


## Bell Sampling from Quantum Circuits

Dominik Hangleiter<sup>\*</sup> and Michael J. Gullans<sup>†</sup>

*Joint Center for Quantum Information and Computer Science, NIST/University of Maryland,  
College Park, Maryland 20742, USA*

 (Received 20 June 2023; accepted 31 May 2024; published 8 July 2024)

A central challenge in the verification of quantum computers is benchmarking their performance as a whole and demonstrating their computational capabilities. In this Letter, we find a universal model of quantum computation, Bell sampling, that can be used for both of those tasks and thus provides an ideal stepping stone toward fault tolerance. In Bell sampling, we measure two copies of a state prepared by a quantum circuit in the transversal Bell basis. We show that the Bell samples are classically intractable to produce and at the same time constitute what we call a “circuit shadow”: from the Bell samples we can efficiently extract information about the quantum circuit preparing the state, as well as diagnose circuit errors. In addition to known properties that can be efficiently extracted from Bell samples, we give several new and efficient protocols: an estimator of state fidelity, an error-mitigated estimator of Pauli expectation values, a test for the depth of a circuit, and an algorithm to estimate a lower bound on the number of  $T$  gates in the circuit. With some additional measurements, the latter algorithm can be used to learn a full description of states prepared by circuits with low  $T$  count.

DOI: 10.1103/PhysRevLett.133.020601

**Introduction.**—As technological progress on fault-tolerant quantum processors continues, a central challenge is to demonstrate their computational advantage and to benchmark their performance as a whole. Quantum random sampling experiments serve this double purpose [1–4] and have arguably surpassed the threshold of quantum advantage [5–10]. However, this approach currently suffers several drawbacks. Most importantly, it can only serve its central goals—benchmarking and certification of quantum advantage—in the classically simulable regime. This deficiency arises because evaluating the performance benchmark, the cross-entropy benchmark, requires a classical simulation of the ideal quantum computation. What is more, the cross-entropy benchmark suffers from various problems related to the specific nature of the physical noise in the quantum processor [9,11,12] and yields limited information about the underlying quantum state. More generally, in near-term quantum computing without error correction, we lack many tools for validating a given quantum computation just using its output samples.

In this Letter, we consider Bell sampling, a model of quantum computation in which two identical copies of a state prepared by a quantum circuit are measured in the transversal Bell basis; see Fig. 1. We show that this model is universal for quantum computation, that the output samples yield a variety of diagnostic information about the underlying quantum state, and that the samples allow for detecting and correcting certain errors in the state preparation. We may thus think of the Bell samples as classical circuit shadows, in analogy to the notion of state shadows coined by Aaronson [13] and Huang *et al.* [14] since we can

efficiently extract specific information about the generating circuit or a family of generating circuits from them. Bell sampling also serves as a stepping stone toward quantum fault tolerance: not only can we naturally detect certain errors from the Bell samples, but the protocol is also compatible with stabilizer codes—the Bell measurement between code blocks is transversal for such codes and allows for the fault-tolerant extraction of all error syndromes. As a concrete application, we demonstrate that Bell sampling from universal quantum circuits exhibits quantum advantage that can be efficiently validated on near-term quantum processors.

Technically, we make the following contributions. We show that Bell sampling is universal and provide complexity-theoretic evidence for the classical intractability of Bell sampling from random universal quantum circuits,

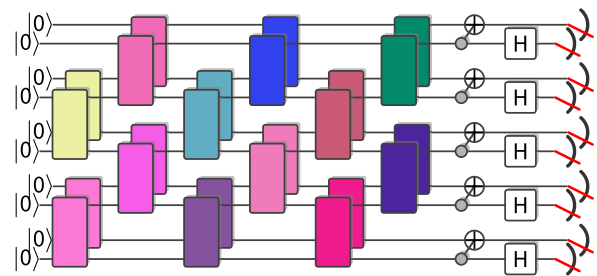


FIG. 1. The Bell sampling protocol. In the Bell sampling protocol we prepare the quantum state  $C|0^n\rangle \otimes C|0^n\rangle$  using a quantum circuit  $C$ , and measure all qubits transversally in the Bell basis across the bipartition of the system.

following an established hardness argument [4,15,16]. We give two new diagnostic primitives based on noiseless Bell samples. First, we introduce a new test to verify the depth of quantum circuits. Here, we make use of the fact that from the Bell basis samples one can compute correlation properties of the two copies and in particular a swap test on any subsystem. Second, we show that the Bell samples can be used to efficiently measure the stabilizer nullity—a magic monotone [17]—and give a protocol to efficiently learn a full description of any quantum state that can be prepared by a circuit with low  $T$  count. Here, we build on a result by Montanaro [18], who has shown that stabilizer states can be learned from Bell samples. In the setting of noisy state preparations, we analytically show that the Bell samples can be used to estimate the fidelity of state preparations and demonstrate the feasibility numerically. We also give a protocol for efficiently detecting errors in the state preparation based only on the properties of the Bell samples.

Of course, the idea to sample in the Bell basis to learn about properties of quantum states is as old as the theory of quantum information itself and has found many applications in quantum computing, including learning stabilizer states [18], testing stabilizerness [19], measuring magic [20,21], and quantum machine learning [22]. The novelty of our approach is to view Bell sampling as a computational model. We then ask what we can learn from the Bell samples about the circuit preparing the underlying quantum state.

*Bell sampling.*—We begin by defining the Bell sampling protocol and noting some simple properties that will be useful in the remainder of this Letter. Consider a quantum circuit  $C$  acting on  $n$  qubits, and define the Bell basis of two qubits as

$$|\sigma_r\rangle = (\sigma_r \otimes \mathbb{1})|\Phi^+\rangle, \quad \text{where } |\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}, \quad (1)$$

and for  $r \in \{0, 1\}^2$  we identify

$$\sigma_{00} = \mathbb{1}, \quad \sigma_{01} = X, \quad \sigma_{10} = Z, \quad \sigma_{11} = i\sigma_{01}\sigma_{10} = Y. \quad (2)$$

The Bell sampling protocol proceeds as follows (see Fig. 1): (1) prepare  $|\mathcal{C}\rangle := |C\rangle \otimes |C\rangle := C|0^n\rangle \otimes C|0^n\rangle$ , and (2) measure all qubit pairs  $(i, i+n)$  for  $i \in [n] := \{1, 2, \dots, n\}$  in the Bell basis, yielding an outcome  $r \in \{0, 1\}^{2n}$ .

It is easy to see that the distribution of the outcomes  $r$  can be written as

$$P_C(r) = \frac{1}{2^n} |\langle C|\sigma_r|\bar{C}\rangle|^2, \quad (3)$$

where  $\sigma_r = \sigma_{r_1 r_{n+1}} \otimes \sigma_{r_2 r_{n+2}} \otimes \dots \otimes \sigma_{r_n r_{2n}}$  is the  $n$ -qubit Pauli matrix corresponding to the outcome  $r = (r_1, r_2, \dots, r_{2n})$ , and  $\bar{C}$  denotes complex conjugation of  $C$ . In order to

perform the measurement in the Bell basis, we need to apply a depth-1 quantum circuit consisting of  $n$  transversal CNOT gates followed by Hadamard gates on the control qubits and a measurement of all qubits in the computational basis.

*Computational complexity.*—We first show that Bell sampling is a universal model of quantum computation. To show this, we observe that we can estimate both the sign and the magnitude of  $\langle C|Z_1|C\rangle$  for any quantum circuit  $C$  from Bell samples from a circuit  $C'(C)$  in which we use a variant of Ramsey interferometry with a single ancilla qubit in each copy of the circuit; see the Supplemental Material (SM) [23]. We then show that approximately sampling from the Bell sampling distribution  $P_C$  is classically intractable on average for universal random quantum circuits  $C$  with  $\Omega(n^2)$  gates in a brickwork architecture (as depicted in Fig. 1), assuming certain complexity-theoretic conjectures are satisfied, via a standard proof technique; see the SM [23] for details. The argument puts the complexity-theoretic evidence for the hardness of Bell sampling from random quantum circuits on a par with that for standard universal circuit sampling [1,5,43–46].

*Bell samples as classical circuit shadows.*—Samples in the computational basis—while difficult to produce for random quantum circuits—yield very little information about the underlying quantum state. In particular, the problem of verification is essentially unsolved since the currently used methods require exponential computing time. In contrast, from the Bell samples, we can *efficiently* infer many properties of the quantum state preparation  $|C\rangle \otimes |C\rangle$ . Known examples include the overlap  $\text{tr}[\rho\sigma]$  of a state preparation  $\rho \otimes \sigma$  via a swap test, the magic of the state  $|C\rangle$  [20], and the outcome of measuring any Pauli operator  $P \otimes P$  [47]. Here, we add new properties to this family. We give efficient protocols for estimating the fidelity, testing the depth of low-depth quantum circuits, for testing its magic, and for learning quantum states that can be prepared by a circuit with low  $T$  count.

Let us begin by recapping how a swap test can be performed using the Bell samples, and observing some properties that are useful in the context of benchmarking random quantum circuits. To this end, write the two-qubit swap operator  $\mathbb{S} = P_{\sqrt{2}} - P_{\wedge^2}$  as the difference between the projectors onto the symmetric subspace  $P_{\sqrt{2}} = |\sigma_{00}\rangle\langle\sigma_{00}| + |\sigma_{01}\rangle\langle\sigma_{01}| + |\sigma_{10}\rangle\langle\sigma_{10}|$  and the antisymmetric subspace  $P_{\wedge^2} = |\sigma_{11}\rangle\langle\sigma_{11}|$ . The overlap  $\text{tr}[\rho\sigma] = \text{tr}[(\rho \otimes \sigma)\mathbb{S}]$  can then be directly estimated up to error  $\epsilon$  from  $M \in O(1/\epsilon^2)$  Bell samples as

$$\frac{1}{M} (|\{r: \pi_Y(r) = 0\}| - |\{r: \pi_Y(r) = 1\}|). \quad (4)$$

For noisy quantum state preparations  $\rho \otimes \rho$ , we can thus estimate the purity  $P = \text{tr}[\rho^2]$  of  $\rho$ . We now argue that the purity is a good estimator for the fidelity  $F = \langle C|\rho|C\rangle$  of

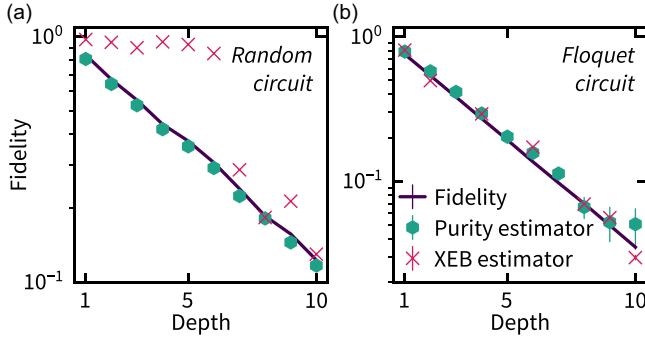


FIG. 2. Fidelity estimation based on noisy Bell sampling. We simulate noisy Bell sampling and XEB, including noisy measurements using  $10^6$  samples, and compute the fidelity (lines), the purity (hexagons), and XEB (crosses) based estimators of fidelity for (a) typical Clifford circuits with two-qubit random gates in an all-to-all connected architecture with XEB 1 on  $n = 20$  qubits and Pauli ( $X, Y, Z$ ) error probabilities  $p = 0.005 \cdot (1, 1/3, 1/10)$ , and (b) crystalline Floquet Clifford circuits that are scrambling [52] on 18 qubits in 1D with (depolarized) two-qubit gate fidelity 0.98. Missing XEB points are due to ideal XEB values 0. Error bars represent 1 standard deviation.

the state preparation if the noise is local circuit-level Pauli noise. Pauli channels naturally appear as the effective noise after repeated rounds of syndrome extraction in stabilizer codes [48,49]. We can also “force” the noise into Pauli noise using randomized compiling implemented independently on two copies of a fixed circuit; this converts experimentally relevant noise into Pauli channels [50,51]. We show that the average fidelity of random circuits with local Pauli noise relates to the average purity as  $\mathbb{E}_C F = \sqrt{\mathbb{E}_C P}$  if the Bell measurement is noise-free [2,12]. The root purity is thus a good estimator of the average fidelity from the Bell samples irrespective of the noise rate and depth of the circuit ensemble with precision  $\sim 1/(F\sqrt{M})$  in the number of Bell samples  $M$ . Assuming that the local Pauli noise channels are independently identically distributed, we can extend this estimator to noisy Bell measurements as

$$\bar{F} = (\mathbb{E}_C P)^{\frac{E}{2(E+2/3)}}, \quad (5)$$

where  $E$  is the number of error locations in the circuit prior to the measurement. We expect this estimator to be accurate even for typical and nonrandom circuits and give numerical evidence that this is the case in Fig. 2 for random Clifford circuits and nonrandom Floquet Clifford circuits.

How does the purity estimator compare to other means of estimating the fidelity of a quantum state? A widely used method is cross-entropy benchmarking (XEB), which is obtained from classical samples in the computational basis [5,53]. XEB is sample-efficient for random circuits, but requires computing ideal output probabilities of  $C$ , making it infeasible for already moderate numbers of qubits and non-Clifford gates. The XEB is a good estimator of the

fidelity in the regime of low local error probabilities  $\eta \lesssim 1/n$  and for depths  $d \in \Omega(\log n)$ , but not outside of those regimes [9,12] as witnessed in Fig. 2(a). In contrast, Bell sampling is computationally and sample efficient independently of the circuit, and the root purity estimator of fidelity is accurate in both the regimes of high noise and of low depths. Correlated coherent errors on both copies naively ruins the correspondence between fidelity and root purity, but independent randomized compiling on the two copies recovers it by removing these correlations.

In the SM [23], we show these results, elaborate on the various estimators, and also discuss the relation of Bell sampling to different means of verifying quantum computations more generally. From now on, we will assume that the purity is close to unity.

*Depth test.*—We now describe a Bell sampling protocol to measure the depth of a quantum circuit  $C$ , which is promised to be implemented in a fixed architecture, i.e., with gates applied in layers according to a certain pattern. The basic idea underlying the depth test is to use swap tests on subsystems of different sizes in order to obtain estimates of subsystem purities. For a subsystem  $A$  of  $[n]$ , the subsystem purity is given by  $P_A(\rho) = \text{tr}[\rho_A^2]$ , where  $\rho_A = \text{tr}_{A^c}[\rho]$  is the reduced density matrix on subsystem  $A \subset [n]$ . It can be estimated from the fraction of outcome strings with even  $Y$  parity  $\pi_Y(r_A)$  on the substrings  $r_A = (r_i, r_{n+i})_{i \in A}$ .

Our test is based on the observation that the amount of entanglement generated by quantum circuits on half-cuts reaches a depth-dependent maximal value until it saturates at a circuit depth that depends on the dimensionality of the circuit architecture; see Fig. 3(a) for an illustration. In order to lower-bound the depth of a circuit family we choose a subsystem size at which the distinguishability between different depths is maximal. This is typically the case at half-cuts, where the Rényi-2 entanglement entropy

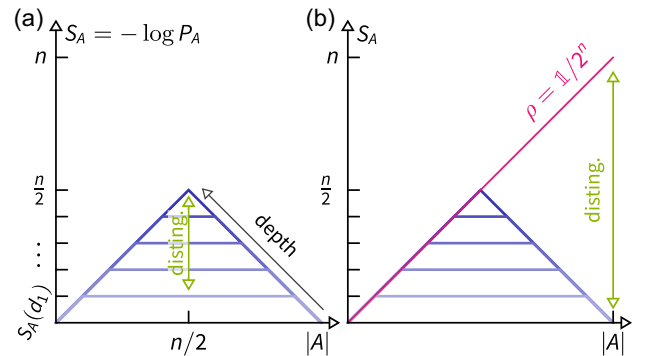


FIG. 3. Depth-dependent Page curves. (a) The maximal subsystem entanglement entropy depends on the circuit architecture and depth (shades of blue) until the half-cut entanglement reaches its maximal value given by  $n/2$ . We measure the subsystem entropy at half-cuts to obtain the maximal sensitivity to different circuit depths. (b) We detect errors in the Bell samples by detecting strings that lead to a nonzero estimate of the purity of  $\rho$ .

$S_A(\rho) = -\log P_A(\rho)$  can be at most  $n/2$ . At the same time, the entanglement entropy is bounded as a function of depth  $S_A(d) \leq d|\partial A|$ , where  $|\partial A|$  is the number of gates applied across the boundary of  $A$  in every layer of the circuit. We now compute an empirical estimate  $\hat{S}_{n/2}$  of  $S_A(|C\rangle\langle C|)$  for a size- $n/2$  subsystem  $A$  using the Bell samples and then compute the maximum  $d$  such that  $\hat{S}_{n/2} - \epsilon \geq d \cdot |\partial A|$  up to an error tolerance  $\epsilon$  depending on the number of Bell samples. We can further refine this test for random quantum circuits by exploiting their average subsystem entanglement properties, known as the ‘‘Page curve’’ [54]. Depth-dependent Page curves have been computed analytically [55] and numerically [52] for a few circuit architectures and random ensembles.

We remark that these entanglement-based tests rely on universal features of quantum chaotic dynamics. As a result, they are also expected to be applicable to generic Hamiltonian dynamics, similar to how ideas for standard quantum random sampling have recently been extended to this case [56,57].

*Magic test and Clifford +  $T$  learning algorithm.*—Another primitive that can be exploited in property tests of quantum states using the Bell samples is the fact that for stabilizer states  $|S\rangle$ , the Bell distribution is supported on a coset of the stabilizer group of  $|S\rangle$  [18]. Leveraging this property allows for efficiently learning stabilizer states [18], testing stabilizerness [19], learning circuits with a single layer of  $T$  gates [58], and estimating measures of magic [20,21]. Here, we describe a simple, new protocol that, from the Bell samples, allows us to efficiently estimate the stabilizer nullity, a magic monotone [17], and learn states that can be prepared by quantum circuits with  $t \in O(\log n)$   $T$  gates.

Our learning algorithm proceeds in two steps. In the first step, we find a compression of the non-Clifford part of the circuit, similarly to Refs. [59,60]. To achieve this, using Bell difference sampling [19], we find a Clifford unitary  $U_C$  corresponding to a subspace  $C \subset \mathbb{F}_2^{2n}$  such that  $U_C|\psi\rangle$  has high fidelity with  $|x\rangle|\varphi\rangle$  for some computational-basis state  $|x\rangle$  on the first  $\dim(C)$  qubits, and a state  $|\varphi\rangle$  on the remaining qubits containing the non-Clifford information. The dimension of  $C$  satisfies  $\dim(C) \geq n - t$ . The number of  $T$  gates  $t$  required to prepare  $|\psi\rangle$  is therefore lower-bounded by the stabilizer nullity  $M(|\psi\rangle) := n - \dim(C)$ , which is a magic monotone [17]. We show that only  $O(n/\epsilon)$  Bell samples are sufficient to ensure that  $|\psi\rangle$  is  $\epsilon$ -close to a state with exact stabilizer nullity given by the estimate  $\hat{M}$  of  $M(|\psi\rangle)$ . To the best of our knowledge this is the most efficient way of measuring the magic of a quantum state to date.

In the second step of the learning algorithm, we characterize the state  $|\varphi\rangle$  on the remaining  $n - \dim(C) \leq t$  qubits using pure-state tomography, for example via the scheme of Ref. [61], giving an estimate  $|\hat{\varphi}\rangle$ . The output of the algorithm is a classical description of  $|\hat{\psi}\rangle = U_C|x\rangle|\hat{\varphi}\rangle$ . The learning

algorithm runs in polynomial time and succeeds with high probability in learning an  $\epsilon$ -approximation to  $|\psi\rangle$  in fidelity using  $O(n/\epsilon)$  Bell samples and  $O(2^t/\epsilon^2)$  measurements to perform tomography of  $|x\rangle|\hat{\varphi}\rangle$ .

Using Clifford +  $T$  simulators [e.g., [62–64]] we can now produce samples from and compute outcome probabilities of  $|\hat{\psi}\rangle$  in time  $O(2^t)$ . We note that the exponential scaling in  $t$  is asymptotically optimal since the description of a state with stabilizer nullity  $t$  has  $2^t$  complex and  $O(n^2)$  binary parameters. Our algorithm generalizes to arbitrary non-Clifford gates.

To summarize, we have given efficient ways to extract properties of the circuit  $C$ —its depth and an efficient circuit description for circuits with low  $T$  count—using only a small number of Bell samples. Further properties of  $|C\rangle$  that can be efficiently extracted from the Bell samples include the expectation values of any diagonal two-copy observables  $A = \sum_r a_r |\sigma_r\rangle\langle\sigma_r|$  and different measures of magic [20]. The Bell samples thus serve as an efficient classical shadow of  $C$ .

*Error detection and correction.*—In the last part of this Letter, we discuss another appealing feature of Bell samples: we can perform error detection and correction. The idea that redundantly encoding quantum information in many copies of a quantum state allows error detection goes back to the early days of quantum computing. Already in 1996, Barenco *et al.* [65] have shown that errors can be reduced by symmetrizing many copies of a noisy quantum state. More recently Refs. [66–68] used measurements on multiple copies to suppress errors in expectation value estimation. In our two-copy setting, some simple *single-sample* error detection properties follow immediately from the tests in the previous section.

First, we observe that an outcome in the antisymmetric subspace, i.e., an outcome  $r$  with  $\pi_Y(r) = 1$ , is certainly due to an error. We can thus reduce the error in the sampled distribution by discarding such outcomes. We show in the SM [23] that such error detection reduces the error rate of a white-noise model by approximately a factor of 2. Quantum computations in the Bell sampling model with error detection can thus achieve comparable fidelities to circuit model computations, where no error detection is possible, in spite of the factor of 2 in qubit overhead.

Second, we note that Bell samples are compatible with stabilizer codes. For such codes, the Bell measurement between code blocks is a transversal measurement, and allows one to extract the syndrome  $\sigma \otimes \sigma$  for  $\sigma \in \mathbb{P}_n$  in the stabilizer of the code [47]. If a detectable or correctable error occurred in one of the code blocks, this syndrome detects or identifies that error up to stabilizer equivalence. The fact that the Bell measurement is transversal implies that an error in the Bell measurement does not spread, so that local error channels or coherent errors in the entangling CNOT gates in the Bell measurement reduce the overall measurement fidelity by  $(1 - \epsilon)^n$ , where  $\epsilon$  is the error rate



per Bell pair. Bell sampling is thus accurate in the regime of  $\epsilon n \ll 1$ . We also note that antisymmetric errors in the Bell measurement are detectable.

Finally, we observe that quadratic error suppression is possible for estimating the expectation values of any Bell-basis-diagonal two-copy observable  $A$ , through the estimate  $\text{tr}[A\rho^{\otimes 2}]/\text{tr}[\mathbb{S}\rho^{\otimes 2}]$ , similar to virtual distillation [66–68]. Specifically, this is true for estimating the expectation  $\langle E_0|P|E_0\rangle^2$  of a Pauli observable  $P$  in the ground state  $|E_0\rangle$  of a gapped Hamiltonian by choosing  $A = (P \otimes P)\mathbb{S}$ ; see the SM [23] for details.

*Discussion and outlook.*—In this Letter, we have proposed and studied Bell sampling as a model of quantum computation. We have shown that many properties of the quantum circuit preparing the underlying state can be extracted efficiently, and that in particular certain errors in the state preparation can be detected from single shots. Based on this, we have argued that the Bell samples are classical circuit shadows. Since Bell sampling is universal this allows us to perform universal quantum computations whose outputs also yield information about the quantum circuit. This makes Bell sampling an interesting computational model, and our main focus in this work is to establish this.

Bell sampling is not only interesting conceptually, however. It is also realistic. Since the Bell basis measurement requires only transversal CNOT and single-qubit gates, it can be naturally implemented in unit depth on various quantum processor architectures with long-range connectivity. These include in particular ion traps [69] and Rydberg atoms in optical tweezers [70]. It is more challenging to implement Bell sampling in geometrically local architectures such as superconducting qubits [5]. In such architectures, one can interleave the two copies in a geometrically local manner such that the Bell measurement is a local circuit; however, this comes at the cost of additional layers of SWAP gates for every unit of circuit depth. Alternatively, one can use looped pipeline architectures to implement the Bell measurement [71].

But is Bell sampling also practical in the near term? Initial experimental results indicate that it is practical for logical qubit architectures [72], but to more fully answer this question various sources of noise need to be analyzed in more detail. For the fidelity estimation protocols we have analyzed the setting of Pauli noise relevant, e.g., to circuits implemented with independent randomized compiling on the two copies or to large-scale fault-tolerant circuits with repeated rounds of error correction. It remains an important open question whether we can develop noise-robust versions of the depth and magic tests. While we have exploited the purity of the state  $|C\rangle$  in our error detection protocol, it is in an interesting question whether it is possible to detect additional errors from the Bell samples. For instance, it might be possible to exploit the fact that the subsystem purity of the target state is low for large subsystems; see Fig. 3.

We have shown that classically simulating the Bell sampling protocol with universal random circuits is classically intractable. An exciting question in this context is whether the complexity of Bell sampling might be more noise robust than computational-basis sampling in the asymptotic scenario. For universal circuit sampling in the computational basis Gao and Duan [73] and Aharonov *et al.* [74] developed an algorithm that simulates sufficiently deep random circuits with a constant noise rate in polynomial time. In the SM [23] we give some initial evidence that this simulation algorithm fails for Bell measurements. If the hardness of Bell sampling indeed turns out to be robust to large amounts of circuit noise, we face the exciting prospect of a scalable quantum advantage demonstration with classical validation and error mitigation.

*Note added.*—While finalizing this Letter, we became aware of Refs. [75,76], where the authors independently report algorithms similar to the one we present above for learning quantum states generated by circuits with low  $T$  count. After this work was completed, we collaborated on the physical implementation of Bell sampling in a logical qubit processor, illustrating the feasibility of our results to near-term devices [72].

D. H. warmly thanks Abhinav Deshpande and Ingo Roth for helpful discussions that aided in the proofs of Lemma 2 and Lemma 5, respectively. We are also grateful to Dolev Bluvstein, Maddie Cain, Bill Fefferman, Xun Gao, Soumik Ghosh, Alexey Gorshkov, Vojtěch Havlíček, Markus Heinrich, Marcel Hinsche, Marios Ioannou, Marcin Kalinowski, Mikhail Lukin, and Brayden Ware for discussions. This research was supported in part by NSF QLCI Grants No. OMA-2120757 and No. PHY-1748958 through the KITP program on “Quantum Many-Body Dynamics and Noisy Intermediate-Scale Quantum Systems.” D. H. acknowledges funding from the US Department of Defense through a QuICS Hartree fellowship.

---

\*Contact author: mail@dhangleiter.eu

†Contact author: mgullans@umd.edu

- [1] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, Characterizing quantum supremacy in near-term devices, *Nat. Phys.* **14**, 595 (2018).
- [2] Y. Liu, M. Otten, R. Bassirianjahromi, L. Jiang, and B. Fefferman, Benchmarking near-term quantum computers via random circuit sampling, [arXiv:2105.05232](https://arxiv.org/abs/2105.05232).
- [3] M. Heinrich, M. Kliesch, and I. Roth, General guarantees for randomized benchmarking with random quantum circuits, [arXiv:2212.06181](https://arxiv.org/abs/2212.06181).
- [4] D. Hangleiter and J. Eisert, Computational advantage of quantum random sampling, *Rev. Mod. Phys.* **95**, 035001 (2023).

- [5] F. Arute *et al.*, Quantum supremacy using a programmable superconducting processor, *Nature (London)* **574**, 505 (2019).
- [6] H.-S. Zhong *et al.*, Quantum computational advantage using photons, *Science* **370**, 1460 (2020).
- [7] Q. Zhu *et al.*, Quantum computational advantage via 60-qubit 24-cycle random circuit sampling, *Science bulletin* **67**, 240 (2022).
- [8] L. S. Madsen, F. Laudenbach, M. F. Askarani, F. Rortais, T. Vincent, J. F. F. Bulmer, F. M. Miatto, L. Neuhaus, L. G. Helt, M. J. Collins, A. E. Lita, T. Gerrits, S. W. Nam, V. D. Vaidya, M. Menotti, I. Dhand, Z. Vernon, N. Quesada, and J. Lavoie, Quantum computational advantage with a programmable photonic processor, *Nature (London)* **606**, 75 (2022).
- [9] A. Morvan *et al.*, Phase transition in random circuit sampling, [arXiv:2304.11119](https://arxiv.org/abs/2304.11119).
- [10] Y.-H. Deng *et al.*, Gaussian boson sampling with pseudo-photon-number resolving detectors and quantum computational advantage, [arXiv:2304.12240](https://arxiv.org/abs/2304.12240).
- [11] X. Gao, M. Kalinowski, C.-N. Chou, M. D. Lukin, B. Barak, and S. Choi, Limitations of linear cross-entropy as a measure for quantum advantage, *PRX Quantum* **5**, 010334 (2024).
- [12] B. Ware, A. Deshpande, D. Hangleiter, P. Niroula, B. Fefferman, A. V. Gorshkov, and M. J. Gullans, A sharp phase transition in linear cross-entropy benchmarking, [arXiv:2305.04954](https://arxiv.org/abs/2305.04954).
- [13] S. Aaronson, The learnability of quantum states, *Proc. R. Soc. A* **463**, 3089 (2007).
- [14] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, *Nat. Phys.* **16**, 1050 (2020).
- [15] S. Aaronson and A. Arkhipov, The computational complexity of linear optics, *Th. Comp.* **9**, 143 (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] M. Beverland, E. Campbell, M. Howard, and V. Kliuchnikov, Lower bounds on the non-Clifford resources for quantum computations, *Quantum Sci. Technol.* **5**, 035009 (2020).
- [18] A. Montanaro, Learning stabilizer states by Bell sampling, [arXiv:1707.04012](https://arxiv.org/abs/1707.04012).
- [19] D. Gross, S. Nezami, and M. Walter, Schur–Weyl duality for the Clifford group with applications: Property testing, a robust Hudson theorem, and de Finetti representations, *Commun. Math. Phys.* **385**, 1325 (2021).
- [20] T. Haug and M. S. Kim, Scalable measures of magic resource for quantum computers, *PRX Quantum* **4**, 010301 (2023).
- [21] T. Haug, S. Lee, and M. S. Kim, Efficient stabilizer entropies for quantum computers, [arXiv:2305.19152](https://arxiv.org/abs/2305.19152).
- [22] H.-Y. Huang, R. Kueng, and J. Preskill, Information-theoretic bounds on quantum advantage in machine learning, *Phys. Rev. Lett.* **126**, 190505 (2021).
- [23] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevLett.133.020601>, which includes details and proofs of the reported results as well as additional Refs. [24–42].
- [24] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, Local random quantum circuits are approximate polynomial-designs, *Commun. Math. Phys.* **346**, 397 (2016).
- [25] T. Zhou and A. Nahum, Emergent statistical mechanics of entanglement in random unitary circuits, *Phys. Rev. B* **99**, 174205 (2019).
- [26] N. Hunter-Jones, Unitary designs from statistical mechanics in random quantum circuits, [arXiv:1905.12053](https://arxiv.org/abs/1905.12053).
- [27] B. Barak, C.-N. Chou, and X. Gao, Spoofing linear cross-entropy benchmarking in shallow quantum circuits, in *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, Leibniz International Proceedings in Informatics (LIPIcs) Vol. 185, edited by J. R. Lee (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2021), pp. 30:1–30:20, [10.4230/LIPIcs.ITCS.2021.30](https://doi.org/10.4230/LIPIcs.ITCS.2021.30).
- [28] A. M. Dalzell, N. Hunter-Jones, and F. G. S. L. Brandão, Random quantum circuits anticentralize in log depth, *PRX Quantum* **3**, 010333 (2022).
- [29] A. M. Dalzell, N. Hunter-Jones, and F. G. S. L. Brandão, Random quantum circuits transform local noise into global white noise, [arXiv:2111.14907](https://arxiv.org/abs/2111.14907).
- [30] M. Ringbauer, M. Hinsche, T. Feldker, P. K. Faehrmann, J. Bermejo-Vega, C. Edmunds, L. Postler, R. Stricker, C. D. Marciniak, M. Meth, I. Pogorelov, R. Blatt, P. Schindler, J. Eisert, T. Monz, and D. Hangleiter, Verifiable measurement-based quantum random sampling with trapped ions, [arXiv:2307.14424](https://arxiv.org/abs/2307.14424).
- [31] S. T. Flammia and Y.-K. Liu, Direct fidelity estimation from few Pauli measurements, *Phys. Rev. Lett.* **106**, 230501 (2011).
- [32] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind quantum computation, *Phys. Rev. A* **96**, 012303 (2017).
- [33] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems, *Nature (London)* **496**, 456 (2013).
- [34] U. Mahadev, Classical verification of quantum computations, in *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, Paris, France, 2018), pp. 259–267, [10.1109/FOCS.2018.00033](https://doi.org/10.1109/FOCS.2018.00033).
- [35] S. Garnerone, T. R. de Oliveira, and P. Zanardi, Typicality in random matrix product states, *Phys. Rev. A* **81**, 032336 (2010).
- [36] B. Collins, C. E. Gonzalez-Guillen, and D. Perez-Garcia, Matrix product states, random matrix theory and the principle of maximum entropy, *Commun. Math. Phys.* **320**, 663 (2013).
- [37] M. Fukuda and R. Koenig, Typical entanglement for Gaussian states, *J. Math. Phys. (N.Y.)* **60**, 112203 (2019).
- [38] J. T. Iosue, A. Ehrenberg, D. Hangleiter, A. Deshpande, and A. V. Gorshkov, Page curves and typical entanglement in linear optics, *Quantum* **7**, 1017 (2023).
- [39] V. Mnih, C. Szepesvári, and J.-Y. Audibert, Empirical Bernstein stopping, in *Proceedings of the 25th International Conference on Machine Learning, ICML '08* (Association for Computing Machinery, Helsinki, Finland, 2008), pp. 672–679.
- [40] P. Erdős and A. Rényi, Probabilistic methods in group theory, *J. Anal. Math.* **14**, 127 (1965).

- [41] S. Grewal, V. Iyer, W. Kretschmer, and D. Liang, Efficient learning of quantum states prepared with few non-Clifford gates II: Single-copy measurements, [arXiv:2308.07175](#).
- [42] M. B. Hastings, Locality in quantum systems, [arXiv:1008.5137](#).
- [43] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, On the complexity and verification of quantum random circuit sampling, *Nat. Phys.* **15**, 159 (2019).
- [44] R. Movassagh, Quantum supremacy and random circuits, [arXiv:1909.06210](#).
- [45] Y. Kondo, R. Mori, and R. Movassagh, Quantum supremacy and hardness of estimating output probabilities of quantum circuits, in *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, Denver, CO, USA, 2022), pp. 1296–1307, [10.1109/FOCS52979.2021.00126](#).
- [46] H. Krovi, Average-case hardness of estimating probabilities of random quantum circuits with a linear scaling in the error exponent, [arXiv:2206.05642](#).
- [47] D. Gottesman, An introduction to quantum error correction and fault-tolerant quantum computation, [arXiv:0904.2557](#).
- [48] S. J. Beale, J. J. Wallman, M. Gutiérrez, K. R. Brown, and R. Laflamme, Quantum error correction decoheres noise, *Phys. Rev. Lett.* **121**, 190501 (2018).
- [49] E. Huang, A. C. Doherty, and S. Flammia, Performance of quantum error correction with coherent errors, *Phys. Rev. A* **99**, 022313 (2019).
- [50] J. J. Wallman and J. Emerson, Noise tailoring for scalable quantum computation via randomized compiling, *Phys. Rev. A* **94**, 052325 (2016).
- [51] A. Winick, J. J. Wallman, D. Dahlen, I. Hincks, E. Ospadov, and J. Emerson, Concepts and conditions for error suppression through randomized compiling, [arXiv:2212.07500](#).
- [52] G. M. Sommers, D. A. Huse, and M. J. Gullans, Crystalline Quantum circuits, *PRX Quantum* **4**, 030313 (2023).
- [53] J. Choi, A. L. Shaw, I. S. Madjarov, X. Xie, R. Finkelstein, J. P. Covey, J. S. Cotler, D. K. Mark, H.-Y. Huang, A. Kale, H. Pichler, F. G. S. L. Brandão, S. Choi, and M. Endres, Preparing random states and benchmarking with many-body quantum chaos, *Nature (London)* **613**, 468 (2023).
- [54] D. N. Page, Average entropy of a subsystem, *Phys. Rev. Lett.* **71**, 1291 (1993).
- [55] A. Nahum, J. Ruhman, S. Vijay, and J. Haah, Quantum entanglement growth under random unitary dynamics, *Phys. Rev. X* **7**, 031016 (2017).
- [56] D. K. Mark, J. Choi, A. L. Shaw, M. Endres, and S. Choi, Benchmarking quantum simulators using ergodic quantum dynamics, *Phys. Rev. Lett.* **131**, 110601 (2023).
- [57] A. L. Shaw, Z. Chen, J. Choi, D. K. Mark, P. Scholl, R. Finkelstein, A. Elben, S. Choi, and M. Endres, Benchmarking highly entangled states on a 60-atom analog quantum simulator, *Nature (London)* **628**, 71 (2024).
- [58] C.-Y. Lai and H.-C. Cheng, Learning quantum circuits of some T gates, *IEEE Trans. Inf. Theory* **68**, 3951 (2022).
- [59] S. Arunachalam, S. Bravyi, C. Nirkhe, and B. O’Gorman, The Parametrized Complexity of Quantum Verification, in *17th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2022)*, Leibniz International Proceedings in Informatics (LIPIcs) (Schloss Dagstuhl—Leibniz-Zentrum für Informatik, 2022), Vol. 232, pp. 3:1-3:18, .
- [60] L. Leone, S. F. E. Oliviero, S. Lloyd, and A. Hamma, Learning efficient decoders for quasi-chaotic quantum scramblers, *Phys. Rev. A* **109**, 022429 (2024).
- [61] M. Guță, J. Kahn, R. Kueng, and J. A. Tropp, Fast state tomography with optimal error bounds, *J. Phys. A* **53**, 204001 (2020).
- [62] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, Simulation of quantum circuits by low-rank stabilizer decompositions, *Quantum* **3**, 181 (2019).
- [63] H. Pashayan, O. Reardon-Smith, K. Korzekwa, and S. D. Bartlett, Fast estimation of outcome probabilities for quantum circuits, *PRX Quantum* **3**, 020361 (2022).
- [64] E. T. Campbell and M. Howard, A unified framework for magic state distillation and multi-qubit gate-synthesis with reduced resource cost, *Phys. Rev. A* **95**, 022316 (2017).
- [65] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, and C. Macchiavello, Stabilisation of quantum computations by symmetrisation, [arXiv:quant-ph/9604028](#).
- [66] J. Cotler, S. Choi, A. Lukin, H. Gharibyan, T. Grover, M. E. Tai, M. Rispoli, R. Schittko, P. M. Preiss, A. M. Kaufman, M. Greiner, H. Pichler, and P. Hayden, Quantum virtual cooling, *Phys. Rev. X* **9**, 031013 (2019).
- [67] B. Koczor, Exponential error suppression for near-term quantum devices, *Phys. Rev. X* **11**, 031057 (2021).
- [68] W. J. Huggins, S. McArdle, T. E. O’Brien, J. Lee, N. C. Rubin, S. Boixo, K. B. Whaley, R. Babbush, and J. R. McClean, Virtual distillation for quantum error mitigation, *Phys. Rev. X* **11**, 041036 (2021).
- [69] A. Bermudez, X. Xu, R. Nigmatullin, J. O’Gorman, V. Negnevitsky, P. Schindler, T. Monz, U. G. Poschinger, C. Hempel, J. Home, F. Schmidt-Kaler, M. Biercuk, R. Blatt, S. Benjamin, and M. Müller, Assessing the progress of trapped-ion processors towards fault-tolerant quantum computation, *Phys. Rev. X* **7**, 041061 (2017).
- [70] D. Bluvstein, H. Levine, G. Semeghini, T. T. Wang, S. Ebadi, M. Kalinowski, A. Keesling, N. Maskara, H. Pichler, M. Greiner, V. Vuletić, and M. D. Lukin, A quantum processor based on coherent transport of entangled atom arrays, *Nature (London)* **604**, 451 (2022).
- [71] Z. Cai, A. Siegel, and S. Benjamin, Looped pipelines enabling effective 3D qubit lattices in a strictly 2D device, *PRX Quantum* **4**, 020345 (2023).
- [72] D. Bluvstein *et al.*, Logical quantum processor based on reconfigurable atom arrays, *Nature (London)* **626**, 58 (2024).
- [73] X. Gao and L. Duan, Efficient classical simulation of noisy quantum computation, [arXiv:1810.03176](#).
- [74] D. Aharonov, X. Gao, Z. Landau, Y. Liu, and U. Vazirani, A polynomial-time classical algorithm for noisy random circuit sampling, [arXiv:2211.03999](#).
- [75] S. Grewal, V. Iyer, W. Kretschmer, and D. Liang, A Polynomial-Time Classical Algorithm for Noisy Random Circuit Sampling, in *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC 2023)* (Association for Computing Machinery, New York, 2023), pp. 945–957, [10.1145/3564246.3585234](#).
- [76] L. Leone, S. F. E. Oliviero, and A. Hamma, Learning T-doped stabilizer states, *Quantum* **8**, 1361 (2024).