Will it glue? On short-depth designs beyond the unitary group

Lorenzo Grevink[1], Jonas Haferkamp[2], Markus Heinrich[3], Jonas Helsen[1], Marcel Hinsche[4], Thomas Schuster[5], and Zoltán Zimborás[6]

[1]QuSoft and CWI, Amsterdam, The Netherlands, [2]Saarland University, Saarbrücken, Germany, [3]Institute for Theoretical Physics, University of Cologne, Cologne, Germany, [4]Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, Berlin, Germany, [5]Walter Burke Institute for Theoretical Physics and Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, USA, [6]QTF Centre of Excellence, Department of Physics, University of Helsinki, P.O. Box 43, FI-00014 Helsinki, Finland

The paper was presented at the QMATH16 conference, a specialized conference on the intersection of quantum information and pure mathematics. Our work was a good fit for the mathematical nature of this conference, however we believe that our results are of interest to a broader audience in quantum information theory.

Background: Random quantum operations are a central tool in quantum information theory and beyond. Applications include quantum system characterization[1–3], quantum learning[4], quantum supremacy experiments[5], quantum machine learning[6,7], quantum cryptography[8,9], quantum many-body physics[10,11], and quantum gravity[12–14].

The most commonly used class of random quantum operators are the Haar-random unitaries, but they need exponential depth to be implemented[15]. Significant effort has thus been spent to find low-depth constructions of random unitaries that appear Haar-random to a restricted observer[16–24].

Approximate unitary k-designs are ensembles of unitaries that appear Haar-random to an observer with access to at most k copies of the sampled unitary. Approximate unitary designs using circuits of depth logarithmic in the number of qubits in the 1D architecture have been found very recently[21,22]. The results of Refs.[21,22] came as a great surprise, because in this regime lightcones are of negligible size compared to the system size and yet the distinguishability to Haar-random unitaries (which generate near-maximally entangled states) decays exponentially. The construction in Ref.[21] "*glues*" designs on local, log-sized patches together to form designs globally. However, Ref.[21] also gives an argument that rules out log-depth constructions of *orthogonal* designs, i.e. based on orthogonal matrices. Orthogonal matrices will thus not glue.

A dichotomy seems to emerge: Either, a class of operations is sufficiently universal to allow for a gluing construction or a linear lower bound can be proven.

Our results: In this paper we delineate the boundaries of this dichotomy and ask generally: *Will it glue?* We study four subgroups of the n-qubit unitary group, namely the Clifford group $\mathrm{Cl}(n)$, the orthogonal group $\mathrm{O}(2^n)$, the unitary symplectic group $\mathrm{USp}(2^n)$, and the matchgate group $\mathrm{M}(n)$. For the four subgroups, we consider different notions of random ensembles, namely approximate group or state designs with additive or relative errors. In addition, we investigate whether local circuits over the mentioned subgroups *anti-concentrate* in logarithmic depth.

For all of these notions, **we either show that they can be constructed in $\mathcal{O}(\log(n))$ depth, or aim at deriving $\Omega(n)$ lower bounds**, where n denotes the number of qubits (we suppress the k and ϵ-dependence). We obtain linear lower bounds unconditionally for 1D architectures, or for circuits constructed from local random gates ("generalized random brickworks") in any architecture.

Table 1 shows an overview of the results of this paper, together with a few known results from the literature. We find lower bounds with two different scalings:

1. We get lower bounds that scale with the maximal lightcone L over the circuit ensemble. They are thus particularly strong in 1D yielding $\Omega(n)$, but still give non-trivial lower bounds in other architectures, for instance $\Omega(n^{1/D})$ in D-dimensional lattices and $\Omega(\log n)$ in all-to-all connectivity.

2. *Generalized random brickworks* are circuits for which the local gates are drawn independently from the Haar measure of the considered group. For this class of circuits, we go beyond architecture-dependent bounds by showing linear depth lower bounds in any architecture. Our results still hold for significant relaxations of generalized random brickworks, to include the vast majority of circuits discussed in the literature.

Notion of randomness	Group				
	$\mathrm{U}(2^n)$	$\mathrm{O}(2^n)$	$\mathrm{USp}(2^n)$	$\mathrm{Cl}(n)$	$\mathrm{M}(n)$
additive-error group designs	$\mathcal{O}(\log(\frac{n}{\epsilon}))$[21,22]	$\Omega(\mathrm{L})$	$\Omega(\mathrm{L})$	$k \geq 4$ $\Omega(L)$	$\Omega(n)$
relative-error state designs	$\Theta(\log(\frac{n}{\epsilon}))$[21,22]	$\Omega(\mathrm{R})^*, \Omega(n)^\dagger$	$\Omega(\mathrm{L})$	$k \geq 4$ $\Omega(\mathrm{R})^*, \Omega(n)^\dagger$	$\Omega(n)$
relative-error group designs	$\Theta(\log(\frac{n}{\epsilon}))$[21,22]	all above	all above, $\Omega(n)^\dagger$	$k \geq 4$ all above	$\Omega(n)$
additive-error state designs	$\mathcal{O}(\log(\frac{n}{\epsilon}))$[21,22]	$\mathcal{O}(\log(\frac{n}{\epsilon}))$	$\mathcal{O}(\log(\frac{n}{\epsilon}))$	$k < 6$: $\mathcal{O}(\log(\frac{n}{\epsilon}))$	$\Omega(n)$
anti-concentration	$\Theta(\log(n))$[25,26]	$\mathcal{O}(\log(n))$[27]	$\mathcal{O}(\log(n))$	$\Theta(\log(n))$[28,29]	$\Omega\left(\frac{n^{1/3}}{\log(n)}\right)$

Table 1: Overview of circuit depth bounds obtained in this work and in the literature, for various notions of k-designs and different subgroups of the unitary group (bounds without references are derived in this work). Here, we always assume $k \geq 2$ and indicate further restrictions on k when necessary, but otherwise suppress the k-dependence in the asymptotic notation. The first set of our lower bounds depend on the architecture through the maximal lightcone L over the circuit ensemble. The ones indicated by a $*$ depend instead on the diameter R, the largest distance of two qubits in the architecture, which can yield a different scaling as the lightcone bounds. The ones indicated by a † are derived for generalized local brickwork circuits and do no longer depend on the underlying architecture. Green indicates an upper bound (it will glue), red indicates a lower bound (it will not glue).

On the other hand, we surprisingly find log-depth constructions for additive-error state designs for the Clifford (for $k < 6$), orthogonal, and unitary symplectic group. This stands in contrast with the lightcone lower bounds for the construction of relative-error state designs.

Outlook: Our results immediately impact constructions of efficient randomization protocols over restricted groups, for instance:

- The circuit complexity of randomized protocols based on Clifford unitaries under circuit re-use (such as thrifty shadow estimation[30]).
- Our results prevent the existence of short-depth matchgate designs, thus fermionic protocols, such as fermionic shadows, may need much deeper circuits than their qubit counterparts. This answer a question raised in Ref.[31] in the negative (at least for geometrically local circuits).

Beyond this, our work raises a number of interesting theoretical questions.

- Our work raises the question which subgroups of the unitary group could actually support a "gluing lemma".
- There is, for a fixed group, also the question which classes of observables (acting on several copies of the unitary) actually witness lightcones.

Techniques for lower bounds: To derive our lower bounds, we build on an observation in Ref.[21] that invariances of the tensor power representation of subgroups can be exploited to construct lightcone arguments that rule out short-depth circuits.

Assume that for a group G, we find *factorizing* $Q = Q_1 \otimes \cdots \otimes Q_n$, where all tensor products of the local operators $Q_i \geq 0$ are in the k-th commutant of G restricted to the respective qubit. Adding a local perturbation to Q, e.g. a Pauli-Z to the first qubit (on the first copy), gives us $Q' := (Z_1 \otimes \mathbb{1}^{\otimes(k-1)})Q(Z_1 \otimes \mathbb{1}^{\otimes(k-1)})$. Now Q' is still psd but, in general, not invariant under G. However, everywhere except on the first qubit it is, i.e. if V is a gate in G that acts trivially on the first qubit, then $VQ'V^\dagger = Q'$.

Hence, if we consider the action of a local G-circuit U on Q', then all gates which are outside of the lightcone of the first qubit cancel: This is most clearly seen at the example of a brickwork circuit,

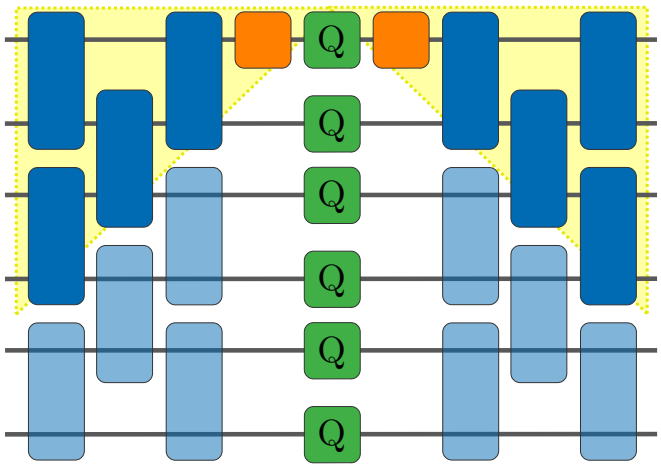

Figure 1: Detection of short-depth local circuits over certain subgroups G by a lightcone argument. We construct a factorizing operator $Q^{\otimes n}$ that commutes with the k-copy action of G. By 'hiding' the first factor behind a single-qubit gate, a local circuit will no longer leave the perturbed operator invariant – instead only the local gates outside the lightcone of the first qubit cancel due to the invariance of the local Q's. If the circuit is too short and the lightcone does not contain all qubits, then some of the qubits stay unentangled with the rest. This can be probed by a suitable observable, allowing to separate short-depth circuits from deep circuits and setting a lower bound on the depth of approximate designs.

cf. Fig. 1. If this lightcone does not include all qubits, then we are left with the operator Q on the remaining qubits, unentangled with the remaining systems, which we can detect by measuring a suitable observable. More precisely, we show that this gives means to distinguish deep circuits (or Haar-random unitaries) from short circuits, setting a lower bound of $\Omega(\mathrm{L})$ (or in some cases $\Omega(\mathrm{R})$) for the depth of k-designs for the specific group, where L is the minimal depth of a lightcone that is supported on a constant fraction of all qubits, and R is the diameter of the architecture.

The second lower-bound technique is built on the insight that the existence of factorizing Q in the commutant allows to reduce some of the 'psd' quantities $\mathrm{tr}\left(PU^{\otimes k}Q'U^{\dagger,\otimes k}\right)$ to *Pauli expectation values*. The former are exactly the functions which can be estimated up to relative error using log-depth random circuits over the unitary group[21,22], while the latter generally need linear depth, even for universal circuits. On a high level, the existence of such a relation between these two types of functions for the here considered subgroups prevents the construction of log-depth (relative-error) designs.

The idea is that if we sample the local gates randomly from the respective group on two qubits, that then there is a constant probability that the locality of Z_1 is preserved. The probability that the final operator is a Z_1 thus decays exponentially in the depth. To achieve the exponentially small Haar value, the depth thus has to be linear. Consequently, we obtain a lower bound of $\Omega(n)$ on the depth of relative-error state designs for the Clifford and orthogonal group, and relative-error group designs for the symplectic group. Crucially, this result holds for generalized brickwork circuits *in any architecture* and is thus considerably stronger than the previously discussed lightcone arguments. We are confident that our arguments can be generalized to an even broader class of circuit ensembles and may even hold for general circuits.

Techniques for upper bounds: The constructions for $\mathcal{O}(\log(n))$-depth designs in this paper are similar to the construction in[21]. The idea is to construct a two-layer brickwork circuit in which the local gates act on $\mathcal{O}(\log n)$ qubits ("superblocks"). In[21] it is proven that this construction forms a relative-error unitary group design, if the superblocks are drawn from a unitary design.

To prove that additive-error state designs can be constructed in depth $\mathcal{O}(\log(n))$ for the Clifford (for $k < 6$), orthogonal and the symplectic group, we use a similar construction in conjection with a new technique: We show that the Haar twirl over these groups is ϵ-close in trace distance to the unitary Haar twirl, for ϵ polynomial in k and 2^{-n}, provided that the input state obeys the positive partial transpose (PPT) condition on every copy of the Hilbert space $\mathcal{H}$. This is proven by projecting on a subspace of the Hilbert space where the commutant of the considered subgroup is identical to the commutant of the unitary group. For the orthogonal group this is the distinct subspace[24] and we define an analogus subspace for the symplectic group. We then observe that if ρ is PPT, then $U^{\otimes k}\rho U^{\otimes k,\dagger}$ is as well. The two-layer superblock brickwork will thus provide a $\mathcal{O}(\log(n))$-depth construction for additive-error state designs by the gluing lemma.

References

1. Emerson, J., Alicki, R. & Życzkowski, K. Scalable noise estimation with random unitary operators. *Journal of Optics B: Quantum and Semiclassical Optics* **7.** Publisher: IOP Publishing, S347 (2005).
2. Helsen, J., Roth, I., Onorati, E., Werner, A. H. & Eisert, J. General framework for randomized benchmarking. *PRX quantum* **3.** Publisher: APS, 020357 (2022).
3. Heinrich, M., Kliesch, M. & Roth, I. *Randomized benchmarking with random quantum circuits* arXiv: 2212.06181. 2023.
4. Huang, H.-Y., Kueng, R. & Preskill, J. Predicting Many Properties of a Quantum System from Very Few Measurements. *Nature Physics* **16.** arXiv: 2002.08953, 1050–1057. ISSN: 1745-2473, 1745-2481 (2020).
5. Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G., Buell, D. A., *et al.* Quantum supremacy using a programmable superconducting processor. *Nature* **574.** Publisher: Nature Publishing Group UK London, 505–510 (2019).
6. McClean, J. R., Boixo, S., Smelyanskiy, V. N., Babbush, R. & Neven, H. Barren plateaus in quantum neural network training landscapes. *Nature communications* **9.** Publisher: Nature Publishing Group UK London, 4812 (2018).
7. Larocca, M., Thanasilp, S., Wang, S., Sharma, K., Biamonte, J., Coles, P. J., Cincio, L., McClean, J. R., Holmes, Z. & Cerezo, M. Barren plateaus in variational quantum computing. *Nature Reviews Physics.* Publisher: Nature Publishing Group UK London, 1–16 (2025).
8. Kretschmer, W. Quantum pseudorandomness and classical complexity. *arXiv preprint arXiv:2103.09320* (2021).
9. Kretschmer, W., Qian, L., Sinha, M. & Tal, A. *Quantum cryptography in algorithmica* in *Proceedings of the 55th Annual ACM Symposium on Theory of Computing* (2023), 1589–1602.
10. Nahum, A., Vijay, S. & Haah, J. Operator Spreading in Random Unitary Circuits. *Phys. Rev. X* **8.** Publisher: American Physical Society, 021014 (2018).
11. Fisher, M. P., Khemani, V., Nahum, A. & Vijay, S. Random quantum circuits. *Annual Review of Condensed Matter Physics* **14.** Publisher: Annual Reviews, 335–379 (2023).
12. Hayden, P. & Preskill, J. Black holes as mirrors: quantum information in random subsystems. *Journal of high energy physics* **2007.** Publisher: IOP Publishing, 120 (2007).
13. Yoshida, B. & Kitaev, A. Efficient decoding for the Hayden-Preskill protocol. *arXiv preprint arXiv:1710.03363* (2017).
14. Brown, A. R. & Susskind, L. Second law of quantum complexity. *Physical Review D* **97.** Publisher: APS, 086015 (2018).
15. Knill, E. Approximation by quantum circuits. *arXiv preprint quant-ph/9508006* (1995).
16. Harrow, A. W. & Low, R. A. Random quantum circuits are approximate 2-designs. *Communications in Mathematical Physics* **291.** Publisher: Springer, 257–302 (2009).
17. Brandao, F. G., Harrow, A. W. & Horodecki, M. Local random quantum circuits are approximate polynomial-designs. *Communications in Mathematical Physics* **346.** Publisher: Springer, 397–434 (2016).
18. Haferkamp, J. Random quantum circuits are approximate unitary t-designs in depth O(nt^5+o(1)). *Quantum* **6,** 795 (2022).
19. Chen, C.-F., Bouland, A., Brandão, F. G., Docter, J., Hayden, P. & Xu, M. Efficient unitary designs and pseudorandom unitaries from permutations. *arXiv preprint arXiv:2404.16751* (2024).

20. Chen, C.-F., Haah, J., Haferkamp, J., Liu, Y., Metger, T. & Tan, X. Incompressibility and spectral gaps of random circuits. *arXiv:2406.07478* (2024).

21. Schuster, T., Haferkamp, J. & Huang, H.-Y. Random unitaries in extremely low depth. *Science* **389.** Publisher: American Association for the Advancement of Science, 92–96 (2025).

22. LaRacuente, N. & Leditzky, F. Approximate Unitary k -Designs from Shallow, Low-Communication Circuits. *arXiv:2407.07876* (2024).

23. Ma, F. & Huang, H.-Y. *How to construct random unitaries* in *Proceedings of the 57th Annual ACM Symposium on Theory of Computing* (2025), 806–809.

24. Metger, T., Poremba, A., Sinha, M. & Yuen, H. *Simple constructions of linear-depth t-designs and pseudorandom unitaries* in *IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2024), 485–492.

25. Barak, B., Chou, C.-N. & Gao, X. *Spoofing Linear Cross-Entropy Benchmarking in Shallow Quantum Circuits* in *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)* (ed Lee, J. R.) **185** (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2021), 30:1–30:20. ISBN: 978-3-95977-177-1.

26. Dalzell, A. M., Hunter-Jones, N. & Brandão, F. G. Random quantum circuits anticoncentrate in log depth. *PRX Quantum* **3.** Publisher: APS, 010333 (2022).

27. Sauliere, A., Magni, B., Lami, G., Turkeshi, X. & Nardis, J. D. *Universality in the Anticoncentration of Chaotic Quantum Circuits* arXiv: 2503.00119. 2025.

28. Magni, B., Christopoulos, A., De Luca, A. & Turkeshi, X. Anticoncentration in Clifford Circuits and Beyond: From Random Tensor Networks to Pseudo-Magic States. *arXiv preprint arXiv:2502.20455* (2025).

29. Aharonov, D., Gao, X., Landau, Z., Liu, Y. & Vazirani, U. *A polynomial-time classical algorithm for noisy random circuit sampling* in *Proceedings of the 55th Annual ACM Symposium on Theory of Computing* (2023), 945–957.

30. Helsen, J. & Walter, M. Thrifty shadow estimation: re-using quantum circuits and bounding tails. *Physical Review Letters* **131.** arXiv: 2212.06240, 240602. ISSN: 0031-9007, 1079-7114 (2023).

31. Chapman, A. & Flammia, S. T. Fermionic Averaged Circuit Eigenvalue Sampling. *arXiv preprint arXiv:2504.01936* (2025).