On Unitary t-Designs from Relaxed Seeds

entropy

MDPI

Article

On Unitary t-Designs from Relaxed Seeds

Rawad Mezher [1,2,*], Joe Ghalbouni [2], Joseph Dgheim [2] and Damian Markham [1,*]

[1] Laboratoire d 'Informatique de Paris 6, CNRS, Sorbonne Université, 4 Place Jussieu, 75252 Paris CEDEX 05, France
[2] Laboratoire de Physique Appliquée, Faculty of Sciences 2, Lebanese University, Fanar 90656, Lebanon; joe.ghalbouni@ul.edu.lb (J.G.); jdgheim@ul.edu.lb (J.D.)
* Correspondence: rawad.mezher@lip6.fr (R.M.); damian.markham@lip6.fr (D.M.)

Received: 9 November 2019; Accepted: 9 January 2020; Published: 12 January 2020

Abstract: The capacity to randomly pick a unitary across the whole unitary group is a powerful tool across physics and quantum information. A unitary t-design is designed to tackle this challenge in an efficient way, yet constructions to date rely on heavy constraints. In particular, they are composed of ensembles of unitaries which, for technical reasons, must contain inverses and whose entries are algebraic. In this work, we reduce the requirements for generating an ε-approximate unitary t-design. To do so, we first construct a specific n-qubit random quantum circuit composed of a sequence of randomly chosen 2-qubit gates, chosen from a set of unitaries which is approximately universal on $U(4)$, yet need not contain unitaries and their inverses nor are in general composed of unitaries whose entries are algebraic; dubbed *relaxed* seed. We then show that this relaxed seed, when used as a basis for our construction, gives rise to an ε-approximate unitary t-design efficiently, where the depth of our random circuit scales as $poly(n, t, log(1/\varepsilon))$, thereby overcoming the two requirements which limited previous constructions. We suspect the result found here is not optimal and can be improved; particularly because the number of gates in the relaxed seeds introduced here grows with n and t. We conjecture that constant sized seeds such as those which are usually present in the literature are sufficient.

Keywords: unitary t-design; *relaxed* seeds; approximately universal

1. Introduction and Summary of the Results

1.1. Unitary t-Designs

A unitary t-design is an ensemble of unitaries, which, when sampled, mimic sampling from the 'truly random' Haar measure which chooses a unitary at random from the full continuous unitary group [1]. The usefulness of a t-design is that it is much simpler and more efficient to produce than sampling from the Haar measure (polynomial compared to exponential cost, respectively, [2] and [3]), yet it retains many of the useful applications. These include, but are not limited to, randomized benchmarking [4], estimating noise [5], private channels [6], photonics [7], quantum metrology [8], modeling thermalization [9], black hole physics [10], and recently demonstrations of quantum computational advantage [11–13].

More precisely, one can distinguish between two types of unitary t-designs, exact unitary t-designs and approximate unitary t-designs [14]. An exact unitary t-design on the n-qubit unitary group $U(2^n)$ is a set of couples (we will refer to this set of couples frequently as a random unitary

ensemble) $\{p_i, U_i\}_{i=1,...D}$, where D is a positive integer and each $U_i \in U(2^n)$ is chosen with probability p_i ($\sum_{i=1,..,D} p_i = 1$). An exact unitary t-design satisfies

$$\sum_i p_i P_{(t,t)}(U_i) = \int_{U(2^n)} P_{(t,t)}(U)\mu_H(dU), \tag{1}$$

where μ_H denotes the Haar measure on the n-qubit unitary group $U(2^n)$, and $P_{(t,t)}(U)$ is *any* polynomial of degree exactly t in the matrix elements of U, and of degree exactly t in the complex conjugates of these matrix elements. It can be shown that an exact unitary t-design is also an exact unitary $t-1$ design [15] (Note that this property also holds for approximate t-designs). Although exact unitary t-designs exist for any t and any dimension of the unitary group [16], the search for exact unitary t-designs on $U(d)$ when $t > 3$ and $d \geq 3$ appears to be a highly nontrivial task [17]. Therefore, a natural step further is to consider a relaxation of the 'exact' requirement and replace it with an 'approximate' version, a so-called ε-approximate unitary t-design [2,14].More explicitly, the definition of ε-approximate unitary t-design (or ε-approximate t-design for simplicity) is as follows.

Definition 1. *[2] Let $\mathcal{H}$ be the n-qubit Hilbert space $(\mathbb{C}^2)^{\otimes n}$. A random unitary ensemble $\{p_i, U_i\}$ with $U_i \in U(2^n)$ is said to be an ε-approximate t-design if the following holds:*

$$(1-\varepsilon)\int_{U(2^n)} U^{\otimes t}\rho U^{\dagger\otimes t}\mu_H(dU) \leq \sum_i p_i U_i^{\otimes t}\rho U_i^{\dagger\otimes t} \leq (1+\varepsilon)\int_{U(2^n)} U^{\otimes t}\rho U^{\dagger\otimes t}\mu_H(dU) \tag{2}$$

for all $\rho \in B(\mathcal{H}^{\otimes t})$, where μ_H denotes the Haar measure on $U(2^n)$. For positive semidefinite matrices A and B, $B \leq A$ means $A - B$ is positive semidefinite, ε is a positive real, and t is a positive integer (This definition is referred to as the strong definition of an ε-approximate t-design. Other definitions of ε-approximate t-designs exist, which are dependent on the application in mind, see for example [18] for an overview of these definitions.).

Note that when $\varepsilon = 0$, one recovers a definition of an exact unitary t-design which is equivalent to the definition in Equation (1) [19]. Moreover, most of the applications of exact unitary t-designs can be adapted to use ε-approximate unitary t-designs, while retaining their efficiency [5,6,8,9,11,13,14]. Finally, efficient explicit constructions of ε-approximate unitary t-designs for any t are well-established both in the circuit model [2,20] as well the measurement-based model of quantum computing [11,21,22]. For these reasons, in this work, we will focus on ε-approximate t-designs.

Due to the broad applications of unitary t-designs, one is interested in finding more efficient, and in other ways 'better', ε-approximate t-designs—for example, limiting the unitary set according to the proposed use or implementation [21]. A limiting factor in doing so is the rigid proof structure that generally follows the proof of an ε-approximate t-design. It is thus of high interest to be able to reduce the technical requirements involved in such a proof, which is the main topic of this work. Indeed, such technical breakthroughs will likely have application beyond t-designs.

1.2. Comparison with Previous Work

In the seminal work of [2], it was shown that $n-$qubit random quantum circuits composed of layers of nearest neighbor unitaries $U \in U(4)$ drawn uniformly at random from a seed $\mathcal{U}_\mathcal{B} \subset U(4)$ (As mentioned in the abstract, a finite set of unitaries which is approximately universal in $U(4)$ will be referred to as a seed.), sampled from an ε-approximate unitary t-design [14] efficiently in $poly(n, t, log(\frac{1}{\varepsilon}))$ depth. However, their proof relied on the following properties of the seed:

- Requirement (i): every $U \in \mathcal{U}_\mathcal{B}$ has an inverse $U^\dagger \in \mathcal{U}_\mathcal{B}$.
- Requirement (ii): the unitaries $U \in \mathcal{U}_\mathcal{B}$ are composed entirely of algebraic entries.

The authors [2] also conjectured that the algebraic entry requirement is a technical issue (due mostly to using a result of [23]), and therefore could be dropped. Later on, in [11], it was shown that these requirements can be reduced to seeds $\mathcal{U}_{\mathcal{B}}$ composed partially of a seed $\mathcal{U}_{\mathcal{M}}$ made up of unitaries with algebraic entries and inverses in $\mathcal{U}_{\mathcal{M}}$; and its complement in $\mathcal{U}_{\mathcal{B}}$, denoted as $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$, which need not necessarily contain unitaries and their inverses nor be composed of algebraic entries (see also [12,20]).

In this work, we completely remove the requirements (i) and (ii) by giving examples of seeds in which every unitary in these seeds does not in general have an inverse in these seeds, nor are the unitaries in these seeds composed of algebraic entries in general, and yet converge efficiently to ε-approximate t-designs in a particular random circuit model which we will define explicitly below, thereby proving the conjecture proposed in [2]. We will refer to these seeds as relaxed throughout this work. However, it is to be noted that we do not mean relaxed in the sense that the unitaries making up these seeds are chosen from the Haar measure on $U(4)$. Indeed, because our proofs are based on the partially invertible universal sets of [11], this endows the unitaries composing the relaxed seeds with some structure which makes them different from Haar distributed unitaries.

1.3. Main Results

The notation we will use here is the same as that in [11], but we will restate it here for the sake of using it in our proofs.

The seed $\mathcal{U}_{\mathcal{B}} \in U(4)$ is a *partially invertible universal* set composed of a seed $\mathcal{U}_{\mathcal{M}}$, which contains unitaries and their inverses, and is composed of unitaries with algebraic entries; and its complement, the seed $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$, which is not in general composed of unitaries and inverses, nor unitaries with algebraic entries. Define the random unitary ensemble

$$B = \{\frac{1}{|\mathcal{U}_{\mathcal{B}}|}, U_i \in \mathcal{U}_{\mathcal{B}}\}. \tag{3}$$

Denote the k-fold concatenation of B by

$$B^k = \{\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|}, \prod_{j=1,...k} U_{\pi(j)} \in \mathcal{U}_{\mathcal{B}^k}\}, \tag{4}$$

where $U_{\pi(j)} \in \mathcal{U}_{\mathcal{B}}$, π is a function acting on $\{1,...,k\}$ resulting in a set $\{\pi(1),...\pi(k)\}$, where $\pi(j) \in \{1,...,|\mathcal{U}_{\mathcal{B}}|\}$, the $\pi(j)'s$ can be identical. There are $|\mathcal{U}_{\mathcal{B}}|^k$ such functions π and the k-fold concatenation includes all of them. $\mathcal{U}_{\mathcal{B}^k}$ is the set of all unitaries of the form $\prod_{j=1,...k} U_{\pi(j)}$, with $|\mathcal{U}_{\mathcal{B}^k}| = |\mathcal{U}_{\mathcal{B}}|^k$. Define (This definition of $block(B^k)$ is for even n, the odd n case follows straightforwardly.)

$$block(B^k) = \{\tfrac{1}{|\mathcal{U}_{\mathcal{B}^k}|^{n-1}}, (1_{2\times 2} \otimes U_{2,3}^{j_1} \otimes U_{4,5}^{j_2} \otimes ... \otimes U_{n-2,n-1}^{j_{\frac{n}{2}-1}} \otimes 1_{2\times 2})(U_{1,2}^{j_{\frac{n}{2}}} \otimes U_{3,4}^{j_{\frac{n}{2}+1}} \otimes ... \otimes U_{n-1,n}^{j_{n-1}}) \in \mathcal{U}_{block(\mathcal{B}^k)}\}, \tag{5}$$

where $U_{i,i+1}^{j} \in \mathcal{U}_{\mathcal{B}^k}$, $i \in \{1,...,n-1\}$ and $j \in \{1,...,|\mathcal{U}_{\mathcal{B}^k}|\}$. Let $block^L(B^k)$ be the L-fold concatenation of $block(B^k)$, defined as

$$block^L(B^k) = \{\frac{1}{|\mathcal{U}_{\mathcal{B}^k}|^{(n-1)L}}, \prod_{j=1,...,L} U_{\pi(j)} \in \mathcal{U}_{block^L(\mathcal{B}^k)}\}, \tag{6}$$

where π is also as defined previously and $U_{\pi(j)} \in \mathcal{U}_{block(\mathcal{B}^k)}$. Finally, let

$$a = \frac{|\mathcal{U}_{\mathcal{M}}|}{|\mathcal{U}_{\mathcal{B}}|}. \tag{7}$$

The following theorem (Theorem 1), which holds for the above defined partially invertible universal set $\mathcal{U}_{\mathcal{B}}$, was one of the main results of [11], saying basically that one can obtain efficient approximate unitary t-designs efficiently from partially invertible universal sets in $poly(n, t, log(\frac{1}{\varepsilon'}), log(\frac{1}{\varepsilon_d})) = O(n^3 t^{12} + log(\frac{1}{\varepsilon'})log(\frac{1}{\varepsilon_d}))$.

Theorem 1. *[11] For any $0 < \varepsilon_d < 1$, and for some $0 < C < 1$, if*

$$k \geq \frac{1}{log_2(\frac{1}{1+(C-1)a})}(10t + n^2 t - nt + n + log_2(\frac{1}{\varepsilon'})) \tag{8}$$

and

$$L \geq \frac{1}{log_2(\frac{1}{\varepsilon' + P(t)})}(4nt + log_2(\frac{1}{\varepsilon_d})), \tag{9}$$

where

$$P(t) = (1 + \frac{(425\lfloor log_2(4t)\rfloor^2 t^5 t^{3.1/log(2)})^{-1}}{2})^{-1/3}, \tag{10}$$

$\varepsilon' < 1 - P(t)$, and $n \geq \lfloor 2.5 log_2(4t)\rfloor$, then $block^L(B^k)$, formed from partially invertible universal set $\mathcal{U}_{\mathcal{B}}$, is an ε_d- approximate t-design on $U(2^n)$, for any t.

Here, $\lfloor . \rfloor$ denotes the floor function. Define

$$\mathcal{U}^k = \mathcal{U}_{\mathcal{B}^k} - \mathcal{U}_{\mathcal{M}^k} \tag{11}$$

to be the seed consisting of unitaries of the form

$$U = U_1 .... U_k,$$

where for all $j \in \{1, ..., k\}$, $U_j \in \mathcal{U}_{\mathcal{B}}$, and such that $\exists\ l \in \{1, .., k\}$ and $U_l \in \mathcal{U}_{\mathcal{B}/\mathcal{M}}$. k is as defined in Equation (8) in Theorem (1). $\mathcal{U}^k$ in Equation (11) is the relaxed seed we will consider in this work.

We will first show that, in general, $\mathcal{U}^k$ truly is relaxed by proving the following theorem, which is the first main result of this work.

Theorem 2. *For a given value of k, there is a choice of the seed $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$ such that $\mathcal{U}^k$ does not verify requirement (ii) and completely violates requirement (i) .*

What is meant by *completely violates* requirement (i) is that, for a choice of $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$, every unitary in $\mathcal{U}^k$ does not have an inverse in $\mathcal{U}^k$. Then, as promised, we will show that a particular random quantum circuit with seed $\mathcal{U}^k$ converges to an ε-approximate t-design efficiently in $O(nt + log(\frac{1}{\varepsilon}))$ depth. But first, define the random unitary ensemble

$$B_1 = \{\frac{1}{|\mathcal{U}^k|}, \mathcal{U}^k\}. \tag{12}$$

It is straightforward to see that

$$|\mathcal{U}^k| = (1 - a^k)|\mathcal{U}_{\mathcal{B}^k}|, \tag{13}$$

since

$$|\mathcal{U}_{\mathcal{M}^k}| = a^k |\mathcal{U}_{\mathcal{B}^k}|, \tag{14}$$

and by looking at Equation (11). $\mathcal{U}_{\mathcal{M}^k}$ is the set formed of unitaries of the form

$$W = W_1 .... W_k, \tag{15}$$

where $W_i \in \mathcal{U}_{\mathcal{M}}, \forall\, i \in \{1, ..., k\}$, and k is as defined in Equation (8). The random quantum circuits considered will be random unitaries in $block^L(B_1)$ defined for the random unitary ensemble B_1 (Equation (12)) in the exact same way as $block^L(B^k)$ in Equation (6) is defined for the random unitary ensemble B^k in Equation (4), and for the exact value of k as in Equation (8). We will show that $block^L(B_1)$ is an ε-approximate t-design, first by showing that $block(B_1)$ (This is defined for B_1 of Equation (12), in the exact same way as $block(B^k)$ of Equation (5) is defined for the random unitary ensemble B^k in Equation (4)) is an $(\eta < 1, t)$-tensor product expander (TPE) [24,25], which is defined as follows:

Definition 2. *[24,25] A random unitary ensemble $\{p_i, U_i \in \mathcal{U}\}$ is said to be an (η, t)-TPE if the following holds,*

$$||M_t[\mu] - M_t[\mu_H]||_\infty \leq \eta < 1, \tag{16}$$

where $M_t[\mu_H] = \int_{U(2^n)} U^{\otimes t,t} \mu_H(dU)$, $M_t[\mu] = \sum_i p_i U_i^{\otimes t,t}$, where μ is the probability measure (As shown in [26] one can shift between a probability distribution over a discrete ensemble $\{p_i, U_i\}$ and a continuous distribution by defining the measure $\mu = \sum_i p_i \delta_{U_i}$.) over the set $\mathcal{U}$, which results in choosing $U_i \in \mathcal{U}$ with probability p_i, $U^{\otimes t,t} = U^{\otimes t} \otimes U^{*\otimes t}$, and U^* is the complex conjugate of U. $M_t[\mu_H]$ and $M_t[\mu]$ are called moment superoperators.

Then, we will use the following proposition [20] to translate our TPE result into a result about t-designs

Proposition 1. *[11,20] If $\{p_i, U_i \in \mathcal{U}\}$ is an $(\eta < 1, t)$-TPE [24,25], then the L-fold concatenation of $\{p_i, U_i\}$: $\{\prod_{j=1,...,L} p_{\pi(j)}, \prod_{j=1,...,L} U_{\pi(j)}\}$ is an ε-approximate t-design in the strong sense (Definition 1) when*

$$L \geq \frac{1}{log_2(\frac{1}{\eta})}(4nt + log_2(\frac{1}{\varepsilon})). \tag{17}$$

π is as defined previously in Equation (4).

We now state the three theorems which establish that relaxed seeds can give rise to efficient approximate t designs—and are the second, third, and fourth main results of this work.

Theorem 3. *$block(B_1)$ is an $(\eta, t) - TPE$ with*

$$\eta = \frac{P(t) + \varepsilon^{'}}{(1 - a^k)^{n-1}} + \frac{1 - (1 - a^k)^{n-1}}{(1 - a^k)^{n-1}}. \tag{18}$$

Theorem (3) holds, as Theorem (1), when $n \geq \lfloor 2.5 log_2(4t) \rfloor$ and $P(t)$, $\varepsilon^{'}$, and k, are exactly as defined in Theorem (1). a is as defined in Equation (7).

Theorem 4. *$\forall\, t, \exists\, n_0 \geq \lfloor 2.5 log_2(4t) \rfloor$ such that $\forall\, n \geq n_0$,*

$$\frac{P(t) + \varepsilon^{'}}{(1 - a^k)^{n-1}} + \frac{1 - (1 - a^k)^{n-1}}{(1 - a^k)^{n-1}} \leq 1. \tag{19}$$

Theorem 5. *$\forall\, t, \exists\, n_0 \geq \lfloor 2.5 log_2(4t) \rfloor$ such that $\forall\, n \geq n_0$, $block^L(B_1)$ is an ε-approximate t-design in $U(2^n)$ in the strong sense, with L given by Equation (17), and η given by Equation (18).*

Note that Theorem (5) means, as Theorem (1), that one can obtain efficient approximate t-designs efficiently from relaxed seeds $\mathcal{U}^k$.

The intuition behind why Theorems (3)–(5) are true is quite straightforward. $block(B^k)$ was shown in [11] to be an $(\eta \leq 1, t)$-TPE [24,25]. An overwhelmingly large fraction of random unitaries (tending to one in the $n, t \to \infty$ limit, see Equation (13)) in $block(B^k)$ are also contained in $block(B_1)$. Therefore, one should expect $block(B_1)$ to be an $(\eta \leq 1, t)$-TPE.

As a final remark in this section, note that Equations (13) and (8) tell us that the number of unitaries in the relaxed seed $\mathcal{U}^k$ (Equation (11)) grows with n and t. This technical issue is due to us using the results on *partially invertible universal* sets [11] in our proofs. This is in contrast with the seeds used in [2] and [11] where these seeds were finite and were composed of a *constant* number of elements. We believe the results presented here are not optimal, and that finite *constant*-sized sets not verifying requirement (ii) and completely violating requirement (i) are sufficient to give approximate unitary t-designs in a random quantum circuit model efficiently in $poly(n, t)$ depth.

1.4. Example: Implementation of Our Construction as a Random Quantum Circuit

In the previous subsection, we presented the main results of this work, Theorems (2)–(5), which show a mathematical construction of an ε-approximate unitary t-design, $block^L(B_1)$, from relaxed seeds. In practice, one can design a random quantum circuit which samples from this ε-approximate unitary t-design. An example of such a construction sampling from $block^L(B_1)$ is shown in Figure 1. This construction is similar to the random circuit construction in [11]. In this example, L is the depth of this circuit, whereas k controls the number of elements of the relaxed seed, which depends on the number of inputs n of the circuit as well as the order t of the design. One could also think of a translation to a measurement-based version of this random quantum circuit along the lines of work done in [11].

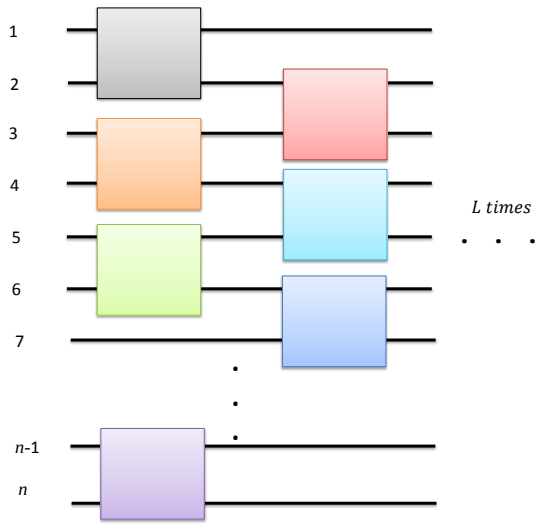

Figure 1. Part of the random quantum circuit sampling from the random unitary ensemble $block^L(B_1)$. The horizontal black lines numbered from 1 to n represent the n input qubits of the random quantum circuit. The colored boxes touching two horizontal lines each represent a two-qubit unitary which is chosen with uniform probability from $\mathcal{U}^k$ (Equation (11)). These two-qubit unitaries act nontrivially only on the horizontal lines (qubits) they touch. The order in which these unitaries are applied is from left to right. Unitaries (boxes) aligned on the same vertical level are applied simultaneously (depth-one). The depth-two unitary shown in this figure is sampled from $block(B_1)$. In order to sample from $block^L(B_1)$, the ε-approximate t-design, the random circuit shown in this figure is repeated L times, with L given by Equation (17) (see also Theorem (5)). This figure is for n-even, the odd n case follows straightforwardly.

An important point to consider is the dependence of the circuit depth of our random circuit construction on the figure of merit a, defined in Equation (7). For fixed t and n, the value of η (Equation (18)) increases as a increases, meaning that the depth L of our construction increases with increasing a, from Equation (17). However, for large values of t or n, $(1-a^k)^{n-1}$ approaches unity, meaning that η scales asymptotically (for large t or n) as $\eta \sim P(t) + \varepsilon^{'}$ (see Equation (18)). Therefore, in the limit of large t and n, the depth L of our random circuit construction is practically independent of a. (Although the value of k in Equation (8), which determines the cardinality of $\mathcal{U}^k$, will still depend on a, but only up to a constant factor (see Equation (8)).) The extremal values of a (i.e., $a = 0$ and $a = 1$) are not applicable to our construction since, when $a = 0$, the lower bound on k (Equation (8)) is not defined, whereas when $a = 1$, $block(B_1)$ is the empty set. However, it should be noted that when $a = 1$, Theorem (1) of [11], which is the basis of the construction in this work, gives a lower bound which is in line with the lower bound on the circuit depth of the construction of approximate t-designs in [2] (see Theorem (1)). (The lower bound of Theorem (1) however is not as tight as that shown in [2], where the dependence on n in their result is linear, whereas that in Theorem (1) is cubic. Indeed, one of the open questions in [11] was whether this cubic lower bound on n could be reduced to a linear lower bound, which is the best one can hope to achieve for 1D random quantum circuits [2,18].)

In the next section, we present the proofs of Theorems (2)–(5).

2. Proofs

2.1. Proof of Theorem (2)

Proving requirement (ii) which is not verified by $\mathcal{U}^k$ is straightforward. By our definition of the relaxed seed $\mathcal{U}^k$ (Equation (11)), any unitary $U \in \mathcal{U}^k$ can be written as a product of k unitaries in $\mathcal{U}_{\mathcal{B}}$ (with k defined in Equation (8)), $U = U_1 ... U_k$ with at least one $U_j \in \mathcal{U}_{\mathcal{B}/\mathcal{M}}$; and since in general $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$ contains unitaries with nonalgebraic entries, then the unitaries $U \in \mathcal{U}^k$ are in general composed of nonalgebraic entries. To see this more clearly, let k be odd, and consider for example

$$U = U_1 .... U_{\frac{k-1}{2}} . U_{\frac{k-1}{2}+1} ... U_{k-1} U_k \in \mathcal{U}^k,$$

where $U_{\frac{k-1}{2}+i} = U^{\dagger}_{\frac{k-1}{2}-i+1}$ for $i \in \{1, ..., \frac{k-1}{2}\}$ and $U_k \in \mathcal{U}_{\mathcal{B}/\mathcal{M}}$ is a unitary with nonalgebraic entries.

Then,

$$U = U_k \in \mathcal{U}^k,$$

and is thus composed of nonalgebraic entries.

We will now prove that (i) is completely violated in general by $\mathcal{U}^k$, this proof will be done by contradiction. Suppose, by contradiction, that $\forall$ choices of $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$ and for a fixed choice of $\mathcal{U}_{\mathcal{M}}$, $\exists\, U, U^{'} \in \mathcal{U}^k$ such that

$$U^{'} = U^{\dagger}. \tag{20}$$

Without loss of generality, we can write

$$U = \prod_{i=1,..,k} V_i^{m_i} W_i^{n_i}, \tag{21}$$

$$U^{'} = \prod_{j=k+1,..,2k} V_j^{m_j} W_j^{n_j}, \tag{22}$$

where $V_i, V_j \in \mathcal{U}_{\mathcal{B}/\mathcal{M}}$, and $W_i, W_j \in \mathcal{U}_{\mathcal{M}}$ for $i \in \{1, .., k\}$; and where $m_i, m_j, n_i, n_j \in \{0, 1\}$ with $n_i \neq m_i$ and $n_j \neq m_j$, $\forall\, i \in \{1, ...k\}$, $\forall\, j \in \{k+1, .., 2k\}$, and such that $\exists\, i_1 \in \{1, .., k\}$ and $j_1 \in \{k+1, .., 2k\}$ such that $m_{i_1} = m_{j_1} = 1$. Equations (20)–(22) imply

$$V_{j_1} = \prod_{j=j_1-1,...,k+1} W_j^{\dagger n_j} V_j^{\dagger m_j} \prod_{i=k,...,1} W_i^{\dagger n_i} V_i^{\dagger m_i} \prod_{j=2k,...,j_1+1} W_j^{\dagger n_j} V_j^{\dagger m_j}. \tag{23}$$

Now, we will prove that Equation (23) does not hold for a general choice of $\mathcal{U}_{\mathcal{B}/\mathcal{M}}$, thereby establishing a contradiction. We will consider all the possible cases as follows.

- **Case 1:** $V_j \neq V_{j_1}\ \forall\ j \neq j_1$ in Equation (23).
  Without loss of generality, let $\mathcal{U}_{\mathcal{M}} = \{W_1, ..., W_n\}$ and $\mathcal{U}_{\mathcal{B}/\mathcal{M}} = \{V_1, ..., V_m\}$, with $m, n \in \mathbb{N}$; and let $V_{j_1} = V_m$. Fix $\{W_1, ..., W_n, V_1, ..., V_{m-1}\}$, and list all the possible relations of the form of the right-hand side of Equation (23), where $W_j \in \{W_1, ..., W_n\}$, $\forall j \in \{k+1, .., 2k\}$, and $V_i, V_j \in \{V_1, ..., V_{m-1}\}$, $\forall i \in \{1, ..., k\}$, $\forall j \in \{k+1, ..., j_1 - 1, j_1 + 1, ...2k\}$. Since there are *countably* many relations of the form of the right-hand side of Equation (23) (and *uncountably* many choices of V_m.), choose $V_{j_1} = V_m$ such that it is not equal to any of the listed relations of the right-hand side of Equation (23). Therefore, Equation (23) does not hold in general in **Case 1**.
- **Case 2:** $\exists\ j \neq j_1$ such that $V_j = V_{j_1}$ in Equation (23).
  Here, it will be convenient to rewrite Equation (23) as

$$V_{j_1} = \prod_{i=1,...,2k-1} C_i^{\pi(i)} (V_{j_1}^{\dagger})^{1-\pi(i)}, \tag{24}$$

  where again we take that $V_{j_1} = V_m$, $C_i \in \{V_1^{\dagger}, ..., V_{m-1}^{\dagger}, W_1^{\dagger}, ..., W_n^{\dagger}\}$, and $\{V_1^{\dagger}, ..., V_{m-1}^{\dagger}, W_1^{\dagger}, ..., W_n^{\dagger}\}$ are fixed (as in **Case 1**). $\pi(.)$ is a map

$$i = \{1, ..., 2k-1\} \rightarrow \pi(i) \in \{0, 1\}.$$

  We consider the two following subcases
- **Case 2a:** $\pi(i) = 0, \forall i \in \{1, ..., 2k-1\}$.
  Equation (24) becomes, in this case,

$$V_{j_1} = (V_{j_1}^{\dagger})^{2k-1}. \tag{25}$$

  Equation (25) does not hold *exactly* for general choices of $V_{j_1} = V_m$, since products of the form of the right-hand side of Equation (25) can only *approximate* V_{j_1} up to a given precision in general [24].
- **Case 2b:** $\exists\ i_1$ such that $\pi(i_1) = 1$.
  Equation (24) can be rewritten in this case as

$$C_{i_1} = \prod_{i=i_1-1,...,1} V_{j_1}^{1-\pi(i)} C_i^{\dagger\pi(i)} V_{j_1} \prod_{i=2k,...,i_1+1} V_{j_1}^{1-\pi(i)} C_i^{\dagger\pi(i)}. \tag{26}$$

  Since $C_{i_1} \in \{V_1^{\dagger}, ..., V_{m-1}^{\dagger}, W_1^{\dagger}, ..., W_n^{\dagger}\}$, and these unitaries are fixed, Equation (26) therefore cannot hold for a general choice of $V_{j_1} = V_m$.
  In order to complete the proof of Theorem (2), we should show that a V_m exists which simultaneously violates the relations imposed in **Case 1** and **Case 2**. For a given fixed integer k and fixed $\{W_1, ..., W_n, V_1, ..., V_{m-1}\}$, there is only a finite number of unitaries V_m satisfying Equation (23) in **Case 1**. Unitaries V_m satisfying Equations (25) and (26) (**Case 2a** and **2b**) also satisfy the relation

$$det(C_{i_1} - \prod_{i=i_1-1,...,1} V_{j_1}^{1-\pi(i)} C_i^{\dagger\pi(i)} V_{j_1} \prod_{i=2k,...,i_1+1} V_{j_1}^{1-\pi(i)} C_i^{\dagger\pi(i)}) = 0. \tag{27}$$

  Using the analysis of [27], the set of unitaries V_m satisfying relations of the form Equation (27) has zero Haar measure on U(4). This follows from the fact that one can show that there is a one-to-one mapping between these (nonidentically zero) polynomial equations in the matrix elements of V_m, and the intersection (Corresponding to partitioning the determinant into real and imaginary parts, each of which can be expressed as a trigonometric function of 16 real valued angles in $[0, 2\pi]$

parametrizing V_m [27].) of the zero sets of two real analytic functions on $\mathbb{R}^{16}$. Each such zero set has a Lebesgue measure zero, therefore, their intersection (which is a subset of the two) also has Lebesgue measure zero (see [27] for more details). Therefore, the set of unitaries generated by relations of the form of Equation (27) has Haar measure zero [27]. The number of possible relations of the form of Equation (27) is countable (for fixed k and fixed $\{W_1, ..., W_n, V_1, ..., V_{m-1}\}$), thus the Haar measure of the set of unitaries V_m satisfying Equations (25) or (26) is also zero, as the countable union of measure zero sets is also measure zero. This means that we can choose V_m to be outside a measure zero set (which is the set of unitaries satisfying Equations (23) in **Case 1**, (25), and (26)), and we would therefore have that V_m simultaneously violates the relations imposed by **Case 1** and **Case 2**. This completes the proof of Theorem (2).

2.2. *Proof of Theorem (3)*

Define the moment superoperators

$$M_t[\mu_{block(B^k)}] = \sum_{i=1,...|\mathcal{U}_{B^k}|^{n-1}} \frac{1}{|\mathcal{U}_{B^k}|^{n-1}} U_i^{\otimes t,t}, \tag{28}$$

where $U_i \in \mathcal{U}_{block(B^k)}$; and

$$M_t[\mu_{block(B_1)}] = \sum_{i=1,...|\mathcal{U}^k|^{n-1}} \frac{1}{|\mathcal{U}^k|^{n-1}} V_i^{\otimes t,t}, \tag{29}$$

where $V_i \in \mathcal{U}_{block(B_1)}$. Let

$$M_t[\mu_{block(B_2)}] = \sum_{i=1,...|\mathcal{U}_{block(B_2)}|} \frac{1}{|\mathcal{U}_{block(B_2)}|} W_i^{\otimes t,t}, \tag{30}$$

where $W_i \in \mathcal{U}_{block(B_2)}$. Note that $\mathcal{U}_{block(B_2)}$ is the complement of $\mathcal{U}_{block(B_1)}$ in $\mathcal{U}_{block(B^k)}$. Straightforward calculation using Equation (13) leads to the following relation

$$M_t[\mu_{block(B^k)}] = (1-a^k)^{n-1} M_t[\mu_{block(B_1)}] + (1-(1-a^k)^{n-1}) M_t[\mu_{block(B_2)}]. \tag{31}$$

Recalling from [11] that $M_t[\mu_{block(B_1)}]$ is an (η, t)-TPE if [24,25]

$$||M_t[\mu_{block(B_1)}] - M_t[\mu_H]||_\infty \leq \eta, \tag{32}$$

where $M_t[\mu_H] = \int_{U(2^n)} U^{\otimes t,t} \mu_H(dU)$ and μ_H is the Haar measure on $U(2^n)$; using Equation (31) and a triangle inequality for norms we get

$$||M_t[\mu_{block(B_1)}] - M_t[\mu_H]||_\infty \leq \frac{1}{(1-a^k)^{n-1}} ||M_t[\mu_{block(B^k)}] - M_t[\mu_H]||_\infty + \frac{1-(1-a^k)^{n-1}}{(1-a^k)^{n-1}} ||M_t[\mu_{block(B_2)}] - M_t[\mu_H]||_\infty. \tag{33}$$

Thus, $block(B_1)$ is an $(\eta, t) - TPE$ with

$$\eta = \frac{1}{(1-a^k)^{n-1}} ||M_t[\mu_{block(B^k)}] - M_t[\mu_H]||_\infty + \frac{1-(1-a^k)^{n-1}}{(1-a^k)^{n-1}} ||M_t[\mu_{block(B_2)}] - M_t[\mu_H]||_\infty. \tag{34}$$

From a result in [11],

$$||M_t[\mu_{block(B^k)}] - M_t[\mu_H]||_\infty \leq P(t) + \varepsilon', \tag{35}$$

where $P(t)$ and $\varepsilon^{'}$ are as defined in Theorem (1). In addition, because $\mathcal{U}_{block(B_2)}$ is approximately universal on $U(2^n)$ (because it is composed of unitaries which are approximately universal on $U(4)$), then by a result of [26],

$$|M_t[\mu_{block(B_2)}] - M_t[\mu_H]||_\infty \leq 1. \tag{36}$$

Replacing Equations (35) and (36) in Equation (34) allows to obtain the value of η in Theorem (3).

2.3. Proof of Theorem (4)

The proof of Theorem (4) will also proceed by contradiction.
Suppose $\exists\ t_m$, such that $\forall\ n \geq \lfloor 2.5log_2(4t) \rfloor$,

$$\frac{P(t_m) + \varepsilon^{'}}{(1-a^k)^{n-1}} + \frac{1-(1-a^k)^{n-1}}{(1-a^k)^{n-1}} > 1. \tag{37}$$

Notice that

$$\lim_{n\to\infty} (1-a^k)^{n-1} = 1, \tag{38}$$

with a and k as given in Equations (8) and (7), and t replaced by t_m. Thus, for large enough n, and by using Equation (38), Equation (37) reduces to

$$P(t_m) + \varepsilon^{'} \sim> 1. \tag{39}$$

Equation (39) leads to a contradiction, since by Theorem (1), $P(t) + \varepsilon^{'} \leq 1, \forall\ t$. This concludes the proof of Theorem (4).

2.4. Proof of Theorem (5)

The proof of Theorem (5) follows directly from applying Theorems (3) and (4) in Proposition (1).

3. Conclusions

In this work, we have shown that one can obtain efficient approximate unitary t-designs from random quantum circuits with support over families of seeds which are relaxed in the sense that any unitary in the seed need not in general have its inverse in the seed, nor are the seed unitaries composed entirely of algebraic entries. This result proves and extends the scope of a conjecture proposed in [2]. The relaxed seeds presented here have a cardinality which increases with n and t (see Equation (13)). These seeds, we believe, are not optimal, and we conjecture that relaxed seeds with a constant number of elements as in [2,11] suffice to get efficient t-designs.

Such relaxations have natural importance when the choice of the seed is not free for various reasons; for example, in the measurement-based approach to implementing t-designs [11,21,22] (see also [12,13]). There, the random selection of the unitary in the ensemble is made via a measurement—that is, relying on quantum randomness, not classical randomness. This has several potential advantages, including nonadaptivity of the setup, true randomness (which may even be beyond efficient classical randomness [28]), as well as the potential for verification [29,30] and integration to broader quantum information tasks through the graph state approach [31]. A difficulty in proofs in this approach is that the strict restrictions of previous approaches [2] heavily limited the allowed measurement-based structures. Indeed, this is what motivated previous works in this direction [11,12,22]. To this end, we expect that our relaxations will allow for more diverse constructions of t-designs, broadening their potential implementability and integrability into quantum information networks. Furthermore, given the natural use of graph states [32] for error correction and fault tolerance [33,34], this approach may lead to much better designs of quantum advantage tolerant to noise.

Another possible application to our result is making progress towards an inverse-free version of the Solovay–Kitaev (SK) theorem [35]. Indeed, there are already hints at relations between the SK construction and unitary t-designs [36] (We are grateful to Michał Oszmaniec for pointing us to this result.), and our construction is the first (to our knowledge (A work which is expected to appear shortly by Oszmaniec, Horodecki, and Sawicki also manages to remove the need for inverses and algebraic entries in the seed.)) to remove the need for inverses in the base set generating the t-design (see technical draft for details [11]).

Author Contributions: Conceptualization, R.M. and D.M.; Investigation, R.M. and D.M.; Methodology, R.M. and D.M.; Project administration, D.M. and J.G.; Software, J.G. and J.D.; Validation, R.M. and D.M.; Writing—original draft, R.M.; Writing—review & editing, R.M., J.G., and D.M. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to acknowledge the National Council for Scientific Research of Lebanon (CNRS-L) and the Lebanese University (LU) for granting a doctoral fellowship to R. Mezher. We acknowledge support of the ANR through the ANR-17-CE24-0035 VanQute project.

Acknowledgments: We thank Michał Oszmaniec, Francesco Arzani, and Robert Booth for fruitful discussions. We thank the anonymous referees whose comments helped improve the presentation of this manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chiffre, M.D.D. The Haar measure. Ph.D. Thesis, Department of Mathematical Sciences, University of Copenhagen, Copenhagen, Denmark, 2011.
2. Brandão, F.G.S.L.; Harrow, A.W.; Horodecki, M. Local Random Quantum Circuits are Approximate Polynomial-Designs. *Commun. Math. Phys.* **2016**, *346*, 397–434. [CrossRef]
3. Knill, E. Approximation by quantum circuits. *arXiv* **1995**, arXiv:quant-ph/9508006.
4. Epstein, J.; Cross, A.W.; Magesan, E.; Gambetta, J.M. Investigating the limits of randomized benchmarking protocols *Phys. Rev. A* **2014**, *89*, 012304. [CrossRef]
5. Emerson, J.; Weinstein, Y.S.; Saraceno, M.; Lloyd, S.; Cory, D.G. Pseudo-random unitary operators for quantum information processing. *Science* **2003**, *302*, 2098–2100. [CrossRef]
6. Hayden, P.; Leung, D.; Shor, P.W.; Winter, A. Randomizing quantum states: Constructions and applications. *Commun. Math. Phys.* **2004**, *250*, 371–391. [CrossRef]
7. Matthews, J.C.F.; Whittaker, R.; O'Brien, J.L.; Turner, P. Testing randomness with photons by direct characterization of optical t-designs. *Phys. Rev. A* **2015**, *91*, 020301. [CrossRef]
8. Oszmaniec, M.; Augusiak, R.; Gogolin, C.; Kołodynski, J.; Acin, A.; Lewenstein, M. Random bosonic states for robust quantum metrology. *Phys. Rev. X* **2016**, *6*, 041044. [CrossRef]
9. Muller, M.; Adlam, E.; Masanes, L.; Wiebe, N. Thermalization and canonical typicality in translation-invariant quantum lattice systems. *Commun. Math. Phys.* **2015**, *340*, 499–561. [CrossRef]
10. Hayden, P.; Preskill, J. Black holes as mirrors: Quantum information in random subsystems. *J. High Energy Phys.* **2007**, *120*. [CrossRef]
11. Mezher, R.; Ghalbouni, J.; Dgheim, J.; Markham, D. Efficient approximate unitary t-designs from partially invertible universal sets and their application to quantum speedup. *arXiv* **2019**, arXiv:1905.01504v3.
12. Haferkamp, J.; Hangleiter, D.; Bouland, A.; Fefferman, B.; Eisert, J.; Bermejo-Vega, J. Closing gaps of a quantum advantage with short-time Hamiltonian dynamics. *arXiv* **2019**, arXiv:1908.08069.
13. Bermejo-Vega, J.; Hangleiter, D.; Schwarz, M.; Raussendorf, R.; Eisert, J. Architectures for quantum simulation showing a quantum speedup. *Phys. Rev. X* **2018**, *8*, 021010. [CrossRef]
14. Dankert, C.; Cleve, R.; Emerson, J.; Livine, E. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A* **2009**, *80*, 012304. [CrossRef]
15. Roy, A.; Scott, A.J. Unitary designs and codes. *Codes Cryptogr.* **2009**, *53*, 13–31. [CrossRef]
16. Seymour, P.D.; Zaslavsky, T. Averaging sets: A generalization of mean values and spherical designs. *Adv. Math.* **1984**, *52*, 213–240. [CrossRef]
17. Bannai, E.; Nakahara, M.; Zhao, D.; Zhu, Y. On the explicit constructions of certain unitary t-designs. *arXiv* **2019**, arXiv:1906.04583.

18. Harrow, A.; Mehraban, S. Approximate unitary t-designs by short random quantum circuits using nearest-neighbor and long-range gates. *arXiv* **2018**, arXiv:1809.06957.
19. Kaznatcheev, A. Structure of Exact and Approximate Unitary t-Designs. Available online: https://www.cs.mcgill.ca/~akazna/kaznatcheev20100509.pdf (accessed on 5 September 2019).
20. Nakata, Y.; Hirche, C.; Koashi, M.; Winter, A. Efficient quantum pseudorandomness with nearly time-independent Hamiltonian dynamics. *Phys. Rev. X* **2017**, *7*, 021006. [CrossRef]
21. Turner, P.; Markham, D. Derandomizing Quantum Circuits with Measurement-Based Unitary Designs. *Phys. Rev. Lett.* **2016**, *116*, 200501 . [CrossRef]
22. Mezher, R.; Ghalbouni, J.; Dgheim, J.; Markham, D. Efficient quantum pseudorandomness with simple graph states. *Phys. Rev. A* **2018**, *97*, 022333. [CrossRef]
23. Bourgain Gamburd, J. A spectral gap theorem in $SU(d)$. *arXiv* **2011**, arXiv:1108.6264.
24. Hastings, M.B.; Harrow, A.W.H. Classical and quantum tensor product expanders. *arXiv* **2008**, arXiv:0804.0011.
25. Hastings, M.B. Random unitaries give quantum expanders. *Phys. Rev. A* **2007**, *76*, 032315. [CrossRef]
26. Harrow, A.; Low, R.A. Random quantum circuits are approximate 2-designs. *Commun. Math. Phys.* **2009**, *291*, 257–302. [CrossRef]
27. Farzani, F.; Ferrini, G.; Grosshans, F.; Markham, D. Random coding for sharing bosonic quantum secrets. *Phys. Rev.* **2019**, 022303. [CrossRef]
28. Hoban, M.J.; Wallman, J.J.; Anwar, H.; Usher, N.; Raussendorf, R.; Browne, D.E. Measurement-based classical computation. *Phys. Rev. Lett.* **2014**, *112*, 140505. [CrossRef]
29. Markham, D.; Krause, A. A simple protocol for certifying graph states and applications in quantum networks. *arXiv* **2018**, arXiv:1801.05057.
30. Takeuchi, Y.; Mantri, A.; Morimae, T.; Mizutani, A.; Fitzsimons, J.F. Resource-efficient verification of quantum computing using Serfling's bound. *NPJ Quant. Inf.* **2019**, *5*, 27. [CrossRef]
31. Markham, D. Quantum Computing. *Ercim News* **2018**, *112*, 19.
32. Bell, B.A.; Tame, M.S.; Markham, D.; Wadsworth, W.J.; Rarity, J.G. Experimental demonstration of graph-state quantum secret sharing. *Nat. Commun.* **2014**, *5*. 5480. [CrossRef]
33. Raussendorf, R.; Harrington, J.; Goyal, K. Topological fault-tolerance in cluster state quantum computation. *Ann. Phys.* **2006**, *321*, 2242–2270. [CrossRef]
34. Nielsen, M.A.; Dawson, C.M. Fault-tolerant quantum computation with cluster states. *Phys. Rev. A* **2005**, *71*, 042323. [CrossRef]
35. Dawson, C.M.; Nielsen, M.A. The solovay-kitaev algorithm. *arXiv* **2005**, arXiv:quant-ph/0505030.
36. Varjú, P.P. Random walks in compact groups. *Doc. Math.* **2013**, *18*, 1137–1175.