Architectures for quantum simulation showing quantum supremacy

Juan Bermejo-Vega,[1] Dominik Hangleiter,[1] Martin Schwarz,[1] Robert Raussendorf,[2] and Jens Eisert[1]

[1]*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*
[2]*University of British Columbia, Department of Physics and Astronomy, Vancouver, BC, V6T 1Z1, Canada*

One of the main aims in the field of quantum simulation is to achieve what is called "quantum supremacy", referring to the experimental realization of a quantum device that computationally outperforms classical computers. In this work, we show that one can devise versatile and feasible schemes of two-dimensional dynamical quantum simulators showing such a quantum supremacy, building on intermediate problems involving IQP circuits. In each of the schemes, an initial product state is prepared, potentially involving an element of randomness as in disordered models, followed by a short time evolution under a translationally invariant Hamiltonian with nearest-neighbor interactions and a mere sampling measurement in a fixed basis. The final state preparation in each scheme is fully efficiently certifiable. We discuss experimental necessities and possible physical architectures, inspired by platforms of cold atoms in optical lattices and a number of others, as well as specific assumptions that enter the complexity-theoretic arguments. This work shows that benchmark settings exhibiting a quantum advantage may require little control in contrast to universal quantum computing.

Introduction

Quantum devices promise to solve computational problems efficiently for which no classical efficient algorithm exists. The anticipated device of a universal quantum computer would solve problems for which no efficient classical algorithm is known, such as integer factorization [1] and simulating many-body Hamiltonian dynamics [2]. However, the experimental realization of such a machine requires fault-tolerant protection of universal dynamics against arbitrary errors [3–5], which incurs in prohibitive qubit overhead [6, 7] beyond reach in available quantum devices. This does not mean, however, that the demonstration of a computational quantum advantage is unfeasible with current technology.

Indeed, in recent years, it has become a major milestone in quantum information processing to identify and build a simple (perhaps non-universal) quantum device that offers a computational speedup compared to classical supercomputers, no matter what. The demonstration of such an advantage based on solid complexity-theoretic arguments has been coined "quantum supremacy" [8]. This important near-term goal still constitutes a challenge, as technological advances seem to be required to achieve it, as well as significant efforts in theoretical computer science, physics, and the numerical study of quantum many-body systems: after all, intermediate problems have to be identified with the potential to act as vehicles in the demonstration of a quantum advantage, in the presence of realistic errors.

There already is evidence that existing dynamical quantum simulators [9, 10] can outperform classical supercomputers. Specifically the experiments of Refs. [11–13] using ultracold atoms strongly suggest such a feature: They probe situations in which for short times [11] or in one spatial dimension [12, 13], the system can be classically simulated in a perfectly efficient fashion using tensor network methods, even equipped with rigorous error bounds. However, for long times [11] or in higher spatial dimensions [12, 13] such a classical simulation is no longer feasible with state-of-the-art simulation tools. Still, taking the role of devil's advocate, one may argue that

this could be a consequence of a lack of imagination, as there could—in principle—be a simple classical description capturing the observed phenomena. Hence, a complexity-theoretic demonstration of a quantum advantage of quantum simulators outperforming classical machines is highly desirable [14].

Several settings for achieving quantum supremacy have been proposed [15–19] based on quantum processes that are classically hard to simulate probabilistically unless the Polynomial Hierarchy (PH) collapses. These processes remain hard to be simulated up to realistic (additive) errors assuming further plausible complexity-theoretic conjectures. The proof techniques used build upon earlier proposals giving rise to such a collapse [20, 21]. However, at the same time they still come along with substantial experimental challenges.

This work constitutes a significant step towards identifying physically realistic settings that show quantum supremacy by laying out a versatile and feasible family of architectures based on quenched local many-body dynamics. We remain close to what one commonly conceives as a dynamical quantum simulator [9–11, 22]. Indeed, it is our aim is to remain as close as possible to experimentally-accessible or at least realistic prescriptions, while at the same not compromising the rigorous complexity-theoretic argument.

Our specific contributions are as follows. We focus on schemes in which random initial states are prepared on the 2D square lattices of suitable periodicity, followed by quenched, constant-time dynamics under a local *nearest-neighbor* (NN), *translation-invariant* (TI) Hamiltonian. Since evolution time is short, decoherence will be comparably small. In a last step, all qubits are measured in a fixed identical basis, producing an outcome distribution that is hard to classically sample from within constant ℓ_1-norm error, requiring no postselection. Technically, our results implement sampling over new families of NNTI two-local constant-depth [20] IQP circuits [16, 21, 23]. We build upon and develop a type of setting [24] in which resource-states for measurement-based quantum computation are prepared (MBQC) [25], but subsequently non-adaptively measured. We lay out the complexity-theoretic assumptions made, detail how they are analog to those in

Refs. [15–19], and present results on anti-concentration.

By doing so, we arrive at surprisingly flexible and simple NNTI quantum supremacy schemes on square lattices, requiring different kinds of translational invariance in the preparation. Interestingly, and possibly counterintuitively, our schemes share the feature that the final state before the readout step can be efficiently and rigorously certified in its correctness. Based on our analysis, we predict that short-time certifiable quantum-simulation experiments on 50×50 qubit square lattices should be intractable for state-of-the-art classical computers [17, 26]. It is important to stress that this assessment includes the rigorous certification part, and no hidden or unknown costs have to be added to this. Our proposed experiments are particularly suited to qubits arranged in two-dimensional lattices, e.g., cold atoms in optical lattices [9, 27–29] and arrays of superconducting qubits [30].

Basic setup of the quantum simulation schemes

We present new physical architectures that exhibit quantum supremacy. All share the basic feature that they are based on the constant-time evolution (quench) of an NNTI Hamiltonian on a square lattice. Each architecture involves three steps:

E1 **Preparations.** Arrange $N := \mu m n$ qubits side-by-side on an n-row m-column square lattice $\mathcal{L}$, with vertices V, edges E, initialized on a product state

$$|\psi_\beta\rangle = \bigotimes_{i=1}^{N} \left(|0\rangle + \mathrm{e}^{\mathrm{i}\beta_i}|1\rangle\right), \ \beta \in \{0, \theta\}^N , \qquad (1)$$

for fixed $\theta \in \{\frac{\pi}{4}, \frac{\pi}{8}\}$, which is chosen uniformly or randomly with probability p_β (e.g., as a ground state of a disordered model). We consider standard square primitive cells. We allow in one scheme each vertex to be equipped with an additional qubit, named "dangling bond qubit". For this, $\mu=2$, otherwise $\mu=1$.

E2 **Couplings.** Let the system evolve for constant time $\tau = 1$ under the effect of an NNTI Ising Hamiltonian

$$H := \sum_{(i,j)\in E} J_{i,j} Z_i Z_j - \sum_{i\in V} h_i Z_i. \qquad (2)$$

This amounts to what is usually referred to as a *quench*. Local fields $\{h_i\}_i$ and couplings $\{J_{i,j}\}_{i,j}$ are set to implement a unitary $U := \mathrm{e}^{\mathrm{i}H}$, giving rise to a final ensemble $\Psi := \{p_\beta, |\Psi_\beta\rangle\}_\beta$, $|\Psi_\beta\rangle := U|\psi_\beta\rangle$.

E3 **Measurement.** Measure primitive-cell qubits on the X basis and (if present) dangling-bond qubits on the Z basis. Since the latter can be traded for a measurement in the X basis by a uniform basis rotation, one can equally well measure all qubits in the same basis.

As we will discuss later, all individual steps have been realized with present technology. Note also that E2 amounts to a
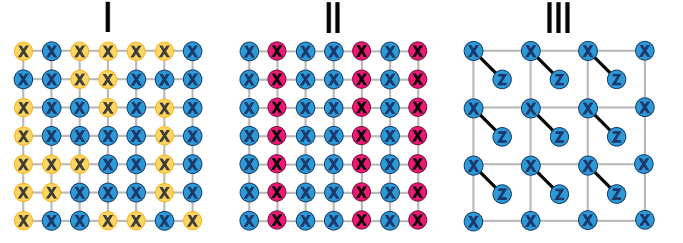

Figure 1. Quantum supremacy architectures I-III. Colors illustrate the rotation angle of the initial state (1): $\beta_i = 0$ (blue), $\beta_i = \pi/4$ (yellow), and $\beta_i = \pi/8$ (crimson). Solid lines between qubits represent Ising-type interactions (2) with coupling constants $J_{i,j} = \pi/4$ (gray) and $J_{i,j} = \pi/8$ (black). X and Z label the basis in which the respective qubits are to be measured.

constant depth quantum circuit [31].

Physical desiderata and concrete schemes

Before presenting concrete schemes, we lay out desiderata that we associate with feasible ones. We require the implementation of each step E1-E3 to be as simple as possible. For preparations, couplings, and measurements, we desire the periodicity as measured by the 2D periods (k_x, k_y) in the xy axes of the TI symmetry to be small. Couplings should further be simple and not to scale with the system size. Last, we want the final measurement to be translationally invariant.

We now present three concrete quantum-supremacy architectures of the form E1-E3 that live up to the above desiderata. We label them I-III and illustrate them in Fig. 1:

I A disordered (DO) product state is prepared on a squared lattice, followed by a quench with an Ising Hamiltonian with couplings $J_{i,j} = h_i = \pi/4$ —which implements controlled-Z (CZ) gates on edges—and a final measurement in the X basis.

II The initial state is TI with period 1 in one lattice direction and uniformly random in the other (TI$_{(1,\infty)}$); couplings and measurements are picked as in I.

III Qubits are prepared on a dangling-bond square lattice. The initial state is TI with period 1 in all directions (TI$_{(1,1)}$). We pick $J_{i,j}, h_i$ as in I-II on bright edges and $J_{i,j} = h_i = \pi/16$ on dark ones—the latter implement controlled-$\mathrm{e}^{-\mathrm{i}\pi/8 Z}$ (CT) gates on dangling bonds. Measurements are in the Z basis for dangling qubits, elsewhere in the X basis.

(Cf. Appendix A for full Hamiltonian specifications.) The resources needed in each architecture are summarized in Table I. It is worth noting that, in all architectures I-III the state prepared after E2 is a resource for postselected measurement-based quantum computation postselecting w.r.t. the measurements in E3 (appendix D), but as such does not amount to universal quantum computation. In fact, architectures I-III require *neither* adaptive measurements (which are key in MBQC [25]) *nor* physical postselection:

Scheme	Geometry	Preparations	Couplings	Measurements
I	Square lattice	DO	$\{\frac{\pi}{4}\}_{(1,1)}$	$\{X\}_{(1,1)}$
II	Square lattice	$\mathrm{TI}_{(1,\infty)}$	$\{\frac{\pi}{4}\}_{(1,1)}$	$\{X\}_{(1,1)}$
III	Dangling-bond square lattice	$\mathrm{TI}_{(1,1)}$	$\{\frac{\pi}{4}, \frac{\pi}{16}\}_{(\sqrt{2},\sqrt{2})}$	$\{X, Z\}_{(\sqrt{2},\sqrt{2})}$
Previous work				
Ref. [18]	7-fold brickwork graph	$\mathrm{TI}_{(1,1)}$	$\{\frac{\pi}{4}\}_{(56,2)}$	$\{X, X_{\pm\frac{\pi}{4}}, X_{\pm\frac{\pi}{8}}\}_{(7,1)}$
Ref. [18]	Square lattice	$\mathrm{TI}_{(1,1)}$	$\{\frac{\pi}{4}\}_{(1,1)}$	$\{X, Y, Z, X_{\pm\frac{\pi}{4}}, X_{\pm\frac{\pi}{8}}\}_{(64,4)}$

Table I. Resource requirements of our quantum-supremacy architectures. Architectures which employ simpler (more ordered) initial states require lattices of higher periodicity and finer controlled-rotations. We compare our results to previous work (cf. main text for a comparison of the underlying complexity-theoretic assumptions). Above, $X_\theta := \mathrm{e}^{\mathrm{i}\frac{\theta}{2}Z} X \mathrm{e}^{-\mathrm{i}\frac{\theta}{2}Z}$.

our result states that if three plausible complexity-theoretic conjectures hold a single-shot readout cannot be classically simulated.

Complexity theory

We now turn to stating that while the above three architectures I-III are physically feasible, the output distributions of measurements cannot be efficiently classically simulated on classical computers, based on plausible assumptions and standard complexity-theoretic arguments.

Theorem 1 (Hardness of classical simulation). *If Conjectures 1-3 below are true then a classical computer cannot sample from the outcome distribution of any architecture I-III up to error 1/22 in ℓ_1 norm in time $O(\mathrm{poly}(n, m))$.*

As in previous works [15, 16, 19, 20, 32–34], Theorem 1 relies on plausible complexity-theoretic conjectures. The first, originally adopted in Ref. [20], is a widely believed statement about the structure of an infinite tower of complexity classes known as "the Polynomial Hierarchy" (PH), the levels of which recursively endow the classes P, NP, and coNP with oracles to previous levels.

Conjecture 1 (Polynomial Hierarchy). *The polynomial hierarchy is infinite.*

The claim generalizes the familiar P $\neq$ NP conjecture in that P $=$ NP would imply a complete collapse of PH to its 0-th level. Furthermore, if two levels k, $k + 1$ coincide, then all classes above level k collapse to it. The available evidence for P $\neq$ NP makes Conjecture 1 plausible, for it would be surprising to find a collapse of PH to some level k but not a full one [35] (cf. [36] for further discussion). Similarly to the Riemann hypothesis in number theory, many theorems in complexity theory have been proven relative to Conjecture 1, probably most notably the Karp-Lipton theorem NP $\nsubseteq$ P/poly [37].

We highlight that, assuming Conjecture 1 only, a classical computer would still not be able to sample from our experiments either exactly or within any constant relative error (cf.

appendix F). However, such level of accuracy is physically unrealistic for it cannot be achieved by a quantum computer. A goal of this work is to understand how unlikely is for architectures I-III to be classically intractable under realistic errors.

Our second conjecture, adopted from Ref. [16], is a qubit analog of the "permanent-of-Gaussians" conjecture [15]. It states that partition functions of (unstructured) random Ising models should be equally hard to approximate in average- and worst-case. Now, let $(a, b) := (a_1, \ldots, a_{N_X}, b_1, \ldots, b_{N_Z})$ be the outcomes of the X and Z measurements in our architectures, with $b_i = 0$ for I-II. In appendix B we show that

$$\mathrm{prob}\,(a, b \,|\, \beta) = |\langle a, b|U|\psi_\beta\rangle|^2 = \frac{|\mathcal{Z}^{(\pi a, \frac{\pi}{4}b + \beta)}|^2}{2^{N_X + \frac{N_Z}{2}}}, \quad (3)$$

where $\mathcal{Z}^{(\alpha,\vartheta)} := \mathrm{tr}(\mathrm{e}^{\mathrm{i}H^{(\alpha,\vartheta)}})$ is the partition function of a random Ising model on an $n \times m$ square lattice $\mathcal{L}_R$:

$$H^{(\alpha,\beta)} := \sum_{(i,j)\in E_R} \frac{\pi}{4} Z_i Z_j - \sum_{i\in V_R} h_i^{(\alpha,\vartheta)} Z_i, \quad (4)$$

$$h_i^{(\alpha,\vartheta)} := h_i - \left(\frac{\alpha_i + \vartheta_i}{2}\right), \alpha_i \in \{0, \pi\}, \vartheta_i \in \{0, \theta\}, \theta \in \{\frac{\pi}{4}, \frac{\pi}{8}\},$$

where α (resp. ϑ) is random and DO- (resp. either DO- or $\mathrm{TI}_{(1,\infty)}$-) distributed.

Conjecture 2 (Average-case complexity). *For random Ising models as in (4), approximating $|\mathcal{Z}^{(\alpha,\beta)}|^2$ up to relative error $\frac{1}{4} + o(1)$ for any 0.3 fraction of the field configurations is as hard as in worst-case.*

We complement Conjecture 2 with the following lemma.

Lemma 2 (#P-hardness). *Let $H^{(\alpha,\beta)}$ be the Ising model (4) on the $n \times m$ square lattice with either (i) DO-distributed ϑ and $\theta \in \{0, \frac{\pi}{4}\}$; or (ii) $\mathrm{TI}_{(1,\infty)}$-distributed ϑ and $\theta \in \{0, \frac{\pi}{8}\}$. Then, for $m \in O(n^2)$, approximating $|\mathcal{Z}^{(\alpha,\beta)}|^2$ with relative error $\frac{1}{4} + o(1)$ is #P-hard.*

Thus, accepting Conjecture 2 implies that approximating $|\mathcal{Z}^{(\alpha,\beta)}|^2$ for these models is as hard in average as any problem in #P [38]. The proof (appendix E) applies MBQC methods [39] to show that I-III are computationally equivalent to

an encoded n-qubit 1D nearest-neighbor circuit comprising random gates of the form

$$\left[\prod_{i=1}^{n-1} CZ_{i,i+1} \right] \left[\bigotimes_{i=1}^{n} Z_i^{c_i} \mathrm{e}^{-\mathrm{i}\theta d_i Z_i} H_i \right], c_i, d_i \in \{0,1\}, \quad (5)$$

where c_i (resp. d_i) is DO (resp. DO-or-TI$_{(1,\infty)}$-) distributed and H is the Hadamard gate. Post-selecting such circuits, we can implement two known universal schemes of quantum computation [40, 41]. We then exploit that universal quantum-circuit amplitudes are #P-hard to approximate. As a last remark, we mention that our bound $m \in O(n^2)$ in Lemma 2 can be improved to $m \in O(n)$ in architectures I-II by introducing new types of input states (appendix H); based on this fact and Haar-random properties of these circuits (cf. below), we believe Lemma 2 should extend to the $m \in O(n)$ regime.

Last, we claim that random circuits of gates of form (5) anti-concentrate.

Conjecture 3 (Anti-concentration). *Let $\mathcal{C}$ be an n-qubit $O(n)$-depth random circuit of gates of form (5), then*

$$\mathrm{prob}_x \left(\left| \langle x | \mathcal{C} | 0 \rangle^{\otimes n} \right|^2 \geq \frac{1}{2^n} \right) \geq \frac{1}{e} \quad (6)$$

for a uniformly random choice of $x = (x_1, \ldots, x_n)$.

In appendix H, we show that Eq. (6) is a sufficient condition for the output distribution of architectures I-III to display anti-concentration. Analog numerically-supported conjectures have been made in Refs. [15, 17, 42]. Analytic proofs of anti-concentration are currently only known for some IQP-circuit families [16, 19]. Here, we ran exact simulations of random circuits with up to 20 logical qubits to test Conjecture 3 (appendix G), and observed, first, that the anti-concentration ratio of Eq. (6) quickly converges to $1/e$ with the system-size; and, second, that measurement outcomes are Porter-Thomas [43] (i.e., exponentially) distributed, which is a signature of chaotic Haar-random unitary processes [17, 44–47].

Previously, Refs. [16, 19, 48] argued that anti-concentration of measurement outcomes on an $n \times n$ lattice should require $\Omega(n)$ physical depth on 2D NN layouts in order not to induce a violation of the counting exponential time hypothesis [49, 50]. This contrasts with the constant-depth nature of our proposal. To clarify this discrepancy, we note that our numerical evidence for anti-concentration is for logical n-qubit 1D circuits (5) of depth $O(n)$ (Fig. 4), which implies anti-concentration of the corresponding constant-depth evolution on a lattice of size $n \times O(n)$. Because this encoding introduces a linear overhead factor $O(n)$ there is no contradiction with Refs. [19, 48]. More critically, the observed signatures of anti-concentration rule out a potential efficient classical simulation of our schemes via sparse-sampling methods [19, 51].

We end this section with a remark: Closest to our work is the approach of Ref. [18], which is an also an NNTI non-adaptive MBQC proposal with larger resource requirements (see Table I for a comparison) and stronger hardness assump-

tions with regards to the required level of approximation. It introduces a variation of Conjecture 2 with an unconventional type of error that is larger than any additive or relative approximation; the latter encapsulates Conjectures 2-3 as presented here. Furthermore, Refs. [17, 19, 42] gave non-TI schemes based on time-dependent NN random circuits acting on square lattices: the latter approaches require less qubits, but also circuits of polynomial depth. In ours and in that of Ref. [18], circuit depth is traded with ancillas and kept constant. For ours and that of Ref. [18], efficient certification protocols also exist and can be used to determine if the experiment has actually worked, as discussed below.

Proof intuition

Besides Lemma 2, a technical ingredient in the proof of Theorem 1 (appendix F) is Stockmeyer's Theorem [52]. By similar arguments as in the Boson-sampling and IQP-circuit settings [15, 16], if an efficient classical algorithm can approximately sample from the output distribution of architectures I-III, then an FBPP^NP algorithm can approximate a large fraction of the amplitudes in (3) if they are sufficiently anti-concentrated. By Conjectures 2-3, the latter algorithm can solve any problem in P^#P. This implies a collapse of the Polynomial Hierarchy to its 3rd level.

Conceivable physical architectures

We now turn to discussing that the above assumptions are plausible in several physical architectures close to what is available with present technology. What we are considering are large-scale quantum lattice architectures on square lattices $\mathcal{L}$ with a quantum degree of freedom per lattice site. On the level of physical implementation, the most advanced family of such architectures is that provided by *cold atoms in optical lattices* [9]. In an optical lattice architecture, internal degrees of freedom are available with hyperfine levels. Also, the encoding in spatial degrees of freedom within double wells is in principle conceivable. Large-scale translationally invariant controlled-Z interactions—precisely of the type as they are required for the preparation of cluster and graph states [39, 53]—are feasible via controlled collisions [28, 54]. Other interactions to nearest neighbors are also conceivable. Interactions such as spin-changing collisions for ^{87}Rb atoms have been experimentally observed [55]. Controlled-T gates require a more sophisticated interaction Hamiltonian. The dangling bonds seem realizable making use of optical superlattices [11, 56]. Single sites—specifically of the sampling type considered here—can be addressed in optical lattice architectures via several methods. E.g., quantum-gas microscopes allow for single-site resolved imaging [57, 58], even though the type of single-site addressing required here remains a significant challenge. Optical superlattices [11, 56] allow for the addressing of entire rows of sites in the same fashion. Entire

rows that contain a fixed particle number neighboring ones left empty can already be routinely prepared [59]. Also, disordered initial states can be prepared [12, 60].

But also other architectures are well conceivable. This includes in particular large arrays of *semiconductor quantum dots* allowing for single-site addressing—a setting that has already been employed to simulate the Mott-Hubbard model in the atomic limit [61]—or polaritons or exciton-polariton systems in *arrays of micro-cavities* [62]. In this type of architecture, the addressing of entire rows is also particularly feasible. *Superconducting architectures* also promise to allow for large-scale array structures of the type anticipated here [30, 63, 64]. *Trapped ions* can also serve as feasible architectures [65]. None of the physical architectures realize all elements required to the necessary precision, but at the same time, the prescriptions presented here are comparably close to what can be done.

Efficient certification

It is key to all schemes proposed that the correctness of the final resource-state preparation in the quantum simulation can be efficiently and rigorously certified. Since the prepared state is the ground state of a gapped and frustration-free parent Hamiltonian, there exists a scheme involving local measurements only that certifies the closeness of the prepared state ρ to anticipated state $|\Psi_\beta\rangle\langle\Psi_\beta|$ immediately before measurement in terms of an upper bound on the trace-distance $\||\Psi_\beta\rangle\langle\Psi_\beta| - \rho\|$ [66, 67]. This directly yields an upper bound on the ℓ_1-norm distance between the respective measurement outcome distributions. The certification scheme is a more difficult prescription that the experiment as such, and assumes the ability to perform noise-free measurements. However, it is key to see that the correctness of the final-state preparation can be certified even the absence of a possibility of efficiently classically sampling the output distribution. This is also in contrast to other similar schemes, where no efficient rigorous scheme for certification of the final state before measurement is known [15–17, 19, 42].

The property of the final-state preparation being certifiable is rooted in the fact that the states prepared are ground states of gapped frustration-free local Hamiltonian models. At the same time they are injective *projected entangled pair states (PEPS)* of constant bond dimension [68, 69]. The protocols discussed here can hence be seen as PEPS sampling protocols that generate samples from local measurement on PEPS.

Conclusion

In this work, we have established feasible schemes for quantum simulation that exhibit quantum supremacy in a complexity-theoretic sense. This work can be seen as an invitation towards a number of further exciting research directions: While the schemes presented do not quite yet constitute experimentally realizable blue-prints, it should be clear that steps already experimentally taken are very similar to those discussed. It seems hence interesting to explore detailed settings for cold atoms or trapped ions in detail, requiring little local control and allowing for comparably short coherence times. What is more, it appears obvious that further complexity-theoretic results on intermediate problems seem needed to fully capture the potential of quantum devices outperforming classical computers without being universal quantum computers. It is the hope that the present work can contribute to motivating such further work, guiding experiments in the near future.

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proc. 50th Ann. Symp. Found. Comp. Sc. (1994).

[2] S. Lloyd, "Universal quantum simulators," Science **273**, 1073–1078 (1996).

[3] P. W. Shor, "Fault-tolerant quantum computation," in *Proceedings of the 37th Annual Symposium on Foundations of Computer Science*, FOCS '96 (IEEE Computer Society, 1996) pp. 56–.

[4] E. Knill, R. Laflamme, and W. Zurek, "Threshold accuracy for quantum computation," preprint (1996), quant-ph/9610011.

[5] D. Aharonov and M. Ben-Or, "Fault-tolerant quantum computation with constant error rate," SIAM J. Comp. **38**, 1207–1282 (2008).

[6] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, "Surface codes: Towards practical large-scale quantum computation," Phys. Rev. A **86**, 032324 (2012).

[7] B. Lekitsch, S. Weidt, A. G. Fowler, K. Mølmer, S. J. Devitt, C. Wunderlich, and W. K. Hensinger, "Blueprint for a microwave trapped ion quantum computer," Science Adv. **3** (2017).

[8] J. Preskill, "Quantum computing and the entanglement frontier," Bull. Am. Phys. Soc. **58** (2013).

[9] I. Bloch, J. Dalibard, and S. Nascimbene, "Quantum simulations with ultracold quantum gases," Nature Phys. **8**, 267 (2012).

[10] J. Eisert, M. Friesdorf, and C. Gogolin, "Quantum many-body systems out of equilibrium," Nature Phys **11**, 124–130 (2015).

[11] S. Trotzky, Y.-A. Chen, A. Flesch, I. P. McCulloch, U. Schollwöck, J. Eisert, and I. Bloch, "Probing the relaxation towards equilibrium in an isolated strongly correlated one-dimensional Bose gas," Nature Phys. **8**, 325–330 (2012).

[12] J.-Y. Choi, S. Hild, J. Zeiher, P. Schauß, A. Rubio-Abadal, T. Yefsah, V. Khemani, D. A. Huse, I. Bloch, and C. Gross, "Exploring the many-body localization transition in two dimensions," Science **352**, 1547 (2016).

[13] S. Braun, M. Friesdorf, S. S. Hodgman, M. Schreiber, J. P.

Ronzheimer, A. Riera, M. del Rey, I. Bloch, J. Eisert, and U. Schneider, "Emergence of coherence and the dynamics of quantum phase transitions," Proc. Natl. Ac. Sc. **112**, 3641 (2015).

[14] "European quantum technologies roadmap," (2016), `www.lmt.lt/download/6691/qtroadmap2016.pdf`.

[15] S. Aaronson and A. Arkhipov, "The computational complexity of linear optics," Th. Comp. **9**, 143–252 (2013).

[16] M. J. Bremner, A. Montanaro, and D. J. Shepherd, "Average-case complexity versus approximate simulation of commuting quantum computations," Phys. Rev. Lett. **117**, 080501 (2016).

[17] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, J. M. Martinis, and H. Neven, "Characterizing quantum supremacy in near-term devices," preprint (2016), arXiv:1608.00263.

[18] X. Gao, S.-T. Wang, and L.-M. Duan, "Quantum supremacy for simulating a translation-invariant Ising spin model," Phys. Rev. Lett. **118**, 040502 (2017).

[19] M. J. Bremner, A. Montanaro, and D. J. Shepherd, "Achieving quantum supremacy with sparse and noisy commuting quantum computations," preprint (2016), arXiv:1610.01808.

[20] B. M. Terhal and D. P. DiVincenzo, "Adaptive quantum computation, constant depth quantum circuits and arthur-merlin games," Quantum Information & Computation **4**, 134–145 (2004).

[21] M. J. Bremner, R. Jozsa, and D. J. Shepherd, "Classical simulation of commuting quantum computations implies collapse of the Polynomial Hierarchy," Proc. Roy. Soc. A **467**, 459–472 (2011).

[22] J. I. Cirac and P. Zoller, "Goals and opportunities in quantum simulation," Nature Phys. **8**, 264 (2012).

[23] D. Shepherd and M. J. Bremner, "Temporally unstructured quantum computation," Proc. Roy. Soc. A **465**, 1413–1439 (2009).

[24] M. J. Hoban, J. J. Wallman, H. Anwar, N. Usher, R. Raussendorf, and D. E. Browne, "Measurement-based classical computation," Phys. Rev. Lett. **112**, 140505 (2014).

[25] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," Phys. Rev. Lett. **86**, 5188–5191 (2001).

[26] S. Bravyi and D. Gosset, "Improved classical simulation of quantum circuits dominated by Clifford gates," Phys. Rev. Lett. **116**, 250501 (2016).

[27] M. Endres, M. Cheneau, T. Fukuhara, C. Weitenberg, P. Schau, C. Gross, L. Mazza, M. C. Bauls, L. Pollet, I. Bloch, and et al., "Single-site- and single-atom-resolved measurement of correlation functions," Appl. Phys. B **113**, 27–39 (2013).

[28] O. Mandel, M. Greiner, A. Widera, T. Rom, T. W. Hänsch, and I. Bloch, "Controlled collisions for multiparticle entanglement of optically trapped atoms," Nature **425**, 937–940 (2003).

[29] W. S. Bakr, J. I. Gillen, A. Peng, S. Fölling, and M. Greiner, "A quantum gas microscope for detecting single atoms in a Hubbard-regime optical lattice," Nature **462**, 74–77 (2009).

[30] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O'Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland, and J. M. Martinis, "Superconducting quantum circuits at the surface code threshold for fault tolerance," Nature **508**, 500–503 (2014).

[31] This also implies that not the entire resource has to necessarily be prepared in a single preparation, but can be sequentially prepared.

[32] M. J. Bremner, R. Jozsa, and D. J. Shepherd, "Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy," Proc. Roy. Soc. **467**, 2126 (2010).

[33] R. Jozsa and M. Van Den Nest, "Classical simulation complexity of extended Clifford circuits," Quant. Inf. Comp. **14**, 633–648 (2014).

[34] B. Fefferman and C. Umans, "On the Power of Quantum Fourier Sampling," in *11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 61 (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016) pp. 1:1–1:19.

[35] S. Aaronson, "P≠NP?" in *Open Problems in Mathematics* (Springer, 2016).

[36] L. Fortnow, "Beyond NP: the work and legacy of Larry Stockmeyer," in *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing* (ACM, 2005) pp. 120–127.

[37] R. M. Karp and R. J. Lipton, "Some connections between nonuniform and uniform complexity classes," in *Proceedings of the twelfth annual ACM symposium on Theory of computing* (ACM, 1980) pp. 302–309.

[38] L. G. Valiant, "The complexity of computing the permanent," Th. Comp. Sc. **8**, 189–201 (1979).

[39] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation on cluster states," Phys. Rev. A **68**, 022312 (2003).

[40] R. Raussendorf, "Quantum computation via translation-invariant operations on a chain of qubits," Phys. Rev. A **72**, 052301 (2005).

[41] A. Mantri, T. F. Demarie, and J. F. Fitzsimons, "Universality of quantum computation with cluster states and (X,Y)-plane measurements," Sci. Rep. **7** (2017).

[42] S. Aaronson and L. Chen, "Complexity-Theoretic Foundations of Quantum Supremacy Experiments," preprint (2016), arXiv:1612.05903.

[43] C. E. Porter and R. G. Thomas, "Fluctuations of nuclear reaction widths," Phys. Rev. **104**, 483–491 (1956).

[44] F. Haake, *Quantum Signatures of Chaos*, Physics and astronomy online library (Springer, 2001).

[45] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd, and D. G. Cory, "Pseudo-random unitary operators for quantum information processing," Science **302**, 2098–2100 (2003).

[46] J. Emerson, E. Livine, and S. Lloyd, "Convergence conditions for random quantum circuits," Phys. Rev. A **72**, 060302 (2005).

[47] W. G. Brown, Y. S. Weinstein, and L. Viola, "Quantum pseudorandomness from cluster-state quantum computation," Phys. Rev. A **77**, 040303 (2008).

[48] A. P. Lund, M. J. Bremner, and T. C. Ralph, "Quantum sampling problems, boson sampling and quantum supremacy," preprint (2017), arXiv:1702.03061.

[49] C. Brand, H. Dell, and M. Roth, "Fine-grained dichotomies for the tutte plane and boolean #CSP," in *11th International Symposium on Parameterized and Exact Computation (IPEC 2016)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 63 (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2017) pp. 9:1–9:14.

[50] R. Curticapean, "Block interpolation: A framework for tight exponential-time counting complexity," in *Automata, Languages, and Programming: 42nd International Colloquium, ICALP 2015, Kyoto, Japan, July 6-10, 2015, Proceedings, Part I* (Springer Berlin Heidelberg, 2015) pp. 380–392.

[51] M. Schwarz and M. Van den Nest, "Simulating quantum circuits with sparse output distributions," preprint (2013), arXiv:1310.6749.

[52] L. Stockmeyer, "On approximation algorithms for #P," SIAM J. Comp. **14**, 849–861 (1985).

[53] M. Hein, J. Eisert, and H. J. Briegel, "Multi-particle entanglement in graph states," Phys. Rev. A **69**, 062311 (2004).

[54] D. Jaksch, H.-J. Briegel, J. I. Cirac, C. W. Gardiner, and P. Zoller, "Entanglement of atoms via cold controlled collisions," Phys. Rev. Lett. **82**, 1975 (1999).

[55] A. Widera, F. Gerbier, S. Fölling, T. Gericke, O. Mandel, and I. Bloch, "Coherent collisional spin dynamics in optical lattices," Phys. Rev. Lett. **95**, 190405 (2005).

[56] S. Nascimbène, Y.-A. Chen, M. Atala, M. Aidelsburger, S. Trotzky, B. Paredes, and I. Bloch, "Experimental realization of plaquette resonating valence-bond states with ultracold atoms in optical superlattices," Phys. Rev. Lett. **108**, 205301 (2012).

[57] W. S. Bakr, A. Peng, M. E. Tai, R. Ma, J. Simon, J. I. Gillen, S. Fölling, L. Pollet, and M. Greiner, "Probing the superfluid-to-mott insulator transition at the single-atom level," Science **329**, 547–550 (2010).

[58] C. Weitenberg, M. Endres, J. F. Sherson, M. Cheneau, P. Schauß, T. Fukuhara, I. Bloch, and S. Kuhr, "Single-spin optaddressing in an atomic Mott insulator," Nature **471**, 319–324 (2011).

[59] C. Gross, (2016), private communication.

[60] M. Schreiber, S. S. Hodgman, P. Bordia, H. P. Lüschen, M. H. Fischer, R. Vosk, E. Altman, U. Schneider, and I. Bloch, "Observation of many-body localization of interacting fermions in a quasi-random optical lattice," Science **349**, 842 (2015).

[61] A. Singha, M. Gibertini, B. Karmakar, S. Yuan, M. Polini, G. Vignale, M. I. Katsnelson, A. Pinczuk, L. N. Pfeiffer, K. W. West, and V. Pellegrini, "Two-dimensional Mott-Hubbard electrons in an artificial honeycomb lattice," Science **332**, 1176 (2011).

[62] T. Jacqmin, I. Carusotto, I. Sagnes, M. Abbarchi, D. D. Solnyshkov, G. Malpuech, E. Galopin, A. Lemaître, J. Bloch, and A. Amo, "Direct observation of dirac cones and a flatband in a honeycomb lattice for polaritons," Phys. Rev. Lett. **112**, 116402 (2014).

[63] A. A. Houck, H. E. Tuereci, and J. Koch, "On-chip quantum simulation with superconducting circuits," Nature Phys. **8**, 292 (2012).

[64] M. R. Geller, J. M. Martinis, A. T. Sornborger, P. C. Stancil, E. J. Pritchett, H. You, and A. Galiautdinov, "Universal quantum simulation with prethreshold superconducting qubits: Single-excitation subspace method," Phys. Rev. A **91**, 062309 (2015).

[65] On the one hand, configurable lattice systems of two-dimensional arrays of individually trapped ions can be conceived [70]. Probably more feasible, on the other hand, are flattened architectures, in which the 2D setting is traded for suitable long-ranged quantum gates.

[66] D. Hangleiter, M. Kliesch, M. Schwarz, and J. Eisert, "Direct certification of a class of quantum simulations," Quant. Sc. Tech. **2**, 015004 (2017).

[67] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, "Efficient quantum state tomography," Nat. Comm. **1**, 149 (2010).

[68] F. Verstraete and J. I. Cirac, "Valence-bond states for quantum computation," Phys. Rev. A **70**, 060302 (2004).

[69] D. Gross and J. Eisert, "Novel schemes for measurement-based quantum computation," Phys. Rev. Lett. **98**, 220503 (2007).

[70] M. Mielenz, H. Kalis, M. Wittemer, F. Hakelberg, R. Schmied, M. Blain, P. Maunz, D. Leibfried, U. Warring, and T. Schaetz, "Freely configurable quantum simulator based on a two-dimensional array of individually trapped ions," preprint (2015), arXiv:1512.03559.

[71] S. Aaronson, "Quantum computing, postselection, and probabilistic polynomial-time," Proc. Roy. Soc. A **461** (2005).

[72] M. A. Nielsen, "Conditions for a class of entanglement transformations," Phys. Rev. Lett. **83**, 436 (1999).

[73] P. Oscar Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, "A new universal and fault-tolerant quantum basis," Inf. Proc. Lett. **75**, 101 – 107 (2000).

[74] R. Raussendorf, "Quantum cellular automaton for universal quantum computation," Phys. Rev. A **72**, 022301 (2005).

[75] A. M. Childs, D. W. Leung, and M. A. Nielsen, "Unified derivations of measurement-based schemes for quantum computation," Phys. Rev. A **71**, 032318 (2005).

[76] K. Fujii and T. Morimae, "Quantum commuting circuits and complexity of Ising partition functions," preprint (2013), arXiv:1311.2128.

[77] L. A. Goldberg and H. Guo, "The complexity of approximating complex-valued Ising and Tutte partition functions," preprint (2014), arXiv:1409.5627.

[78] M. Soeken, D. M. Miller, and R. Drechsler, "Quantum circuits employing roots of the Pauli matrices," Phys. Rev. A **88**, 042322 (2013).

[79] A. W. Harrow and Richard A. Low, "Random quantum circuits are approximate 2-designs," Commun. Math. Phys. **291**, 257–302 (2009).

[80] H. Kim and D. A. Huse, "Ballistic spreading of entanglement in a diffusive nonintegrable system," Phys. Rev. Lett. **111**, 127205 (2013).

[81] P. Hosur, X.-L. Qi, D. A. Roberts, and B. Yoshida, "Chaos in quantum channels," J. High En. Phys. **2016**, 4 (2016), arXiv:1511.04021.

[82] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, "Local random quantum circuits are approximate polynomial-designs," Commun. Math. Phys. **346**, 397–434 (2016).

[83] D. Wecker and K. M. Svore, "LIQUi| >: A software design architecture and domain-specific language for quantum computing," (2014).

[84] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H.-J. Briegel, "Entanglement in graph states and its applications," in *Quantum Computers, Algorithms and Chaos*, International School of Physics Enrico Fermi (IOS Press, 2006).

[85] S. Bravyi and R. Raussendorf, "Measurement-based quantum computation with the toric code states," Phys. Rev. A **76**, 022304 (2007).

[86] M. Van den Nest, W. Dür, and H. J. Briegel, "Completeness of the classical 2D Ising model and universal quantum computation," Phys. Rev. Lett. **100**, 110501 (2008).

Appendix

(A): Full Hamiltonian (2)

For any architecture I-III (Fig. 1), let $\mathcal{L}_P = (V_P, E_P)$ be the sublattice of $\mathcal{L}$ containing all primitive qubits (i.e., the square lattice subgraph of $\mathcal{L}$). Further, let $\mathcal{L}_{DB} = (V_{DB}, E_{DB})$ be $\mathcal{L}$'s sublattice containing all dangling-bonds for architecture III and the empty graph otherwise. For any $i \in V$, let $\deg_P(i)$ (resp. $\deg_{DB}(i)$) be the number of primitive (resp. dangling-bond) qubits connected to i in $\mathcal{L}$. Then, the full Hamiltonian (2) of the experiment reads

$$H = \underbrace{\sum_{(i,j) \in E_P} \frac{\pi}{4} Z_i Z_j - \sum_{i' \in V_P} \frac{\pi}{4} \deg_P(i') Z_{i'}}_{H_{CZ}} + \underbrace{\sum_{(k,l) \in E_{DB}} \frac{\pi}{16} Z_k Z_l - \sum_{k' \in V_{DB}} \frac{\pi}{16} \deg_{DB}(k') Z_{k'}}_{H_{CT}}. \tag{7}$$

Above, the Hamiltonian H_{CZ} (resp. H_{CT}) implements a CZ (resp. CT) gate on every edge of the bright (resp. dark) sublattice in Fig. 1. Note that H_{CT} is not present in architectures I-II. Also, realize that $\deg_P(i)$ takes value 4 on bulk qubits, 2 on the corners and 3 elsewhere on edges; for architecture III, $\deg_{DB}(i)$ takes value 1 everywhere.

(B): Mapping output probabilities to Ising partition functions

Let $\mathcal{L}_X = (V_X, E_X)$ (resp. $\mathcal{L}_Z = (V_Z, \emptyset)$) be the primitive-qubit square sublattice of $\mathcal{L}$ (resp. the disjoint union of all dangling-bond qubits), and pick $\mathcal{L}_X$ to be the lattice $\mathcal{L}_P$ in the main text. Let $\alpha := \pi a$, $\vartheta := \beta + \frac{\pi}{4} b$, where we let b be the string of outcomes of the Z measurements in architecture III, and define $b_i := 0, i = 1, \ldots, N_Z$, by convention, for architectures I-II. Further, let $\theta = \pi/8$ for architecture II and $\theta = \pi/4$ otherwise. We now prove equation (3) using formula (7):

$$|\langle a,b|e^{-iH}|\psi_\beta\rangle| = |\langle a,b|e^{-i(H+\sum_{i \in V} \frac{\beta_i}{2} Z_i)}|+\rangle^{\otimes N}| = |\langle a,b|e^{-i(\sum_{(i,j) \in E} J_{i,j} Z_i Z_j - \sum_{i \in V} (h_i - \frac{\beta_i}{2}) Z_i)}|+\rangle^{\otimes N}|$$

$$= \frac{1}{\sqrt{2}^{N_Z}} |\langle a|e^{-i(\sum_{(i,j) \in E_X} \frac{\pi}{4} Z_i Z_j - \sum_{i \in V_X} \sum_{(i,k) \in E_Z} (h_i - \frac{\beta_i}{2} - \frac{\pi b_i}{8}) Z_i)}|+\rangle^{\otimes N_X}|$$

$$= \frac{1}{\sqrt{2}^{N_Z}} |\langle +|e^{-i\sum_{i \in V_X} \frac{\alpha_i}{2} Z_i} e^{-i(\sum_{(i,j) \in E_X} \frac{\pi}{4} Z_i Z_j - \sum_{i \in V_X} \sum_{(i,k) \in E_Z} (h_i - \frac{\vartheta_i}{2}) Z_i)}|+\rangle^{\otimes N_X}|$$

$$= \frac{1}{\sqrt{2}^{N_Z}} |(\langle 0|H)^{\otimes N_X} e^{-iH^{(\alpha,\beta)}} (H|0\rangle)^{\otimes N_X}| = \frac{1}{\sqrt{2}^{N_Z} 2^{N_X}} \left| \sum_{x,y \in \{0,1\}^{N_X}} \langle x|e^{-iH^{(\alpha,\beta)}}|y\rangle \right|$$

$$= \left| \frac{\mathrm{tr}\left(e^{-iH^{(\alpha,\beta)}}\right)}{\sqrt{2}^{N_Z+2N_X}} \right| = \frac{|\mathcal{Z}^{(\alpha,\beta)}|}{\sqrt{2}^{N_Z+2N_X}},$$

where we have defined $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$ in the second step, and used that $H^{(\alpha,\beta)}$ is diagonal in the final one. We obtain (3) by squaring; therein, $\alpha_i \in \{0, \pi\}$, $\vartheta \in \{0, \theta\}$ follows from the definition.

(C): Mapping experiments E1-E3 to cluster state MBQCs

We show that any architecture E1-E3 can be mapped via a bijection to a computationally-equivalent sequence of X-Y-plane single-qubit measurements on the 2D cluster state [25]. Below, $T := \mathrm{diag}\left(1, e^{i\pi/4}\right)$ and $\sqrt{T} := \mathrm{diag}\left(1, e^{i\pi/8}\right)$. First, note that (via teleportation) the effect of measuring a dangling-qubit (if present) is equivalent to generating a uniformly-random classical bit $b \in \{0,1\}$ and, subsequently, implementing the gate T^b onto its neighbor; we can thus replace all dangling-bond qubits by introducing a uniformly-random measurement of X or $X_{-\frac{\pi}{4}} = T^\dagger X T \propto X - Y$ on every primitive qubit. Furthermore, we can re-write the input $|\psi_\beta\rangle$ in E1 as

$$|\psi_\beta\rangle = \bigotimes_{i=1}^{N} \sqrt{T}^{kb_i}|+\rangle^{\otimes N}, \tag{8}$$

where $|+\rangle \propto |0\rangle + |1\rangle$, $k \in \{1,2\}$ and $b = (b_1, \ldots, b_N)$ is a random bit-string defined via $b_i := \beta_i/\theta$, with β, θ as in E1. Since $\sqrt{T}$ gates in (8) commute with the Hamiltonian (2) and their effect is unobserved by Z measurements, they can be propagated out of the experiment by measuring $X_{-\frac{\pi}{8}} = \sqrt{T}^{b_i\dagger} X_i \sqrt{T}^{b_i}$ instead of X on every primitive qubit $i \in V$. Combining these facts, we obtain the following mappings:

(C1) Architectures I and III are computationally equivalent to a quantum circuit that prepares a 2D cluster state on their underlying primitive square lattice and measures $\{X, X_{-\frac{\pi}{4}}\}$ randomly on each vertex.

(C2) Architecture II is computationally equivalent to an analogous circuit that performs random $\{X, X_{-\pi/8}\}$ single-qubit measurements, which chooses the latter measurements to be identical along the columns of the 2D cluster state.

(D): Universality of architectures I-III for post-selected MBQC

For each of our architectures I-III, we prove that the ensemble $\{p_\beta, |\Psi_\beta\rangle\}_\beta$ is a universal resource for postselected MBQC w.r.t. the measurements in step E3. Precisely, this means that if the ability to post-select the outcomes of the experiment's random variables (the qubit outcomes in step E3 and the random vector β) is provided as an oracle [20, 71], then it is possible to implement any poly-size quantum circuit [72] with arbitrarily high-fidelity in a subregion of the lattice using (at most) polynomially-many qubits. Our proof is constructive and shows how to simulate universal circuits of Clifford $+ T$ gates [73] via postselection.

Below, we call a quantum circuit *1D homogeneous* if it consists of 1D nearest-neighbor gates that and parallel operations are identical modulo translation. The latter do not need to be translation-invariant: e.g., an arbitrary S-size 1D nearest-neighbor circuit can be serialized to be 1D homogeneous in depth $O(S)$. In Fig. 3 below, we give an example of an S-size IQP circuit that can be implemented in depth $O(\sqrt{S})$ (by bringing single-qubit gates to the end). 1D homogeneous circuits, as defined here, can be regarded as examples of quantum cellular automata [74].

Lemma 3 (Postselected universality). *Let V be an n-qubit D-depth 1D homogeneous circuit of Clifford+T gates. Then, for any architecture* I-III*, it is possible to prepare the right-most primitive qubits of an $O(n) \times O(Dn)$-qubit lattice on a state $|\psi\rangle := (V|0\rangle^{\otimes n}) |0\rangle^{\otimes r}$, $r \in O(n)$, using postselection.*

We highlight that the complexity of the simulation in Lemma 3 scales with the depth of the input circuit (not the size), allowing to parallelize concurrent nearest-neighbor gates. To prove this result, we assumes basic knowledge of MBQC on cluster states [25, 39]. Additionally, we make use of two technical lemmas.

Lemma 4. *Let V be an n-qubit D-depth 1D homogeneous Clifford+T circuit. Then, the state $|\psi\rangle := (V|0\rangle^{\otimes n}) |0\rangle^{\otimes 3n-2}$ can be efficiently prepared exactly via an MBQC of single-qubit $\{X, X_{\pm\pi/8}\}$ measurements on an $(4n-2) \times O(Dn)$-qubit 2D cluster state, and even if measurements are constrained to act "quasi-periodically" as follows: for every column, each of its qubits is measured in either the X basis, or in one of the $X_{\pm\pi/8}$ bases (where the sign can be picked freely on distinct sites).*

Lemma 5. *Let V be an n-qubit D-depth 1D homogeneous Clifford+T. Then, the state $|\psi\rangle = V|0\rangle^{\otimes n}$ can be efficiently prepared exactly via an MBQC of single-qubit $\{X, X_{\pm\pi/4}\}$ measurements on an $n \times O(Dn)$-qubit 2D cluster state.*

Lemma 4 is an MBQC implementation of a 1D quantum-computation scheme given in Ref. [40]. Lemma 5 follows from Lemma 3 in Ref. [41] by using that commuting-gate measurement-patterns can be applied simultaneously in MBQC.

Proof of Lemma 4. We first show how to implement a universal set of gates that can be converted to the Clifford+T gate-set. We begin by picking a translationally-invariant gate set with the desired property [40]:

$$\left\{ E := \left(\prod_{i=1}^{M-1} CZ_{i,i+1} \right) \left(\bigotimes_{j=1}^{M} H_i \right), \quad Y_{\text{all}} := \bigotimes_{j=1}^{M} Y_i, \quad U_A(\alpha) := \bigotimes_{j=1}^{N} e^{-i\frac{\alpha}{2} A_i}, \text{ where } A \in \{X, Z\} \right\}. \tag{9}$$

Above, gates act on a one-dimensional chain of $M := 4n - 2$; H is the Hadamard gate; $CZ_{i,i+1}$ is the CZ gate on qubits $i, i+1$; E is a global entangling gate; and E^{M+1} implements a "mirror" permutation $i \rightarrow \bar{i} := M + 1 - i$ of the qubits. The computation is encoded on n logical qubits with physical positions $[i] := 2i - 1, 1 \le i \le n$. The remaining qubits are kept in the state $|0\rangle$. Ref. [40] shows how to implement generators for the Clifford+T gate-set using the following sequences of (9) operations:

(S1) $\left(E^{M+1-i} Y_{\text{all}} E Y_{\text{all}} E^{i-1} U_Z \left(\mp \frac{\pi}{8} \right) \right) \left(E^{M+1-i} Y_{\text{all}} E Y_{\text{all}} E^{i-1} U_Z \left(\pm \frac{\pi}{8} \right) \right)$, which implements a $e^{\mp i \frac{\pi}{8} Z_i}$ gate;

(S2) $\left(E^{M-i}Y_{\mathrm{all}}EY_{\mathrm{all}}E^{i}U_{X}\left(\mp\frac{\pi}{8}\right)\right)\left(E^{M-i}Y_{\mathrm{all}}EY_{\mathrm{all}}E^{i}U_{X}\left(\pm\frac{\pi}{8}\right)\right)$ implements a $\mathrm{e}^{\mp\mathrm{i}\frac{\pi}{8}X_{i}}$ gate;

(S3) $\left(E^{M-2-[i]}Y_{\mathrm{all}}EY_{\mathrm{all}}E^{[i]+1}U_{X}\left(\mp\frac{\pi}{8}\right)E\right)\left(E^{M-2-[i]}Y_{\mathrm{all}}EY_{\mathrm{all}}E^{[i]+1}U_{X}\left(\pm\frac{\pi}{8}\right)E\right)$ implements a logical $\mathrm{e}^{\mp\mathrm{i}\frac{\pi}{8}X_{[i]}X_{[i+1]}}$ gate.

We will now show that any of the above gate sequences can be implemented directly on an MBQC on an $(4n-2)\times O(n)$-qubit 2D cluster state with quasi-periodic $\{X,X_{\pm\pi/8}\}$ measurements. W.l.o.g., we make E (resp. non-entangling unitaries) act on even steps (resp. odd ones) by introducing identity gates when necessary. We now reorder operations in the creation and measurement of the cluster state as indicated in Fig 2a: therein, balls denote qubits prepared in $|+\rangle$; steps Fig. 2a.(1) and Fig. 2a.(2) implement CZ gates for the preparation of the cluster state; and Fig. 2a.(3) implements a round of measurements. In MBQC, Y_{all} gates can
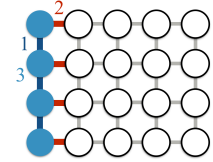
(a) Mapping the TI quantum computation scheme of Ref. [40] to a cluster-state MBQC.
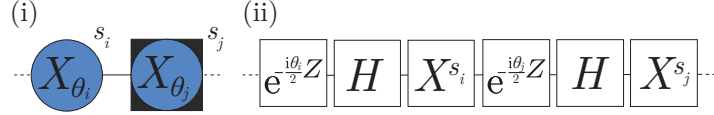
(b) (i) Measurement of $X_{\theta_i}, X_{\theta_j}$ on an edge of a 1D cluster state : the outcomes $s_i, s_j \in \{0,1\}$ are uniformly random. (ii) The associated logical circuit: the byproduct operator X^{s_i} can be propagated forward in circuit by substituting θ_j with $(-1)^{s_1}\theta_j$. The argument extends to the full cluster by induction, choosing the 1st qubit to be measured in the X basis (this fixes the input of the logical circuit and does not change its universality properties). The 2D cluster-state case is analogous [25, 39].

Figure 2. MBQC techniques used in proofs of Lemmas 3-5.

be treated as byproduct Pauli operators and do not need to be enacted [39]. Further, performing a periodic measurement of X in Fig. 2a.(3) implements the E gate in (9). In turn, a quasi-periodic $X_{\pm\pi/8}$ measurement, where observables' signs are chosen adaptively to counteract random byproduct operators, can be used to implement E followed by a $U_Z(\pm\pi/8)$ gate. Similarly, and last, we can implement $EU_X(-\pi/8)$ by delaying the measurement to the next step and propagating a $U_Z(-\pi/8)$ backwards: this works because U_Z and U_X never occur in subsequent odd steps in sequences (S1)-(S2)-(S3). We thus have an MBQC simulation of the translation-invariant computation in Ref. [40].

Last, we show that an n-qubit D-depth homogeneous circuit of $\mathrm{e}^{\mp\mathrm{i}\pi Z_{[i]}/8}$, $\mathrm{e}^{\mp\mathrm{i}\pi X_{[i]}/8}$, $\mathrm{e}^{\mp\mathrm{i}\pi X_{[i]}X_{[i+1]}/8}$ gates can be implemented on an $(4n-2)\times O(Dn)$-qubit cluster-state MBQC using the above protocol. Here, we invoke that measurement-patterns on disjoint-regions of a cluster-state MBQC can be simultaneously applied for commuting logical gates (hence, also concurrent ones): the latter fact is easily verified in the logical-circuit picture of the MBQC [39, 75]. $\square$

Proof of Lemma 5. Lemma 3 in Ref. [41] shows that performing an $X_{\pm\pi/4}$ measurement on a boundary qubit of an $n\times(n+2)$ one can selectively implements any logical gate of form $\mathrm{e}^{\mp\mathrm{i}\pi Z_i/8}$, $\mathrm{e}^{\mp\mathrm{i}\pi X_i/8}$, $\mathrm{e}^{\mp\mathrm{i}\pi Z_j X_{j+1}/8}$, $\mathrm{e}^{\mp\mathrm{i}\pi X_j Z_{j+1}/8}$, $1 \le i \le n, 1 \le j \le n-1$ on an n-qubit 1D chain. As in proof of Lemma 5, measurement-patterns associated to commuting gates can be implemented simultaneously. The result of Ref. [41] thus yields an exact $n \times (n+2)$ cluster-state MBQC implementation of any circuit of form

$$\bigotimes_{i=1}^{n}\mathrm{e}^{-\mathrm{i}\frac{\pi b_i}{8}X_i}C\bigotimes_{i=1}^{n}\mathrm{e}^{-\mathrm{i}\frac{\pi a_i}{8}Z_i}, \quad b_i, a_i \in 0,1 \tag{10}$$

for any n-qubit 1D commuting circuit C of $\mathrm{e}^{-\mathrm{i}\frac{\pi}{8}Z_j X_{j+1}}$, $\mathrm{e}^{-\mathrm{i}\frac{\pi}{8}X_j Z_{j+1}}$ gates. The proof follows as the one of Lemma 4. $\square$

We now proof the main claim of this appendix.

Proof of Lemma 3. Recall that our experiments can be re-casted as a non-adaptive cluster-state MBQCs via mappings (C1)-(C2). Hence, it suffices to show how to prepare $|\psi\rangle = (V|0\rangle^{\otimes n})|0\rangle^{\otimes r}$ exactly for some $r \in O(n)$ using two kinds of operations:

(D1) Postselected random $\{X, X_{-\frac{\pi}{4}}\}$ measurements on a $(n+r) \times O(Dn)$-qubit cluster state.

(D2) Postselected random $\{X, X_{-\frac{\pi}{8}}\}$ measurements, chosen identically on columns, on a $(n+r) \times O(Dn)$-qubit cluster state.

Statement (D1) (resp. (D2)) covers the case for I and III (resp. architecture II).

To prove (D1)-(D2), we show that if an MBQC scheme on a cluster state is universal w.r.t. a family of X-Y measurements $\{X_{\theta_i}\}_i$, $X_{\theta_i} := \mathrm{e}^{\mathrm{i}\frac{\theta_i}{2}Z}X\mathrm{e}^{-\mathrm{i}\frac{\theta_i}{2}Z}$, then, the reduced positive-angle family $\{X_{|\theta_i|}\}_i$ is universal for postMBQC; in combination with Lemmas 5- 4, the claims follow. Recall that any non-final measurement in cluster-state MBQC [25, 39] produces a uniformly random outcome $s \in \{0,1\}$ (cf. appendix E, Eq. (12) for an explicit formula), whose effect in the logical circuit is to

introduce a random byproduct Pauli operator X^s on its associated qubit-line. If not accounted for (e.g., by adapting the measurement basis) and an X_θ is subsequently performed, the latter effectively implements a $X_{(-1)^s\theta}$ measurement: this can be seen by propagating X^s forward in the circuit using conjugation relationships, and it is illustrated in Fig 2b. □

(E): #P-hardness of approximating output probabilities (proof of Lemma 2)

In this appendix, we prove Lemma 2 of the main text.

Lemma 2 (#P-hardness)**.** *Let $H^{(\alpha,\beta)}$ be the Ising model (4) on the $n \times m$ square lattice with either (i) DO-distributed ϑ and $\theta \in \{0, \frac{\pi}{4}\}$; or (ii) $\mathrm{TI}_{(1,\infty)}$-distributed ϑ and $\theta \in \{0, \frac{\pi}{8}\}$. Then, for $m \in O(n^2)$, approximating $|\mathcal{Z}^{(\alpha,\beta)}|^2$ with relative error $\frac{1}{4} + o(1)$ is #P-hard.*

We stress that our upper bound $m \in O(n^2)$ in Lemma 2 is not known to be optimal. In fact, we believe the result should still hold for $m \in O(n)$ (possibly for a different constant error) based on two pieces of evidence. On the one hand, our anti-concentration numerics (appendix F), indicate that the $O(n)$-depth universal random circuits of gates of form (5)—whose output probabilities are in on-to-one correspondence via (6) with the instances of $|\mathcal{Z}^{(\alpha,\beta)}|^2$—are Porter-Thomas distributed: the latter is a signature of quantum chaos, and of our quantum circuits being approximately Haar-random [17, 43–47]. Hence, our numerics suggest that our $n \times n$-qubit lattices efficiently encode chaotic approximately-Haar-random n-qubit unitaries. On the other hand, we analytically show that #P-hardness arises for $m \in O(n)$ and slightly- different choices of input states (resp. dangling-bonds) in architectures I-II (resp. III) (cf. appendix H) .

Our proof below shows that the ability to approximate the given Ising partition function can be used to approximate the output probabilities of the "dense" 2-local long-range IQP circuits of Ref. [16]. The proof further exploits a new technique to implement $O(n^2)$-size long-range IQP circuits in $O(n)$-depth in a 1D nearest-neighbor architecture, which is asymptotically optimal. We regard this result of independent interest since the latter dense IQP circuits were argued in Ref. [16] to exhibit quantum-supremacy but, to our best knowledge, linear-depth 1D implementations for them were not previously known. On the other hand, recently, it has been shown that a "sparse" sub-family of the latter IQP circuits can be implemented in depth $O(n\log n)$ in a 2D nearest-neighbor architecture [19].

A 1D linear-depth implementation of dense IQP circuits. We first derive our intermediate result for IQP circuits.

For any positive n, we let $\mathcal{C}$ be any "dense" random n-qubit IQP circuit whose gates are uniformly chosen from the set

$$\left\{ e^{i\theta_{i,j}X_iX_j}, e^{i\theta_iX_i} \ : \ i,j \in \{1,\dots,n\}, \theta_i,\theta_{i,j} \in \left\{ \frac{\pi k}{8}, k = 0,\dots,7 \right\} \right\}, \tag{11}$$

which contains arbitrary long-range interactions in a fully-connected architecture.

Lemma 6. *Dense n-qubit IQP circuits of (11) gates can be implemented in $\Theta(n)$-depth in a 1D nearest-neighbor architecture.*

Proof. It is easy to see that n^2-size 2-local quantum circuits require $\Omega(n)$ depth to be implemented. Our proof gives a matching upper bound for the given IQP circuits.

Recall that IQP gates can performed in any order (as they commute). Hence, by reordering gates and redefining the $\theta_{i,j}$ angles, any given IQP circuit $\mathcal{C}$ can be put in a normal form $\mathcal{C}'$ that contains at most one single-qubit gate per qubit and one two-qubit gate per pair of qubits. Our approach now is to introduce additional layers of nearest-neighbor SWAP gates following layers of two-qubit gates (Fig.3). To illustrate the algorithm, we regard qubits as "particles" moving up or down the line by the action
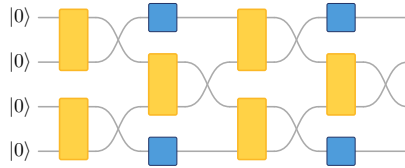

Figure 3. Linear depth implementation of dense IQP circuits (11). We illustrate our algorithm for 4-qubits. Yellow- (resp. blue-) blocks implement the two- (resp. one-) qubit gates in (11). The contains 4 single-qubit gates (resp. 6 two-qubit ones), which coincides with the number of vertices (resp. edges) of the complete graph K_4.

of the SWAP gates. At a given step t, we apply a two-qubit IQP gate followed by a SWAP to all pairs of form $(2i-1, 2i)$ for $1 \le i \le \lfloor n/2 \rfloor$ when t is even (resp. $(2i, 2i+1)$ for $1 \le i \le \lfloor (n-1)/2 \rfloor$ when t is odd). By iterating this process n-times, the qubit initially in the ith position in the line (with arbitrary i) travels to the $n-i+1$th position, meeting every other qubit exactly one time along the way due to the Intermediate Value Theorem; each 2-qubit gate of $\mathcal{C}'$ is implemented in one of these

crossing. Furthermore, each qubit spends one step without meeting any qubit when they reach the line's boundary; at these points, single-qubit gates can be implemented. $\qquad\square$

Proof of Lemma 2. Below, we let $\Gamma := \{\beta \in \{0, \theta\}^{mn} : p_\beta \neq 0\}$ be the set of allowed configurations for β in step E1; $x \in \{0, 1\}^n$ (resp. $y \in \{0, 1\}^{N-n}, N = \mu mn$) be the measurement outcomes of the n right-most primitive qubits (resp. remaining ones) after step E3; and $q(x, y, \beta)$ be the final total probability of observing the values x, y, β.

As in appendix D, it will be convenient to recast our architectures as non-adaptive using mappings (C1)-(C2). In this picture, the following identity readily follows from standard properties of X-teleportation circuits [75]:

$$q(x, y, \beta) = q(x, y|\beta)p_\beta = q(x|y, \beta)\frac{1}{2^{N-n}}\frac{1}{|\Gamma|}, \quad \text{for any } x \in \{0, 1\}^n, y \in \{0, 1\}^{N-n}, \beta \in \Gamma, \tag{12}$$

where we use that p_β is uniformly supported over Γ (by design) as well as $q(y|\beta) = 1/2^{N-n}$, which follows from standard properties of X-teleportation circuits [75]. Note that $\text{prob}(a, b|\beta)$ in (3) and $q(x, y|\beta)$ as above are identical probability distributions up to a relabeling $(x, y) = \ell(a, b)$ of the random variables. Thus, if $\widetilde{q}(\ell(a, b)|\beta)$ approximates $q(\ell(a, b)|\beta)$ up to relative error $1/4 + o(1)$, then, $|\widetilde{\mathcal{Z}}^{(\pi a, \frac{\pi}{4}b+\beta)}|^2 := \widetilde{q}(\ell(a, b)|\beta)2^{N_X + N_Z/2}$ approximates $|\mathcal{Z}^{(\pi a, \frac{\pi}{4}b+\beta)}|^2$ with the same error. Hence, the proof reduces to showing that approximating $q(x, y|\beta)$ for architectures I-III is #P-hard for the given error and $m \in O(n^2)$.

Next, recall that the output probabilities $a_z = |\langle z_1, \ldots, z_k|\mathcal{C}|0\rangle^{\otimes k}|^2$ of an arbitrary k-qubit dense IQP circuits $\mathcal{C}$ as in (11) are #P-hard to approximate up to relative error $1/4 + o(1)$ [76, 77]. Via Lemmas 3 and 6, the latter can further be implemented in our architectures using lattices with $n \times O(n^2)$ qubits for some $n := k + r$ with $r \in O(k)$; to apply Lemma 3, we can either decompose $\mathcal{C}$ exactly as a 1D homogeneous Clifford+T circuits [78], or use the gadgets in the proofs of Lemmas 4-5 to directly implement the IQP gates. Now, let $|\psi\rangle_{y, \beta}$ denote the state of the n right-most primitive qubits after observing y, β. It follows from our discussion that $|\psi\rangle_{y, \beta} = (\mathcal{C}|0\rangle^{\otimes k})|0\rangle^{\otimes r}$ for some efficiently-computable value of y, β. Defining $\overline{z} := (z_1, \ldots, z_k, 0_{k+1}, \ldots, 0_{k+r})$, it follows that $a_x = q(\overline{z}|y, \beta)$. Further, if $\widetilde{q}(\overline{z}, y|\beta)$ approximates $q(\overline{z}, y|\beta)$ up to relative error $\eta > 0$, then, $\widetilde{q}(\overline{z}|y, \beta) := \widetilde{q}(\overline{z}, y|\beta)2^{N-n}$ approximates $q(\overline{z}|y, \beta)$ with the same error. Hence, approximating $q(\overline{z}|y, \beta)$ up to relative error $1/4 + o(1)$ is #P-hard. $\qquad\square$

(F): Hardness argument (proof of theorem1)

We prove Theorem 1. Similarly to Refs. [15, 16], we apply Stockmeyer's Theorem [52] to relate the problems of approximately sampling from output distributions of quantum circuits to approximating individual output probabilities. Our proof is by contradiction: assuming that the worst-case #P-hardness of estimating the partition functions of the Ising models (4) extends to average-case (Conjecture 2) and that the output probabilities of experiments E1-E3 are sufficiently anti-concentrated (Conjecture 3), we show that the existence of a classical algorithm for sampling from the latter within constant ℓ_1-norm implies that an FBPP$^{\text{NP}}$ algorithm can solve #P-hard problems; this leads to a collapse of the polynomial hierarchy to its third level in contradiction with Conjecture 1.

Let $\Gamma := \{\beta \in \{0, \theta\}^{mn} : p_\beta \neq 0\}$ be the set of allowed β configurations in step E1; $x \in \{0, 1\}^n$ (resp. $y \in \{0, 1\}^{N-n}, N = \mu mn$) be the measurement outcomes of the n right-most primitive qubits (resp. remaining ones) after step E3; and $q(x, y, \beta)$ be the final total probability of observing the values x, y, β. As a preliminary, we prove that if Conjecture 3 holds, then the probability distribution $q(x, y, \beta)$ associated to random-input states and measurement outcomes of architectures I-III is anti-concentrated. We first note that $q(x|y, \beta)$ in (12) coincides with the output distribution of some n-qubit $O(m)$-depth circuit $\mathcal{C}_{y, \beta}$ of gates of form (5): this is easily seen from mappings (C1)-(C2) and standard properties of X-teleportation [39, 75] (cf. also the next appendix and Fig. 4). Let us now define

$$\gamma_{y, \beta} := \frac{|\{x \in \{0, 1\}^n : q(x|y, \beta) \geq 1/2^n\}|}{2^n}, \ y \in \{0, 1\}^{N-n}, \beta \in \Gamma; \quad \alpha := \frac{|\{y \in \{0, 1\}^{N-n}, \beta \in \Gamma : \gamma_{y, \beta} \geq 1/e\}|}{2^{N-n}|\Gamma|}; \tag{13}$$

$\gamma_{y, \beta}$ is the fraction of $\mathcal{C}_{y, \beta}$'s output probabilities larger than $1/2^n$, and α is the fraction of $\mathcal{C}_{y, \beta}$ circuits that fulfill (6). Conjecture 3 states that $\gamma_{y, \beta} \geq 1/e$ for $m \in O(n)$. Consequently, for $n \times O(n)$ lattices, (12) implies that

$$\text{prob}_{x, y, \beta}\left(q(x, y, \beta) \geq \frac{1}{2^N|\Gamma|}\right) \geq 1/e. \tag{14}$$

Furthermore, since $q(y, \beta)$ is uniformly distributed over its support, it also follows from (12) that

$$\text{prob}_{x,y,\beta} \left(q(x, y, \beta) \geq \frac{1}{2^N |\Gamma|} \right) = \sum_{y,\beta} \frac{\gamma_{y,\beta}}{2^{N-n}|\Gamma|} = \mathbb{E}_{y,\beta} \left(\gamma_{y,\beta} \right) \geq \frac{\alpha}{e}, \text{ for a uniformly random } x, y \in \{0, 1\}^N, \beta \in \Gamma. \quad (15)$$

Eq. (15) tells us that the robustness of the anti-concentration inequality (14) can be tested by computing the average value $\mathbb{E}_{y,\beta} \left(\gamma_{y,\beta} \right)$ of $\gamma_{y,\beta}$, or by estimating the fraction α. As it will be discussed in appendix G, $\gamma_{y,\beta} \times e$ and α are expected to converge to one for universal 1D nearest-neighbor circuits as n grows asymptotically [45–47, 79] in the regime $m \in O(n)$ [80–82]. In appendix G, Fig. 5, we present numerical evidence that $\mathbb{E}_{y,\beta} \left(\gamma_{y,\beta} \right) \to 1/e$, $\alpha \to 1$ in the asymptotic limit and a tight agreement for $n \geq 9$; more strongly, we also find that $\gamma_{y,\beta}$ is nearly $1/e$ for almost every uniformly-sampled instance for $n \geq 9$ and that $q(x|y, \beta)$ is Porter-Thomas distributed, which is a signature of Haar-random chaotic unitary processes [17, 43–47].

We are now ready to prove Theorem 1. For any architecture I-III, we let a denote an element of $\{0, 1\}^N \times \Gamma$, and assume that the output distribution $p_c(a)$ of a classical BPP algorithm fulfills that

$$\sum_{a \in \{0,1\}^N \times \Gamma} |p_c(a) - q(a)| \leq \varepsilon, \quad (16)$$

for a constant $\varepsilon \geq 0$. By Stockmeyer's Theorem [52] and the triangle inequality, there exists an $\mathsf{FBPP}^{\mathsf{NP}}$ algorithm that computes an estimate $\widetilde{p_c(a)}$ such that

$$|\widetilde{p_c(a)} - q(a)| \leq \frac{q(a)}{\text{poly}(N)} + |p_c(a) - q(a)| \left(1 + \tfrac{1}{\text{poly}(N)} \right), \quad (17)$$

where we used $\log |\Gamma| \in O(N)$ to remove dependencies on $|\Gamma|$. From Markov's inequality and (16), we get that

$$\text{prob}_a \left(|p_c(a) - q(a)| \geq \frac{\varepsilon}{2^N |\Gamma| \delta} \right) \leq \delta, \quad \text{for any constant } 0 < \delta < 1, \quad (18)$$

when $a \in \{0, 1\}^N \times \Gamma$ is picked uniformly at random. Hence,

$$|\widetilde{p_c(a)} - q(a)| \leq \frac{q(a)}{\text{poly}(N)} + \frac{\varepsilon (1 + o(1))}{\delta 2^N |\Gamma|} \quad (19)$$

with probability at least $1 - \delta$ over the choice of a.

We now claim that Eqs. (19) and (14) simultaneously hold for a single $q(a)$ with probability $(1/e) \cdot (1 - \delta)$, since a classical description of I-III does not reveal to a classical sampler which output probabilities are #P-hard to approximate: hence, the latter cannot adversarially corrupt the latter. This is manifestly seen at the encoded random circuit level, due to the presence of random byproduct operators of form $\bigotimes_i X_i^{y_i}$ (with random y_i), which obfuscate the location of the #P-hard probabilities from the sampler [16, 48]. Hence, setting $\varepsilon = \gamma/8, \delta = \gamma/2, \gamma = 1/e$, we obtain that

$$|\widetilde{p_c(a)} - q(a)| \leq \left(\frac{1}{4} + o(1) \right) q(a) \quad (20)$$

with probability at least $\gamma(1 - \gamma/2) > 0.3$ over the choice of a. Setting $\varepsilon = 1/22 < \gamma/8$, the above procedure yields an approximation $\widetilde{p_c(a)}$ of $q(a)$ up to relative error $1/4 + o(1)$. Using (3) and (12), we obtain an $\mathsf{FBPP}^{\mathsf{NP}}$ algorithm that approximates $|\mathcal{Z}^{\alpha,\beta}|^2$ with relative error $1/4 + o(1)$ for at least a 0.3 fraction of the instances. This yields a contradiction.

As final remarks, note that the above argument is robust to small finite-size variations to the threshold $\gamma = 1/e$ in Conjecture 3, Eq. (6) since the constants $\varepsilon = \gamma/5, \delta = \gamma/2$, and $\gamma(1 - \gamma/2)$ have only linear and quadratic dependencies on γ. Also, notice that Conjectures 2 and 3 enter the above argument in order to allow for a constant additive error ε, which is key for a real-life demonstration of quantum supremacy. However, in the ideal case where one assumes no-sampling errors, or multiplicative sampling errors, our result holds even without these conjectures via the arguments in Refs. [20, 21].

(G): Numerical evidence for anti-concentration of the output distribution

In this appendix we present numerical evidence for the validity of Conjecture 3, which is exploited in the proof of Theorem 1 as discussed in appendix F. Therein, we discussed that for any architectures I-III, given an initial n-row, m-column square
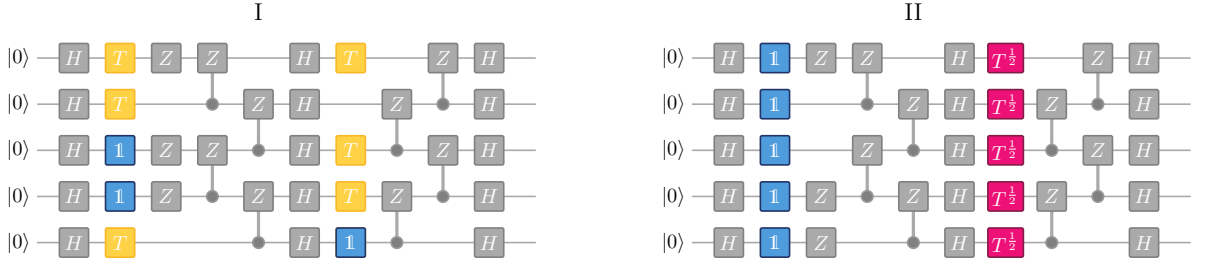
Figure 4. We show the logical circuit corresponding to architectures I and III (left) and II (right) for a 5-row 2-column lattices prepared with uniformly random $\beta_i \in \{0, \pi/4\}$ (blue, yellow) (I and III) and column-random $\beta_i \in \{0, \pi/8\}$ (blue, crimson) (II). At those qubits that have been prepared with $\beta_i = 0$ an identity gate is applied, on those with $\beta_i = \pi/4$ a T gate and on those with $\beta_i = \pi/8$ a $\sqrt{T}$ gate.

lattice, there exists an n-qubit D-depth circuit family $\{\mathcal{C}_{\beta,y}\}_{y,\beta}$ of gates of form (5), with $D \in O(m)$, such that $q(x|y,\beta) = |\langle x|\mathcal{C}_{\beta,y}|0\rangle|^2$. If the circuits $\{\mathcal{C}_{\beta,y}\}_{y,\beta}$ exhibit anti-concentration as in Conjecture 3, then $q(x,y,\beta)$ is anti-concentrated as in Eq. (14). This is used in appendix F to turn an approximate classical sampler into an $\mathsf{FBPP}^{\mathsf{NP}}$ algorithm to approximate single output probabilities with high-accuracy.

The concrete circuit families associated to each architecture are derived below and depicted in Fig. 4. To numerically test Conjecture 3, we have performed simulations of randomly generated circuits of gates of form (5) (for each circuit family) in LIQUiD [83] with up to 20 logical qubits. For each system size, we generated 100 random instances for circuits associated to $n \times n$ and $n \times n^2$ lattices. For each instance, we evaluated exactly the fraction $\gamma_{y,\beta}$ (Eq. 13) of output-probabilities fulfilling (6). Our results are summarized in Fig. 5: therein, one can see that both for circuits associated to $n \times n$ and $n \times n^2$ lattices, this fraction quickly approaches a constant $\gamma = 1/e$ with rapidly decreasing variance with respect to the choice of circuits. We can conclude that, with very high probability, in a realization of the proposed experiment the amplitude of the final state of the computation anti-concentrates

As discussed in Refs. [16, 19, 48], it might seem a priori counter-intuitive that constant-depth nearest-neighbor architectures anti-concentrate. However, the above connections between our architectures and random circuits shed key insights into why this behavior is actually natural. As shown in appendix D, the random logical circuits of gates of form (5) encoded in our architectures are universal for quantum computation. Universal random quantum circuits of increasing depth are known to approximate the Haar measure under various settings [45–47, 79, 82]. For 1D nearest-neighbor layouts, the latter are expected to reach a chaotic Porter-Thomas-distributed regime [43–45] in depth $D \in O(n)$ [80–82] (cf. [17] for further discussion). As an additional piece of supporting evidence for anti-concentration, we numerically confirmed that our output-probabilities are close to being Porter-Thomas-distributed in ℓ_1-norm (Fig. 6). Furthermore, our numerics are in agreement with prior numerical works on MBQC settings [47] and other gate sets in 2D layouts [17, 42].

Circuit families. For the sake of completeness, we spell out the logical circuits that are effectively implemented in architectures I-II. The latter are derived via mappings (C1)-(C2) and X-teleportation properties [75]. Examples for 4×2 lattices are depicted in Fig. 4. The logical circuit family corresponding to I and III (resp. to II) is denoted $\mathcal{F}_{\mathrm{DO}}$ (resp. $\mathcal{F}_{\mathrm{col}}$). Let us now label primitive-lattice sites by row-column coordinates $[i, j]$. The circuits are generated inductively, starting from the left column $j = 1$. Measurements are ordered from left to right. The computation begins on the $|+\rangle^{\otimes n}$ state and proceeds as follows:

1. Apply the gate $\exp\left(\mathrm{i}\beta_{[i,j]} Z_{[i,j]}\right)$ to qubit $[i, j]$, with $\beta_{[i,j]}$ chosen as in step E1 for I-II; for III, we let $\beta_{[i,j]} := s_{[i,j]}\pi/4$, where $s_{[i,j]}$ is the outcome after measuring the dangling-neighbor of $[i, j]$.
2. If $j < m$, apply a random $Z_{[i,j]}^{a_{[i,j]}}$ gate to every qubit $[i, j]$, where $a_{[i,j]}$ is the outcome of the measurement at site $[i, j]$.
3. Apply CZ on all neighboring qubits.
4. Apply a Hadamard gate to each qubit.
5. If $j = m$, measure in the standard basis and terminate; otherwise increase $j := j + 1$.

Convergence to the chaotic regime. It is an interesting detail that the value of $\gamma = 1/e$, which we observe above, is a signature of the exponential distribution (also known as Porter-Thomas distribution) that is known to emerge in chaotic quantum systems for large system sizes [17, 42–45, 47]. This distribution is given by

$$P_{PT}(p) = 2^n \exp(-2^n p), \tag{21}$$

and thus anti-concentrates in precisely the fashion observed here. Note that the same behavior was observed in previous work investigating random MBQC settings [47], as well as in a recent quantum-supremacy proposal based on a 2D architecture in a superconducting-qubit platform [17]. Notably, the finite and universal gate sets considered in these works are very similar to
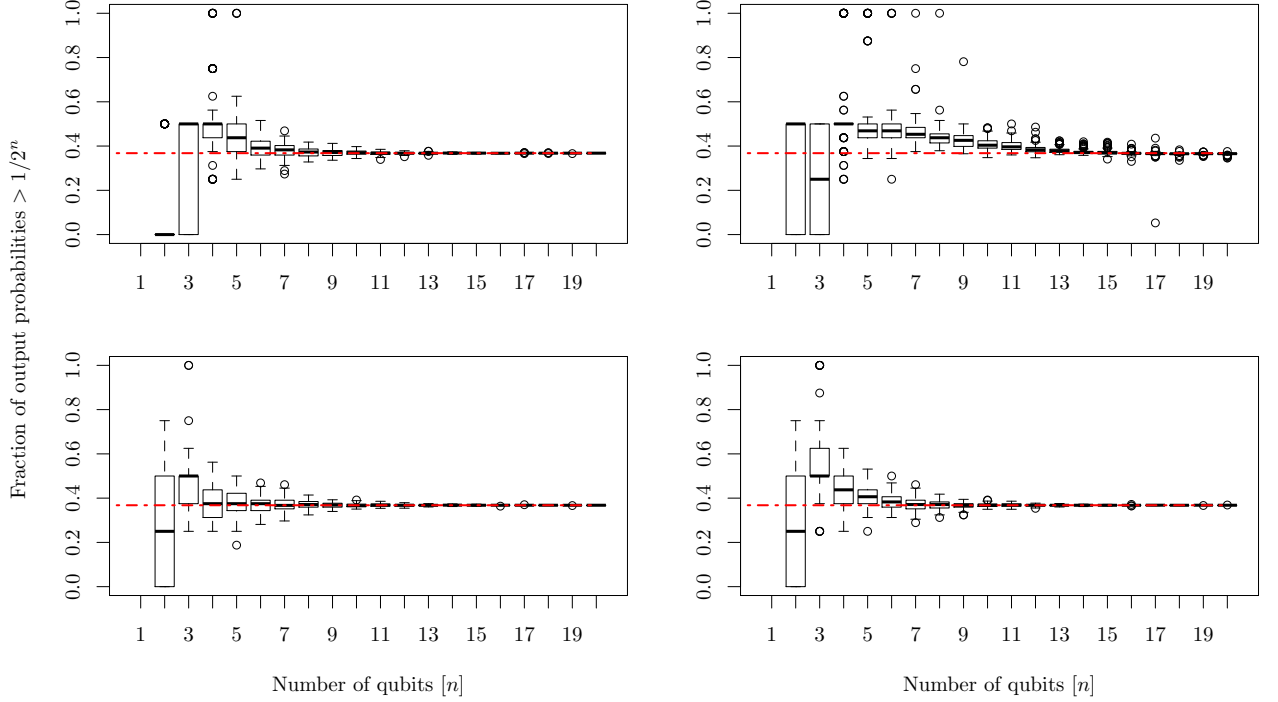
Figure 5. Fraction of output probabilities larger than $1/2^n$ of random circuits drawn from the families $\mathcal{F}_{\text{DO}}$ (l.h.s.) and $\mathcal{F}_{\text{col}}$ (r.h.s.) for both linear (top) and quadratic (bottom) circuit depth in the number of qubits the circuit acts upon n, i.e., lattices of size $n \times n$ (top) and $n \times n^2$ (bottom). For each n we draw 100 i.i.d. realizations (β, y) and thus of the circuit $\mathcal{C}_{\beta,y}$ and plot the resulting distribution in the form of a box plot. The red dashed line shows the value of $1/e$, which is precisely the value to be expected if the output probabilities are Porter-Thomas distributed.

the ones considered here. Likewise, convergence to the exponential distribution was observed in Ref. [42] for approximately Haar-random two-qubit unitaries in a 2D setup.

In Fig. 6 we show the total variation distance between the empirical distributions of output probabilities of the random circuits generated in our numerical experiments and the discretized Porter-Thomas distribution. We can see that as the number of qubits increases, the output distributions of random circuits approach Porter-Thomas distribution.

To calculate the total variation distance to the exponential distribution (21), we discretized the interval $[0, 1]$ into m bins each of which contains probability weight $1/m$. In other words, the discretization $(p_0, p_1, \ldots, p_m)$ is defined by given $p_0 = 0$, $p_m = 1$ and

$$\int_{p_i}^{p_{i+1}} P_{PT}(p)\mathrm{d}p = \frac{1}{m}. \tag{22}$$

Denote by $Q(p)$ the numerically observed distribution of output probabilities $p = |\langle x|\mathcal{C}|0\rangle|^2$ over the set $\Omega = \{[p_i, p_{i+1}]\}_{i=0,\ldots,m}$. The total variation distance between P and the exponential distribution is then given by

$$\|P - Q\|_{\text{TV}} = \frac{1}{2} \sum_{X \in \Omega} |P(X) - 1/m|. \tag{23}$$

Since the number of samples we obtain in each run is given by 2^n we choose the number of bins m depending on n. Specifically, we choose $m = \min\{\lceil 2^n/5\rceil, 100\}$ to allow fair comparison for small n.

(H): #P-hardness from $n \times O(n)$ lattices

In this appendix, we show that #P-hardness of approximating output probabilities in Lemma 2 arises already for $n \times m$-qubit lattices with $m \in O(n)$. Specifically, we prove this by introducing two slight modifications in architectures I-II without changing
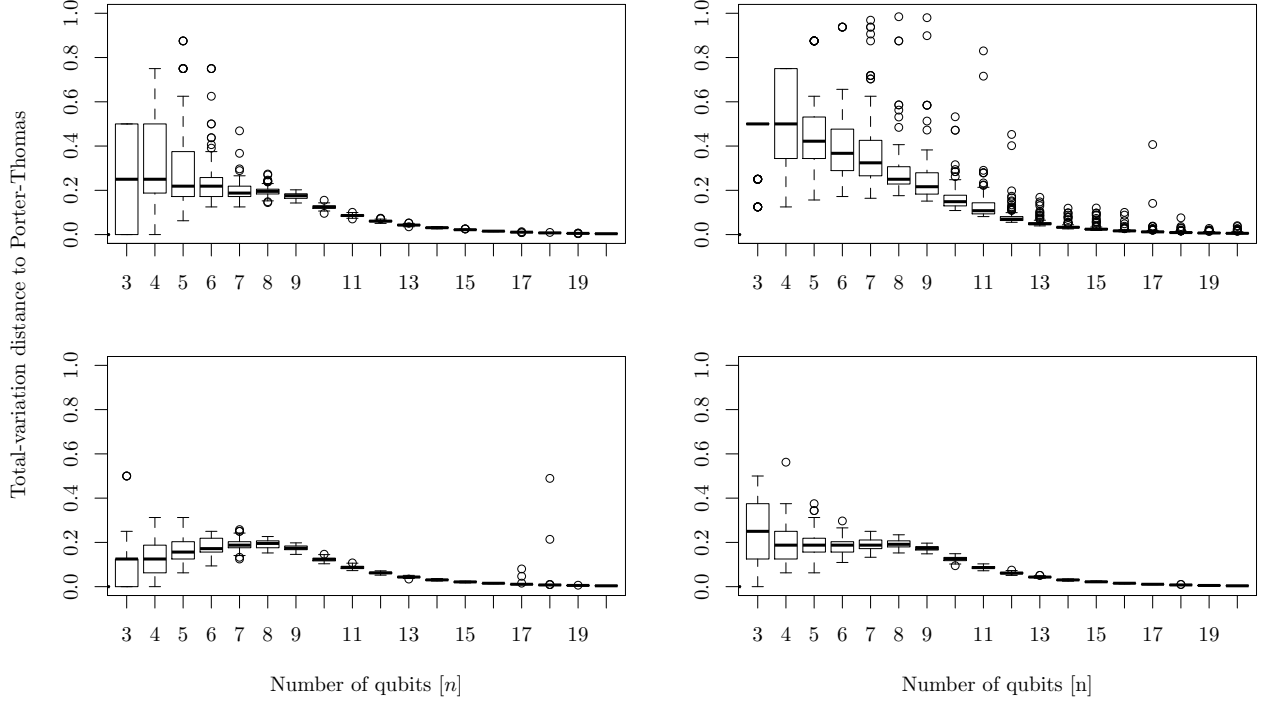
Figure 6. Total variation distance to the Porter-Thomas distribution of the empirical distribution of output probabilities of random circuits from the families $\mathcal{F}_{\mathrm{DO}}$ (l.h.s.) and $\mathcal{F}_{\mathrm{col}}$ (r.h.s.) for both linear (top) and quadratic (bottom) circuit depth in the number of qubits the circuit acts on n, i.e., lattice of size $n \times n$ (top) and $n \times n^2$ (bottom). For each n we draw 100 i.i.d. realizations (β, y) and thus of the circuit $\mathcal{C}_{\beta,y}$ and plot the resulting distribution in the form of a box plot.

the fundamental structure of the basic layout of the steps E1-E3.

The key idea is to introduce different types of input states (with different β_is) in the preparation step E3: specifically, we pick $\beta_i \in \{0, \theta\}$ for qubits on odd-row sites, $\beta_i \in \{0, \pi/2\}$ on even-row ones; additionally, we perform a local Hadamard rotation on even-row sites before the Ising Hamiltonian evolution in step E2 begins. The net effect is to initialize even-site qubits on either $|0\rangle$ (the +1-eigenstate of Z) or $|-i\rangle := |0\rangle - i|1\rangle$ (the -1-eigenstate of Y) at random. Qubits initialized in $|0\rangle$ are invisible to the Ising evolution (E2) and effectively become unentangled from the computation. Further, preparing a qubit in $|-i\rangle$, evolving (E2) and measuring X is equivalent to preparing $|+\rangle$ and measuring Y instead at the end of the computation. Again, we choose the $|\psi_\beta\rangle$ to be fully disordered (DO) for architecture I. For architecture II, we pick $|\psi_\beta\rangle$ to be TI in one direction with period at most 4, i.e., $\mathrm{TI}_{(4,\infty)}$-symmetric in our notation.
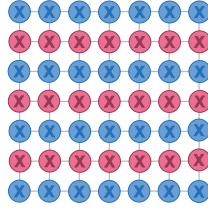

Figure 7. Modified architectures I-II. Sites were we introduce changes are marked in pink. Therein, we pick $\beta_i \in \{0, \pi/2\}$ and perform local Hadamard rotation: for architecture I, β_i is uniformly-random; for architecture II, β_i is TI on columns with period less than or equal to 4.

The full experiment can now be mapped to non-adaptive MBQC analogue to (C1) with two differences: first, the MBQC acts on a graph state $|G\rangle$ [84], instead of a cluster state, whose underlying graph G is derived from the 2D lattice by deleting $|0\rangle$-state vertices (the output probabilities of the computation can be mapped to an Ising model on G using the tools of appendices A-B); second, the remaining vertices on even columns are measured on the Y basis. We now pick $n = 2k - 1$ and study the logical-circuit of the MBQC in two scenarios:

(i) All even-row qubits are initialized in $|0\rangle$. The MBQC acts on a graph-state $|G'\rangle$ that is the product of k disconnected 1D

cluster states. Modulo byproduct operators, the local measurements drive a random logical k-qubit circuit of single-qubit gates $\{R_i^{a_i}(\theta) := H_i e^{i(a_i\theta)Z_i}, a_i \in \{0,1\}\}$ and depth $m-1$ (information flows on odd rows). For architecture II, the latter circuit inherits a $\mathrm{TI}_{(2,\infty)}$-symmetry from the $\mathrm{TI}_{(4,\infty)}$-one of the input state $|\psi_\beta\rangle$.

(ii) Even-column even-row qubits are initialized in $|0\rangle$; even-column odd-row ones are left unspecified. The MBQC acts on a cluster-state with "holes" $|G''\rangle$ as in Refs. [85, 86]. Information flows again on odd-rows. If an even-column odd-row qubit i is prepared in $|{-}i\rangle$ and measured in the X basis (or, equivalently, in $|+\rangle$ and measured in the Y basis), we obtain a reduced graph-state $|G'''\rangle$ whose graph G''' is obtained from G'' by contracting the edges incident to i [85, 86]. Thus, $|{-}i\rangle$ states between the odd qubit lines let us implement logical entangling gates of form

$$E^{b,c}(\theta) := \left(\bigotimes_{i=1}^{k} H_i\right)\left(\prod_{i=1}^{k-1} CZ_{i,i+1}^{b_i}\right)\left(\bigotimes_{i=1}^{k} e^{i(c_i\theta)Z_i}\right), \qquad b_i, c_i, \in \{0,1\},$$

where $b_i = 1$ if the qubit between lines $2i, (2i-1)$ is in $|{-}i\rangle$ and zero otherwise; and c_i indicates whether we measure X or $X_{-\theta}$ on the $(2i-1)$th line. Postselecting b_i gives us the ability to implement non-translation-invariant 2-qubit entangling gates between qubit lines at will. Again, for architecture II, the gate $E^{b,c}(\theta)$ inherits a $\mathrm{TI}_{(2,\infty)}$ symmetry.

Combining the above facts, it follows that we can simulate arbitrary k-qubit nearest-neighbor Clifford+T circuits in the modified architecture I via postselection, using lattices with $(2k-1) \times (2k-1)$ qubits. The latter can efficiently implement the #P-hard IQP circuits of Lemma 6 with a constant-overhead factor.

In the modified architecture II, observation (i) and postselection of byproduct operators (Fig. 2b) yields $\mathrm{TI}_{(2,\infty)}$-symmetric circuits of $\{H_i, e^{\pm i\frac{\pi}{16}Z_i}, e^{\pm i\frac{\pi}{16}X_i}\}$ gates. In combination with the gadgets in the proof of Lemma 4, this lets us implement k-qubit $\mathrm{TI}_{(2,\infty)}$-symmetric nearest-neighbor circuits of $e^{\mp i\frac{\pi}{8}X_iX_{i+1}}$ gates. Furthermore, byproduct operators also let us break the $\mathrm{TI}_{(2,\infty)}$ symmetry via the identities below, and allow us to implement non-TI arbitrary nearest-neighbor Clifford+T circuits as in the previous case with constant overhead:

$$\bigotimes_{i=1}^{\lfloor k/2 \rfloor} e^{ia_i\frac{\pi}{4}X_{[i]}X_{[i+1]}} = \left(\bigotimes_{i=1}^{\lfloor k/2 \rfloor} e^{i\frac{\pi}{8}X_{[i]}X_{[i+1]}}\right)\left(\bigotimes_{i=1}^{\lfloor k/2 \rfloor} Z_{[i]}^{a_i}\right)\left(\bigotimes_{i=1}^{\lfloor k/2 \rfloor} e^{-i\frac{\pi}{8}X_{[i]}X_{[i+1]}}\right), \quad [i] := 2i - x_0, x_0 \in \{0,1\}, a_i \in \{0,1\},$$

$$\bigotimes_{i=1}^{\lfloor k/2 \rfloor} e^{ib_i\frac{\pi}{8}X_{[i]}} = \left(\bigotimes_{i=1}^{\lfloor k/2 \rfloor} e^{i\frac{\pi}{16}X_{[i]}}\right)\left(\bigotimes_{i=1}^{\lfloor k/2 \rfloor} Z_{[i]}^{b_i}\right)\left(\bigotimes_{i=1}^{\lfloor k/2 \rfloor} e^{-i\frac{\pi}{16}X_{[i]}}\right), \qquad [i] := 2i - x_0, x_0 \in \{0,1\}, b_i \in \{0,1\}.$$

Again, this yields an efficient and exact postselected implementation of the desired IQP circuits on k logical qubits.