

# Credibility of Real-World Quantum Computers (and Simulators)

Animesh Datta

Department of Physics, University of Warwick, UK

October 13, 2026

Eighth Annual UK HPC & AI Conference  
Leicester



- Samuele Ferracin, Theodoros Kapourniotis, Andrew Jackson





Department for  
Science, Innovation  
& Technology

Policy paper

## National Quantum Strategy Missions

Updated 14 December 2023

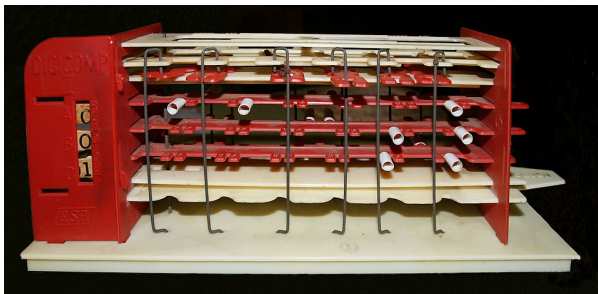
### Mission 1

By 2035, there will be accessible, UK-based quantum computers capable of running 1 trillion operations and supporting applications that provide benefits well in excess of classical supercomputers across key sectors of the economy.



# Computers?

- Quantum computer: Operates as per the laws of quantum mechanics
  - many-particle quantum mechanics
  - Quantum 2.0
- Present supercomputers are classical devices



- May use single-particle quantum mechanics – Quantum 1.0



# Quantum computer

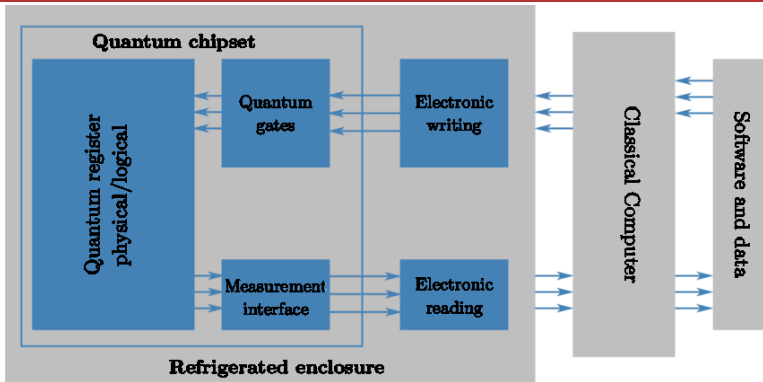


Figure: Khan/Robles-Kelly, IEEE Access, 8, 219275 (2020)

- Inputs and outputs are classical bit strings
- **Probability distributions** of classical bit strings
- Randomness in quantum measurements



# Quantum algorithms

|                                                                             |          |
|-----------------------------------------------------------------------------|----------|
| <b>Areas of application</b>                                                 | <b>8</b> |
| 1 Condensed matter physics                                                  | 10       |
| 1.1 Fermi–Hubbard model                                                     | 11       |
| 1.2 Spin models                                                             | 22       |
| 1.3 SYK model                                                               | 31       |
| 2 Quantum chemistry                                                         | 36       |
| 2.1 Simulating electrons in molecules and materials                         | 37       |
| 2.2 Simulating vibrations in molecules and materials                        | 53       |
| 3 Nuclear and particle physics                                              | 59       |
| 3.1 Quantum field theories                                                  | 60       |
| 3.2 Nuclear physics                                                         | 67       |
| 4 Combinatorial optimization                                                | 72       |
| 4.1 Search algorithms à la Grover                                           | 74       |
| 4.2 Beyond quadratic speedups in exact combinatorial optimization           | 80       |
| 5 Continuous optimization                                                   | 89       |
| 5.1 Zero-sum games: Computing Nash equilibria                               | 90       |
| 5.2 Conic programming: Solving LPs, SOCPs, and SDPs                         | 94       |
| 5.3 General convex optimization                                             | 102      |
| 5.4 Nonconvex optimization: Escaping saddle points and finding local minima | 105      |
| 6 Cryptanalysis                                                             | 109      |
| 6.1 Breaking cryptosystems                                                  | 110      |
| 6.2 Weakening cryptosystems                                                 | 119      |
| 7 Solving differential equations                                            | 123      |
| 8 Finance                                                                   | 140      |
| 8.1 Portfolio optimization                                                  | 142      |



# Quantum algorithms

|     |                                                     |     |
|-----|-----------------------------------------------------|-----|
| 8   | Finance                                             | 140 |
| 8.1 | Portfolio optimization                              | 142 |
| 8.2 | Monte Carlo methods: Option pricing                 | 150 |
| 9   | Machine learning with classical data                | 157 |
| 9.1 | Quantum machine learning via quantum linear algebra | 159 |
| 9.2 | Quantum machine learning via energy-based models    | 170 |
| 9.3 | Tensor PCA                                          | 178 |
| 9.4 | Topological data analysis                           | 182 |
| 9.5 | Quantum neural networks and quantum kernel methods  | 188 |

Figure: arXiv:2310.03011

## Quantum Algorithm for the Vlasov-Poisson System

Christensen/Goffrey/AD, arXiv:2607.28426



# Quantum algorithms

- Seek more efficient algorithms - number of operations for problem size  $n$
- More efficient **does not mean faster**: 'Clock' speeds may vary
- Desirably exponential: Polynomial, logarithmic, constant



# Credibility question

Is the output of my quantum computer correct?



# Credibility question

Is the output of my quantum computer correct?

Why would it not be?

✗ Solving wrong problem

Validation

✗ Implement wrong programme: Apply wrong gates

Verification

✗ Uncertainties in model

UQ



# Credibility question

Is the output of my quantum computer correct?

Why would it not be?

✗ Solving wrong problem

Validation

✗ Implement wrong programme: Apply wrong gates

Verification

✗ Uncertainties in model

UQ

✓ Hardware noisy and imperfect (even after error correction)

Errors: Classical  $\sim 10^{-16}$ /gate. Quantum  $\sim 10^{-2}$ /gate.

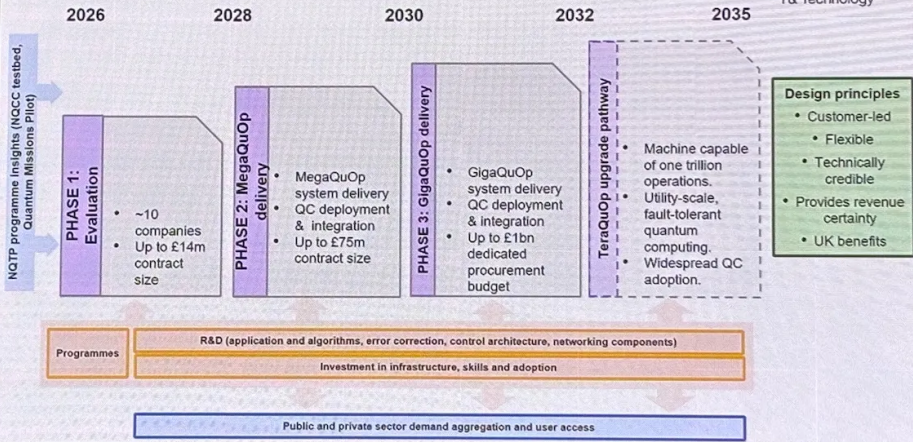


# What to pay for?

## ProQure: Scaling UK Quantum Computing



Department for  
Science, Innovation  
& Technology



# Companies



IONQ



Google

Quantum AI



QUANTINUUM

IQM

IQuEra>  
Computing Inc.



PsiQuantum

rigetti



XANADU



Microsoft



AZURE  
QUANTUM



PASQAL

Infleqtion



# Is the output of a quantum computer correct?

Solves a problem in NP : check the correctness efficiently.

- Integer factoring:  $O(\exp(n^{1/3}))$
- Shor:  $O(n^3)$ . Multiplication  $O(n^2)$

Solves a problem (not in NP) : Differential eqn., optimization, ...

- Cannot check efficiently on a classical computer

Must work independently of computation & hardware



# Mathematically,

- Outputs of quantum devices are classical probability distributions
- Real device produces  $p_{\text{real}}$  instead of  $p_{\text{ideal}}$

Is the solution correct, or close to correct?

$$VD(p_{\text{ideal}}, p_{\text{real}}) \equiv \frac{1}{2} \sum_{s=1}^{2^n} |p_{\text{ideal}}(s) - p_{\text{real}}(s)|$$

Total variation distance:  $0 \leq VD(p_{\text{ideal}}, p_{\text{real}}) \leq 1$

- ✗ Exponential to classically compute  $p_{\text{ideal}}$
- ✗ Exponential to measure  $p_{\text{real}}$



# Mathematically,

- Outputs of quantum devices are classical probability distributions
- Real device produces  $p_{\text{real}}$  instead of  $p_{\text{ideal}}$

Is the solution correct, or close to correct?

$$VD(p_{\text{ideal}}, p_{\text{real}}) \equiv \frac{1}{2} \sum_{s=1}^{2^n} |p_{\text{ideal}}(s) - p_{\text{real}}(s)| \stackrel{?}{\leq} \text{small}$$

Total variation distance:  $0 \leq VD(p_{\text{ideal}}, p_{\text{real}}) \leq 1$

- ✗ Exponential to classically compute  $p_{\text{ideal}}$
- ✗ Exponential to measure  $p_{\text{real}}$



How is it usually done?



# Classical verification of quantum computation

- Compute  $p_{\text{real}}, p_{\text{ideal}}$  classically, and compare with measured
- Cross entropy (Google), quantum volume (IBM)

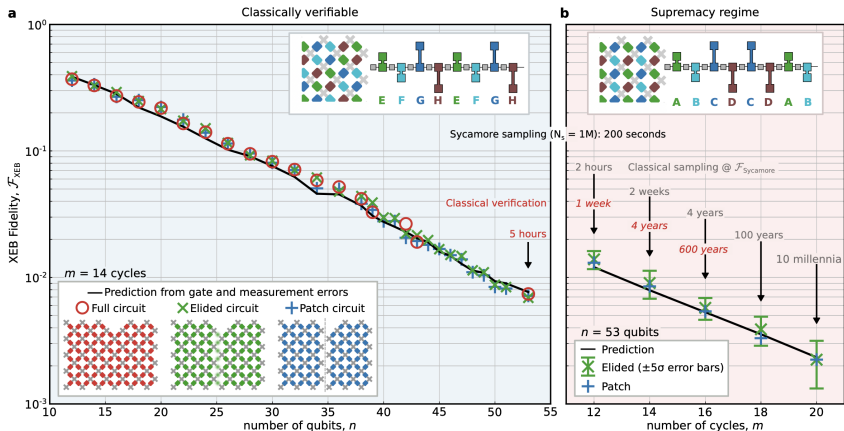


Figure: Nature, 574, 505 (2019)

# Classical verification of quantum computation

- Fidelity: Closeness of quantum states

## Sampling hard circuits with verifiably high fidelity

Simon Martiel<sup>\*1</sup>, Jay-U Chung<sup>\*1</sup>, Alireza Seif<sup>1</sup>, Soumik Ghosh<sup>2</sup>, Ian Hincks<sup>1</sup>,  
Abhinav Deshpande<sup>1</sup>, Hidetaka Manabe<sup>3</sup>, Hanfeng Gu<sup>4</sup>, Feng Pan<sup>3</sup>,  
Bill Fefferman<sup>2</sup>, Jay M. Gambetta<sup>1</sup>, and Ali Javadi-Abhari<sup>†1</sup>

<sup>1</sup>*IBM Research*      <sup>2</sup>*University of Chicago*

<sup>3</sup>*Singapore University of Technology and Design*      <sup>4</sup>*NVIDIA Corporation*

Sampling-based proposals are prominent candidates for demonstrating quantum computations beyond the reach of classical supercomputers. However, it has been difficult to combine their complexity-theoretic hardness with two capabilities needed for scalable quantum computing more generally: suppressing hardware errors, and verifying the quantum computation itself. Here we address both issues by introducing structured circuits, which, in addition to provable hardness guarantees, admit an encoding in a quantum code. This allows us to simultaneously reach high fidelities at high circuit depths, and to certify an experimental fidelity via the circuit structure and measurement of code syndromes. The resulting certificate is device dependent, but requires substantially weaker noise assumptions than existing fidelity proxy benchmarks. We demonstrate our proposal with a 64-qubit, depth-73 Clifford

Figure: [arXiv:2607.25941](https://arxiv.org/abs/2607.25941)



# Classical verification of quantum computation

- PHYS:
- Exponential – defeats the purpose
  - Impossible – Commercial secrets

Boulard *et al.*, Nat. Phys. (2018)



# Classical verification of quantum computation

- PHYS:**
- Exponential – defeats the purpose
  - Impossible – Commercial secrets

Boulund *et al.*, Nat. Phys. (2018)

**TCS:** Quantum interactive proofs

Childs, Aharonov, Ben-Or, Broadbent, Hayashi, Kashefi,...

- $\sim \mathcal{O}(|C|^3)$

Mahadev, FOCS 2018

- $\sim \mathcal{O}(|C|)$

Zhang, arXiv:2202.13997

- Assumptions: Some problems too hard for quantum computers

Scalable  $\neq$  Practical



Question: Given a quantum circuit, is the solution close to correct?

$$VD(p_{\text{ideal}}, p_{\text{real}}) \equiv \frac{1}{2} \sum_{s=1}^{2^n} |p_{\text{ideal}}(s) - p_{\text{real}}(s)| \stackrel{?}{\leq} \text{small}$$

$$0 \leq VD(p_{\text{ideal}}, p_{\text{real}}) \leq 1$$

Answer

Quantum Accreditation

Without measuring  $p_{\text{real}}$  or calculating  $p_{\text{ideal}}$ .



# Inspiration: Interactive proofs

- Hard computation: 'Target'
- Build easy 'trap' computations similar to hard computation
- Run 'trap' and 'target' computations on same hardware
- Check the correctness of the 'traps'
- Bound distance between ideal ( $p_{\text{ideal}}$ ) and actual ( $p_{\text{real}}$ ) output

Childs, Aharonov, Ben-Or, Broadbent, Fitzsimons, Kashefi, Mahadev, Olivier, ... , ... , Vidick, Zhang



# What is new?

|             | Interactive proofs | Accreditation                 |
|-------------|--------------------|-------------------------------|
| Assumptions | Hardness (LWEs)    | Easiness (Good 1-qubit gates) |
| Overheads   | Polynomial         | Constant                      |
| Model       | MBQC               | Circuit                       |

Combine the best of theoretical CS and experimental physics



## Theorem

*An  $n$ -qubit quantum computation with noise given by N1-N3, with probability  $\geq 1 - 4^{-n}$ , obeys*

$$VD(p_{\text{ideal}}, p_{\text{real}}) = \frac{1}{2} \sum_s |p_{\text{ideal}}(s) - p_{\text{real}}(s)| \leq 2\hat{p}_{\text{inc}},$$

*where  $\hat{p}_{\text{inc}}$  is the probability that a trap output is incorrect.*

Ferracin/Kapourniotis/AD, NJP, 21 113038 (2019)

Ferracin/Merkel/McKay/AD,PRA, 104, 042603 (2021)



## Theorem

*An  $n$ -qubit quantum computation with noise given by N1-N3, with probability  $\geq 1 - 4^{-n}$ , obeys*

$$VD(p_{\text{ideal}}, p_{\text{real}}) = \frac{1}{2} \sum_s |p_{\text{ideal}}(s) - p_{\text{real}}(s)| \leq 2\hat{p}_{\text{inc}},$$

*where  $\hat{p}_{\text{inc}}$  is the probability that a trap output is incorrect.*

$\hat{p}_{\text{inc}}$  is experimentally estimated to accuracy  $\theta$  with confidence  $\alpha$

$$\text{prob} \left( \left| \hat{p}_{\text{inc}} - \frac{N_{\text{inc}}}{v} \right| \leq \theta \right) \geq 1 - \alpha$$

Ferracin/Kapourniotis/AD, NJP, 21 113038 (2019)

Ferracin/Merkel/McKay/AD,PRA, 104, 042603 (2021)



**N1:** Noisy single-qubit gates are (weakly gate-dependent) CPTP maps

$$\tilde{\mathcal{U}}_j = \mathcal{E}_j(\mathcal{U}_j)$$

**N2:** Noisy state preparation, entangling gates, measurements are (operation-dependent) CPTP maps

$$\tilde{\mathcal{G}}_j = \mathcal{E}_{j,\mathcal{G}}(\mathcal{G}_j)$$

**N3:** Noise processes independent and identically distributed (iid)

Ferracin/Merkel/McKay/AD, PRA, 104, 042603 (2021)



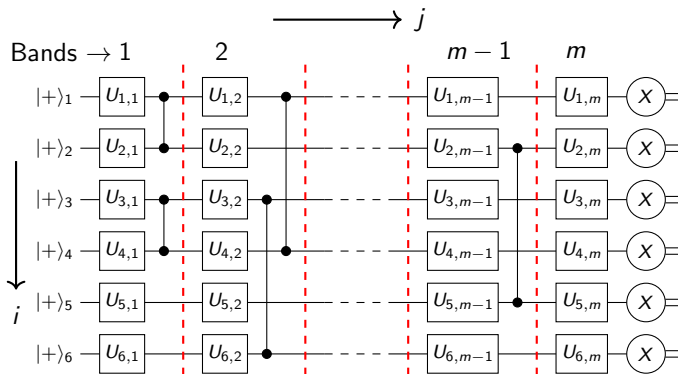
Table: Quantum Hardware Gate and Measurement Error Profiles

| Hardware        | 1-qubit (%)      | 2-qubit (%) | Measurement (%) |
|-----------------|------------------|-------------|-----------------|
| Superconducting | 0.01 – 0.05      | 0.1 – 0.5   | 0.5 – 2.0       |
| Trapped Ions    | $10^{-4}$ – 0.01 | 0.05 – 0.2  | 0.1 – 0.4       |
| Neutral Atoms   | 0.05 – 0.1       | 0.2 – 1.0   | 1.0 – 4.0       |
| Silicon Spins   | 0.05 – 0.1       | 0.5 – 1.5   | 1.0 – 3.0       |

Empirical fact: Single-qubit gates the best components in hardware



# Target

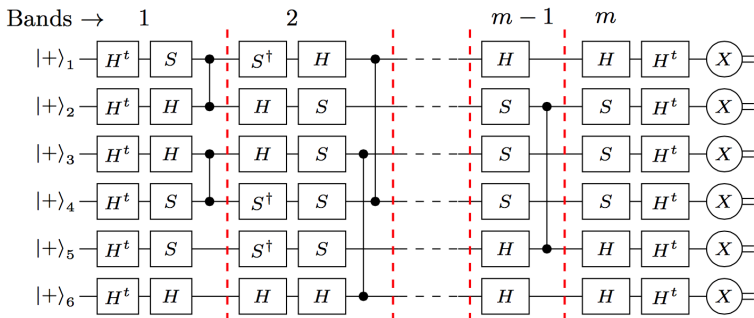


- Trap circuits of same size as target
  - Same sequence of preparations, gates, measurements
- Traps see same noise as target



# Traps

- Trap circuits are Clifford & random



- Scatter  $H$  and  $S$  gates to avoid cancelling errors in traps

If no noise, trap output = 000....0



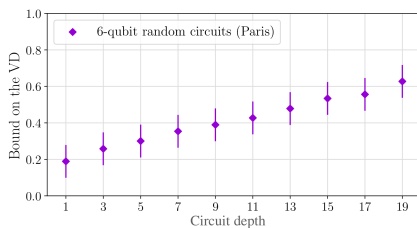
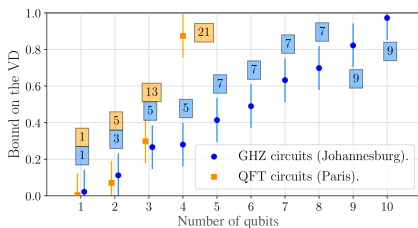
- Implement  $v$  trap computations with target on same hardware
- $v \geq \frac{\log(2/\alpha)}{2\theta^2}$  set by confidence ( $\alpha$ ) and accuracy ( $\theta$ )
- User sets confidence ( $\alpha$ ) and accuracy ( $\theta$ )
- User decides tradeoff between  $v, \alpha, \theta$

$v$  independent of

- **computational task** (simulation, optimisation, sampling, ..)
- depth and width of quantum circuit
- hardware



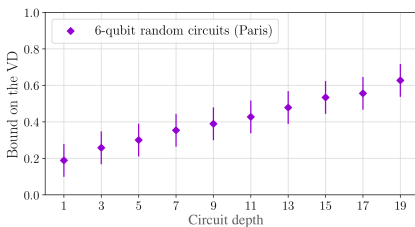
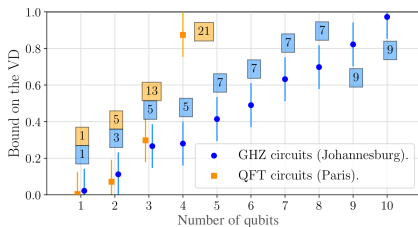
# Experiments



Ferracin/Merkel/McKay/AD, PRA, 104, 042603 (2021)

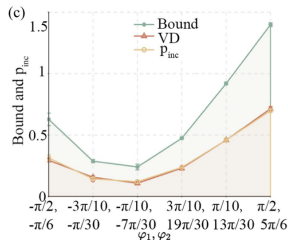
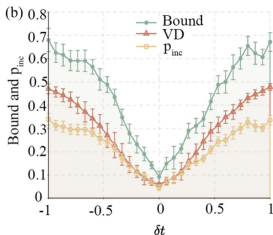
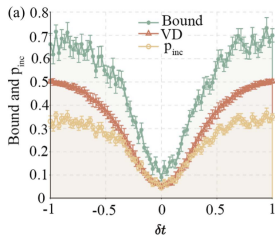


# Experiments



Ferracin/Merkel/McKay/AD, PRA, 104, 042603 (2021)

Liu et al., Chinese Optics Letters 24, 042701 (2026)



# To conclude,

Is the output of my quantum computer correct? Accreditation

- Applicability: Independent of hardware & problem (nature & size)
- Cost: Constant depending of accuracy and confidence
- 'Better' bounds rely on detailed hardware modelling
  - Not what a user could/would do
  - Impossible, Exponential



# To conclude,

Is the output of my quantum computer correct? Accreditation

- Applicability: Independent of hardware & problem (nature & size)
- Cost: Constant depending of accuracy and confidence
- 'Better' bounds rely on detailed hardware modelling
  - Not what a user could/would do
  - Impossible, Exponential

Thank you!



## Appendix



## Analogue (= continuous-time) accreditation

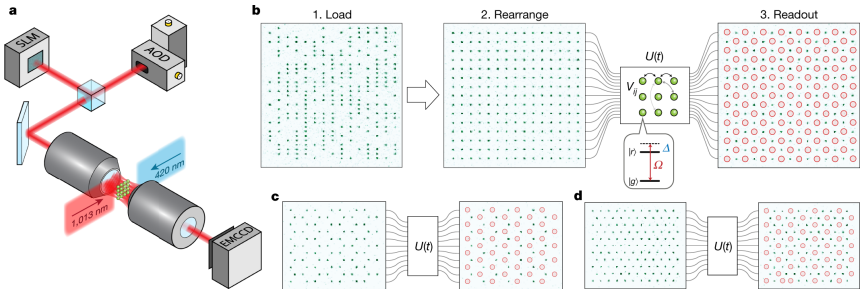


Figure: Picture from Lukin group.

UK groups in Strathclyde, Durham, Cambridge, ...  
Companies: PasQal, QueRa, ...



# Analogue Quantum Simulators: Two challenges

**Old:** Classical simulation of quantum Hamiltonians - exponential

**New:** Variety of Hamiltonians - lack of universality



## Universal quantum Hamiltonians

Toby S. Cubitt<sup>a,1,2</sup>, Ashley Montanaro<sup>b,1</sup>, and Stephen Piddock<sup>b,1</sup>

<sup>a</sup>Department of Computer Science, University College London, London WC1E 6BT, United Kingdom; and <sup>b</sup>School of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom

Edited by Peter W. Shor, Massachusetts Institute of Technology, Cambridge, MA, and approved August 3, 2018 (received for review March 23, 2018)

Quantum many-body systems exhibit an extremely diverse range of phases and physical phenomena. However, we prove that the entire physics of any quantum many-body system can be replicated by certain simple, “universal” spin-lattice models. We first characterize precisely what it means for one quantum system to simulate the entire physics of another. We then fully classify the simulation power of all two-qubit interactions, thereby

two-body interactions, and the largest possible local symmetry [full  $SU(2)$  invariance]. Yet our results prove that, if all of the coupling strengths can be varied individually, this model is universal. Thus, it can replicate in a rigorous sense the full physics of models with higher spatial dimensions, long-range interactions, other symmetries, higher-dimensional spins, and even bosons and fermions.

## Strongly Universal Hamiltonian Simulators

Leo Zhou<sup>1,\*</sup> and Dorit Aharonov<sup>2,†</sup>

<sup>1</sup>*Department of Physics, Harvard University, Cambridge, MA 02138, USA*

<sup>2</sup>*School of Computer Science and Engineering, The Hebrew University, Jerusalem 91904, Israel*

(Dated: Feb 4, 2021)

A universal family of Hamiltonians can be used to simulate any local Hamiltonian by encoding its full spectrum as the low-energy subspace of a Hamiltonian from the family. Many spin-lattice model Hamiltonians—such as Heisenberg or XY interaction on the 2D square lattice—are known to be universal. However, the known encodings can be very inefficient, requiring interaction energy that scales exponentially with system size if the original Hamiltonian has higher-dimensional, long-range, or even all-to-all interactions. In this work, we provide an efficient construction by which these universal families are in fact “strongly” universal. This means that the required interaction energy and all other resources in the 2D simulator scale polynomially in the size of the target Hamiltonian



# Accreditation of analogue quantum simulators

Theoretical Physics: Universal hamiltonians

Experimental Physics: Hybrid analogue-digital simulators (HQS)

PNAS

RESEARCH ARTICLE

COMPUTER SCIENCES  
PHYSICS



## Accreditation of analogue quantum simulators

Q:1 Andrew Jackson<sup>a,1,2</sup> , Theodoros Kapourniotis<sup>a,1</sup>, and Animesh Datta<sup>a</sup>

Edited by Peter Shor, Massachusetts Institute of Technology, Cambridge, MA; received June 28, 2023; accepted December 5, 2023

We present an accreditation protocol for analogue, i.e., continuous-time, quantum simulators. For a given simulation task, it provides an upper bound on the variation distance between the probability distributions at the output of an erroneous and error-free analogue quantum simulator. As its overheads are independent of the size and nature of the simulation, the protocol is ready for immediate usage and practical for the long term. It builds on the recent theoretical advances of strongly universal Hamiltonians and quantum accreditation as well as experimental progress toward the realization of programmable hybrid analogue–digital quantum simulators.

analogue quantum simulation | verification | simulation | accreditation

### Significance

Quantum computers and simulators hold the potential to revolutionize the computational landscape. Among these are analogue quantum simulators: devices that simulate quantum systems by physically

Figure: Jackson/Kapourniotis/AD, PNAS, 121, e2309627121 (2024)

