Unitary t-designs & Quantum Circuits

Juspreet Singh Sandhu (jus065@g.harvard.edu)

December 19, 2018

Abstract

Unitary t-designs have fast gained prominence in the regime of Classical Simulation of Quantum Circuits, and recently in Quantum Complexity [Ha08]. As t-designs provide a rigorous way to measure how well a certain subset of the Unitaries approximates the Haar measure, they provide a quantification of the "power" of Quantum Circuits constructed from them. Lower bounds on these designs are of interest to understand the minimum number of Unitaries needed to approximate the Haar measure (to some finite t). To that extent, it has been shown that the Clifford Group forms an exact 2-design [Ma14] and that any 2-design requires atleast $\mathcal{O}(d^4)$ d-dimensional Unitaries [Gr07]. Another interesting realm of questions is investigating random, efficient quantum circuits and how well they approximate the Haar measure (to some degree of approximation for a finite t). [Ha08] show that efficient random circuits are approximate 2-designs. In this paper, we present an overview of these results. We end by listing two open questions; the first a conjecture by [Gr07] for a tight lower-bound on the size of Unitary 2-designs, and the second on a possible lower bound for efficient circuits that are exact 2-designs.

1 Introduction

To begin this survey, we will introduce the motivating notions of Spherical designs and their similarities to Unitary t-designs. Moving on, we will introduce and define the notion of "twirling" quantum states. We will then see 2 equivalent definitions of Unitary t-designs, but focus (for the most part) on the definition based on the "twirling" action. To end, we'll move on to state elementary lemmas from the Representation Theory of Groups that will be useful when we give an exposition of the proof that the Clifford Group of Unitaries form an exact 2-design.

Definition 1 (Spherical Design)**.** $\forall$ *polynomials* $p_n : \mathcal{S}(\mathbb{R}^n) \to \mathbb{R}$ *with homogeneous monomial terms in n-variables with degree* $\leq t$*, if there is a finite subset*

of the unit-sphere $D = \{x \mid x \in \mathcal{S}(\mathbb{R}^n)\}$*, such that:*

$$\frac{1}{|D|}\sum_{x\in D}(p_n(x)) = \int_{x\in\mathcal{S}(\mathbb{R}^n)}(p_n(x))d\mu(x) \tag{1}$$

we say that D forms a Spherical t-design.

In the definition above, $\mathcal{S}(\mathbb{R}^n)$ denotes the unit sphere in $\mathbb{R}^n$ and $d\mu$ the uniform spherical measure. The definition here formalizes our geometric notion of how well a particular discrete shape will approximate the "sphere" for some fixed value of t. For instance, if we had set $t = 1$ and wanted to approximate the linear polynomials, we'd simply choose a geometric shape (a distribution of points to construct D) with its average at the origin. As t increases, our shape makes better approximations to the sphere and our shape will have more antipodal positions.

A generalization of Spherical designs leads to Complex Projective designs, which are directly related to Unitary t-designs. An important result links these two concepts, and Unitary t-designs can be seen as a generalization of Complex Projective Designs to Unitary Matrices.

Definition 2 (Complex Projective Design)**.** $\forall$ *polynomials* $p_n : \mathcal{S}(\mathbb{C}^n) \to \mathbb{C}$ *with n homogeneous monomials in degree* $\leq t$ *and n degree t conjugate monomials, if there is a finite subset of the unit sphere* $D = \{x \mid x \in \mathcal{S}(\mathbb{C}^n)\}$*, such that:*

$$\frac{1}{|D|}\sum_{x\in D}(p_n(x)) = \int_{x\in\mathcal{S}(\mathbb{C}^n)}(p_n(x))d\mu(x) \tag{2}$$

we say that D forms a Complex Projective t-design.

In the definition above, $\mathcal{S}(\mathbb{C}^n)$ denotes the unit complex sphere in $\mathbb{C}^n$ and $d\mu$ the uniform Haar measure. Note that a Complex Projective t-design has $2n$ variables, while a Spherical design has n variables. Given that the homogeneity constraints on monomials are the same and the Haar measure generalizes the Spherical measure, it is natural to ask whether there is a way to transform one to the other. A simple result which we will state (but not prove) establishes this relationship.

Lemma 3. $\forall$ *Spherical t-designs over* $\mathcal{S}(\mathbb{R}^n)$*,* $\exists$ *a Complex Projective* $\frac{t}{2}$*-design over* $\mathcal{S}(\mathbb{C}^{\frac{n}{2}})$*.*

We now introduce the notion of "twirling", which will allow us to state the 3 equivalent definitions of Unitary t-designs.

Definition 4 (Twirling States)**.** $\forall\rho \in \mathcal{B}(\mathcal{H}\otimes\mathcal{H})$*, the t-twirl on* ρ *is given by averaging over the conjugation action of the unitaries on* ρ*:*

$$\int_{U(n)}(U^{\otimes t})\rho(U^{\dagger})^{\otimes t}d\mu \tag{3}$$

Here, ρ denotes any arbitrary impure quantum state:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{4}$$

over some arbitrary probability distribution $\sum_i p_i = 1$ and pure states $|\psi_i\rangle \in \mathcal{H}$. This twirling average can also be captured by some finite subset of the unitaries if we compare the average over the Haar measure. This can be framed as:

$$\frac{1}{|D|} \sum_{U \in D} (U^{\otimes t}) \rho (U^\dagger)^{\otimes t} = \int_{U(n)} (U(n)^{\otimes t}) \rho (U(n)^\dagger)^{\otimes t} d\mu \tag{5}$$

The formulation stated above in (5) is equivalent to the definition of a Unitary t-design introduced further in (6). This equivalence allows us to study the properties of t-designs, originally defined as extensions of Complex Projective designs (which are averages over polynomials) via Representation Theoretic techniques by evaluating these averages through the properties of the irreducible representations of the Unitary group and its subgroups.

Definition 5 (Unitary t-designs)**.** *$\forall$ polynomials $P_{t,t}(U)$ homogeneous with degree $\leq t$ for U and degree $\leq t$ for $U^\dagger$ over $2n^2$ variables, if there exists a finite subset $D = \{U \mid U \in U(n)\}$, such that:*

$$\frac{1}{|D|} \sum_{U \in D} P_{t,t}(U) = \int_{U(n)} P_{t,t}(U(n)) d\mu \tag{6}$$

we say that D forms a Unitary t-design.

The notion defined above can be thought of as using finite subsets of the uncountably many unitaries to approximate the Haar measure to some degree of accuracy, measured by some fixed $t \in \mathbb{N}$. In general, as $t \to \infty$, we get a precise measurement. However, in such cases, the lower bounds on $|D|$ start approximating infinity as well. We are, therefore, interested in regimes where we fix some finite t in accordance with the degree of approximation we desire and to minimize $|D|$ in order to achieve the approximation.

We now recall a few elementary results from the Representation Theory of Groups.

Definition 6 (Schur's Lemma)**.** *Given 2 vector spaces V, W over $\mathbb{F} = \mathbb{C}$, along with the irreducible representations $\rho_V : G \to V$ and $\rho_W : G \to W$, we have that:*
i) If $V \ncong W$, then $\nexists A : V \to W$, such that, A is non-trivial and G-linear.
ii) If $V = W$ and $\rho_V = \rho_W$, then the only non-trivial family of G-linear maps are scalar multiples of the identity.

Put simply, the definition above simply asserts a way to compare when two irreducible representations are same (up to identity scaling) and when they are

not. When decomposing a group into the finite sum of its irreducible representations, this lemma helps factor the representation by providing a way to determine when 2 irreducible representations are equivalent.

Lemma 7. *Given a compact group G and its linear representation $\rho : G \to GL(V)$, such that $\chi(V) = 0$ (the field has characteristic 0), we can express ρ as a finite sum of irreducible representations.*

This lemma leads us to a unique, canonical decomposition upto isomorphism. However, in order to achieve the unique decomposition, we must identify all irreducible representations that are isomorphic. This is where Schur's Lemma comes to our aid, and allows us to write the direct sum as a unique, canonical decomposition (upto isomorphism).

2 The Clifford Group & Unitary 2-designs

This section will primarily be devoted to the study of Unitary 2-designs, and in particular, showing that the Clifford Group forms an exact 2-design. These are designs that approximate the Haar measure upto quadratic polynomials defined over the unitaries. Note that the Haar measure is well defined on $U(n)$ because it is compact. This does not hold in general, for example, as $GL(\mathbb{C})$ is not compact.

Plugging $t = 2$ in our "twirling" definition of a Unitary t-design above (5), we recover that a 2-design is a set $D \subset U(n)$, such that:

$$\frac{1}{|D|} \sum_{U \in D} (U \otimes U)\rho(U^\dagger \otimes U^\dagger) = \int_{U(n)} (U(n) \otimes U(n))\rho(U(n) \otimes U(n))^\dagger d\mu \quad (7)$$

Let us introduce the notion of a Quantum Channel, and extend the equivalence of (5) and (6) to a notion of "twirling" of quantum channels. We will then evaluate the expression of the average of the Haar measure for $t = 2$ and the finite average over the Clifford group and show that they are equal.

Definition 8 (Quantum Channel)**.** *A quantum channel $\hat{\Lambda}$ is a super-operator that acts on any state ρ by conjugation as:*

$$\hat{\Lambda}(\rho) = A(\rho)B \quad (8)$$

where, A, B are arbitrary linear operators.

We can use this definition to come up with an equivalent "twirl" over a quantum channel using the conjugation action. The action of a "twirled" quantum channel on a state can be thought of as an average over the conjugation of the action of the quantum channel by all unitaries. More formally:

Definition 9 (Twirling Channels)**.** *Given a quantum channel* $\hat{\Lambda}$*, a quantum state* ρ*, the channel twirls the state as:*

$$\rho \mapsto \int_{U(n)} U^\dagger \Lambda(U\rho U^\dagger) U d\mu = \int_{U(n)} U^\dagger A U \rho (U^\dagger B U) d\mu \tag{9}$$

The definition in (9) is equivalent to a Unitary t-design (for $t = 2$) as defined in (5) and (6). We now define the Clifford Group ($\mathcal{C}_m$) over m-qubits, claim that it forms a 2-design, and lay out the proof.

Definition 10 (Clifford Group)**.** *The Clifford group over m-quibits* $\mathcal{C}_m$ *is those subset of the unitaries* $U(2^m)$ *that preserve the Pauli operators* $\mathcal{P}_m$ *up to conjugation. More formally:*

$$\mathcal{C}_m = \{U \in U(2^m) \mid UpU^\dagger \in \mathcal{P}_m, \forall p \in \mathcal{P}_m\} \tag{10}$$

The formal statement of the lemma:

Lemma 11 ($\mathcal{C}_m$ form an exact 2-design)**.**

$$\frac{1}{|\mathcal{C}_m|} \sum_{C \in |\mathcal{C}_m|} C^\dagger A C \rho (C^\dagger B C) = \int_{U(n)} U^\dagger A U \rho (U^\dagger B U) d\mu \tag{11}$$

Proof: To prove this lemma as shown by [Mat14], we will first state the result of evaluating the RHS, which is the average over the Haar measure. Note that the interesting result in constructing designs comes from the LHS, as that depends on the choice of D (in this case $D = \mathcal{C}_m$). However, the RHS is fully evaluated and depends only on t. In our case $t = 2$, and we use an application of Schur's Lemma on the irreducible representations of the linear operators and the unitaries in conjunction with the fact that the Haar-superoperator is $U(n)$ invariant to arrive at a closed form. More details of a proof for the evaluation of the RHS can be found in the Appendix of Emerson et al (2005).
We now state the closed-form evaluation of the RHS of (11):

$$\int_{U(n)} U^\dagger A U \rho (U^\dagger B U) d\mu = \alpha + \beta \tag{12}$$

where,

$$\alpha = \frac{Tr(AB)Tr(\rho)\mathrm{Id}}{d^2} \tag{13}$$

$$\beta = \left(\frac{n(Tr(A)Tr(B)) - Tr(AB)}{d(d^2-1)}\right)\left(\rho - \frac{Tr(\rho)\mathrm{Id}}{d}\right) \tag{14}$$

To evaluate the LHS we will need to perform a twirling operation on a state ρ via elements of the Pauli group. We use the fact that the Pauli's form a basis for the joint Hilbert Space to expand the Linear Operators $A, B \in \mathcal{B}(H \otimes H)$ as a linear combination of Paulis.

Twirling ρ by the Paulis, we obtain:

$$\rho \mapsto \frac{1}{n^2} \sum_{k=1}^{n^2} P_k A P_k \rho (P_k B P_k) \tag{15}$$

where we collapse the † for the Paulis since they are Hermitian. Additionally, we express our Linear Operators as Linear sums of Paulis:

$$A = \sum_{i=1}^{n^2} a_i P_i \tag{16}$$

$$B = \sum_{j=1}^{n^2} b_j P_j \tag{17}$$

Substituting (16) and (17) into (15) yields:

$$\rho \mapsto \frac{1}{n^2} \sum_{i=1}^{n^2} \sum_{j=1}^{n^2} a_i b_j (\sum_{k=1}^{n^2} P_k P_i P_k \rho (P_k P_j P_k)) \tag{18}$$

We then use the fact that exactly half the elements of the Pauli commute with each other, and the other anti-commute to reduce the product $P_k P_i P_k$ (and equivalently, $P_k P_j P_k$). This tells us that the only non-zero contributions (that survive the anti-commutativity annihilation) occur when $i = j$, leading to the final result:

$$\rho \mapsto \sum_{i=1}^{n^2} a_i b_i P_i \rho (P_i) = \hat{\Lambda}_p \rho \tag{19}$$

where $\hat{\Lambda}_p$ is the Pauli channel. Since we are seeking 2-designs, we will twirl our channel once more, and as we shall see, this gives us a form for our LHS that is equivalent to the one in (12). We now twirl using the Clifford, rewriting with elements from the cosets of $\mathcal{C}_m/\mathcal{P}_m$, since the Pauli is a normal subgroup of the Clifford. As such, every $C \in \mathcal{C}_m$ can be written as $C = QP$, where $Q \in \mathcal{C}_m/\mathcal{P}_m$ and $P \in \mathcal{P}_m$. Formally, using Lagrange's Theorem for counting the number of sums and the coset product to rewrite the Clifford twirl, we arrive (after a bit of algebra) at:

$$\rho \mapsto a_1 b_1 \rho + \frac{|\mathcal{P}_m|}{|\mathcal{C}_m|} \sum_{i=1}^{\frac{|\mathcal{C}_m|}{|\mathcal{P}_m|}} \sum_{j=2}^{n^2} a_j b_j (Q_i^\dagger P_j Q_i \rho) Q_i^\dagger P_j Q_i \tag{20}$$

where we sum from $j = 2$ as we drop the identity element from the Paulis. We consider the action of the entire Clifford Group on a non-identity element from the Pauli and note that each C gets mapped to every Pauli $n^2 - 1$ times. This

allow us to rearrange (20) as:

$$\rho \mapsto a_1 b_1 \rho + \frac{1}{n^2-1} \sum_{j=2}^{n^2} a_j b_j \sum_{k=2}^{n^2} P_k \rho(P_k) \tag{21}$$

As stated in [Mat14], we now use identities that relate the traces of A, B to a_i, b_i and the trace of ρ so as to rewrite (21) in the desired form:

$$a_1 b_1 = \frac{Tr(A)Tr(B)}{n^2} \tag{22}$$

$$\sum_{k=1}^{n^2} a_k b_k = \frac{Tr(AB)}{n} \tag{23}$$

$$\sum_{k=1}^{n^2} P_k \rho(P_k) = nTr(\rho)Id \tag{24}$$

Some algebra after substituting (22), (23) and (24) into (21) yields that (21) is equivalent to (12). This shows that the LHS of (11) is equivalent to the evaluated RHS. Hence, $\mathcal{C}_m$ forms an exact 2-design.
QED.

The reason Lemma (11) is important is that it tells us that there exists a representative, finite subset of the unitaries $U(n)$ ($\mathcal{C}_m$) over which we can efficiently (using $\mathcal{O}(n^2)$ 1/2 qubit gates) synthesize a circuit to realize an element from it. The reason that this subset (the Clifford Group - $\mathcal{C}_m$) is chosen is because sampling/building a Haar random Unitary from $U(n)$ requires $\mathcal{O}(n^2 2^{2n})$ 1/2 qubit gates. Therefore, the realization of the Cliffords forming a 2-design allows us to construct a representative set that can be efficiently sampled from to build Quantum circuits.

3 Lower Bounds on |D| for 2-designs

In Section 2, we saw that the choice for D can greatly affect power of our design (t-value) and the ability to efficiently synthesize a circuit that has an element from $d \in D$. Having defined the degree to which we want some finite $D \subset U(n)$ to be representative of $U(n)$ (say $t = 2$), we can ask what the minimum size of D should be.
To answer this question (at least partially), we present a lower bound constructed by [GAE07] on $|D|$ for 2-designs in n-dimensional Hilbert Space and a proof for the bound by analyzing the representations of the unitaries in the construction of the twirling of an arbitrary channel.

Lemma 12 (Lower Bound)**.** *$\forall D \subset U(n)$, such that $|D| < \infty$ and D is (over n-dimensions) a 2-design, $|D| \geq n^4 - 2n^2 + 2$.*

Proof: To prove this lemma as shown by [GAE07], we analyze the rank of the channel Λ that gets defined by constructing a certain homogeneous (2,2) polynomial from a maximally entangled state $|v_0\rangle$. We assume that our states belong to a n-dimensional Hilbert space $\mathcal{H}$.
Let the constructed state be:

$$|v_U\rangle = U \otimes Id|v_0\rangle \tag{25}$$

This allows us to define a (2, 2) homogeneous polynomial:

$$p(U) = \langle v_U|A|v_U\rangle tr(|v_U\rangle\langle v_U|B) \tag{26}$$

where $A, B \in \mathcal{B}(\mathcal{H} \otimes \mathcal{H})$. We can verify that this polynomial respects the averaging required from a 2-design in (6) for some D. Therefore, by using the equivalence between (6) and (9) we know that $\exists\Lambda$, such that:

$$\Lambda(A) = \int_{U(n)} \langle v_U|A|v_U\rangle(|v_U\rangle\langle v_U|)d\mu \tag{27}$$

In order to compute rank(Λ), we need to understand the kernel of Λ. To do so, we can apply Schur's Lemma to understand the irreducible decompositions of $U, U^\dagger$ and use that to analyze Λ in terms of projections onto invariant subspaces for which Λ's action is covariant. It is easy to verify by inspection that Λ is $U \otimes V$-covariant.
Furthermore, it is well known that the Unitaries of the form $U \cdot U^\dagger$ decompose into 2 classes of irreducibles:
i) Multiples of the identity: M
ii) Their orthogonal complement, the span of traceless operators: $M^\perp$
Since we are looking at 2-designs, we will take the tensor product of the spaces and examine which are invariant under $U \otimes V$:

$$M \otimes M^\perp \tag{28}$$

$$M^\perp \otimes M \tag{29}$$

$$M \otimes M \tag{30}$$

$$M^\perp \otimes M^\perp \tag{31}$$

It is easy to see that (28), (29), (30) and (31) are all invariant under $U \otimes V$.
We see that only (28), (29) are subspaces of ker(Λ). Therefore, we can now measure the rank of Λ using the Rank-Nullity theorem:

rank(Λ) = n^4 - dim($M \otimes M^\dagger$) - dim($M^\dagger \otimes M$) = $n^4 - 2(n^2 - 1)$
So, $|D| \geq$ rank(Λ) = $n^4 - 2n^2 + 2$.

QED.

This result tells us that the minimum number of elements required for a 2-design are $\mathcal{O}(n^4)$. Note, however, that the Clifford group with $\#qubits = m$

has cardinality:

$$|C_m| = 2^{m^2+2m} \prod_{j=1}^{n} (4^j - 1) = \mathcal{O}(2^{m^2}) \tag{32}$$

Using $n = 4$ (the case of 2 qubits) in the lower bound, we see that $|D| \geq 226$. However, for $m = 2$, $|C_2| = 11520$ (using (32)). Therefore, even the Clifford group has far more elements than required to form a 2-design. This motivates the interesting question of whether there exist other neatly characterized finite sets $D \subset U(n)$ that form 2-designs and are even more efficient to sample from. As we shall see in the next section, most random quantum circuits $\mathcal{C} \in BQP$ are approximate 2-designs, which makes reducing the size of D a worthy challenge.

4 Approximate 2-designs

In this section, we will review a pivotal result from [HL08] which gives us an efficient bound on the size of a random circuit $\mathcal{C} \in BQP$ to be an approximate 2-design. We will then state another result by [CLLW16] that has improved the bound in [HL08] (and is stronger). This section aims to lay down the definition of approximate 2-designs and give a survey of some of the results and is, therefore, less rigorous than the previous sections.

Definition 13 (Twirled Channel with arbitrary measure)**.** *We define a twirled channel with arbitrary measure* Γ *as an average of the twirling action of some* Λ *with respect to that measure:*

$$\mathbb{E}_\Gamma(\Lambda) = \rho \mapsto \int_{U(n)} U^\dagger \Lambda(U\rho U^\dagger) U d\Gamma \tag{33}$$

Notice that this is essentially the same definition as that of a 2-design, except the measure is arbitrary and not the Haar measure.
This definition naturally leads us to a notion of approximation when we use the diamond norm($\diamond$) to measure the distance between the average of an arbitrary measure (Γ) and the Haar measure (μ).

Definition 14 (ϵ-approximate 2-designs)**.** *An* ϵ*-approximate 2-design is a channel* $\mathbb{E}_\Gamma(\Lambda)$*, such that:*

$$\|\mathbb{E}_\Gamma(\Lambda) - \mathbb{E}_\mu(\Lambda)\|_\diamond \leq \epsilon \tag{34}$$

An important result in constructing efficient quantum circuits that used gates sampled from the universal gate set came from [HL08]:

Lemma 15 (Random Quantum Circuits are Approximate 2-designs)**.** *Random Quantum Circuits $\mathcal{C}$ of size $\mathcal{O}(n(n + log\frac{1}{\epsilon}))$ built using 1/2 qubit gates sampled from the Universal Gate are ϵ-approximate 2-designs.*

The model of randomness uses randomly sampled unitaries from $U(4)$, which allowed for sampling from the Haar measure over $U(4)$. To read about the model in more detail, refer to Section 1.1 of Harrow et al (2008).
This result improved the previous bound of $\mathcal{O}(n^6(n^2 + log\frac{1}{\epsilon}))$, but was not tight because we know that we can construct a Clifford gate in size $\mathcal{O}(n^2)$ which give the construction of exact 2-designs (albeit in exponential size). Therefore, a tighter bound (specifically, less than $\mathcal{O}(n^2)$) would be a more desirable bound.

A much tighter bound was discovered recently by [CLLW16], where a near-linear size circuit of logarithmic depth can be used to construct exact 2-designs ($\epsilon = 0$). This is a major result, and the main lemma is the following:

Lemma 16 ($\tilde{\mathcal{O}}(n)$ circuits for 2-designs)**.** *$\exists$ circuits $\{\mathcal{C}\}$ of 1/2 qubit gates, such that, $size(\mathcal{C}) = \mathcal{O}(nlog(n)log(log(n)))$ and $\mathcal{C}$ is an exact ($\epsilon = 0$) 2-design.*

In order to use only Clifford gates in constructing the circuit $\mathcal{C}$, we need to assume that the Extended Riemann Hypothesis is true. However, if we allow $\mathcal{C}$ over non-Clifford universal gates, then we can recover the same bound on $size(\mathcal{C})$ without making that assumption.

5 Open Questions

We end this paper by listing 2 questions that, to the knowledge of the author, are open:

1) *Conjecture*(Gr15): The Clifford bound $\Omega(|D|) = n^4 - n^2$ is a lower bound for Unitary 2-designs over a n-dimensional Hilbert Space.

Note that this is a tighter bound than the one we proved above, and our current method that relies on using the Rank-Nullity theorem cannot be extended to prove it as is because the bound on $rank(\Lambda)$ calculated is tight. One possible option may be to attempt to create a cleverer (2,2) homogeneous polynomial that has irreducible representations of lower dimensions.

2) *Question*: $\exists$? circuits $\{\mathcal{C}\}$, such that, $size(\mathcal{C}) < \mathcal{O}(nlog(n)log(log(n)))$ and $\mathcal{C}$ is an exact 2-design ? What is the lower bound $\Omega(size(\mathcal{C}))$ to recognize a circuit of 1/2 qubit gates that is an exact 2-design over the Cliffords ?

Note that our result from [CLLW16] makes use of the assumption of the Extended Riemann Hypothesis being true when constructing circuits that run over Clifford gates. Investigating a lower bound on the size of the circuits that are

exact 2-designs when the gates are only Clifford without assuming the ERH would be an interesting question to answer. Another interesting question would be to come up with a (tight) lower bound on the size of circuits for various gate sets that constitute exact t-designs, as a function of t. For the question posed above, we merely set $t = 2$.

6 Acknowledgements

The author would like to thank Prof. Hyeon for his excellent teaching of MATH-278 in the Fall-2018 semester at Harvard, which motivated this survey paper. In particular, the sections on Quantum Information Theory and various talks with Prof. Hyeon post the lectures were major sources of information and inspiration to write a survey paper at the intersection of Unitary t-designs, Quantum Circuits and Representation Theory.

References

[CLLW16] R. Cleve, D. Leung, L. Liu, and C. Wang. Near-linear constructions of exact unitary 2-designs. *ArXiv e-prints*, June 2016.

[GAE07] D. Gross, K. Audenaert, and J. Eisert. Evenly distributed unitaries: on the structure of unitary d esigns. *ArXiv e-prints*, May 2007.

[HL08] A. Harrow and R. Low. Random Quantum Circuits are Approximate 2-designs. *ArXiv e-prints*, February 2008.

[Mat14] O. Matteo. A short introduction to unitary 2-designs. November 2014.