Local random quantum circuits are approximate polynomial-designs

Fernando G.S.L. Brandão, Aram W. Harrow, Michał Horodecki

An approximate unitary t-design is a distribution of unitaries which mimics properties of the Haar measure for polynomials of degree up to t (in the entries of the unitaries). Approximate designs have a number of interesting applications in quantum information theory. It has been a conjecture in the theory of quantum pseudo-randomness that polynomial sized random quantum circuits on n qubits form an approximate unitary $\mathrm{poly}(n)$-design. However, up to now, the best result known was that polynomial random quantum circuits are unitary 3-designs [1]. Moreover, efficient constructions of quantum t-designs were only known for $t = O(n/\log(n))$ [2]. In our work [3] we make substantial progress in the problem of unitary t-designs. In particular

- We prove that local random quantum circuits acting on n qubits composed of polynomially many nearest neighbour two-qubit gates form an approximate unitary $\mathrm{poly}(n)$-design, settling the conjecture in the affirmative.
- We consider pseudo-randomness properties of local random quantum circuits of *small depth* and prove they constitute a quantum $\mathrm{poly}(n)$-copy tensor product expander.
- As a first application of the result, we show the following pseudo-randomness property of efficiently generated quantum states: almost every circuit on n qubits of size n^k generates a state that cannot be distinguished from the maximally mixed state by circuits of size $n^{(k+4)/6}$. This provides a data-hiding scheme against computationally bounded adversaries.
- As a second application, we reconsider a recent argument of Masanes, Roncaglia, and Acin [4] concerning local equilibration of time-evolving quantum systems, and strengthen the connection between fast equilibration of small subsystems and the circuit complexity of the unitary which diagonalizes the Hamiltonian.

The proof of the first result is based on an interplay of techniques from quantum many-body theory, representation theory, and the theory of Markov chains. In particular we employ a result of Nachtergaele [5] for lower bounding the spectral gap of frustration-free quantum local Hamiltonians; a quasi-orthogonality property of permutation matrices; and a result of Oliveira [6] which extends to the unitary group the path coupling method [7] for bounding the mixing time of random walks.

The proof of the second result also rests on techniques from quantum many-body theory, in particular on the detectability lemma of Aharonov, Arad, Landau, and Vazirani [8].

Main result: We define the diamond norm of a superoperator $\mathcal{T}$ as follows $\|\mathcal{T}\|_\diamond := \sup_d \|\mathcal{T} \otimes \mathbb{I}_d\|_{1\to 1}$ with $\|\mathcal{T} \otimes \mathbb{I}_d\|_{1\to 1} := \sup_{X\neq 0} \frac{\|\mathcal{T}(X)\|_1}{\|X\|_1}$. For a distribution ν on $\mathbb{U}(N)$ define

$$\Delta_{\nu,t}(\rho) := \int_{\mathbb{U}(N)} U^{\otimes t} \rho (U^\dagger)^{\otimes t} \nu(dU). \tag{1}$$

and let μ_{Haar} be the Haar measure on $\mathbb{U}(N)$. Then

Definition. *Let ν be a distribution on $\mathbb{U}(N)$. Then ν is an ϵ-approximate unitary t-design if*

$$\left\|\Delta_{\nu,t} - \Delta_{\mu_{Haar},t}\right\|_\diamond \leq \epsilon. \tag{2}$$

We consider the *local random circuit model*, defined in the following way: In each step of the walk an index i is chosen uniformly at random from $[n]$ and a unitary $U_{i,i+1}$ drawn from the Haar measure on $\mathbb{U}(4)$ is applied to the two neighbouring qubits i and $i+1$. The main result of [3] is the following:

Theorem. *Local random circuits of size* $\log(1/\epsilon)\log(t)t^5n^2$ *form an* ϵ*-approximate unitary* t*-design.*

Applications: In [3] we present two applications of the main result. The first is related to pseudo-randomness properties of efficiently generated states. An old open question in this respect is the following [9]: can we find a state which can be created by a circuit of size s, yet is indistinguishable from the maximally mixed state by any measurement implementable by circuits of size r, for r not too much smaller than s? Using the main theorem we can show that this is indeed the case. In fact, this is a generic property of states which can be greated by circuits of sufficient large size:

Corollary. *All but a* $2^{-\Omega(n)}$*-fraction of circuits of size* n^k *(for* $k \geq 2$*) on* n *qubits map* $|0\rangle^{\otimes n}$ *to a state that cannot be distinguished from the maximally mixed state with bias larger than* $n^{-\Omega(1)}$ *by any circuit of size* $n^{\frac{k+4}{6}}\,\mathrm{polylog}^{-1}(n)$.

The second application is related to the problem of understading dynamical equilibration of subsystems of a time-envolving quantum system. Here we show how the Theorem can be used to strengthen a recent connection [4] between the time of equlibration of small subsystems of a closed quantum system and the circuit complexity of the unitary which diagonalizes the Hamiltonian of the system. See [3] for more details.

Summary of the Proof: The proof consists of four steps, summarized below (see [3] for details).

1. Relating to Spectral Gap: In the first step we relate the question of showing that local random circuits are a unitary design to lower bounding the spectral gap of a local quantum Hamiltonian, defined as: $H_{n,t} := \sum_{i=1}^{n} h_{i,i+1}$, with local terms $h_{i,i+1} := \mathbb{I} - P_{i,i+1}$ acting on subsystems $i, i+1$ and $P_{i,i+1}$ defined as $P_{i,i+1} := \int_{\mathbb{U}(4)} (U_{i,i+1})^{\otimes t,t}\, \mu_{\mathrm{Haar}}(dU)$, with $U^{\otimes t,t} := U^{\otimes t} \otimes (U^*)^{\otimes t}$.

For a measure ν on $\mathbb{U}(d^n)$, let $g(\nu,t) := \left\| \int_{\mathbb{U}(d^n)} U^{\otimes t,t}\nu(dU) - \int_{\mathbb{U}(d^n)} U^{\otimes t,t}\mu_{\mathrm{Haar}}(dU) \right\|_\infty$, so that ν is a (d^n, g, t)-tensor product expander. Also let μ_n be the measure on $\mathbb{U}(2^n)$ induced by one step of the random walk given by the local random circuit model (when applied initially to the identity). Then with $\Delta(H_{n,t})$ the spectral gap of $H_{n,t}$ we prove

Lemma 1. *For every* $k > 0$, $\quad g((\mu_n)^{*k}, t) = g(\mu_n, t)^k = \left(1 - \frac{\Delta(H_{n,t})}{n}\right)^k$, *with* $(\mu_n)^{*k}$ *the* k*-fold convolution of the measure* μ_n.

2. The Structure of $H_{n,t}$: It turns out that $H_{n,t}$ has a few special properties which make the estimation of its spectral gap feasible.

Lemma 2. *For every* $n, t > 0$ *the following properties of* $H_{n,t}$ *hold true:*

1. *the minimum eigenvalue of* $H_{n,t}$ *is zero and the zero eigenspace is given by*

$$\mathcal{G}_{n,t} := \mathit{span}\left\{ |\psi_\pi\rangle^{\otimes n},\ \ |\psi_\pi\rangle := (\mathbb{I} \otimes V(\pi))|\Phi\rangle \ :\ \pi \in S_t \right\}, \tag{3}$$

with $|\Phi\rangle := d^{-t/2}\sum_{k=1}^{d^t} |k,k\rangle$ *the maximally entangled state on* $(\mathbb{C}^d)^{\otimes t} \otimes (\mathbb{C}^d)^{\otimes t}$, S_t *the symmetric group of order* t, *and* $V(\pi)$ *the representation of* $\pi \in S_t$ *which acts on* $(\mathbb{C}^d)^{\otimes t}$ *as* $V(\pi)|l_1\rangle \otimes ... \otimes |l_t\rangle = |l_{\pi^{-1}(1)}\rangle \otimes ... \otimes |l_{\pi^{-1}(t)}\rangle$;

2. let $G_{n,t}$ be the projector onto $\mathcal{G}_{n,t}$. Then

$$\sum_{\pi\in S_t} |\langle\psi_{\sigma,d}|\psi_{\pi,d}\rangle|^n \leq 1 + \frac{2t^2}{d^n}, \quad \textit{and} \quad \left\| \sum_{\pi\in S_t} (|\psi_{\pi,d}\rangle\langle\psi_{\pi,d}|)^{\otimes n} - G_{n,t} \right\|_\infty \leq \frac{2t^2}{d^n} \tag{4}$$

3. Lower Bounding the Spectral Gap: With the properties given by Lemma 2 we are in position to lower bound $\Delta(H_{n,t})$. To this aim we use a result of Nachtergaele [5], originally proposed to lower bound the spectral gap of frustration-free local Hamiltonians with a groundspace spanned by matrix-product states. We show:

Lemma 3. *For every integers n, t with $n \geq \lceil 10\log(t)\rceil$, $\quad \Delta(H_{n,t}) \geq \frac{\Delta(H_{\lceil 2\log(t)\rceil,t})}{8\log(t)}$.*

4. Bounding Convergence with Path Coupling: The last step in the proof consists in lower bounding $\Delta(H_{\lceil 2\log(t)\rceil,t})$. We achieve this by bounding the convergence time of the random walk on $\mathbb{U}(2^n)$ defined by the local random circuit in order to lower bound the spectral gap of $\Delta(H_{\lceil 2\log(t)\rceil,t})$. The point is that now any bound on the convergence time is useful. Actually, in light of Lemma 3, it sufficies to prove an *exponentially small* bound on the convergence time in order to obtain the theorem, and this is what we accomplish.

We consider the convergence of the random walk in the *Wasserstein distance* between two probability measures ν_1 and ν_2 on $\mathbb{U}(r)$, defined as $W(\nu_1,\nu_2) := \sup\left\{ \int_{\mathbb{U}(r)} f(U)\nu_1(dU) - \int_{\mathbb{U}(r)} f(U)\nu_2(dU) \;:\; f : \mathbb{U}(r) \to \mathbb{R} \text{ is 1-Lipschitz} \right\}$, where we say that f is 1-Lipschitz if for every two unitaries U, V, $|f(U) - f(V)| \leq \|U - V\|_2$, with $\|X\|_2 := \mathrm{tr}(X^\dagger X)^{1/2}$ the Frobenius norm.

Lemma 4. *For $k, n > 0$, $\quad W((\mu_n)^{*(n-1)k}, \mu_{Haar}) \leq \left(1 - \frac{1}{e^n 5^{n-2}}\right)^{\frac{k}{n-1}} 2^{\frac{n+1}{2}}$.*

The proof of Lemma 4 rests on Bubley and Dyer *path-coupling* method [7] for bounding the mixing time of Markov chains. In particular, we use a version of path coupling for Markov chains on the unitary group recently obtained by Oliveira [6].

Finally, we use Lemma 5 to lower bound the spectral gap of $\Delta(H_{\lceil 2\log(t)\rceil,t})$.

Lemma 5. *For $k, n, t > 0$, $\quad \left(1 - \frac{\Delta(H_{n,t})}{n}\right)^k \leq 2tW((\mu_n)^{*k}, \mu_{Haar})$.*

The theorem then follows easily from the previous lemmas.

---

[1] F.G.S.L. Brandão and M. Horodecki. arXiv:1010.3654.
[2] A.W. Harrow and R. Low. arXiv:0811.2597.
[3] F.G.S.L. Brandão, A.W. Harrow, M. Horodecki. arXiv:1108.09XX.
[4] L. Masanes, A. Roncaglia, A. Acin. 1108.0374.
[5] B. Nachtergaele. Commun. Math. Phys. **175**, 565 (1996).
[6] R. Oliveira. arXiv:0705.2253.
[7] R. Bubley and M. Dyer. FOCS'97: Proceedings of the 38th Annual Symposium on the Foundations of Computer Science (1997).
[8] D. Aharonov, A. Arad, Z. Landau, and U. Vazirani. arXiv:1011.3445.
[9] The ten most annoying questions in quantum computing - question 9. http://www.scottaaronson.com/blog/?p=112