Extended abstract: Efficient unitary designs with a system-size independent number of non-Clifford gates

J. Haferkamp, F. Montealegre-Mora, M. Heinrich, J. Eisert, D. Gross, I. Roth

Introduction

Unitary designs are a ubiquitous concept in quantum information theory and have numerous applications. These range from randomized benchmarking to circuit complexity in the context of black hole information scrambling. Uniform randomness is a central object in information theory and unitary t-designs are defined to mimic Haar randomness on the unitary group up to t-th moments. In many applications considering a finite order of moments suffices.

A major advantage of unitary designs compared to full Haar randomness is that unitary designs often require considerably fewer resources. Importantly, exact unitary 3-designs can be implemented by drawing a random unitary from the multi-qubit Clifford group. Clifford unitaries are well-behaved in a number of ways: They can be efficiently simulated classically and are comparably easy to implement fault-tolerantly. In fact, the difference to non-Clifford gates is so stark that modern resource theories of quantum computing treat Clifford gates as a free resource.

However, recent mathematical results show that higher designs can not be obtained exactly without implementing full Haar-randomness [1, 2]. In seminal work [3], Brandao, Harrow and Horodecki have proven that t-designs can, nevertheless, be implemented approximately with local random quantum circuits of depth $O(n^2t^{10})$. This is a powerful result with many implications for assessing properties of random dynamics. That said, the full implementation of local random quantum circuits is daunting especially for near-term technology as it requires a fully fledged quantum computer. Moreover, the resulting circuits will not be simulable in polynomial time even for small fixed t. This is in stark contrast to the case of $t = 3$, where a unitary design can be implemented with a randomly drawn Clifford unitary. This state of affairs suggest that – in some ways costly – non-Clifford gates have to be inserted into a random Clifford circuit in order to uplift unitary 3-designs to approximate higher-order unitary designs. This leads us to the central question underlying this work: *How many non-Clifford gates are required to generate an approximate unitary t-design?*

Results

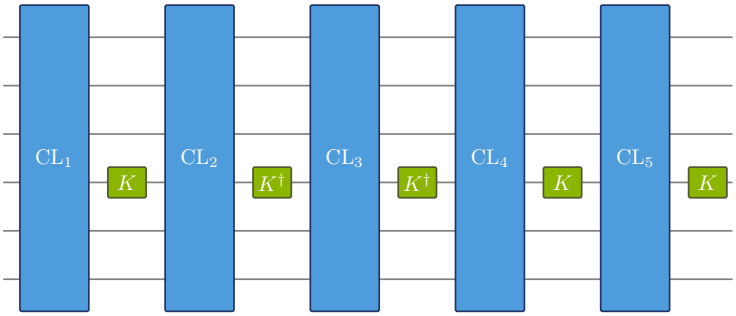
In this work, we show that strikingly, the number on non-Clifford gates that need to be inserted into a random Clifford circuit to generate a unitary t-design is independent of the system size and the polynomial in t, provided that t is not too large, $n \geq O(t^2)$.

Our result can be easily stated formaly. Let ν be a probability measure on the unitary group $U(d)$. The measure ν gives rise to a quantum channel

$$\Delta_t(\nu)(\rho) := \int_{\mathrm{U}(d)} U^{\otimes t}\rho\big(U^\dagger\big)^{\otimes t}\mathrm{d}\nu(U), \tag{1}$$

which applies $U^{\otimes t}$, with U chosen according to ν. We call a probability distribution ν an *(additive) ε-approximate t-design* if

$$\|\Delta_t(\nu) - \Delta_t(\mu_{\mathrm{Haar}})\|_\diamond \leq \varepsilon. \tag{2}$$



Here, $\|\cdot\|_\diamond$ is the diamond norm, which meaningfully captures channel distinguishability.

We consider uniformly drawn Clifford unitaries interleaved with a random single qubit gate drawn from $\{K, K^\dagger, \mathrm{id}\}$, where K is an arbitrary but fixed non-Clifford gate as illustrated in the figure. Note that these circuits are simulable on a classical computer in polynomial time for any fixed t. Our main result about these circuits is the following theorem:

Theorem 1 (Unitary designs with few non-Clifford gates)**.** *Let $K \in U(2)$ be a non-Clifford unitary. Then a K-interleaved Clifford circuit with depth $O(t^4 \log^2(t) \log(1/\varepsilon))$ acting on $n = O(t^2)$ qubits is an additive ε-approximate t-design.*

Surprisingly, again, the number of non-Clifford gates in this result is system-size independent. Hence, their density is allowed to go down to zero in the limit of large system sizes. Our result has several intriguing consequences: First, combined with the asymptotically optimal decomposition of Clifford unitaries [4] into standard generators, our construction features an overall number of gates needed to generate a unitary t-design of $O(n^2 t^4 \log^2(t)/\log(n))$. This is an improved scaling compared to Ref. [3] in both t and n (for small t). Our construction can be seen as a classical-quantum hybrid construction of unitary designs: The scaling is significantly improved by outsourcing as many tasks as possible to a classical computer. Second, Theorem 1 ensures the existence of families of ε-approximate $\log^{1/4}(n)$-designs that are classically simulable in polynomial time by additionally invoking Ref. [5]. Third, in the light of the connection of unitary designs and complexity developed in Ref. [6], we find that strong circuit complexity scales as $\Omega(k^{1/4})$ with the number of non-Clifford gates k independent of the system size.

In order to make contact with a circuit constructions with random local gates, we in our work additionally identify rigorous bounds on the convergence of random walks of local Clifford generators to the moments of the uniform distribution on the Clifford group.

Theorem 3 (Local random Clifford designs)**.** *Let $n \geq 12t$, then a local random Clifford circuit of depth $O(n^2 \log^{-2}(t) t^9 \log(1/\varepsilon))$ constitutes an ε-approximate t-design with respect to the uniform distribution on the Clifford group.*

This result is of independent interest and signifcantly improves the previously indicated scaling of $O(n^8)$ [7]. Together with Theorem 1 it provides a construction for unitary t-designs with a system-size-independent number of non-Clifford gates in terms of a circuit only consisting of random local gates.

Techniques

A key tool we use is a recently established variant of the Schur-Weyl duality for the Clifford group [8]. This describes the commutant of the t-th diagonal action of the Clifford group in terms

of a concept from symplectic geometry over finite fields: so-called stochastic Lagrangian subspaces $T \in \Sigma_{t,t}$ of the vector space $\mathbb{F}_2^{2t}$.

We prove various auxiliary results about these subspaces interesting in their own right. This includes a quantitative bound on the Gram-Schmidt orthogonalization of the resulting basis, the proof of which involves careful combinatorial bounds based on the statistics of cycles in random permutations. One of the most involved auxiliary results is a structural bound on the overlap of Lagrangian subspaces with the moment operator corresponding to the Haar measure.

Lemma 13 (Overlap of Lagrangian subspaces)**.** *For all t and for all $T \in \Sigma_{t,t} \setminus S_t$, it holds that*

$$(Q_T| \, P_{\mathrm{Haar}} \, |Q_T) \, \leq \, \frac{7}{8}, \tag{3}$$

where Q_T is the basis vector of the t-th commutant of the Clifford group corresponding to T and $P_{\mathrm{Haar}} = \Delta_t(\mu_{\mathrm{Haar}})$ is the t-th moment operator of the single-qubit unitary group $\mathrm{U}(2)$.

This is proven using a geometrical argument involving finite phase space methods. It is moreover essentially optimal, as we find examples that saturate a lower bound of $7/10$. We combine the before-mentioned bounds with deep results from harmonic analysis about spectral gaps of Hecke operators restricted to irreducible representations of Lie groups due to P. Varjú [9].

For our results on the convergence of random Clifford circuits, we use and further develop the martingale method for lower bounding spectral gaps of frustration-free Hamiltonians pioneered by Nachtergaele [10] and comparison techniques for random walks on finite groups by Diaconis and Saloff-Coste [11]. In order to apply these techniques, we obtain bounds on the difference between the uniform moment operator and the frame operator corresponding to the basis Q_T.

---

[1] E. Bannai, G. Navarro, N. Rizo, and P. H. Tiep, "Unitary t-groups," J. Math. Soc. Japan Advance publication.

[2] R. M. Guralnick and P. H. Tiep, "Decompositions of small tensor powers and larsen's conjecture," Represen. Theory **9**, 138–208 (2005).

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

[4] S. Aaronson and D. Gottesman, "Improved simulation of stabilizer circuits," Phys. Rev. A **70**, 052328 (2004).

[5] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, "Simulation of quantum circuits by low-rank stabilizer decomposition," Quantum **3**, 181 (2019).

[6] F. G. S. L. Brandao, W. Chemissany, N. Hunter-Jones, R. Kueng, and J. Preskill, "Models of quantum complexity growth," (2019), arXiv:1912.04297.

[7] D. P DiVincenzo, D. W. Leung, and B. M. Terhal, "Quantum data hiding," IEEE, Trans. Inf Theory **48**, 3580–599 (2002).

[8] D. Gross, S. Nezami, and M. Walter, "Schur-Weyl duality for the Clifford group with applications," (2017), arXiv:1712.08628.

[9] P. Varju, "Random walks in compact groups," Doc. Math. **18**, 1137–1175 (2013).

[10] B. Nachtergaele, "The spectral gap for some spin chains with disrete symmetry breaking," Commun. Math. Phys. **175**, 565–606 (1996).

[11] P. Diaconis and L. Saloff-Coste, "Comparison techniques for random walk on finite groups," Ann. Probab. **21**, 2131–2156 (1993).