundary conditions), yielding the lower bound $\mathcal{C}_\mathrm{u}(U) \geq \frac{R}{9n(n-1)} - \frac{n}{3}$. Another familiar example is the staircase architecture. A staircase's blocks can have the least L possible, $n-1$, which yields the strongest bound.

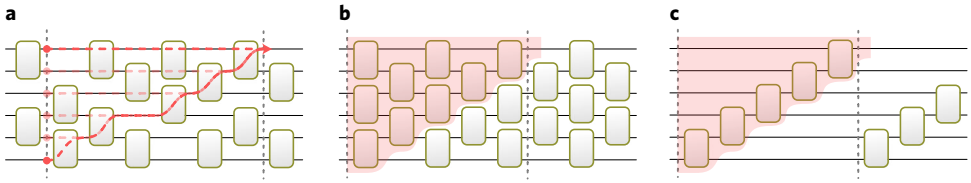

Fig. 2 | Our result relies on architectures and their backwards light cones. a, An architecture specifies how R two-qubit gates are arranged in an n-qubit circuit. The gates need not be applied to neighbouring qubits, although they are depicted in this way for convenience. Our result involves blocks with the following property: the block contains a qubit reachable from each other qubit via a path (red dashed line), possibly unique to the latter qubit, that passes only through gates in the block. **b**, The brickwork architecture interlaces layers of gates on a one-dimensional (1D) chain. In a 1D architecture with geometrically local gates, such as the brickwork architecture, each block has a backwards light cone (light red region) that touches the qubit chain's edges. In the brickwork architecture, a minimal backwards-light-cone-containing block consists of ~n^2 gates. **c**, The staircase architecture, too, acts on a 1D qubit chain. The circuit consists of layers in which $n-1$ gates act on consecutive qubit pairs. A minimal backwards-light-cone-containing block consists of $n-1$ gates.

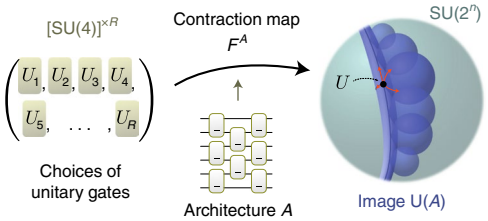

Fig. 3 | The *R*-gate architecture *A* is associated with a contraction map F^A. F^A maps a list of input gates (a point in $[SU(4)]^{\times R}$) to an n-qubit unitary U in $SU(2^n)$. The unitary results from substituting the gates into the architecture. F^A has an image $\mathcal{U}(A)$, which consists of the unitaries implementable with the architecture. A has an accessible dimension, d_A, equal to the dimension of $\mathcal{U}(A)$. Our core technical result is that d_A grows linearly with R. To bridge this result to complexity, consider an arbitrary architecture A' formed from fewer gates than a constant fraction of R. Such an architecture's accessible dimension satisfies $d_{A'} < d_A$, as we show. Therefore, every unitary in $\mathcal{U}(A)$ has a complexity linear in R, except for a measure-0 set. The proof relies on algebraic geometry. A key concept is the rank of F^A at a point. The rank counts the local degrees of freedom in the image (orange arrows).

High-level overview of the proof of Theorem 1. Consider fixing an R-gate architecture A, then choosing the gates in the architecture. The resulting circuit implements some n-qubit unitary. All the unitaries implementable with A form a set $\mathcal{U}(A)$ (compare Fig. 3). Our proof relies on properties of $\mathcal{U}(A)$—namely, on the number of degrees of freedom in $\mathcal{U}(A)$. We define this number as the architecture's accessible dimension, $d_A = \dim(\mathcal{U}(A))$ (Fig. 3. The following section contains a formal definition; here, we provide intuition. As the n-qubit unitaries form a space of dimension 4^n, $d_A \in [0, 4^n]$. The greater the d_A, the more space $\mathcal{U}(A)$ fills in the set of n-qubit unitaries. Considering $\mathcal{U}(A)$ circumvents the intractability of calculating a unitary's circuit complexity. To better understand the form of $\mathcal{U}(A)$, we study the set's dimension, which is the accessible dimension. Importantly, the accessible dimension enables us to compare the sets $\mathcal{U}(A)$ generated by different architectures. Distinct accessible dimensions imply that the lower-dimensional set has measure zero in the higher-dimensional set. As a proxy for quantum complexity, the accessible dimension plays a role similar to t-designs in refs. [19,28]. Our first technical result lower-bounds the sufficiently connected architecture's accessible dimension.

Proposition 1. (Lower bound on accessible dimension) *Let A_T denote an architecture formed by concatenating T blocks of $\leq L$ gates each, each block containing a backwards light cone. The architecture's accessible dimension is lower-bounded as*

$$d_{A_T} \geq T \geq \frac{R}{L}. \tag{2}$$

We can upper-bound d_A, for an arbitrary architecture A, by counting parameters. To synopsize the argument in Supplementary Appendix B, 15 real parameters specify each two-qubit unitary. Each qubit shared by two unitaries makes three parameters redundant. Hence

$$d_A \leq 9R + 3n. \tag{3}$$

The accessible dimension reaches its maximal value, 4^n, after a number of gates exponential in n. Similarly, the circuit complexity reaches its maximal value after exponentially many gates. This parallel suggests d_A as a proxy for the circuit complexity. The next section justifies the use of d_A as a proxy.

The proof of Theorem 1 revolves around the accessible dimension d_{A_T} of a certain R-gate architecture A_T. The main idea is as follows. Let R' be less than a linear fraction of R. More specifically, let $9R' + 3n < T = R/L$. For every R'-gate architecture A', $d_{A'} < d_{A_T}$ holds by a combination of equations (2) and (3). Consequently, Supplementary Appendix B shows that $\mathcal{U}(A')$ has zero probability in $\mathcal{U}(A_T)$, according to the measure in Definition 2. Therefore, almost every unitary $U \in \mathcal{U}(A_T)$ has a complexity greater than the greatest possible R'. Inequality (1) follows.

Discussion

We have proven a prominent physics conjecture proposed by Brown and Susskind for random quantum circuits[4,14]: a local random circuit's quantum complexity grows linearly in the number of gates until reaching a value exponential in the system size. To prove this conjecture, we have introduced a technique for bounding complexity. The proof rests on our connecting the quantum complexity to the accessible dimension, the dimension of the set of unitaries implementable with a given architecture (arrangement of gates). Our core technical contribution is a lower bound on the accessible dimension. The bound rests on techniques from differential topology and algebraic geometry.

Theorem 1 is a rigorous demonstration of the linear growth of random qubit circuits' complexities for exponentially long times. The bound holds until the complexity reaches $\mathcal{C}_u(U) = \Omega(4^n)$—the scaling, up to polynomial factors, of the greatest complexity achievable by any n-qubit unitary[29]. One hurdle has stymied attempts to prove that the quantum complexity of local random circuits grows linearly: most physical properties (described with, for example, local observables or correlation functions) reach fixed values in times subexponential in the system size. One must progress beyond such properties to prove that the complexity grows linearly at

superpolynomial times. We overcome this hurdle by identifying the accessible dimension as a proxy for the complexity.

Theorem 1 complements another rigorous insight about complexity growth. In ref. [19], the linear growth of complexity is proven in the limit of large local dimension q and for a strong notion of quantum circuit complexity, with help from ref. [30]. Furthermore, depth-T random qubit circuits have complexities that scale as $\Omega(T^{1/11})$ until $T=\exp(\Omega(n))$ (refs. [19,22]). The complexity scales the same way for other types of random unitary evolution, such as a continuous-time evolution under a stochastically fluctuating Hamiltonian[31]. Finally, ref. [19] addresses bounds on convergence to unitary designs[22,30–32], translating these bounds into results about circuit complexity. Theorem 1 is neither stronger nor weaker than the results of ref. [19], which govern a more operational notion of complexity—how easily $U|0^n\rangle\langle 0^n|U^\dagger$ can be distinguished from the maximally mixed state.

Our work is particularly relevant to the holographic context surrounding the Brown–Susskind conjecture. There, random quantum circuits are conjectured to serve as proxies for chaotic quantum dynamics generated by local time-independent Hamiltonians[33]. Reference [34] has introduced this conjecture into black hole physics, and ref. [1] has discussed the conjecture in the context of holography. A motivation for invoking random circuits is that random circuits can be analysed more easily than time-independent Hamiltonian dynamics. Time-independent Hamiltonian dynamics are believed to be mimicked also by time-fluctuating Hamiltonians[31] and by random ensembles of Hamiltonians. Furthermore, complexity participates in analogies with thermodynamics, such as a second law of quantum complexity[4]. Our techniques can be leveraged to construct an associated resource theory of complexity[35].

In the context of holography, the complexities of thermofield double states have attracted recent interest[1,36–38]. Thermofield double states are pure bipartite quantum states for which each subsystem's reduced state is thermal. In the context of holography, thermofield double states are dual to eternal black holes in anti-de-Sitter space[36]. Such a black hole's geometry consists of two sides connected by a wormhole, or Einstein–Rosen bridge. The wormhole's volume grows for a time exponential in the number of degrees of freedom of the boundary theory[1,4]. As discussed above, random quantum circuits are expected to capture the (presumed Hamiltonian) dynamics behind the horizon. If they do, the growth of the wormhole's volume is conjectured to match the growth of the boundary state's complexity[1,2,4]; both are expected to reach a value exponentially large in the number of degrees of freedom. Our results govern the random circuit that serves as a proxy for the dynamics behind the horizon. That random circuit's complexity, our results show strikingly, indeed grows to exponentially large values. This conclusion reinforces the evidence that quantum circuit complexity is the right quantity with which to resolve the wormhole-growth paradox[1].

Outlook

Our main result governs exact circuit complexity. In Supplementary Corollary 2, we generalize the result to a slightly robust notion of circuit complexity. There, the complexity depends on our tolerance of the error in the implemented unitary. Yet, the error tolerance can be uncontrollably small. The main challenge in extending our results to approximate complexity is that the accessible dimension crudely characterizes the set of unitaries implementable with a given architecture. Consider attempting to enlarge this set to include all the n-qubit unitaries that lie close to the set in some norm. The enlarged set's dimension is 4^n. The reason for this is that the enlargement happens in all directions of $\mathrm{SU}(2^n)$. Therefore, our argument does not work as for the exact complexity. Extending our results to approximations therefore offers an opportunity for future work. Approximations may also illuminate random circuits as instruments for identifying quantum advantages[39,40]; they would show that a polynomial-size quantum circuit cannot be compressed substantially while achieving a good approximation. These observations motivate an uplifting of the present work to robust notions of quantum circuit complexity allowing for implementation errors in the distinguishability of states or channels[41] (see, for example, ref. [19]). A possible uplifting might look as follows. Let A denote an R-gate architecture, and let A' denote an R'-gate architecture. Suppose that the accessible dimensions obey $d_{A'}<d_A$. A unitary implemented with A has no chance of occupying the set $\mathcal{U}(A')$, which has a smaller dimension than $\mathcal{U}(A)$. Consider enlarging $\mathcal{U}(A')$ to include the unitaries that lie ϵ-close, for some $\epsilon>0$. If $\mathcal{U}(A')$ is sufficiently smooth and well-behaved, we expect the enlarged set's volume, intersected with $\mathcal{U}(A)$, to scale as $\sim\epsilon^{d_A-d_{A'}}$. Furthermore, suppose that unitaries implemented with A are distributed sufficiently evenly in $\mathcal{U}(A)$ (rather than being concentrated close to $\mathcal{U}(A')$). All the unitaries in $\mathcal{U}(A)$ except a small fraction $\sim\epsilon^{d_A-d_{A'}}$ could not lie in $\mathcal{U}(A')$. We expect, therefore, that all the unitaries in $\mathcal{U}(A)$ except a fraction $\sim\epsilon^{d_A-d_{A'}}$ have ϵ-approximate complexities greater than R'.

A related opportunity is a proof that Nielsen's geometric complexity measure grows linearly under random circuits. Such a proof probably requires a more refined characterization of $\mathcal{U}(A)$ than its dimension. The quantum complexity in Theorem 1 does not lower-bound Nielsen's complexity. Hence our main results do not immediately imply a similar bound for Nielsen's complexity. However, proving the approximate circuit complexity's linear growth would suffice to lower-bound Nielsen's complexity because of the known inequalities between Nielsen's complexity and the circuit complexity (Fig. 1b; for example, ref. [12]).

We expect our machinery based on geometry[42–47] and properties of the Clifford[27,48,49] group to be applicable to random processes that more closely reflect a variety of systems that are studied in the many-body physics community. Examples include randomly fluctuating dynamics[31], which implement random quantum circuits when Trotterized, and thermofield double states undergoing random 'shocks'[5,50,51]. Additionally, hybrid circuits—random unitary circuits punctuated by intermediate measurements—have recently attracted much interest[52,53], as the amount of entanglement present in such systems appears to undergo phase transitions induced by the rate at which they are measured. A generalization of the accessible dimension to such systems might reveal to what extent circuit complexity, as a measure of entanglement in deep dynamics, undergoes similar phase transitions. We hope that the present work, by innovating machinery for addressing complexity, stimulates further quantitative studies of holography, scrambling and chaotic quantum dynamics.

Online content

Any methods, additional references, Nature Research reporting summaries, source data, extended data, supplementary information, acknowledgements, peer review information; details of author contributions and competing interests; and statements of data and code availability are available at https://doi.org/10.1038/s41567-022-01539-6.

Received: 5 July 2021; Accepted: 4 February 2022;
Published online: 28 March 2022

References

1. Susskind, L. Computational complexity and black hole horizons. *Fortsch. Phys.* **64**, 24–43 (2016).
2. Stanford, D. & Susskind, L. Complexity and shock wave geometries. *Phys. Rev. D.* **90**, 126007 (2014).
3. Brown, A. R., Roberts, D. A., Susskind, L., Swingle, B. & Zhao, Y. Complexity, action and black holes. *Phys. Rev. D.* **93**, 086006 (2016).
4. Brown, A. R. & Susskind, L. Second law of quantum complexity. *Phys. Rev. D.* **97**, 086015 (2018).
5. Bouland, A., Fefferman, B. & Vazirani, U. Computational pseudorandomness, the wormhole growth paradox and constraints on the AdS/CFT duality. In *Proc. ITCS'20* (2020).

6. Brown, A. R., Roberts, D. A., Susskind, L., Swingle, B. & Zhao, Y. Holographic complexity equals bulk action? *Phys. Rev. Lett.* **116**, 191301 (2016).
7. Poulin, D., Qarry, A., Somma, R. & Verstraete, F. Quantum simulation of time-dependent Hamiltonians and the convenient illusion of Hilbert space. *Phys. Rev. Lett.* **106**, 170501 (2011).
8. Gosset, D., Kliuchnikov, V., Mosca, M. & Russo, V. An algorithm for the *T*-count. *Quant. Inf. Comput.* **14**, 1277–1301 (2014).
9. Nielsen, M. A. A geometric approach to quantum circuit lower bounds. Preprint at https://arxiv.org/abs/quant-ph/0502070 (2005).
10. Nielsen, M. A., Dowling, M. R., Gu, M. & Doherty, A. C. Quantum computation as geometry. *Science* **311**, 1133–1135 (2006).
11. Nielsen, M. A., Dowling, M. R., Gu, M. & Doherty, A. C. Optimal control, geometry and quantum computing. *Phys. Rev. A* **73**, 062323 (2006).
12. Dowling, M. R. & Nielsen, M. A. The geometry of quantum computation. *Quant. Inf. Comput.* **8**, 861–899 (2008).
13. Eisert, J. Entangling power and quantum circuit complexity. *Phys. Rev. Lett.* **127**, 020501 (2021).
14. Susskind, L. Black holes and complexity classes. Preprint at https://arxiv.org/abs/1802.02175 (2018).
15. Eisert, J., Friesdorf, M. & Gogolin, C. Quantum many-body systems out of equilibrium. *Nat. Phys.* **11**, 124–130 (2015).
16. Polkovnikov, A., Sengupta, K., Silva, A. & Vengalattore, M. Nonequilibrium dynamics of closed interacting quantum systems. *Rev. Mod. Phys.* **83**, 863–883 (2011).
17. Swingle, B. Unscrambling the physics of out-of-time-order correlators. *Nat. Phys.* **14**, 988–990 (2018).
18. Maldacena, J., Shenker, S. H. & Stanford, D. A bound on chaos. *J. High Energy Phys.* **1608**, 106 (2016).
19. Brandao, F. G. S. L., Chemissany, W., Hunter-Jones, N., Kueng, R. & Preskill, J. Models of quantum complexity growth. *PRX Quantum* **2**, 030316 (2021).
20. Gross, D., Audenaert, K. M. R. & Eisert, J. Evenly distributed unitaries: on the structure of unitary designs. *J. Math. Phys.* **48**, 052104 (2007).
21. Dankert, C., Cleve, R., Emerson, J. & Livine, E. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A* **80**, 012304 (2009).
22. Brandão, F. G. S. L., Harrow, A. W. & Horodecki, M. Local random quantum circuits are approximate polynomial-designs. *Commun. Math. Phys.* **346**, 397–434 (2016).
23. Bolt, B., Room, T. G. & Wall, G. E. On the Clifford collineation, transform and similarity groups. I. *J. Austr. Math. Soc.* **2**, 60–79 (1961).
24. Bolt, B., Room, T. G. & Wall, G. E. On the Clifford collineation, transform and similarity groups. II. *J. Austr. Math. Soc.* **2**, 80–96 (1961).
25. Calderbank, A. R., Rains, E. M., Shor, P. W. & Sloane, N. J. A. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.* **78**, 405 (1997).
26. Calderbank, A. R., Rains, E. M., Shor, P. M. & Sloane, N. J. A. Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory* **44**, 1369–1387 (1998).
27. Gottesman, D. Stabilizer codes and quantum error correction. Preprint https://arxiv.org/abs/quant-ph/9705052 (1997).
28. Brandão, F. G. S. L., Harrow, A. W. & Horodecki, M. Efficient quantum pseudorandomness. *Phys. Rev. Lett.* **116**, 170502 (2016).
29. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2000).
30. Hunter-Jones, N. Unitary designs from statistical mechanics in random quantum circuits. Preprint at https://arxiv.org/abs/1905.12053 (2019).
31. Onorati, E. et al. Mixing properties of stochastic quantum Hamiltonians. *Commun. Math. Phys.* **355**, 905 (2017).
32. Nakata, Y., Hirche, C., Koashi, M. & Winter, A. Efficient quantum pseudorandomness with nearly time-independent Hamiltonian dynamics. *Phys. Rev. X* **7**, 021006 (2017).
33. Nahum, A., Vijay, S. & Haah, J. Operator spreading in random unitary circuits. *Phys. Rev. X* **8**, 021014 (2018).
34. Hayden, P. & Preskill, J. Black holes as mirrors: quantum information in random subsystems. *J. High Energy Phys.* **0709**, 120 (2007).
35. Yunger Halpern, N. et al. Resource theory of quantum uncomplexity. Preprint at https://arxiv.org/abs/2110.11371 (2021).
36. Maldacena, J. M. Eternal black holes in anti-de Sitter. *J. High Energy Phys.* **04**, 021 (2003).
37. Chapman, S. et al. Complexity and entanglement for thermofield double states. *SciPost Phys.* **6**, 034 (2019).
38. Susskind, L. Entanglement is not enough. Preprint at https://arxiv.org/abs/1411.0690 (2014).
39. Neill, C. et al. A blueprint for demonstrating quantum supremacy with superconducting qubits. Prepreint at https://arxiv.org/abs/1709.06678 (2017).
40. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).
41. Watrous, J. Semidefinite programs for completely bounded norms. *Theory Comput* **5**, 217–238 (2009).
42. Bochnak, J., Coste, M. & Roy, M.-F. *Real Algebraic Geometry* Vol. 36 (Springer, 2013).
43. Hall, B. *Lie Groups, Lie Algebras and Representations: an Elementary Introduction* Vol. 222 (Springer, 2015).
44. Lee, J. M. in *Introduction to Smooth Manifolds* (eds Axler, s. & Ribet, K.) 1–31, 2nd edn (Springer, 2013).
45. Milne, J. S. *Algebraic Groups: the Theory of Group Schemes of Finite Type over a Field* Vol. 170 (Cambridge Univ. Press, 2017).
46. Sard, A. Hausdorff measure of critical images on Banach manifolds. *Am. J. Math.* **87**, 158–174 (1965).
47. Khaneja, N. & Glaser, S. Cartan decomposition of $SU(2^n)$, constructive controllability of spin systems and universal quantum computing. Preprint at https://arxiv.org/abs/quant-ph/0010100 (2000).
48. Cleve, R., Leung, D., Liu, L. & Wang, C. Near-linear constructions of exact unitary 2-designs. *Quant. Inf. Comput.* **16**, 0721–0756 (2016).
49. Aaronson, S. & Gottesman, D. Improved simulation of stabilizer circuits. *Phys. Rev. A* **70**, 052328 (2004).
50. Shenker, S. H. & Stanford, D. Black holes and the butterfly effect. *J. High Energy Phys.* **2014**, 67 (2014).
51. Shenker, S. H. & Stanford, D. Multiple shocks. *J. High Energy Phys.* **2014**, 1–20 (2014).
52. Li, Y., Chen, X. & Fisher, M. P. A. Measurement-driven entanglement transition in hybrid quantum circuits. *Phys. Rev. B* **100**, 134306 (2019).
53. Skinner, B., Ruhman, J. & Nahum, A. Measurement-induced phase transitions in the dynamics of entanglement. *Phys. Rev. X* **9**, 031009 (2019).

Methods

Having overviewed the proof at a high level, here we fill in the key mathematics. Three points need clarifying. First, we must rigorously define the accessible dimension, or the dimension of $\mathcal{U}(A)$, which is not a manifold. Second, we must prove Proposition 1. Finally, we must elucidate steps in the proof of Theorem 1. We address these points using the toolbox of algebraic geometry. We associate with every R-gate architecture A a contraction map F^A: $\mathrm{SU}(4)^{\times R} \to \mathrm{SU}(2^n)$. This function maps a list of gates to an n-qubit unitary. The unitary results from substituting the gates into the architecture A (Fig. 3). The map contracts every edge (qubit) shared by two vertices (gates) in A.

The image of F^A is the set $\mathcal{U}(A)$ of unitaries implementable with the architecture A. $\mathcal{U}(A)$ is a semialgebraic set, consisting of the solutions to a finite set of polynomial equations and inequalities over the real numbers (Supplementary Appendix A provides a review). That $\mathcal{U}(A)$ is a semialgebraic set follows from the Tarski–Seidenberg principle, a deep result in semialgebraic geometry (Supplementary Appendix A). A semialgebraic set's dimension quantifies the degrees of freedom needed to describe the set locally. More precisely, a semialgebraic set decomposes into manifolds. The greatest dimension of any such manifold equals the semialgebraic set's dimension. The dimension of $\mathcal{U}(A)$ is the architecture A's accessible dimension. More restricted than a semialgebraic set is an algebraic set, which consists of the solutions to a finite set of polynomial equations.

Just as the contraction map's image will prove useful, so will the map's rank, defined as follows. Let $x = (U_1, U_2, \ldots, U_R) \in \mathrm{SU}(4)^{\times R}$ denote an input into F^A, such that the U_j denote two-qubit gates. The map's rank at x is the rank of a matrix that approximates F^A linearly around x (the rank of the map's Jacobian at x). The rank is low at x if perturbing x can influence the n-qubit unitary only along few directions in $\mathrm{SU}(2^n)$.

Crucially, we prove that F^A has the same rank throughout the domain, except on a measure-zero set, where F^A has a lesser rank. The greater, 'dominating' rank is the dimension of $\mathcal{U}(A)$. To formalize this result, let E_r denote the locus of points at which F^A has a rank of $r \geq 0$. Let $E_{<r} = \bigcup_{r' < r} E_{r'}$ denote the set of points where F^A has a lesser rank. Let $r_{\max}$ denote the maximum rank achieved by F^A at any point x. We prove the following lemma in Supplementary Appendix B, using the dimension theory of real algebraic sets.

Lemma 1. (Low-rank locus) *The low-rank locus $E_{<r_{\max}}$ is an algebraic set of measure 0 and so is closed (in the Lie-group topology). Equivalently, $E_{r_{\max}}$ is an open set of measure 1. Consequently, $d_A = r_{\max}$.*

Lemma 1 guarantees that the contraction map's rank equals the accessible dimension d_A almost everywhere in $\mathcal{U}(A)$.

We now turn to the proof of Proposition 1. The rank r of F^A at each point x lower-bounds $r_{\max}$, by definition. Consider an architecture A_T of T blocks, each containing a backwards light cone. We identify an x at which r is lower-bounded by a quantity that grows linearly with R (the number of gates in the architecture A_T). We demonstrate the point's existence by constructing circuits from Clifford gates.

Consider a choice $x = (U_1, U_2, \ldots, U_R) =: (U_j)_j$ of unitary gates. Perturbing a U_j amounts to appending an infinitesimal unitary: $U_j \mapsto \tilde{U}_j = e^{i\epsilon H} U_j$. The H denotes a two-qubit Hermitian operator and $\epsilon \in \mathbb{R}$. H can be written as a linear combination of two-qubit Pauli strings S_k. (An n-qubit Pauli string is a tensor product of n single-site operators, each of which is a Pauli operator [X, Y or Z] or the identity, $\mathbb{1}_1$. The 4^n n-qubit Pauli strings form a basis for the space of n-qubit Hermitian operators.) Consider perturbing each gate U_j using a combination of all 15 nontrivial two-qubit Pauli strings (Supplementary Fig. 4a): $x = (U_j)_j \mapsto \tilde{x} = (\exp(i \sum_{k=1}^{15} \epsilon_{j,k} S_k) U_j)_j$, wherein $\epsilon_{j,k} \in \mathbb{R}$. The perturbation $x \mapsto \tilde{x}$ causes a perturbation $U = F^{A_T}(x) \mapsto \tilde{U} = F^{A_T}(\tilde{x})$ of the image under F^{A_T}. The latter perturbation is, to first order, $\partial_{\epsilon_{j,k}} \tilde{U}|_{\epsilon_{j,k}=0}$. This derivative can be expressed as the original circuit with the Pauli string S_k inserted immediately after the gate U_j (Supplementary Fig. 4b).

The rank of F^{A_T} at x is the number of parameters $\epsilon_{j,k}$ needed to parameterize a general perturbation of $U = F^{A_T}(x)$ within the image set $\mathcal{U}(A_T)$. To lower-bound the rank of F^{A_T} at a point x, we need only show that $\geq r$ parameters $\epsilon_{j,k}$ perturb $F^{A_T}(x)$ in independent directions. To do so, we express the derivative as

$$\partial_{\epsilon_{j,k}} F^{A_T}(\tilde{x})|_{\epsilon_{j,k}=0} = K_{j,k} F^{A_T}(x), \tag{4}$$

where $K_{j,k}$ denotes a Hermitian operator (Supplementary Fig. 4c). $K_{j,k}$ results from conjugating S_k, the Pauli string inserted into the circuit after gate U_j, with the later gates. The physical significance of $K_{j,k}$ follows from perturbing the gate U_j in the direction S_k by an infinitesimal amount $\epsilon_{j,k}$. The image $F^{A_T}(x)$ is consequently perturbed, in $\mathrm{SU}(2^n)$, in the direction $K_{j,k}$.

We choose for the gates U_j to be Clifford operators. The Clifford operators are the operators that map the Pauli strings to the Pauli strings, to within a phase, via conjugation. For every Clifford operator C and Pauli operator P, $CPC^\dagger$ equals a phase times a Pauli string by definition of the Clifford group. As a result, the operators $K_{j,k}$ are Pauli strings (up to a phase). Two Pauli strings are linearly independent if and only if they differ. For Clifford circuits, therefore, we can easily verify whether perturbations of x cause independent perturbation directions in $\mathrm{SU}(2^n)$: we need only show that the resulting operators $K_{j,k}$ are distinct.

We apply that fact to prove Proposition 1, using the following observation. Consider any Pauli string P and any backwards-light-cone-containing block of any architecture. We can insert Clifford gates into the block such that two operations are equivalent: (1) operating on the input qubits with P before the extended block and (2) operating with the extended block, then with a one-qubit Z. Supplementary Fig. 4d depicts the equivalence, which follows from the structure of backwards light cones. We can iteratively construct a Clifford unitary that reduces the Pauli string's weight until producing a single-qubit operator. See Supplementary Appendix B for details.

We now prove Proposition 1 by recursion. Consider an R'-gate architecture $A_{T'}$ formed from $T' < 4n-1$ blocks, each containing a backwards light cone and each of $\leq L$ gates. Assume that there exists a list x' of Clifford gates, which can be slotted into $A_{T'}$, such that $F^{A_{T'}}$ has a rank $\geq T'$ at x'. Consider appending a backwards-light-cone-containing block to $A_{T'}$. The resulting architecture corresponds to a contraction map whose rank is $\geq T' + 1$.

By assumption, we can perturb x' such that its image, $F^{A_{T'}}(x')$, is perturbed in $\geq T'$ independent directions in $\mathrm{SU}(2^n)$. These directions can be represented by Pauli operators K'_{j_m,k_m}, wherein $m = 1, 2, \ldots, T'$, by equation (4). Let P denote any Pauli operator absent from $\{K'_{j_m,k_m}\}$. We can append to $A_{T'}$ a backwards-light-cone-containing block, forming an architecture $A_{T'+1}$ of $T' + 1$ backwards light cones. We design the new block from Clifford gates such that two operations are equivalent: (1) applying P to the input qubits before the extended blocks and (2) applying the extended block, then a single-site Z. We denote by x'' the list of gates in x' augmented with the gates in the extended block. Conjugating the K'_{j_m,k_m} with the new block yields operators K'_{j_m,k_m}, for $m = 1, 2, \ldots, T'$. They represent the directions in which the image $F^{A_{T'+1}}(x'')$ is perturbed by the original perturbations of $A_{T'}$. The K'_{j_m,k_m} are still linearly independent Pauli operators. Also, the K'_{j_m,k_m} and the single-site Z form an independent set, because P is not in $\{K'_{j_m,k_m}\}$. Meanwhile, the single-site Z is a direction in which the last block's final gate can be perturbed. The operators K_{j_m,k_m}, augmented with the single-site Z, therefore span $T' + 1$ independent directions along which $F^{A_{T'+1}}(x'')$ can be perturbed. Therefore, $T' + 1$lower-bounds the rank of $F^{A_{T'+1}}$.

We apply the above argument recursively, starting from an architecture that contains no gates. The following result emerges: consider any architecture A_T that consists of T backwards-light-cone-containing blocks. At some point x, the map F^{A_T} has a rank lower-bounded by T. Lemma 1 ensures that the same bound applies to d_{A_T}.

To conclude the proof of Theorem 1, we address an architecture A' whose accessible dimension satisfies $d_{A'} < d_{A_T}$. Consider sampling a random circuit with the architecture A_T. We must show that the circuit has a zero probability of implementing a unitary in $\mathcal{U}(A')$. To prove this claim, we invoke the constant-rank theorem: consider any map whose rank is constant locally—in any open neighbourhood of any point in the domain. In that neighbourhood, the map is equivalent to a projector, up to a diffeomorphism. We can apply the constant-rank theorem to the contraction map: F^{A_T} has a constant rank throughout $E_{r_{\max}}$, by Lemma 1. Therefore, F^{A_T} acts locally as a projector throughout $E_{r_{\max}}$—and so throughout $\mathrm{SU}(4)^{\times R}$, except on a measure-0 region, by Lemma 1. Consider mapping an image back, through a projector, to a pre-image. Suppose that the image forms a subset of dimension lower than the whole range's dimension. The backward mapping just adds degrees of freedom to the image. Therefore, the pre-image locally has a dimension less than the domain's dimension. Hence the pre-image is of measure 0 in the domain. We use the unitary group's compactness to elevate this local statement to the global statement in Theorem 1.

Data availability

No data or code have been generated in this work.

Acknowledgements

We thank A. Harrow and R. Küng for discussions and P. Varjú for introducing us to the algebraic geometrical methods used in this Article. N.Y.H. thanks S. Chapman, M. Walter and the other organizers of the 2020 Lorentz Center workshop 'Complexity: from quantum information to black holes' for inspiration. This work has been funded by the DFG (EI 519/14-1 to J.E. and J.H.; CRC 183 to J.E.), for which this is an inter-node Berlin-Cologne project, and FOR 2724 (to J.E., P.F.), by the Einstein Research Foundation, the FQXi ('Information as fuel') (to J.E., J.H.) and by an NSF grant for the Institute for Theoretical Atomic, Molecular and Optical Physics at Harvard University and the Smithsonian Astrophysical Observatory (to N.Y.H.). Administrative support was provided by the MIT CTP (N.Y.H.).

Author contributions

J.H. developed the basic proof technique. J.H., P.F., N.B.T.K., J.E. and N.Y.H. wrote the manuscript and contributed to the results.

Funding

Open access funding provided by Freie Universität Berlin

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41567-022-01539-6.

Correspondence and requests for materials should be addressed to Jonas Haferkamp.

Peer review information *Nature Physics* thanks the anonymous reviewers for their contribution to the peer review of this work.