nature communications

Article

https://doi.org/10.1038/s41467-026-77776-7

Short-depth designs beyond the unitary group

Received: 10 April 2026

Accepted: 3 September 2026

Published online: 02 November 2026

Check for updates

Lorenzo Grevink[1] ✉, Jonas Haferkamp[2], Markus Heinrich[3], Jonas Helsen[1], Marcel Hinsche[4], Thomas Schuster[5,6,7] & Zoltán Zimborás[8]

Random quantum operations are a central tool in quantum information and beyond, having applications ranging from benchmarking and cryptography to many-body physics. While recent advances have shown that shallow-depth circuits can realize approximate unitary designs, which are ensembles that appear to be random to a restricted observer, it remained unclear whether similar constructions extend to other groups that play important roles in quantum computing. We provide a range of results on several groups of broad interest in quantum information science: the Clifford group, the orthogonal group, the unitary symplectic groups, and the matchgate group. For these groups we prove that designs cannot be generated by any circuit ensemble with lightcones that are smaller than the system size. We moreover show that commonly considered circuit ensembles cannot generate designs in sub-linear depth on any circuit architecture. On the other hand, we prove that slightly weaker forms of randomness—including additive-error state designs and anti-concentration—nevertheless emerge at logarithmic depths in many cases. Our results reveal that the onset of randomness in shallow quantum circuits is a widespread yet subtle phenomenon, dependent on the interplay between the group itself and the context of its application.

Random quantum operations are a central tool in quantum information theory and beyond. Applications include a wide range of research fields, such as 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].

A natural, and the most commonly used, candidate for a random class of quantum operations is the Haar-random unitaries given by the unique uniform distribution on the unitary group. While easy to work with in theory, the Haar measure is often far from practical: Standard counting arguments show that exponential circuit depth is required to implement a Haar random unitary[15]. A second, independent objection to Haar-random unitaries is that they require access to a universal gate set, rendering them potentially expensive to implement on early fault-tolerant devices. Significant effort has thus been spent to find low-depth constructions of random unitaries that appear Haar-random to a restricted observer[16–24]. Roughly, these constructions fall into two categories: Approximate unitary k-designs[25] that appear Haar-random to an observer with access to at most k copies of the sampled unitary, and pseudorandom unitaries that appear Haar-random to a computationally bounded observer[23,26].

While approximate unitary designs and pseudorandom unitaries using circuits of depth linear in the number of qubits have been known for a few years[17], sub-linear depth constructions were only found very recently[21,22]. There, such ensembles are constructed in logarithmic and polylogarithmic depth, respectively, even in a 1D geometry. The results

[1]QuSoft, 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, California Institute of Technology, Pasadena, CA, USA. [6]Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, CA, USA. [7]Google Quantum AI, Venice, California 90291, USA. [8]QTF Centre of Excellence, Department of Physics, University of Helsinki, Helsinki, Finland. ✉e-mail: lorenzo.grevink@cwi.nl

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. Indeed, previous methods – often based on analyzing the spectrum of so-called moment operators – also apply to classical analogs of random quantum operations, such as random reversible circuits. But mixing in logarithmic depth appears to be a quantum phenomenon and can be proven to be false for classical analogs[21]. What is more, ref. 21 gives an argument that rules out log-depth construction of orthogonal designs, i.e., based on orthogonal matrices. Not only do classical circuits not mix at logarithmic depth, but even the absence of complex numbers results in a linear lower bound. Instead, the construction in ref. 21 glues designs on local, log-sized patches together to form designs globally. A dichotomy seems to emerge: Either the class of operations is sufficiently universal to allow for a gluing construction or a linear lower bound can be proven.

In this paper, we delineate the boundaries of this phenomenon and ask generally: Will it glue? More precisely, we use lightcone arguments to prove strong lower bounds on the circuit depth for additive-error group designs over the Clifford group, the orthogonal group, the unitary symplectic group, and the matchgate group. These results are particularly strong in one dimension, setting linear lower bounds on the required circuit depth. In general architectures, these bounds depend on the connectivity in the form of the lightcone of qubits and still constitute non-trivial results. Intriguingly, we are also able to show linear lower bounds independent of the underlying architecture for a vast majority of circuit ensembles considered in the literature, such as the popular brickwork circuits. We derive these bounds for relative-error state designs generated by such circuits, which implies analogous circuit lower bounds for relative-error group designs. These findings indicate that lightcones underestimate the mixing time of non-universal circuits, while ref. 21,22 show that they overestimate in the case of universal circuits. In this sense, lightcone considerations may generally be misleading when studying designs. However, for the strictly weaker notion of additive-error state k-designs, we instead give logarithmic depth constructions for the orthogonal and symplectic groups, as well as the Clifford group (if $k < 6$). Moreover, we show that for all of these cases, we have a generalized notion of anti-concentration in logarithmic depth. For the matchgate group, we show that linear depth is still necessary for additive-error state designs, and we moreover give a (probably suboptimal) $\Omega(n/\log(n))$ depth lower bound for anti-concentration (relative to the corresponding value for the uniform matchgate group average), specifically for a gluing-type construction.

Results

We will begin by introducing some notation and the various notions of randomness we use in our results. We then give an overview of the results, followed by a more detailed discussion for each group individually.

Notation and concepts

Let G be a (compact) subgroup of the unitary group $\mathrm{U}(2^n)$ on the n-qubit Hilbert space $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ (in this work, we focus on n-qubit systems, although some of our results can be readily generalized to qudit systems). The Haar measure on G should be thought of as the most uniform probability measure on G – Formally, it is the unique probability measure that is both left and right invariant under multiplication with elements of G. We write $\mathbb{E}_{U\sim G}$ for the expectation value over the Haar measure on G.

We often call general probability distributions over G ensembles and typically denote them by $\mathcal{E}$. These will always be implemented by quantum circuits, so we will also sometimes speak of circuit ensembles. To quantify how close an ensemble $\mathcal{E}$ is to the Haar measure, we consider moments of the distribution, given as

$$\mathbb{E}_{U\sim\mathcal{E}}\mathrm{tr}(BU^{\otimes k}AU^{\dagger,\otimes k}) \tag{1}$$

for suitably sized matrices A and B. If all k-th moments of $\mathcal{E}$ agree with those of the Haar measure, we call $\mathcal{E}$ a unitary k-design over the group G. We note that if A (or B) commutes with $U^{\otimes k}$ for all $U \in G$ (we say they are in the k-th commutant of G), then the moments trivially agree.

We typically only require that moments are reproduced up to a (small) error – we then call $\mathcal{E}$ an approximate k-design. However, there are different notions of approximation, which are not equivalent in their resource demands.

Additive-error group k-designs over G require that k-th moments are reproduced up to an additive error. For this to be well-defined, the matrices A and B in Eq. (1) have to be suitably restricted. Here, we typically take A to be a quantum state and B to be a POVM element – such that the error relates to the probability of distinguishing the averaging (or twirling) channels $\Phi_{\mathcal{E}}^{(k)} := \mathbb{E}_{U\sim\mathcal{E}}U^{\otimes k}(\cdot)U^{\dagger,\otimes k}$ and $\Phi_{G}^{(k)} := \mathbb{E}_{U\sim G}U^{\otimes k}(\cdot)U^{\dagger,\otimes k}$ and can be alternatively written in terms of the diamond norm as $||\Phi_{G}^{(k)} - \Phi_{\mathcal{E}}^{(k)}||_{\diamond} < \epsilon$. Strictly speaking, we would need to include auxiliary systems in Eq. (1), but we omit this detail for this discussion.

Relative-error group k-designs over G require the reproduction of k-th moments up to a multiplicative error. We keep A and B restricted, but as overall normalizations do not matter for relative errors, we take them to be arbitrary positive semi-definite (psd) matrices (i.e., Hermitian matrices with non-negative eigenvalues). A relative error ϵ always implies an additive error 2ϵ[17]. Even more, given a relative-error ϵ-approximate unitary k-design $\mathcal{E}$, any quantum experiment that queries a unitary U from $\mathcal{E}$ at most k times outputs a state that is, on average, 2ϵ-close in trace distance to the output state obtained if U were sampled from the Haar measure instead. For an additive-error ϵ-approximate unitary k-design, the same statement holds, but then for non-adaptive quantum experiments[21]. An additive error is thus a weaker requirement than a relative error.

We have analogous statements for state ensembles: Haar-random quantum states over G are given by $\mathcal{S}_G = \{U|0^n\rangle \mid U \in G\}$ with the induced measure. The moments of a state ensemble $\mathcal{E}_\prime$ are given as

$$\mathbb{E}_{\psi\sim\mathcal{E}'}\mathrm{tr}(B|\psi\rangle\langle\psi|^{\otimes k}). \tag{2}$$

Additive-error state k-designs over G are those for which these moments are ϵ-close to the Haar moments (for any POVM element B), or equivalently the one with trace distance error $||\mathbb{E}_{\psi\sim\mathcal{S}_G}|\psi\rangle\langle\psi|^{\otimes k} - \mathbb{E}_{\psi\sim\mathcal{E}'}|\psi\rangle\langle\psi|^{\otimes k}||_1 \le \epsilon$.

Relative-error state k-designs over G reproduce all k-th moments with psd B up to multiplicative error. Unlike with group designs, additive-error state designs suffice for indistinguishability from Haar random in every quantum experiment that queries a state $|\psi\rangle$ at most k times. That is because there is no such notion as adaptivity when considering states. There is thus no clear operational interpretation for relative-error state designs. However, for certain procedures like shadow tomography[4,27], one really needs relative errors. If $\mathcal{E}$ is a relative-error unitary k-design, then $\{U|0^n\rangle | U \sim \mathcal{E}\}$ is a relative-error state k-design. A similar statement holds for additive error. State designs are thus a weaker notion than group designs.

Anti-concentration is the weakest notion of randomness that we consider. We here adopt a common misusage of this word in the random circuit community and mean that the moments in Equation (1) of the ensemble $\mathcal{E}$ with $A = B = |0^n\rangle\langle 0^n|^{\otimes k}$ approximate the Haar value over G up to a relative error. We then say that $\mathcal{E}$ anti-concentrates up to order k. In contrast, anti-concentration in the conventional sense is a property of the ensemble of outcome distributions. The conventional notion is implied if the $k = 2$ Haar moment scales as 4^{-n}, which is, however, not necessarily true for any subgroup G, e.g., the matchgate

group does not scale like that. We note that if $\mathcal{E}$ forms a relative-error state k-design, then it anti-concentrates up to order k.

Most of our bounds depend on the architecture according to which the qubits are ordered and connected. An architecture is described by a graph, where the vertices of the graph are the qubits, and an edge between two vertices indicates that a 2-qubit gate can be applied on those 2 qubits. Commonly studied architectures are 1D and 2D lattices (with open or closed boundary conditions), or all-to-all connectivity (the complete graph). We define the diameter (often denoted as dia) as the largest possible distance between two vertices in the architecture, e.g. the diameter of 1D is dia = $\Theta(n)$, for 2D dia = $\Theta(\sqrt{n})$, and for the all-to-all connectivity dia = $\Theta(1)$. Note, however, that many known constructions of designs in the all-to-all connectivity actually use architectures of higher diameter. For example, the construction of Clifford 3-designs in ref. 21 in $\mathcal{O}(\log\log(n))$ depth implicitly uses an architecture of diameter $\mathcal{O}(n/\log(n))$.

Finally, we elaborate a bit on the assumptions we impose on the circuit ensembles to derive lower bounds that are independent of the architecture. Due to their clearly defined structure, we obtain the strongest results for so-called generalized random brickworks. We define them as a circuit ensemble that is a concatenation of independently chosen r-local Haar-random gates, for some constant r.

Definition 1. (Generalized random brickworks) Let $A_1, \ldots, A_s$ be subsets of $[n]$ of size at most some constant r, and such that the qubits in A_i are connected w.r.t the underlying architecture. For each A_i draw a unitary U_i from the Haar measure of the group G and apply it to the respective qubits. Let $\mathcal{E}$ denote the ensemble of circuits generated by composing all these unitaries. We call an ensemble of this form a fixed brickwork. A generalized random brickwork is defined as a convex combination of (different) fixed brickworks.

See refs. 18,20,28,29, and Corollary 1, first bullet point, in ref. 21 for examples of fixed brickworks that are thus generalized random brickworks as well. See Def. 1.4, first bullet point, in ref. 20 for an example of a generalized random brickwork which is not a fixed brickwork. See refs. 24,30,31 and Corollary 1, second bullet point, in ref. 21 for examples of ensembles that are not generalized random brickworks.

We define a locally independent ensemble as an ensemble such that the local gates acting on a qubit are drawn independently from the local gates acting on qubits that are far away.

Definition 2. (Locally independent ensemble) Let $\mathcal{E}$ be an ensemble of unitary circuits on a fixed architecture. Let $S_x(U)\{U_1^x, \ldots, U_{m_U}^x\}_U$ be the set of local unitaries that act on qubit x for a circuit U. If for every pair of qubits x, y that have distance at least dia/2 we have that $S_x(U)$ and $S_y(U)$ are independent variables when U is sampled from $\mathcal{E}$, then $\mathcal{E}$ is locally independent.

Note that the notion of a locally independent ensemble does not make any sense in the all-to-all architecture, as there we have that dia = 1. Almost all of the ensembles named in the previous paragraph are locally independent. Only the ones in ref. 32 and Def. 1.4, first bullet point, in ref. 20 are not, as these ensembles use the all-to-all architecture.

Summary of results

We study four subgroups of the n-qubit unitary group, namely the Clifford group Cl(n), the orthogonal group O(2^n), the unitary symplectic group USp(2^n), and the matchgate group M(n). For all the notions of randomness discussed in the previous section, 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). Our lower bounds come in two different flavors, which both build on the existence of suitable

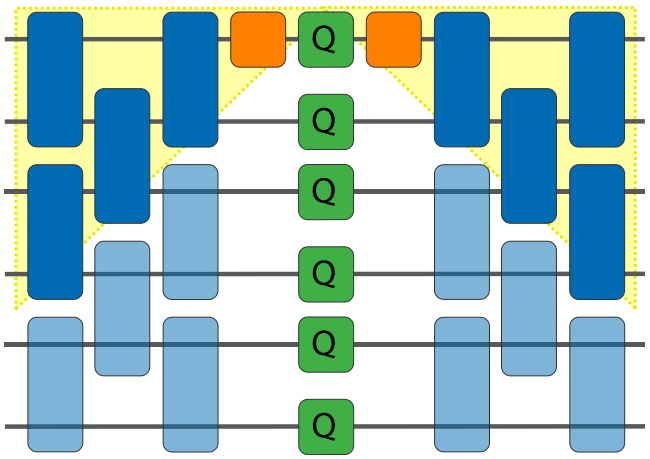


Fig. 1 | Detection of short-depth local circuits over certain subgroups G by a lightcone argument. We construct a factorizing operator $Q^{\otimes n}$ that commutes with the k-copy action of G. By hiding the first factor behind a single-qubit gate, a local circuit will no longer leave the perturbed operator 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.

invariances of the tensor power representation of G, i.e., an operator Q that commutes with $U^{\otimes k}$ for all $U \in G$.

The first flavor uses lightcone arguments to rule out short-depth designs, cf. Fig. 1, generalizing an observation in ref. 21. The lower bounds derived in this way scale with the minimal depth of a lightcone that is supported on a constant fraction of all qubits; we let $\ell(n)$ denote this minimal depth. Note that $\ell(n)$ depends on the underlying architecture. These lower bounds are 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. In some cases, however, we only manage to prove (slightly) weaker lower bounds depending on the diameter of an architecture. The diameter is the maximal distance between any two qubits in the architecture. For D-dimensional lattices, the diameter scales the same as the minimal depth of a lightcone that supports (a constant fraction of) the qubits, dia $\propto \ell(n) = \Theta(n^{1/D})$, but in the all-to-all connectivity the diameter equals 1.

For the second flavor, we go beyond architecture-dependent bounds by noting that for many classes of random circuits, at every layer of the circuit there is a finite probability that a lightcone does not grow. We show a linear-depth lower bound rigorously for generalized random brickwork circuits. The technique used provides us with linear lower bounds $\Omega(n)$ in any architecture, even with all-to-all connectivity. We emphasize that these lower bounds still hold under a significant relaxation of the definition of generalized random brickwork, and we decided for Def. 1 to simplify the presentation. More precisely, we do not necessarily need that the local gates are uniformly distributed, and their distributions do not have to be identical either (but they should be sampled independently). Instead, our proofs require that the local gates preserve some single-qubit Pauli operator (up to a phase) with a finite probability or, more generally, that they can be replaced by such a distribution up to second moments (see also Section 4 for a sketch of the argument). This includes a vast majority of the random circuits considered in the literature; it, for example, also includes the circuits considered in ref. 31 that are not generalized random brickworks.

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)

Notion of randomness	Group				
	U(2^n)	O(2^n)	USp(2^n)	Cl(n)	M(n)
relative-error group designs	$\mathcal{O}(\log(n))$[21,22]	$\Omega(\ell(n))$, $\Omega(n)^\dagger$	$\Omega(\ell(n))$, $\Omega(n)^\dagger$	$k<4$: $k\geq 4$: $\mathcal{O}(\log(n))$[21,22] $\Omega(\ell(n))$, $\Omega(n)^\dagger$	$\Omega(n)$
additive-error group designs	$\mathcal{O}(\log(n))$[21,22]	$\Omega(\ell(n))$	$\Omega(\ell(n))$	$k<4$: $k\geq 4$: $\mathcal{O}(\log(n))$[21,22] $\Omega(\ell(n))$	$\Omega(n)$
relative-error state designs	$\mathcal{O}(\log(n))$[21,22]	$\Omega(\mathrm{dia})^*$, $\Omega(n)^\dagger$	$\Omega(\ell(n))$	$k<4$:$k\geq 4$: $\mathcal{O}(\log(n))$[21,22] $\Omega(\mathrm{dia})^*$, $\Omega(n)^\dagger$	$\Omega(n)$
additive-error state designs	$\mathcal{O}(\log(n))$[21,22]	$\mathcal{O}(\log(n))$	$\mathcal{O}(\log(n))$	$k<6$: $\mathcal{O}(\log(n))$	$\Omega(n)$
anti-concentration	$\mathcal{O}(\log(n))$[21,22,29,43]	$\mathcal{O}(\log(n))$[35]	$\mathcal{O}(\log(n))$	$\mathcal{O}(\log(n))$[36,44]	$\Omega\left(\frac{n}{\log(n)}\right)$

Here, we always assume $k\geq 2$ and indicate further restrictions on k when necessary, but otherwise suppress the k-and ϵ-dependence in the asymptotic notation. The first set of our lower bounds depend on the architecture through $\ell(n)$, the minimal depth of a lightcone that is supported on a constant fraction of all qubits. This translates to $\ell(n)=\Theta(n^{1/D})$ on a D-dimensional lattice and to $\ell(n)=\Theta(\log n)$ on all-to-all architectures. The other lower bounds are derived under mild structural assumptions on the used circuit: The ones indicated by a * depend instead on the diameter dia, the largest distance between two qubits in the architecture, which can yield a different scaling as the lightcone bounds. The ones indicated by a † are derived for so-called generalized brickwork circuits and do no longer depend on the underlying architecture. The upper bounds are derived for the two-layer superblock circuits from Ref. 21. Note that some notions of randomness imply others. In this table, the relative-error group design is the strongest notion.

Our upper bounds, on the other hand, all explicitly pass through the gluing lemma of ref. 21 (thus proving that it will glue). We extend this construction by various non-trivial statements of unitary k-designness of the Clifford, orthogonal, and symplectic groups when restricting the input states to being positive partial transpose (PPT) on all copies of the state.

For all notions of randomness, we assume that the considered ensemble consists of unitaries from the considered group. However, the local gates from which the unitaries are constructed need not be from the subgroup. Table 1 shows an overview of all the results in this paper, together with a few known results from the literature. We now discuss our results for each group individually.

Clifford group

We know that the multi-qubit Clifford group is an exact unitary 3-design[33], thus, the results from refs. 21,22 carry over to random Clifford circuits for $k\leq 3$. It is therefore interesting to see that a clear distinction can be made between Clifford 3-designs and Clifford 4-designs in terms of circuit depth. Indeed, we prove that if the lightcone starting from the first qubit does not contain a constant fraction of all qubits, an ensemble cannot be an (additive or relative-error) Clifford 4-design. In the 1D architecture, this gives us a lower bound of $\Omega(n)$, which is exponentially worse than for $k=3$. For the all-to-all architecture this gives a lower bound of $\Omega(\log(n))$.

We also prove a lower bound of $\Omega(\mathrm{dia})$ for relative-error Clifford state 4-designs, where dia is the architecture's diameter, under the additional assumption that the circuits are locally independent. This assumption is typically satisfied for the commonly considered random quantum circuits and thus a minor restriction only. We also believe that the assumption can be eventually dropped.

For generalized random brickwork circuits, we also prove a strong $\Omega(n)$ lower bound on relative-error state designs in any architecture. Of course, this implies the same lower bound for relative-error group designs for this class of random circuits.

Given these linear lower bounds, it is somewhat surprising that the construction of additive-error Clifford state 4- and 5-designs of depth $\mathcal{O}(\log(n))$ in 1D is possible. This result follows from the fact that, for $k\leq 5$, the k-copy ensemble of stabilizer states is close in trace distance to Haar-random states with an error $\mathcal{O}(2^{-n})$. It is notable that our proof technique fails for $k\geq 6$, as these stabilizer states can be efficiently distinguished from Haar-random states through Bell difference sampling. After the release of the first version of this work, the existence of $\mathcal{O}(\log(n))$-depth additive-error Clifford state designs for $k\geq 6$ was proven in ref. 34.

Proofs and further details on the Clifford group are given in Supplementary Note 2.

Orthogonal group

A lower bound on the depth of relative-error orthogonal group designs was already known in ref. 21, based on a similar lightcone argument as we use in this work. We extend the lower bound $\Omega(\ell(n))$ to an additive-error statement. We also extend their argument to relative-error orthogonal state designs, provided the same nuances on local independence as in the Clifford case. We moreover prove the same strong $\Omega(n)$ depth lower bound for generalized random brickwork circuits in any architecture.

Surprising is the fact that we can construct additive-error state designs in $\mathcal{O}(\log(n))$ depth. We prove a theorem that states that the unitary and orthogonal Haar twirl are equal on PPT states, up to an exponentially small additive error, more precisely, with n-dependence $\frac{1}{2^{n/2}}$. Note that an additive error of ϵ implies a relative error of $\epsilon\cdot 4^{nk}$[17]. The exponent of our additive error is thus not small enough to imply a relative error statement.

We also show that random orthogonal circuits anti-concentrate in depth $\mathcal{O}(\log(n))$ for $k=2$ at the example of the two-layer superblock circuits from ref. 21. We note that anti-concentration at higher k was shown for orthogonal MPS in ref. 35, and we think that the analogous statement for superblock circuits can also be derived along the lines of ref. 36.

Proofs and further details on the orthogonal group are given in Supplementary Note 3.

Unitary symplectic group

Our results for the unitary symplectic group are similar to those for the orthogonal group. Note that we obtained a slightly stronger statement for relative-error state designs, as we do not need the assumption of local independence.

The result on state designs is surprising, as we know that Haar-random ensembles of symplectic and unitary states are indistinguishable[37], i.e., symplectic state designs are identical to unitary state designs. We know that these relative-error state designs can be constructed in $\mathcal{O}(\log(n))$ depth using local unitary gates in the 1D architecture[21,22]. It is therefore quite surprising that relative-error state designs cannot be constructed in $\mathcal{O}(\log(n))$ depth using local symplectic gates. The indistinguishability between symplectic and unitary state designs combined with the unitary gluing lemma[21] does however, directly imply symplectic anticoncentration in $\mathcal{O}(\log(n))$ depth.

Proofs and further details on the unitary symplectic group are given in Supplementary Note 4.

Matchgate group

Finally, we provide lower bounds for the matchgate group. We prove two main results. The first result states that the superblock architecture does not attain the minimal anti-concentration value (which is $\Theta(\sqrt{n})$, in the context of fermions this quantity is also called an inverse participation ratio[38]) for any circuit that has less than $\Omega(n/\log(n))$ circuit depth. We suspect that this scaling behavior is (slightly) non-optimal and that a linear-depth lower bound should be possible. Interestingly, our proof is entirely combinatorial in nature and uses no lightcone arguments. The second result states that matchgate additive-error state designs are not possible for any depth less than $\Omega(n)$, with the minor technical caveat that the proof only covers errors (in both the relative and additive cases) of size $\mathcal{O}(1/n)$. This argument is essentially lightcone-based, but is substantially less subtle than similar arguments for other groups, as the matchgate group is inherently local with respect to a 1D architecture.

Proofs and further details on the matchgate group are given in Supplementary Note 5.

Discussion

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[27]).
- 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 answers a question raised in ref. 39 in the negative (at least for geometrically local circuits).

Beyond this, our work raises a number of interesting theoretical questions, of which we list several key ones in the following:

- Our work raises the question of which subgroups of the unitary group could actually support a gluing lemma. Beyond its strict meaning, gluing-type constructions succeed in many settings, as demonstrated in this work. We believe that at least the strong existence question could be rigorously decided, as there are rather few relevant groups. Perhaps this could be done following a logic similar to the work of Tiep and Guralnick[40]. However, we suspect that any of these questions are highly nontrivial to answer.
- There is, for a fixed group, also the question of which classes of observables (acting on several copies of the unitary) actually witness lightcones in state designs. We see that anti-concentration is generally possible in short depth even when designs cannot be formed, so $|0^n\rangle\langle 0^n|^{\otimes k}$ is an observable that does not witness lightcones. Is there a natural class of anti-concentration-like observables? We suspect that the PPT condition we use in several proofs could serve as at least a sufficient condition, but a general statement of that form is unclear.
- It is known that barren plateaus arise when optimizing over orthogonal or symplectic 2-designs[41], and our results on additive-error state designs imply that barren plateaus will also emerge when optimizing over shallow orthogonal or symplectic circuits. If one could find an interesting group which does not allow shallow-depth designs even in the weaker notions, and is not classically simulatable like the matchgate group, then it might be possible to optimize efficiently over sub-linear depth circuits of this group.

While finishing this manuscript, we became aware of the work[42], which shares several goals and results with our work. There, it is shown that G-invariant pure states (in the sense that $U^{\otimes k}|\psi\rangle \propto |\psi\rangle$) can be used to discriminate short-depth circuits from G-Haar-random unitaries, which yields a lower bound on the diamond distance between the respective twirls. This implies that there cannot be additive-error designs over G in such depth. Both our work and ref. 42 consider the same set of examples for G and arguments based on lightcones. However, we consider a more general notion of invariance, namely the existence of factorizing positive-semidefinite operators Q in the k-fold commutant (i.e., $[U^{\otimes k}, Q] = 0$). This allows us to already give lower bounds on Clifford 4-designs, while the criterion in ref. 42 only applies to 8-designs. Moreover, we also rule out relative-error state designs over the considered subgroups, which is not implied by ref. 42. Going beyond lightcone arguments, we prove stronger results for generalized random brickwork circuits, which set linear lower bounds on relative designs in any architecture. Finally, we also construct additive-error state designs and prove anticoncentration over all but the matchgate groups in logarithmic depth, and prove (almost) linear lower bounds for the matchgate group.

Methods

In the following, we will give an overview of the methods used in this work and sketch the arguments used to derive our results. We refer the reader to the Supplementary Information for the exact statements of our results and detailed proofs.

Lower bounds

Most of the lower bounds in this paper are based on a similar lightcone technique as used in ref. 21 to give a lower bound on the depth of orthogonal designs. The exception are the lower bounds for generalized random brickwork circuits, on which we will elaborate more below.

Lightcone arguments. To give circuit depth lower bounds for group and state designs over subgroups G, we make use of the existence of specific positive semi-definite (psd) operators $Q \geq 0$ in the group's k-th order commutant. The structure of these operators allows us to effectively test for lightcones of individual qubits and thus to separate deep from shallow circuits. Properly normalized, Q can be seen as either a (mixed) quantum state or a POVM element, thus allowing us to use this argument in different variations for both additive-error and relative-error designs.

More specifically, suppose we can find a factorizing Q in the sense that $Q = Q_1 \otimes \cdots \otimes Q_n$, where all tensor products of the local operators $Q_i \geq 0$ are in the k-th commutant of G restricted to the respective qubits. Consider a local perturbation to Q by applying a Pauli-Z operator to the first qubit: $Q' := (Z_1 \otimes \mathbb{1}^{\otimes k-1})Q(Z_1 \otimes \mathbb{1}^{\otimes(k-1)})$. Now Q' is still psd but, in general, not invariant under G. However, if $V \in G$ acts trivially on the first qubit, then $V^{\otimes k} Q' V^{\dagger,\otimes k} = Q'$.

Hence, if we consider the action of a local G-circuit U on Q', 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, cf. Fig. 1. In the first layer, all gates cancel except the gates that act on the first qubit. In the second layer, again all gates cancel except the ones that act on qubits which were acted upon by the first layer, i.e., the first two qubits. Iterating this argument shows that the only gates left after d layers are the gates that form a lightcone starting from the first qubit.

If this lightcone does not include all qubits, then we are left with operators Q_i on the remaining ones, which we can test for by measuring their local expectation values.

We show that this gives a means to distinguish deep circuits (or Haar-random unitaries) from short circuits, setting a lower bound of $\Omega(\ell(n))$ for the depth of k-designs for the specific group, where $\ell(n)$ is the minimal depth of a lightcone that is supported on a constant fraction of all qubits. In the 1D architecture this implies a lower bound of $\Omega(n)$, in the all-to-all connectivity a lower bound of $\Omega(\log(n))$.

We note that finding such Q for the considered groups is not difficult. For the orthogonal and unitary symplectic group, we can simply vectorize the preserved bilinear forms (the identity matrix $\mathbb{1}_n$ or the symplectic form J_n) to construct Q. We obtain Q in the $k = 2$

commutant as the projector onto the maximally entangled state $|\Omega_n\rangle$ or on $|J_n\rangle \equiv (J_n \otimes \mathbb{1}_n)|\Omega_n\rangle$, respectively. For the Clifford group, we can find a suitable Q in the $k = 4$ commutant as the infamous stabilizer code projector $\propto \sum_P P^{\otimes 4}$, where the sum runs over all n-qubit Pauli operators. Note that all three examples are PSD and factorize in the desired way.

Pauli scrambling arguments. The second lower-bound technique is built on the insight that the existence of factorizing Q in the commutant allows to reduce psd moments $\mathrm{tr}(PU^{\otimes k}Q'U^{\dagger,\otimes k})$ (with $P \geq 0$) 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. More precisely, applying the random circuit to Q' and taking the right POVM, we are left with probabilities of the form $\propto |\langle 0|UZ_1U^\dagger|0\rangle|^4$. For the previously introduced generalized random brickwork circuits, we then explicitly show that these Pauli expectation values need linear depth to approximate their Haar values within relative error. Intuitively, there is a constant probability in every layer that the locality of Z_1 is preserved and thus the probability that the final operator is Z_1 decays exponentially with the depth. To achieve the exponentially small Haar value, the depth thus has to be linear. Using this technique, we obtain a lower bound of $\Omega(n)$ on the depth of relative-error state designs for the Clifford and orthogonal groups, and relative-error group designs for the symplectic group. Crucially, this result holds for generalized random 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 (cf. the comment below in Section 2).

Arguments for matchgates. Finally, we use slightly different techniques to deal with the case of the matchgate group. The inherently one-dimensional nature of matchgates makes them relatively straightforward to deal with. We prove a lower bound on the anti-concentration value by relating it to a path counting problem in the commutant of the second moment averaged circuit. We cut a short depth circuit into roughly square pieces and lower bound the number of paths that pass through such cuts, which leads directly to a lower bound on the anticoncentration value. Our proof only deals with superblock circuits, but we believe the technique can be easily generalized to arbitrary matchgate circuit distributions. Finally, the absence of state designs is proven by a straightforward one-dimensional lightcone argument at the level of Majorana operators.

Upper bounds

The constructions for $\mathcal{O}(\log(n))$-depth designs (of various types) in this paper are similar to the construction in ref. 21. The idea is to construct a two-layer brickwork circuit in which the local gates act on a large number of qubits (superblocks). We organize n qubits in m local patches, each consisting of $\xi = n/m$ qubits. We choose m to be even. In the first layer we apply superblocks to the local patches $(1, 2), (3, 4), \ldots, (m-1, m)$, and in the second layer to the local patches $(2, 3), (4, 5), \ldots, (m, 1)$. In the first layer we thus have $m/2$ superblocks, that act on 2ξ qubits each. The second layer is the same as the first layer, except that the superblocks act on patches that are shifted ξ qubits from the patches the superblocks in the first layer act on. The superblocks are independently drawn from the Haar measure of a given group G (or from k-designs if required). The key step in ref. 21 is then the gluing lemma.

Lemma 1. (Gluing lemma, Theorem 1 in ref. 21) Let $\mathcal{E}$ be the ensemble of matrices drawn from the two-layer superblock architecture for the unitary group U. If we choose $\xi = \mathcal{O}(\log(nk/\epsilon))$, then $\mathcal{E}$ is a relative-error ϵ-approximate unitary k-design.

In ref. 20 it is shown that random brickwork circuits form unitary k-designs in depth $\mathcal{O}((nk + \log(1/\epsilon))\,\mathrm{poly}\log(k))$. If we thus insert random brickwork circuits of this depth in the superblock construction $\mathcal{E}$, we get a relative-error ϵ-approximate unitary k-design in depth $d = \mathcal{O}(\log(n/\epsilon)k\,\mathrm{poly}\log(k))$. Note that this construction is a generalized random brickwork.

To prove that additive-error state designs can be constructed in depth $\mathcal{O}(\log(n))$ for the orthogonal and the symplectic group, we use a similar construction in conjunction 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 with respect to 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 analogous 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.

To obtain expressive circuit depth upper bounds on anti-concentration, we have to restrict the considered circuits to a relevant class of interest. This is because we can otherwise find constant-depth circuits that anti-concentrate but are otherwise not interesting (for instance, a layer of parallel Hadamard gates trivially anti-concentrates for the unitary group). For concreteness, we here focus on the two-layer superblock construction from ref. 21. The bounds then follow by an explicit calculation using Weingarten calculus in the orthogonal case. In the unitary symplectic case, this follows readily from the fact that the twirl over USp-Haar random states is the same as over U-Haar random states and thus the result follows directly from the gluing lemma.

Data availability

Data sharing is not applicable as no datasets were generated or analyzed during the current study.

References

1. Emerson, J., Alicki, R. & Życzkowski, K. Scalable noise estimation with random unitary operators. *J. Opt. B Quantum Semiclassical Opt.* **7**, S347 (2005).
2. Helsen, J., Roth, I., Onorati, E., Werner, A. H. & Eisert, J. General framework for randomized benchmarking. *PRX Quantum* **3**, 020357 https://doi.org/10.1103/PRXQuantum.3.020357 (2022).
3. Heinrich, M., Kliesch, M. & Roth, I. Randomized benchmarking with random quantum circuits, https://doi.org/10.48550/arXiv.2212.06181 (2023).
4. Huang, H.-Y., Kueng, R. & Preskill, J. Predicting many properties of a quantum system from very few measurements. *Nat. Phys.* **16**, 1050–1057 https://doi.org/10.1038/s41567-020-0932-7 (2020).
5. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).
6. McClean, J. R., Boixo, S., Smelyanskiy, V. N., Babbush, R. & Neven, H. Barren plateaus in quantum neural network training landscapes. *Nat. Commun.* **9**, 4812 (2018).
7. Larocca, M. et al. Barren plateaus in variational quantum computing. *Nat. Rev. Phys.* **7**, 174–189 (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 *Proc. 55th Annual ACM Symposium on Theory of Computing*, 1589–1602 (ACM, 2023).

10. Nahum, A., Vijay, S. & Haah, J. Operator spreading in random unitary circuits. *Phys. Rev. X* **8**, 021014 https://doi.org/10.1103/PhysRevX.8.021014 (2018).
11. Fisher, M. P., Khemani, V., Nahum, A. & Vijay, S. Random Quantum Circuits. *Annu. Rev. Condens. Matter Phys.* **14**, 335–379 https://doi.org/10.1146/annurev-conmatphys-031720-030658 (2023).
12. Hayden, P. & Preskill, J. Black holes as mirrors: quantum information in random subsystems. *J. High. Energy Phys.* **2007**, 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. *Phys. Rev. D.* **97**, 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. *Commun. Math. Phys.* **291**, 257–302 (2009).
17. Brandao, F. G., Harrow, A. W. & Horodecki, M. Local random quantum circuits are approximate polynomial-designs. *Commun. Math. Phys.* **346**, 397–434 (2016).
18. Haferkamp, J. Random quantum circuits are approximate unitary t-designs in depth $o(nt^{5+o(1)})$. *Quantum* **6**, 795 https://doi.org/10.22331/q-2022-09-08-795 (2022).
19. Chen, C.-F. et al. Efficient unitary designs and pseudorandom unitaries from permutations. *arXiv preprint arXiv:2404.16751* (2024).
20. Chen, C.-F. et al. Incompressibility and spectral gaps of random circuits. In *Proc. IEEE 66th Annual Symposium on Foundations of Computer Science (FOCS)*, 1304–1312 (IEEE, 2025).
21. Schuster, T., Haferkamp, J. & Huang, H.-Y. Random unitaries in extremely low depth. *Science* **389**, 92–96, https://doi.org/10.1126/science.adv8590 (2025).
22. LaRacuente, N. & Leditzky, F. Approximate unitary k-designs from shallow, low-communication circuits. *Commun. Math. Phys.* **407**, 51 (2026).
23. Ma, F. & Huang, H.-Y. How to construct random unitaries. In *Proc. 57th Annual ACM Symposium on Theory of Computing*, 806–809 (ACM, 2025).
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)*, 485–492 (IEEE, 2024).
25. Gross, D., Audenaert, K. & Eisert, J. Evenly distributed unitaries: on the structure of unitary designs. *J. Math. Phys.* **48**, 052104 (2007).
26. Ji, Z., Liu, Y.-K. & Song, F. Pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38*, 126–152 (Springer, 2018).
27. Helsen, J. & Walter, M. Thrifty shadow estimation: reusing quantum circuits and bounding tails. *Phys. Rev. Lett.* **131**, 240602 (2023).
28. Harrow, A. W. & Mehraban, S. Approximate unitary t-designs by short random quantum circuits using nearest-neighbor and long-range gates. *Commun. Math. Phys.* **401**, 1531–1626 (2023).
29. Dalzell, A. M., Hunter-Jones, N. & Brandão, F. G. Random quantum circuits anticoncentrate in log depth. *PRX Quantum* **3**, 010333 (2022).
30. Jiang, J. et al. Optimal space-depth trade-off of CNOT circuits in quantum logic synthesis. In *Proc. Fourteenth* Annual ACM-SIAM Symposium on Discrete Algorithms, 213–229 (SIAM, 2020).
31. Suzuki, R. et al. More global randomness from less random local gates. *Physical Review A* **114**, 022424 (2026).
32. Ghosh, S., Hangleiter, D. & Helsen, J. Random regular graph states are complex at almost any depth. *PRX Quantum* **6**, 040344 (2025).
33. Zhu, H., Kueng, R., Grassl, M. & Gross, D. The Clifford group fails gracefully to be a unitary 4-design. *arXiv:1609.08172 [quant-ph]* (2016).
34. Zhang, Y., Vijay, S., Gu, Y. & Bao, Y. Designs from magic-augmented clifford circuits. *PRX Quantum* **7**, 010344 (2026).
35. Sauliere, A., Magni, B., Lami, G., Turkeshi, X. & Nardis, J. D. Universality in the anticoncentration of chaotic quantum circuits, https://doi.org/10.48550/arXiv.2503.00119. 2503.00119 (2025).
36. Magni, B., Christopoulos, A., De Luca, A. & Turkeshi, X. Anticoncentration in Clifford circuits and beyond: From random tensor networks to pseudomagic states. *Phys. Rev. X* **15**, 031071 (2025).
37. West, M., Mele, A. A., Larocca, M. & Cerezo, M. Random ensembles of symplectic and unitary states are indistinguishable. *arXiv preprint arXiv:2409.16500* (2024).
38. Collura, M., De Nardis, J., Alba, V. & Lami, G. The non-stabilizerness of fermionic Gaussian states. *Quantum* **10**, 2036 (2026).
39. Chapman, A. & Flammia, S. T. Fermionic averaged circuit eigenvalue sampling. *Quantum* **10**, 2053 (2026).
40. Guralnick, R. & Tiep, P. Decompositions of small tensor powers and Larsen's conjecture. *Representation Theory Am. Math. Soc.* **9**, 138–208 (2005).
41. Cerezo, M. et al. Does provable absence of barren plateaus imply classical simulability? *Nat. Commun.* **16**, 7907 (2025).
42. West, M., García-Martín, D., Diaz, N. L., Cerezo, M. & Larocca, M. No-go theorems for sublinear-depth group designs, https://doi.org/10.48550/arXiv.2506.16005. 2506.16005 (2025).
43. Barak, B., Chou, C.-N. & Gao, X. Spoofing Linear Cross-Entropy Benchmarking in Shallow Quantum Circuits. In Lee, J. R. (ed.) *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, **185** of *Leibniz International Proceedings in Informatics (LIPIcs)*, 30:1–30:20, https://doi.org/10.4230/LIPIcs.ITCS.2021.30 (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2021).
44. Aharonov, D., Gao, X., Landau, Z., Liu, Y. & Vazirani, U. A polynomial-time classical algorithm for noisy random circuit sampling. In *Proc. 55th Annual ACM Symposium on Theory of Computing*, 945–957 (ACM, 2023).

Acknowledgements

We are tremendously grateful to Yuzhen Zhang, Yimu Bao, and Yingfei Gu for several clarifying discussions regarding short-depth Clifford state designs for $k > 5$, and to Xhek Turkeshi and Ingo Roth for general discussions on short-depth random circuits. We are also grateful to the authors of ref. 42 for the motivation to finish our manuscript with greater than usual alacrity.

Author contributions

L.G., J.H., M.H., J.H., M.H., T.S. and Z.Z. contributed to the conceptualization and development of the theoretical framework, participated in writing and revising the manuscript, and approved the final version. L.G. led the writing of the manuscript.

Funding

L. Grevink and J. Helsen acknowledge funding from NWO through NGF.1623.23.005 and Veni.222.331. T. Schuster acknowledges support from the Walter Burke Institute for Theoretical Physics at Caltech and the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator. The Institute for Quantum Information and Matter, with which T. Schuster is affiliated, is an NSF Physics Frontiers Center (NSF Grant PHY-2317110). M. Hinsche acknowledges funding by the German Federal Ministry for Education and Research (MUNIQC-Atoms). M. Heinrich acknowledges funding by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 547595784 and under Germany's Excellence Strategy - Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1 – 390534769. Z. Zimborás was supported by the Horizon Europe program HORIZON-CL4-2022-QUANTUM-01-SGA via the project 101113946 OpenSuperQPlus100 and the QuantERA II project HQCC-101017733 as well as by the NKFIH OTKA grant FK 135220.

A substantial part of this work was developed during the Random Quantum Circuits workshop 2024 in Amsterdam.

Competing interests
The authors declare no competing interests.

Additional information
Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41467-026-77776-7.

Correspondence and requests for materials should be addressed to Lorenzo Grevink.

Peer review information : *Nature Communications* thanks the anonymous reviewer(s) for their contribution to the peer review of this work. A peer review file is available.

Reprints and permissions information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

© The Author(s) 2026