Local random quantum circuits are approximate polynomial-designs: numerical results

Piotr Ćwikliński¹, Michal Horodecki¹²³, Marek Mozrzymas⁴, Łukasz Pankowski¹²³ and Michał Studziński¹²³

¹ Institute for Quantum Information, RWTH Aachen University, D-52056 Aachen, Germany
² Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland
³ National Quantum Information Centre of Gdańsk, 81-824 Sopot, Poland
⁴ Institute for Theoretical Physics, University of Wrocław, 50-204 Wrocław, Poland

E-mail: fizpc@ug.edu.pl

Received 23 January 2013, in final form 20 June 2013
Published 5 July 2013
Online at stacks.iop.org/JPhysA/46/305301

Abstract
We numerically investigate the statement that local random quantum circuits acting on \( n \) qubits composed of polynomially many nearest-neighbor two-qubit gates form an approximate unitary poly\((n)\)-design (BrandÃO et al 2012 arXiv:1208.0692). Using a group theory formalism, spectral gaps that give a ratio of convergence to a given \( t \)-design are evaluated for a different number of qubits \( n \) (up to 20) and degrees \( t \) (\( t = 2, 3, 4 \) and 5), improving previously known results for \( n = 2 \) in the case of \( t = 2 \) and 3. Their values lead to the conclusion that the previously used lower bound that bounds spectral gaps values may give very little information about the real situation and in most cases, only tells us that a gap is closed. We compare our results to another lower bounding technique, again showing that its results may not be tight.

PACS numbers: 03.67.-a, 03.65.Fd

Online supplementary data available from stacks.iop.org/JPhysA/46/305301/mmedia
(Some figures may appear in colour only in the online journal)

1. Introduction

Random unitary matrices have established their place as a useful and powerful tool in the theory of quantum information and computation. For example, they are used in the encoding protocols for sending information down a quantum channel [1], approximate encryption of quantum information [2], quantum datahiding [2], information locking [2], process tomography [3], state distinguishability [4], and the equilibration of quantum states [5–8], and some other problems in the foundation of statistical mechanics [9].
There is, however, a problem with them—they are not very favorable from a computational point of view. Why? The answer is as follows. To implement a random Haar unitary one needs an exponential number of two-qubit gates and random bits (in other words, to sample from the Haar measure with error $\epsilon$, one needs $\exp(4^n \log(\frac{1}{\epsilon}))$ different unitaries). To bypass this problem, one can construct so-called approximate random unitaries or pseudo-random unitaries. Using them, an efficient implementation is possible.

An approximate unitary $t$-design is a distribution of unitaries which mimic properties of the Haar measure for polynomials of degree up to $t$ (in the entries of the unitaries) [10–23]. Approximate designs have a number of interesting applications in quantum information theory replacing the use of truly random unitaries (see e.g. [13, 14, 21, 22, 24, 25]). What is more, other particular constructions of approximate unitary $t$-designs, together with some applications in quantum physics, have been formulated; let us mention here, for example, a recent construction of diagonal unitary $t$-designs [26, 27].

In 2009, Harrow and Low [15] stated a conjecture that polynomial-sized random quantum circuits acting on $n$ qubits form an approximate unitary poly$(n)$-design. To give an example supporting their statement, the authors, also in 2009, presented efficient constructions of quantum $t$-designs, using a polynomial number of quantum gates and random bits for $t = O(\log(n))$ [23].

However, it took some time to verify the conjecture from [15]. At that time, it was already known that there exist efficient approximate unitary 2-designs in $U(d^n)$, where ‘efficient’ means that unitaries are created by a polynomial (in $n$) number of two-qubit gates and the distribution of unitaries can also be sampled in polynomial time (in other words, random circuits are approximate unitary 2-designs) [13–18, 28]. In 2010, Brandão and Horodecki [21], went one step further, proving that polynomial random quantum circuits are approximate unitary 3-designs. Quite recently, a breakthrough has been made for the above problem. In [29], the authors proved that local random quantum circuits acting on $n$ qubits composed of polynomially many nearest-neighbor two-qubit gates form an approximate unitary poly$(n)$-design, setting the conjecture from [15] to be affirmative. Their proof is based on techniques from many-body physics, representation theory and combinatorics. In particular, one of the tools used to obtain the main result was the estimation of the spectral gap of the frustration-free local quantum Hamiltonian, which can be used to study the problem (instead of a quantum circuit).

In this paper, we analyze two aspects of their statement. First, we numerically verify and investigate it, calculating spectral gaps for the increasing number of qubits (in a circuit) $n$ (up to $n = 20$, in the best case) and degree $t$ ($t = 2, 3, 4, 5$). Previously, exact values were known only for $n = 2$ and $t = 2, 3$. This may be of independent interest since, in many-body physics, the knowledge of spectral gaps of local Hamiltonians is useful in studying many-body systems (see, for example, [5, 30–32]). In addition, in [21], the authors obtained that for $n = 2$, gap values for $t = 2$ and 3 are the same; we obtain the matching of all calculated spectral gap values in the case of $t = 2$ and 3, which is a unique feature for this exact degree $t$. Second, in [29], in order to prove the main statement, a lower bound for spectral gaps was derived (independent from the number of qubits). However, based on our results, it can be concluded that lower bounding of spectral gaps may not be tight. We show that there could be a large difference in the actual values of spectral gaps and the corresponding lower bounds. What is more, our calculations for increasing values of $n$ and $t$ lead to the conclusion that firstly, the lower bound from [29] is hard to estimate; secondly, it gives only limited information about the actual value of spectral gaps (that a gap is closed). Simultaneously, we also compare our results to another lower bound, derived in [33], and show that predictions obtained according to it can be better than that from [29]. Nevertheless, also in this case, predictions according
to that bound can be inconclusive in some cases, showing that, in principle, obtaining a good bound is a demanding task.

Our paper is structured as follows. In section 2 we start by introducing local (random) quantum circuits which, using the formalism of superoperators, we connect with approximate unitary $t$-designs. In section 3 we recall the statement that local quantum circuits of a given length form approximate unitary $t$-designs. We also recall that to verify and check this connection, calculations of spectral gaps and the second largest eigenvalues of local Hamiltonians connected to the problem are necessary. Section 4 is the key section of this paper. We first show how to connect our problem of checking the connection between local quantum circuits and $t$-designs (calculating the spectral gaps) with symmetric groups $S(t)$, where $t$ corresponds to a degree in $t$-design. Then, we present our numerical calculations for spectral gaps for a different number of qubits $n$ and different degrees $t$, which we later compare to results obtained using the techniques for lower bounding the spectral gaps.

2. Random unitary circuits and approximate $t$-designs

In this section, we present the formalism of local random quantum circuits and approximate unitary designs. We wish to point out here that sections 2 and 3 are mainly based on [21, 29], so for the full analysis (proofs, etc), we refer to these papers.

We consider $n$ qubits (from now on $d = 2$), and apply $l$ steps of a random circuit (random walks on $U(d^n)$).

**Definition 1** (Local quantum circuit). In each step of the walk an index $i$ is chosen uniformly at random from $[n]$ and then a unitary $U_{i,i+1}$, drawn from the Haar measure on $U(d^2)$, is applied to the two neighboring qubits $i$ and $i + 1$.

There are several different definitions of $\varepsilon$-approximate unitary $t$-designs [34] from which we should mention the following.

**Definition 2** (Approximate unitary $t$-design). Let $\{\mu, U\}$ be an ensemble of unitary operators from $U(2^n)$. Define

$$\mathcal{G}_{\mu,t}(\rho) = \int_{U(d^2)} U^{\otimes t} \rho(U^\dagger)^{\otimes t} \mu(\text{d}U)$$

(2.1)

and

$$\mathcal{G}_{H,t}(\rho) = \int_{U(d^2)} U^{\otimes t} \rho(U^\dagger)^{\otimes t} \mu_H(\text{d}U),$$

(2.2)

where $\mu_H$ is the Haar measure. Then the ensemble is a $\varepsilon$-approximate unitary $t$-design if

$$||\mathcal{G}_{\mu,t} - \mathcal{G}_{H,t}||_{2\rightarrow 2} \leq \varepsilon,$$

(2.3)

where the induced Schatten norm $||\Lambda(X)||_{p\rightarrow q} = \sup_{X \neq 0} \frac{||\Lambda(X)||_q}{||X||_p}$ is used.

3. Local random quantum circuits are approximate polynomial-designs

In this section we will review some basic facts about local random circuits. At the end, we will recall the statement that local quantum circuits of a given length form approximate unitary $t$-designs.

Let $\mu$ be a measure on $U(2^n)$ induced by one step of the local random circuit model and $\mu^l$ be a measure induced by $l$ steps on the model. One can then show the following (bearing in mind that for a superoperator $\mathcal{G}$ and an operator $G$ that have the same set of eigenvalues holds $||\mathcal{G}||_{2\rightarrow 2} = ||G||_{\infty}$; see appendix C).

3
Figure 1. A local Hamiltonian acting on \( n \) subsystems \( H_{n,t} = \sum_{i=1}^{n-1} h_{i,i+1} \), each of dimension \( d^2 \). Its spectral gap value \( \Delta(H_{n,t}) \) can be connected with the second largest eigenvalue of the operator \( G_{\mu,t} \).

**Theorem 3** [29].

\[
||G_{\mu,t} - G_{\mu,t}||_\infty = \lambda_2 \left( \int_{U(d)} U^{\otimes t} \otimes (U^*)^{\otimes t} \mu(dU) \right)
\]

(3.1)

where \( G_{\mu,t} = \int_{U(d)} U^{\otimes t} \otimes (U^*)^{\otimes t} \mu(dU) \) and \( \lambda_2 \) stands for the second largest eigenvalue of \( G_{\mu,t} \). However, \( \mu = \frac{1}{n} \sum_{i=1}^{n-1} \mu_H(i, i + 1) \), so

\[
\lambda_2 \left( \int_{U(d)} U^{\otimes t} \otimes (U^*)^{\otimes t} \mu(dU) \right) = 1 - \frac{\Delta(H_{n,t})}{n}.
\]

(3.2)

with \( H_{n,t} = \sum_{i=1}^{n-1} h_{i,i+1} \), with local terms \( h_{i,i+1} = I - \int_{U(d)} U_{i,i+1}^{\otimes t} \otimes (U_{i,i+1}^*)^{\otimes t} \mu_H(dU) \) and \( \Delta(H_{n,t}) \) the spectral gap of the local Hamiltonian \( H_{n,t} \) (see figure 1).

After a successful estimation of the spectral gap from equation (3.1), one can show the following.

**Theorem 4** [29]. Local random circuits of size \((\log(\frac{1}{\epsilon})2\log(d))\log(t) t^5 n^2\) form a \( \epsilon \)-approximate unitary \( t \)-design.

Thus the problem reduces to analysis of the spectral gap of the operator \( G_{\mu,t} \). Now, it is important to ask the following.

- How does a spectral gap depend on the number of qubits \( n \) and the degree of design \( t \)?

In the next section, an answer to this question is provided.

**4. Spectral gaps: numerical results**

In this section, we present our numerical results for spectral gaps for different degrees \( t \) in \( t \)-designs (for simplicity, we gather all results in table 1). What is more, we compare our results (where possible) with two lower bounds for spectral gaps: (1) the ‘local’ lower bound obtained in [33]; (2) the ‘global’ lower bound derived in [29]. To evaluate the spectral gaps, the Mathematica and Matlab software and a C++ code have been used (the code for the basis generation from Appendix A and a short description of spectral gap calculations is available as supplementary data (available from stacks.iop.org/JphysA/46/305301/mmedia)).

**4.1. Local Hamiltonians as a tool for calculating spectral gaps**

We have already shown that calculations of spectral gaps can be connected with the second largest eigenvalue of \( G_{\mu,t} \). Now we will show how to connect calculations of spectral gaps (equivalently, second largest eigenvalues) with symmetric groups \( S(t) \), where \( t \) plays the role of the degree of the \( t \)-design, using techniques for local Hamiltonians introduced in section 3.
At the beginning, let us remind ourselves that our Hamiltonian is of the form
\[ H_{n,t} = \sum_{i=1}^{n-1} h_{i,i+1}, \]
with local terms \( h_{i,i+1} = I - P_{i,i+1} \), and with notation as in section 3.

Let us consider superoperators associated with projectors \( P_{i,i+1} \)
\[ P_{i,i+1}(X) = \int_{U(d)} U_{i,i+1}^{\otimes t} X (U_{i,i+1}^{\dagger})^{\otimes t} \mu_H(dU). \] (4.1)

Now we can find, as a consequence of the Schur–Weyl duality \[35\] that all operators \( X \), invariant under action of \( P_{i,i+1} \), can be written as a sum of permutation operators \( V_{\pi} \),
\[ P_{i,i+1} \subset V_{\pi} \otimes V_{\pi}, \]
where the operators \( P_i \) are given by the expression
\[ P_i = \int_{U(d)} U_i^{\otimes t} \otimes (U_i^{\dagger})^{\otimes t} \mu_H(dU). \] (4.2)

Thanks to the above consideration, we can deduce that operator \( X \) can identify with the operator \( G_{\mu,t} \) from theorem 3 and is written according to the formula
\[ G_{\mu,t} = P_{1,2} \otimes I_3 \otimes \cdots \otimes I_n + I_1 \otimes P_{2,3} \otimes I_4 \otimes \cdots \otimes I_n + \cdots + I_1 \otimes I_2 \otimes \cdots \otimes P_{n-1,n}. \] (4.3)

In a subspace spanned by permutation operators acting on Hilbert space \( \mathcal{H}^{\otimes t} \) we are able to construct an operator basis which is orthogonal in the Hilbert–Schmidt scalar product (see appendix A). Using this basis we can calculate the two biggest eigenvalues of operators \( X \) which are necessary to find out the spectral gap.

**Table 1.** Numerically calculated spectral gaps for different degrees \( t \) and number of qubits \( k \).

| \( t \) | \( k \) | \( \Delta(H_{k,t}) \) |
|---|---|---|
| 2,3 | 2 | 0.6 |
| 2,3 | 3 | 0.434 31 |
| 2,3 | 4 | 0.352 79 |
| 2,3 | 5 | 0.307 18 |
| 2,3 | 6 | 0.279 22 |
| 2,3 | 7 | 0.2609 |
| 2,3 | 8 | 0.248 25 |
| 2,3 | 9 | 0.239 15 |
| 2,3 | 10 | 0.232 41 |
| 2 | 11 | 0.2273 |
| 2 | 12 | 0.2232 |
| 2 | 13 | 0.2201 |
| 2 | 14 | 0.2175 |
| 2 | 15 | 0.2154 |
| 2 | 16 | 0.2136 |
| 2 | 17 | 0.2122 |
| 2 | 18 | 0.2109 |
| 2 | 19 | 0.2098 |
| 2 | 20 | 0.2089 |
| 4 | 2 | 0.5 |
| 4 | 3 | 0.452 986 444 03 |
| 4 | 4 | 0.424 860 357 53 |
| 4 | 5 | 0.410 228 555 73 |
| 5 | 2 | 0.373 734 696 02 |
| 5 | 3 | 0.329 125 484 83 |
4.2. Lower bounding a spectral gap

Herewith, we present two methods for lower bounding the spectral gaps that we will use later to compare to values of spectral gaps obtained numerically.

1. ‘Global’ bound.

**Lemma 5** [29]. For every integer \( n \) (number of qubits) and \( t \) (in \( t \)-design), with \( n \geq \lceil 10 \log(t) \rceil \), the spectral gap \( \Delta(H_{n,t}) \) can be lower bounded as follows:

\[
\Delta(H_{n,t}) \geq \frac{\Delta(H_{\lceil 2\log(d)^{-1}\log(t) \rceil,t})}{8(\log(d))^{-1}\log(t)},
\]

with \( d \) being the dimension of the Hilbert space and \( \lceil a \rceil \) denoting the smallest integer \( k \) satisfying \( k \geq a \).

2. ‘Local’ bound.

**Lemma 6** [33]. For every integer \( n \) and \( t \), the spectral gap \( \Delta(H_{n,t}) \) of the local Hamiltonian can be lower bounded in the following way:

\[
\Delta(H_{n,t}) \geq \frac{k\Delta(H_{k,t}) - 1}{k - 1},
\]

where \( \Delta(H_{k,t}) \) is the Hamiltonian restricted to \( k \) qubits: \( H_k = \sum_{i=1}^k h_{i,i+1} \).

Let us now explain why we used the terms ‘global’ and ‘local’ to describe these two bounds. From equation (4.4) it can be noticed that to lower bound a given spectral gap, one needs to compute only one spectral gap—the one given by \( t \) and the dimension of the system (but we consider qubits only, so the value \( d = 2 \) is set). The bound is global in the sense that it does not change with the number of qubits—it remains constant for an arbitrary length of a quantum circuit. On the contrary, the second bound (from equation (4.5)) has a total reverse property. There, the gap for a higher number of qubits implies better precision of the bound.

Of course, as we will see later, both bounds have pros and cons. For example, the ‘global’ bound usually bounds the spectral gap value in a harsh way (only giving the information that a gap is open) and, what is more, one can observe that for large values of \( t \), one needs to know a value of the spectral gap for a large number of qubits in order to estimate that bound. Keeping in mind that calculating spectral gaps is, in principle, a computationally hard problem, the effectiveness of the ‘global’ bound is limited. The good thing about it is that it is always positive (thus giving a nonzero convergence rate of random circuits to a given \( t \)-design). On the other hand, it is not true for the second bound. For small numbers of qubits, the ‘local’ bound can be negative and it means that one needs to increase its precision by calculating the lower bound using a gap for a bigger number of qubits. Moreover, the value of the bound sometimes fluctuates, so the value of the bound for a number of qubits \( k \) can potentially be worse than that for \( k - 1 \) qubits. The advantage of this bound is that when it is positive its value is usually closer to the exact value than that predicted by the bound from equation (4.4).

4.3. Method of calculations

In this section we will present some methods of calculations used in this paper. Notation is mostly taken from [21].

We know that for an arbitrary subspace of operator space we are able to construct a basis of operators which is orthonormal in the Hilbert–Schmidt scalar product. For this construction we use a linear combination of nonorthogonal permutation operators acting on \( \mathcal{H}^\otimes t \):

\[
R_k = \sum_{\pi \in \mathcal{S}(t)} b_{2^k}(t) V_{\pi}.
\]
Figure 2. The figure presents a $t \times n$ lattice. We have $n$ columns and in every column there are $t$ qubits on which permutations from $S(t)$ act. In the blue rectangle, we marked the $i$th and $(i+1)$th column on which the operator $R_k^{(i+1)}$ acts.

Using operators $R_k$ we can rewrite operators $P_{i,i+1}$ and $P_i$ from equations (4.1) and (4.2) in a form

$$P_{i,i+1} = \sum_k |R_k^{(i+1)}\rangle \langle R_k^{(i+1)}|, \quad P_i = \sum_k |R_k^{(i)}\rangle \langle R_k^{(i)}|.$$  (4.7)

To illustrate the action of operators $R_k^{(i+1)}$, consider a $t \times n$ lattice (see figure 2), then $R_k^{(i+1)}$ acts jointly on systems from the $i$th and $(i+1)$th column.

Finally to obtain a representation of an operator $X$ from equation (4.3) in our product basis i.e.

$$X = \sum_{kl} a_{kl} |R_k^{(1)}\otimes \cdots \otimes R_k^{(n)}| R_l^{(1)}\otimes \cdots \otimes R_l^{(n)}|,$$  (4.8)

where $k = (k_1, \ldots, k_n)$ and $l = (l_1, \ldots, l_n)$ are multiindices, we have to express the operators $P_{i,i+1}$ in terms of a product basis. For this purpose we use argumentation from [21], having:

$$R_k^{(1,2)} = \sum_{k,u} r_{k,u}^{(1)} R_k^{(1)} \otimes R_u^{(2)},$$  (4.9)

where $r_{k,u}^{(1)}$ are some coefficients which we want to know. In this paper, to calculate the numbers $r_{k,u}^{(1)}$ we use the Schur basis (see, for example, [36]). Then every operator $R_k^{(1,2)}$ corresponds to a linear combination of $E_{ij}^{(1)} \otimes E_{mn}^{(2)}$, where operators $E_{ij}^{(1)}$ form an operator basis in a given invariant subspace of $H^{\otimes n}$ labeled by $\alpha$. Now we see that an index $k$ in equation (4.9) is indeed a multiindex. The general method of constructing such an operator basis via representation theory is given in appendix A. Of course, computing eigenvalues in an arbitrary basis (also in our basis) is quite hard, because the complexity of calculations grows very fast with the parameter $t$.

4.4. Numerical results

Here, we present our numerically calculated values of the spectral gaps for different cases, together with the corresponding lower bounds (both ‘local’ and ‘global’ when possible). In figure 3, there are spectral gaps $\Delta(H_{t,2})$ for the symmetric group $S(2)$ and a different number of qubits $n$, corresponding to the 2-design. Both lower bounds are also marked. Similarly, values of spectral gaps $\Delta(H_{t,t})$ for $t = 3, 4, 5$ (3-, 4-, 5-designs) can be found in figures 4–6.

Notice that with increasing $t$, the ‘global’ bound tends to less and less information, telling us that gaps are closed. What is more, for the last plot (figure 6), the ‘local’ bound does not give any bound since it takes a negative value. Knowledge of the gaps for $k \geq 4$ is required to resolve this problem.
Figure 3. Numerically evaluated spectral gaps $\text{Gap} = \Delta(H_{k,t})$ for $t = 2$ (dots) versus ‘local’ bound for $k$ qubits (squares) versus ‘global’ bound for a given $n$ (here, $n = 2$) (line).

Figure 4. Numerically evaluated spectral gaps $\text{Gap} = \Delta(H_{k,t})$ for $t = 3$ (dots) versus ‘local’ bound for $k$ qubits (squares) versus ‘global’ bound for a given $n$ (here, $n = 4$) (line).

From figures 3 and 4 one can observe that, in the case of $t = 2$ and $t = 3$, all spectral gaps are the same. This could (possibly) imply the following.

**Conjecture 7.** Knowledge of the spectral gaps of the local Hamiltonian $H_{k,2}$ from theorem 3 is sufficient to know those for $H_{k,3}$, since there is a one-to-one correspondence between them.

**Remark 8.** Let us explain here one important thing about our notation. For simplicity and transparency, we mark each lower bound from equation (4.5) corresponding to some spectral gap as a ‘square’ in figures 3–6.
4.5. Basic examples

Consider the case when \( t = 2 \). The spectral gap for \( k = 2 \) is equal to \( \Delta(H_{2,2}) = \frac{6}{10} \). Using theorem 3.1, we have that, in this case, the second largest eigenvalue \( \lambda_2 \) of \( G_{2,2} \) equals to \( \frac{1}{2} \). Applying this to the ‘local’ bound, we get that the bounded gap is equal to \( \frac{3}{10} \), which implies (according to definition 2 and fact 16) that a \( 5n \log \left( \frac{\epsilon}{\lambda_2} \right) \)-sized random quantum circuit is a \( \epsilon \)-approximate 2-design. From the ‘global’ bound, we get that a \( 13n \log \left( \frac{\epsilon}{\lambda_2} \right) \)-sized random quantum circuit is a \( \epsilon \)-approximate 2-design. Looking carefully at figure 3, one can observe that \( \Delta(H_{20,2}) \approx 0.21 \) seems to be bounding the convergence of the values of gaps quite well.
It tells us that the length of a circuit should scale as $4.76n \log(\frac{1}{\varepsilon})$. See the references from the introduction (especially [10]) for possible applications of these results.

When $t = 3$, $\Delta(H_{2,3}) = \frac{6}{\pi}$ and thus again the above result from the ‘local’ bound and the convergence is valid. Using the ‘global’ bound we have that a $35.95n \log(\frac{1}{\varepsilon})$-sized random quantum circuit is a $\varepsilon$-approximate 3-design. Note that 3-designs can be used to solve the $U$-circuit checking problem [21].

The results for $t = 2, 3$, obtained using the ‘local’ bound, are in accordance with those from [21] and what is more, for $t = 2$ our outcomes match those from [10], but are a little bit more precise.

For 4-designs, which can be used to bound the equilibration time in some cases (see, [5, 6]), from the ‘local’ bound, we have that a $2.44n \log(\frac{1}{\varepsilon})$-sized circuit can form them. On the other hand, if the gap $\Delta(H_{5,4}) \approx 0.41$ for 5 qubits, which is the best explicitly calculated value, can be approximately used as the bound to which all others converge, we get that a $3.81n \log(\frac{1}{\varepsilon})$-sized random quantum circuit is a $\varepsilon$-approximate 4-design. Here, the ‘global’ bound gives the following length: $37.66n \log(\frac{1}{\varepsilon})$. The result from the first bound seems to be interesting. Why? We accept that the length of a circuit should increase with increasing $t$ and comparing the results from the ‘local’ bound, we have that the circuit for $t = 4$ is shorter than for $t = 2, 3$.

For $t = 5$, not much can be said. All values calculated according to the ‘local’ bound are negative and $\Delta(H_{2,5}) \approx 0.29$ cannot be used as the value that bounds all others. Here, a prediction from the ‘global’ bound also cannot be reported since the value of a gap for $H_{5,5}$ is needed to calculate it.

It is worth asking whether these results can be improved. As proved in [29] (see proposition 8 from that paper), neither the $t$ nor $n$ dependence can be improved by more than polynomial factors.

5. Conclusions and open problems

In this paper, we numerically studied the recent statement that local random quantum circuits acting on $n$ qubits and composed of polynomially many two-qubit gates form an approximate unitary poly($n$)-design.

To this end, we evaluated spectral gaps of local Hamiltonians acting on $n$ qubits, using techniques from many-body physics and relating the degree $t$ in the $t$-design to the symmetric group $S(t)$. As an additional result, it occurs that for a given $k$, $H_{k,2}$ is equal to $H_{k,3}$, while there is no such connection between $H_{k,t}$ for higher values of $t$.

What is more, we compare our results to two lower bounds for spectral gaps, leading to the conclusion that for a small number of qubits, lower bounding is usually not sufficient to obtain a reliable result—there is a big difference in actual values of spectral gaps and the lower bound. For large numbers of qubits and high orders of $t$, there is another problem: to obtain a ‘good’ lower bound, one needs to first calculate first a spectral gap for quite a large value of $n$ and $t$, which is a quite complicated task from the computational point of view. That is why we were unable to compute the ‘global’ lower bound for the case when $t = 5$, since it requires initial knowledge of the spectral gap for $k = 5$.

Here, a possible way of obtaining better results would be to use a supercomputer and/or the power of parallel computing for calculations of spectral gaps. Another way would be to find a ‘better’ basis in which our operator $X$ takes a diagonal form or at least a block diagonal form. We leave these tasks open.

Finally, we would like to point out one problem which should be of some interest. Is it possible to approximate values of spectral gaps by some function with dependence on
parameters \( k \) and \( t \)? Based on the numerics, the function \( (a(t) - \frac{\hbar c}{2})^{-1} \) looks to be a promising candidate.

Also, two interesting questions relating to the structure of \( t \)-designs, namely, why all spectral gaps for \( t = 2 \) and \( t = 3 \) are the same and why for \( t = 4 \) the circuit is shorter than for \( t = 2, 3 \), remain without answer.

Acknowledgments

We wish to thank Fernando G S L Brandão for discussions. PČ acknowledges helpful discussions with Norbert Schuch. MS is supported by the International PhD Project ‘Physics of future quantum-based information technologies’, grant MPD/2009-3/4 from the Foundation for Polish Science. The work is also supported by the Polish Ministry of Science and Higher Education grant no. IdP2011 000361. Part of this work was done at the National Quantum Information Centre of Gdańsk.

Appendix A. Orthogonalization of representation operators of finite groups

In this section we briefly recall some properties of the algebra generated by a given complex finite-dimensional representation of the finite group \( G \).

The content of this section can be found in standard books on representation theory of finite groups and algebras, for example, in [37, 38].

Any complex finite-dimensional representation \( D : G \rightarrow \text{Hom}(V) \) of the finite group \( G \), where \( V \) is a complex linear space, generates an algebra \( A_V[G] \subset \text{Hom}(V) \) which is isomorphic to the group algebra \( \mathbb{C}[G] \) if the representation \( D \) is faithful. Obviously

\[
A_V[G] = \text{span}_\mathbb{C}\{D(g), \ g \in G\}. 
\tag{A.1}
\]

If the operators \( D(g) \) are linearly independent, then they form a basis of the algebra \( A_V[G] \) and \( \dim A_V[G] = |G| \). It is also possible, using matrix irreducible representations, to construct a new basis which has remarkable properties, which is very useful in applications of representation theory. Below we describe this construction.

Notation 9. Let \( G \) be a finite group of order \( |G| = n \) which has \( r \) classes of conjugated elements. Then \( G \) has exactly \( r \) inequivalent, irreducible representations, in particular \( r \) inequivalent, irreducible matrix representations. Let

\[
D^\alpha : G \rightarrow \text{Hom}(V^\alpha), \quad \alpha = 1, 2, \ldots, r, \quad \dim V^\alpha = d_\alpha
\tag{A.2}
\]

be all inequivalent, irreducible representations of \( G \) and let us choose these representations to be all unitary (always possible) i.e.

\[
D^\alpha (g) = (D^\alpha_{ij}(g)), \quad \text{and} \quad (D^\alpha_{ij}(g))^{-1} = (D^\alpha_{ij}(g))^{-1},
\tag{A.3}
\]

where \( i, j = 1, 2, \ldots, d_\alpha \).

The matrix elements \( D^\alpha_{ij}(g) \) will play a crucial role in the following.

Definition 10. Let \( D : G \rightarrow \text{Hom}(V) \) be an unitary representation of a finite group \( G \) such that the operators \( D(g), \ g \in G \) are linearly independent i.e. \( \dim A_V[G] = |G| \) and let \( D^\alpha : G \rightarrow \text{Hom}(V^\alpha) \) be all inequivalent, irreducible representations of \( G \) as described in notation 9 above. Define

\[
E_{ij}^\alpha = \frac{d_\alpha}{n} \sum_{g \in G} D^\alpha_{ij} (g^{-1}) D(g),
\tag{A.4}
\]

where \( \alpha = 1, 2, \ldots, r, \ i, j = 1, 2, \ldots, d_\alpha \), \( E_{ij}^\alpha \in A_V[G] \subset \text{Hom}(V) \).
The operators have noticeable properties listed in the following.

**Theorem 11.**

(I) There are exactly $|G| = n$ nonzero operators $E_{ij}^a$ and

$$D(g) = \sum_{ij\alpha} D_{ij}^\alpha (g) E_{ij}^a$$  \hspace{1cm} (A.5)

(II) the operators $E_{ij}^a$ are orthogonal with respect to the Hilbert–Schmidt scalar product in the space $\text{Hom}(V)$.

$$\langle E_{ij}^a, E_{kl}^b \rangle = \text{Tr} \left( \left( E_{ij}^a \right)^\dagger E_{kl}^b \right) = k_a \delta^{ab} \delta_{jk} \delta_{il}$$  \hspace{1cm} (A.6)

where $k_a$ is equal to the multiplicity of the irreducible representation $D^a$ in $D$ and does not depend on $i, j = 1, 2, \ldots, d_a$

(III) the operators $E_{ij}^a$ satisfy the following composition rule

$$E_{ij}^a E_{kl}^b = \delta^{ab} \delta_{jk} E_{il}^a$$ \hspace{1cm} (A.7)

in particular $E_{ii}^a$ are orthogonal projections.

**Remark 12.** From point (II) of the theorem it follows that the equations

$$E_{ij}^a = \frac{d_a}{n} \sum_{g \in G} D_{ij}^\alpha (g^{-1}) D(g)$$ \hspace{1cm} (A.8)

describe the transformation of orthogonalization of operators $D(g), \ g \in G$ in the space $\text{Hom}(V)$ with the Hilbert–Schmidt scalar product.

**Remark 13.** We can look at operators $E_{ij}^a$ as vectors in $\mathbb{C}^n$, then they are orthonormal (with a coefficient $\sqrt{\frac{1}{d_a}}$) with respect to the usual scalar product in $\mathbb{C}$. So in fact we have double orthogonality.

The operators $E_{ij}^a$ are not only orthogonal projections onto their proper subspaces in $V$ but they are also orthogonal with respect to the Hilbert–Schmidt scalar product in the space $\text{Hom}(V)$.

The basis $\{E_{ij}^a\}$ plays an essential role when $D : G \to \mathbb{C}[G]$ is the regular representation. In this case the properties of the basis $\{E_{ij}^a\}$ express the well-known fact that the group algebra $\mathbb{C}[G]$ is a direct sum of simple matrix algebras generated by the irreducible representations of the group $G$. It is always possible to construct the operators $E_{ij}^a$ even if the operators $D(g)$ are not linearly independent, but in this case some of them will be zero.

From theorem 11 it follows directly that

**Corollary 14.**

$$E_{ij}^{(12)} = \frac{d_g}{n} \sum_{g \in G} D_{ii}^\alpha (g^{-1}) D(g) \otimes D(g)$$

$$= \sum_{\alpha, \beta} \sum_{kl} \sum_{mn} \left( \frac{d_g}{n} \sum_{g \in G} D_{ik}^\alpha (g^{-1}) D_{kk}^\beta (g) \right) \left( \frac{d_g}{n} \sum_{g \in G} D_{mm}^\beta (g^{-1}) D_{nn}^\alpha (g) \right) E_{kl}^\alpha \otimes E_{mn}^\beta$$ \hspace{1cm} (A.9)

thus the coefficients on rhs are expressed only by the matrix elements of irreducible representations.
Appendix B. The largest eigenvalue of $G_{\mu,t}$

Let us once more recall the fact present in theorem 3 (after a slight modification).

**Fact 15.** We have

$$\|G_{\mu^*,t} - G_{\mu,t}\|_\infty = \lambda_2^1,$$

where $\lambda_2$ is the second largest eigenvalue of $G_{\mu,t}$. Moreover, the largest eigenvalue $\lambda_1$ of $G_{\mu,t}$ is equal to 1, and the corresponding eigenprojector is equal to $G_{\mu,t}$.

Now, we will prove that the largest eigenvalue of $G_{\mu,t}$ is equal to 1.

**Proof.** We know that $G_{\mu,t}$ is an operator such that $0 \leq G_{\mu,t} \leq I$. Bearing this in mind, let us eigen-decompose the operator $G_{\mu,t}$ in some basis such as

$$G_{\mu,t} = \frac{1}{n} \sum_{i=1}^{n} P_{i} \otimes v_{w} Q_{w},$$

where $v_{w}$ are eigenvalues, so they follow the constraint $0 \leq v_{w} \leq 1$, and $Q_{w}$ are the corresponding eigenvectors. Now, let us extend equation (B.2) to $l$ walks in the random walk:

$$G_{\mu^*,t} = \left( \sum_{w} v_{w} Q_{w} \right)^{l} = \sum_{w} v_{w}^{l} Q_{w},$$

since $Q_{w}$ are projectors. We also have the following:

$$\lim_{l \to \infty} G_{\mu^*,t} = G_{\mu,t}.$$  

Then, it is easy to observe that the correspondence is valid only when $v_{w} = 1$ and the eigenprojector $Q_{w}$ is equal to $G_{\mu,t}$.

□

Appendix C. Superoperators and operators

Here, we explore some connections between superoperators and operators. For a superoperator $\mathcal{G}$ given by

$$\mathcal{G}(X) = \sum_{k} A_{k} X B_{k}^{\dagger},$$

where $\dagger$ denotes the Hermitian conjugate, we define the operator

$$G = \sum_{k} A_{k} \otimes B_{k}^{*},$$

with $\star$ being the complex conjugate.

Let $X$ be a normalized operator, such that $\text{tr}(XX^\dagger) = 1$. What is more, assume that $\mathcal{G}(X) = \lambda X$, for a complex eigenvalue $\lambda$, i.e., $X$ is an eigenoperator of $\mathcal{G}$ with eigenvalue $\lambda$. Then, defining $|X\rangle = X \otimes |\phi\rangle$, with

$$|\phi\rangle = \sum_{k} |k\rangle \otimes |k\rangle,$$

it holds that $G|X\rangle = \lambda |X\rangle$, i.e., $|X\rangle$ is an eigenvector of $G$ with eigenvalue $\lambda$.

A direct implication of this correspondence is that

**Fact 16.**

$$||G||_{2 \to 2} = ||G||_{\infty},$$

where the norm $2 \to 2$ is defined as in definition 2.
Proof. Using equations (C.1) and (C.2) we have that
\[ ||\Lambda (X)||_{2\to 2}^2 = \sup ||\Lambda (X)||_2^2 \] (C.5)
Decomposing \( X = \sum_k c_k X_k \), \( \Lambda (X_k) = \lambda_k X_k \) and noting that \( \sum_k |c_k|^2 = 1 \),
\[ ||\Lambda||_{2\to 2}^2 = \sup \sum_k |c_k|^2 |\lambda_k|^2 X_k^2 = \lambda_{max}^2 \] (C.6)
Recalling the definition of the norm \( ||.||_\infty \), one can observe that equation (C.6) proves fact 16. □

References

[1] Abeyesinghe A, Devetak I, Hayden P and Winter A 2009 Proc. R. Soc. A 465 2537
[2] Hayden P, Leung D, Shor P and Winter A 2004 Commun. Math. Phys. 250 371
[3] Emerson J, Alicki R and Życzkowski K 2005 J. Opt. B: Quantum Semiclass. Opt. 7 S347 (arXiv:quant-ph/0503243)
[4] Radhakrishnan J, Rötteler M and Sen P 2009 Algorithmica 55 490 (arXiv:quant-ph/0512085)
[5] Brandão F G S L, Ćwikliński P, Horodecki M, Horodecki P, Korbicz J K and Mozrzymas M 2012 Phys. Rev. E 86 031101
[6] Masanes L, Roncaglia A J and Acín A 2013 Phys. Rev. E 87 032137 (arXiv:1108.0374)
[7] Vinayak and Znidaric M 2012 J. Phys. A: Math. Theor. 45 125204 (arXiv:1107.6035)
[8] Cramer M 2012 New J. Phys. 14 053051 (arXiv:1112.5295)
[9] Garnerone S, de Oliveira T R, Haas S and Zanardi P 2010 Phys. Rev. A 82 052312
[10] Dankert C, Cleve R, Emerson J and Livine E 2009 Phys. Rev. A 90 012304
[11] Gross D, Audenaert K and Eisert J 2007 J. Math. Phys. 48 052104
[12] Emerson J, Livine E and Lloyd S 2005 Phys. Rev. A 72 060302
[13] Oliveira R, Dahlsten O C O and Plenio M B 2007 Phys. Rev. Lett. 98 130502
[14] Dahlsten O C O, Oliveira R and Plenio M B 2007 J. Math. Phys. 40 8081
[15] Harrow A W and Low R A 2009 Commun. Math. Phys. 291 275
[16] Diniz I and Jonathan D 2011 Commun. Math. Phys. 304 281
[17] Arnaud L and Braun D 2008 Phys. Rev. A 78 062329
[18] Znidaric M 2008 Phys. Rev. A 78 032324
[19] Roy A and Scott A J 2009 Designs, Codes Cryptogr. 53 13
[20] Brown W and Viola L 2010 Phys. Rev. Lett. 104 250501
[21] Brandão F G S L and Horodecki M 2013 Q. Inf. Comput. 13 0901 (arXiv:1010.3654)
[22] Hayden P and Preskill J 2007 J. High Energy Phys. JHEP09(2007)120
[23] Harrow A and Low R 2009 Proc. Random 5687 548
[24] Emerson J, Weinstein Y S, Saraceno M and Lloyd S 2003 Science 302 2098
[25] Low R 2009 Proc. R. Soc. A 465 3289
[26] Nakata Y and Murao M 2012 Diagonal-unitary t-designs and their constructions arXiv:1206.4451
[27] Nakata Y, Turner P S and Murao M 2012 Phys. Rev. A 86 012301 (arXiv:1111.2747)
[28] DiVincenzo D, Leung D and Terhal B 2002 IEEE Trans. Inform. Theory 48 580
[29] Brandão F G S L, Harrow A and Horodecki M 2012 Local random quantum circuits are approximate polynomial-designs arXiv:1208.0692
[30] Schwarz M, Temme K and Verstraete F 2012 Phys. Rev. Lett. 108 110502
[31] Hastings M B 2007 J. Stat. Mech. 2007 P08024
[32] Nachtergaele B and Sims R 2006 Commun. Math. Phys. 265 119
[33] Knabe S 1988 J. Stat. Phys. 52 627
[34] Low R A 2010 PhD Thesis University of Bristol
[35] Weyl H 1939 The Classical Groups. Their Invariants and Representations (Princeton, NJ: Princeton University Press)
[36] Boerner H 1970 Representations of Groups (Amsterdam: North-Holland)
[37] Curtis C W and Reiner I 1988 Representation Theory of Finite Groups and Associative Algebras (New York: Wiley)
[38] Littlewood D E 2006 The Theory of Group Characters and Matrix Representations of Groups (Providence, RI: AMS Chelsea Publishing)