Structure of exact and approximate unitary t-designs

Artem Kaznatcheev

May 9, 2010

Abstract

When studying "random" operators it is essential to be able to integrate over the Haar measure, both analytically and algorithmically. Unitary t-designs provide a method to simplify integrating polynomials of degree less than t over $U(d)$. In particular, by replacing averages over the Haar measure by averages over a finite set, they allow applications in algorithms. We provide three equivalent definitions for unitary t-designs and introduce group and approximate designs. The main tool in this note is our generalization of an important result - the trace double sum inequality - into the trace $2p$-sum inequality. We use the trace double sum inequality to produce a correspondence between minimal designs and unique minimal weight functions. We culminate our exploration of the structure of t-designs by showing that t-designs span $\{U^{\otimes t} | U \in U(d)\}$. This result produces two conjectures which we believe are an important step in the classification of minimum unitary t-designs.

Contents

List of theorems

1 Introduction

In classical computation, we represent a state of a computer as a string of n bits $b = b_1...b_n$ where each $b_i \in \{0, 1\}$. If the model of computation is deterministic, then each bit string b produces a unique bit string b' at the next time step. In a probabilistic model, a bit string b produces a probability distribution over all possible outcome strings. In this general model of classical computation we can think of the state of the computer as a vector s on the unit $(2^n - 1)$-simplex. In other words, with each bit string b is associated a probability p_b and the sum of probabilities over all possible bit strings is 1. This is seen as the most general model of classical computation, and it is in this framework that we model current computers.

Quantum computation, or more generally quantum information processing, proposes an extension of this model - a transition from bit to qubit. Instead of thinking of each bit as either a 0 or a 1 we can start to think of them as existing in a superposition of the two: $\alpha|0\rangle + \beta|1\rangle$. We represent the computer's state as a vector $|\psi\rangle \in \mathbb{C}^d$ (for n qubits we would have $d = 2^n$). At the end of the computation (or sometimes at intermediate steps) we want to observe the state of the computer through measurement. When we perform a measurement, we consider an orthonormal basis $\{|e_i\rangle...|e_d\rangle\}$ as a set of possible outcomes. The probability that the computer is in state $|e_i\rangle$ is then given by $|\langle e_i|\psi\rangle|^2$. Since the particle must be in one of the d states, we want our state to be normalized:

$$|\langle e_1|\psi\rangle|^2 + ... + |\langle e_d|\psi\rangle|^2 = 1 \tag{1}$$

For any choice of orthonormal basis. If we consider the standard basis then equation 1 simply corresponds to the norm of $|\psi\rangle$ and can be rewritten as $|| \, |\psi\rangle \, || = 1$.

To carry out the next operation and change a computer's state we act on it with matrices. For example, $|\psi_{t+1}\rangle = M|\psi_t\rangle$ is a discrete time-step evolution of a state $|\psi_t\rangle$ at time t to a state $|\psi_{t+1}\rangle$ at time $t + 1$. Throughout the evolution of a state, we want it to remain normalized. Thus, our matrix M must be norm-preserving.

In $\mathbb{C}^d$ the set of norm-preserving matrices corresponds to $U(d)$ - the d-by-d unitary matrices. Thus, every step of a computation can be described by a unitary transformation. However, we might want to borrow ideas from the correspondence between discrete and probabilistic classical computation and sometimes apply a "random" transformation. Such transformations are useful for quantum data hiding [DLT02], pseudo random operators [EWS$^+$03, Dan05], and approximately encrypting quantum states [HLSW04] among others. The difficulty is in implementing this "randomness" and doing so efficiently.

To even discuss "random" operators we need to first define a measure. $U(d)$ forms a group that is topologically compact and connected. This permits us to introduce a unique left-invariant measure - the Haar measure - on $U(d)$. Having a measure allows us to integrate functions f of $U \in U(d)$ to find their averages $\langle f\rangle$ by computing

$$\langle f\rangle = \int_{U(d)} f(U) \, dU.$$

For convenience, and to have $\langle f\rangle$ correspond to the average as we are used to, we need to normalize integration by assuming that:

$$\int_{U(d)} dU = 1$$

The primary goal of unitary t-designs is to replace integration over the space of unitaries with a finite sum. This provides us with an easier method for finding the average of functions over unitaries and proving theorems about such functions. Unitary t-designs in particular are used to evaluate the average of polynomials.

In section 2 we introduce the necessary background by elaborating on what we mean by 'polynomials' and introduce our first two definitions of unitary t-designs. We prove the equivalence of the two definitions, and use the tensor product definition to prove the existence of designs for all values of d and t. In subsection 2.4, we introduce approximate designs and show how approximation might arise due to faulty implementation of design elements. In section 3 we generalize the earlier trace double-sumSecond, we generalize the trace double-sum inequality [Sco08, Kaz09] into the trace $2p$-sum inequality. We use the

restriction to $p = 1$ to provide a metric definition. In working with the metric definition we observe the importance of minimal designs and their characterization in terms of unique minimal weight functions. In subsection 3.3 we pursue another strategy for working with the trace $2p$-sum inequality - restricting it to group designs. We definite both exact and approximate group designs and derive some simple properties. Finally, in section 4 we explore the structure of designs. We provide simple lower bounds for approximate designs with respect to the Frobenius norm and show how to construct 1-designs. We highlight the section with our most important result - theorem 4.6 - describing the spaces designs span. Through out the sections, we raise open questions for future research. Culminating, in subsection 4.3, with a presentation of our two most promising conjectures.

2 Background

The most popular models of quantum computation is the circuit model [NC00]. In this model, we represent a quantum computation as a circuit acting on n registers. Each element of the circuit is selected from a finite universal gate set. In terms of operators, we can multiply out each element of the circuit, and represent the whole circuit as a single unitary operator from the group generated by the universal gate set [NC00]. If we want to select some of the transformations "randomly" then we can instead write down the circuit as a polynomial in the variable U, where U is the random operation we select. To understand the expected result of the computation, we need to evaluate the expected value of the polynomial. To physically realize the computation, we do not have the luxury of selecting a "random" unitary, and instead need a finite set from which to select the transformation. Unitary t-designs provide such finite sets, and homogeneous polynomials are the first thing we need to understand in order to discuss them.

2.1 Homogeneous polynomials

We will let $\mathrm{Hom}(r, s)$ denote polynomials homogeneous of degree r in entries of $U \in U(d)$ and homogeneous of degree s in the entries of U^*. As an example we can look at the universal commutator:

$$U, V \mapsto U^*V^*UV \in \mathrm{Hom}(2, 2)$$

Here the total power of U, V is 2, same with U^*, V^*. If we fix V and only vary U then we get:

$$U \mapsto U^*V^*UV \in \mathrm{Hom}(1, 1) \tag{2}$$

Since the action of a fixed V, V^* is linear, their presence does not increase the degree of the polynomial. In particular, we can consider any linear function of U acting on a polynomial without increasing its degree, thus:

$$U \mapsto \frac{tr(U^*U)}{d} \in \mathrm{Hom}(1, 1) \tag{3}$$

Since tr, and division by a constant are linear functions.
As a last example consider:

$$U, V \mapsto tr(U^*V)U^2 + VU^*VU \in \mathrm{Hom}(3, 1)$$

Here, the degree is simply the sum of the powers in each summand. However, if we fix V then the polynomial becomes inhomogeneous:

$$U \mapsto \underbrace{tr(U^*V)U^2}_{\mathrm{Hom}(2,1)} + \underbrace{VU^*VU}_{\mathrm{Hom}(1,1)} \notin \mathrm{Hom}(2, 1)$$

Understanding $\mathrm{Hom}(r, s)$ allows us to present the most useful definition of t-designs from the point of view of applications.

2.2 Functional definitions of unitary t-designs

First we introduce an important component of designs:

Definition 2.1 *A function $w : X \to (0, 1]$ is a* weight function on X *if for all $U \in X$ we have $w(U) > 0$ and:*

$$\sum_{U \in X} w(U) = 1$$

This allows to define designs:

Definition 2.2 (Functional definition of unitary t-designs) *A tuple (X,w) with finite $X \subset U(d)$ and weight function w on X is a* unitary t-design *if*

$$\sum_{U \in X} w(U) f(U) = \int_{U(d)} f(U)\, dU \tag{4}$$

for all $f \in \mathrm{Hom}(t,t)$.

Further, there is a special subtype of designs:

Definition 2.3 (Unweighted unitary t-designs) *A finite $X \subset U(d)$ is an* unweighted t-design *if it is a* unitary t-design *with a uniform weight function (i.e. $w(U) = \frac{1}{|X|}$ for all $U \in X$).*

This definition might seem a bit restrictive since it limits us to functions in a single variable in $\mathrm{Hom}(t,t)$. However, with simple arguments we can show that definition

is rather flexible. In particular, we can use t-designs to evaluate all polynomials in a finite number of variables with degrees less than or equal to t.

First, we need to know how to evaluate polynomials of lower degree:

Proposition 2.4 *Every t-design is a $(t-1)$-design.*

Proof Consider any $f \in \mathrm{Hom}(t-1, t-1)$ then multiplying by the polynomial in equation 3:

$$g := U \mapsto \frac{tr(U^*U)}{d} f(U) \in \mathrm{Hom}(t,t)$$

However, we know that equation 3 is equal to 1 for all $U \in U(d)$. Thus, $g(U) = f(U)$ for all $U \in U(d)$. ∎

For the other cases, we need to establish basic property of polynomials over unitaries.

Lemma 2.5 *For any $f \in \mathrm{Hom}(r,s)$, $U \in U(d)$, and $c \in \mathbb{C}$ we have $f(cU) = c^r \bar{c}^s f(U)$*

Proof We will prove this by induction on r and s.

For the base case, consider $\mathrm{Hom}(1,0)$ and $\mathrm{Hom}(0,1)$. Any $f \in \mathrm{Hom}(1,0)$ is a linear function, thus $f(cU) = cf(U)$. For any $f \in \mathrm{Hom}(0,1)$, the conjugate $\bar{f}$ is linear, thus $f(cU) = \bar{c} f(U)$.

Now consider $f \in \mathrm{Hom}(r,s)$ (which we assume, without loss of generality, to be a single summand). We can represent it as $f(U) = L(g(U)h(U))$ for some linear function L and $g \in \mathrm{Hom}(r_1, s_1)$, $h \in \mathrm{Hom}(r_2, s_2)$ with $r_1 + s_1 \geq 1$, $r_2 + s_2 \geq 1$, $s_1 + s_2 = s$ and $r_1 + r_2 = r$. So, by induction we have:

$$\begin{aligned} f(cU) &= L(g(cU)h(cU)) \\ &= L(c^{r_1}\bar{c}^{s_1} g(U) c^{r_2}\bar{c}^{s_2} h(U)) \\ &= c^{r_1+r_2}\bar{c}^{s_1+s_2} L(g(U)h(U)) \\ &= c^r \bar{c}^s f(U) \end{aligned}$$

∎

Proposition 2.6 *For any $f \in \mathrm{Hom}(r,s)$ with $r \neq s$*

$$\int_{U(d)} f(U)\, dU = 0$$

Proof For each r and s and any $U \in U(d)$ by Lemma 2.5 we have $f(e^{\frac{i\pi}{r-s}} U) = -f(U)$. Since $U \mapsto e^{\frac{i\pi}{r-s}} U$ is a bijection we can write our integral:

$$\begin{aligned} \int_{U(d)} f(U) dU &= \frac{1}{2} \int_{U(d)} f(U) + f(e^{\frac{i\pi}{r-s}} U)\, dU \\ &= \frac{1}{2} \int_{U(d)} f(U) - f(U)\, dU \\ &= 0 \end{aligned}$$

∎

The average of any polynomial with degrees in U and U^* less than t can be evaluated one summand at a time using a t-design by Proposition 2.4 or set to zero by Proposition 2.6. Note that using a t-design to evaluate $f \in \mathrm{Hom}(r, s)$ with $r \neq s$ will not always yield zero. Thus we must set such terms to zero by Proposition 2.6.

If we have a polynomial $f(U_1, ..., U_n)$ of several independent variables $U_1, ..., U_n \in U(d)$ then we can evaluate the average over all of them by computing the averages over one variable at a time:

$$\int_{U(d)} \cdots \int f(U_1, ..., U_n) dU_1 ... dU_n = \sum_{U_1 \in X} ... \sum_{U_n \in X} w(U_1) ... w(U_n) f(U_1, ..., U_n)$$

Where $X \subset U(d)$ is a t-design and f has degree $s_i \leq t$ in each U_i and U_i^* with $1 \leq i \leq n$. Therefore, definition 2.2 is general enough for applications.

2.3 Tensor product definition and existence of unitary t-designs

The downside of definition 2.2 is that it is not very easy to check if a given $X \subset U(d)$ can form a t-design. In particular, to verify that X is a t-design we would need to prove that it evaluates to the integral of each function in $Hom(t, t)$. For the most naive approach to this, we would need to know the average of all the functions we are trying to use t-designs to evaluate. Thus, we need an alternative definition.

Definition 2.7 (Tensor product definition of unitary t-designs) *A tuple (X,w) with finite $X \subset U(d)$ and weight function w on X is a* unitary t-design *if*

$$\sum_{U \in X} w(U) U^{\otimes t} \otimes (U^*)^{\otimes t} = \int_{U(d)} U^{\otimes t} \otimes (U^*)^{\otimes t} dU \tag{5}$$

This definition is much more tractable for verification and the literature has explicit formula for the RHS for many choices of t and d [Col03, CS06]. The equivalence of the two definitions is not self-evident, and we provide a proof:

Proposition 2.8 (Equivalence of definitions) *Definitions 2.2 and 2.7 are equivalent.*

Proof ($\Rightarrow$) It is easy to see that def. 2.2 implies def. 2.7 because $U \mapsto U^{\otimes t} \otimes (U^*)^{\otimes t}$ is in $\mathrm{Hom}(t, t)$. Hence, any (X, w) that satisfies the former definition, will also satisfy the latter.

($\Leftarrow$) For the reverse direction, we need to understand arbitrary functions in $\mathrm{Hom}(t, t)$ in terms of their arguments. It is easiest to do this by considering an arbitrary element $e(f(U))$ given a specific function $f \in \mathrm{Hom}(t, t)$ and input unitary $U \in U(d)$. In general, e can be written in terms of elements of U as:

$$e(f(U)) \quad = \sum_{\mu = \{(i_1, j_1), (k_1, l_1), ..., (i_t, j_t), (k_t, l_t)\}} v_\mu (U_{i_1, j_1} ... U_{i_t, j_t})(U^*_{k_1, l_1} ... U^*_{k_t, l_t}) \tag{6}$$

Where we have the indexes $1 \leq i, j, k, l \leq d$ and v_μ an arbitrary complex number that depends only on the particular choice of function f and not on U. Further, note that the product over elements of U for each μ will correspond to one entry in $U^{(t,t)} := U^{\otimes t} \otimes (U^*)^{\otimes t}$. Thus, we can talk about the entry $U^{(t,t)}_\mu$ and rewrite eq. 6 as:

$$e(f(U)) = \sum_\mu v_\mu U^{(t,t)}_\mu \tag{7}$$

Thus, we can think of $f \circ e$ as a linear function on a larger vector space that $U^{(t,t)}$ inhabits as a column vector. By linearity, we can find the average from eq. 7:

$$\langle f \circ e \rangle = \sum_\mu v_\mu \langle U^{(t,t)} \rangle_\mu \tag{8}$$

Since def. 2.7 ensures that $\langle U^{(t,t)} \rangle$ is a linear combination of design elements, everything else in eq. 8 is linear and commuting, and e is arbitrary, we can produce every term of the average for any function $f \in \mathrm{Hom}(t, t)$ as def. 2.2 requires. ∎

With this equivalence in hand, we can also prove that unitary t-designs exist in every dimension, by using a powerful theorem of Seymour and Zaslavsky [SZ84]:

Theorem 2.9 (Seymour and Zaslavsky 1984) *Let Ω be a path-connected topological space endowed with a measure $d\Omega$ with full support and normalized to unity and let $f : \Omega \to \mathbb{C}^{n\times m}$ be a continuous, integrable function. Then there exists a finite set $X \subseteq \Omega$ such that:*

$$\frac{1}{|X|}\sum_{x\in X} f(x) = \int_\Omega f(x)d\Omega$$

$|X|$ may be any number, with a finite number of exceptions.

From this result and definition 2.7, the existence of t-designs follows as a corollary:

Corollary 2.10 (Existence of designs) *A minimum unitary t-design $(X \subset U(d), w)$ exists for all $d, t \geq 1$.*

Proof Since $U(d)$ is a compact, topologically connected group we can set $\Omega = U(d)$ and $d\Omega = dU$ where dU is the normalized Haar measure on $U(d)$. Further, $U^{\otimes t} \otimes (U^*)^{\otimes t}$ is a polynomial in U and hence continuous and integrable, so we set $f = U \mapsto U^{\otimes t} \otimes (U^*)^{\otimes t}$ and it follows from thm. 2.9 that there exists a finite $X \subset U(d)$ that is a unweighted unitary t-design by def. 2.7. Since there are only a finite number of exceptions for the size of X there must be a minimum one. ∎

Our overall goal is to find constructions for these minimum designs (since our proof also shows that designs can be arbitrarily large) or bounds on their size. However, it would be advantageous to have a definition that not only tells us when something is a t-design but also how far a given set is from being a design. For this we will define approximate designs by building on definition 2.7 and prove the trace $2p$-sum inequality from which we can derive a metric definition.

2.4 Approximate unitary t-designs

Due to how hard designs are to construct, and how fast they increase in size as the dimensionality d and power t increase, it has been of paramount importance to discuss approximate designs. Most of the literature on approximate designs, usually deals with constructions and not bound. It it our goal to provide lower bounds on the size of not only actual designs, but also approximate ones.

Usually, the notion of an approximate design is introduces at the level of definition 2.7 and not definition 2.2 since for the latter we would need to renormalize by some norm of the function, while in the former we might only need to normalize by dimension (depending on our choice of norm). Since the literature does not yet have a widely accepted definition of approximate unitary t-designs we introduce one. Our definition is based on similar ones used for approximate quantum t-designs [AE07].

Definition 2.11 (Approximate unitary t-design) *A tuple (X,w) with finite $X \subset U(d)$ and weight function w on X is an* ϵ-approximate unitary t-design *if*

$$\| \sum_{U\in X} w(U)U^{\otimes t} \otimes (U^*)^{\otimes t} - \int_{U(d)} U^{\otimes t} \otimes (U^*)^{\otimes t} dU \| < \epsilon \tag{9}$$

A glaring omission in definition 2.11 is a specification of which norm to use on the left-hand side of eq. 9. There are many operator norms from which to chose, but in quantum information theory the important norms are the Schatten norms. In particular the trace (1-norm), Frobenius (2-norm), and spectral (∞-norm) norms are important. Of the above three norms, the most useful one is probably the spectral norm.

An alternative approach, is to formulate unitary t-designs as super-operators. For this approach we would have to provide a slight alternative to definition 2.7 in terms of super-operators. In this framework we can use either the trace super-operator norm, or the diamond norm [Kit97]. The diamond norm is of particular interest because it is the most useful for applications in quantum computing and cryptography. For future approaches we will concentrate on the diamond norm to generalize the constructions provided by Dankert et.al. [DCEL09] for 2-designs.

2.5 Implementation errors

As mentioned in the introduction, quantum circuits are constructed from a finite set of gates. Any transformation realized by a quantum circuit is an element of the group generated by this set of gates. Since the set is finite, it can only generate countable groups. The unitary group, however, is uncountable, thus any choice of gates will miss elements of $U(d)$. A gate set is universal if the group it generates is dense in $U(d)$, in simpler terms: if it can approximate any element of $U(d)$ to arbitrary precision [NC00]. It is important to understand the effect of such an error in implementation of a design element on the precision of the whole design:

Proposition 2.12 *If (X, w) is a unitary t-design and we implement each gate $U \in X$ imperfectly as U' with $\|U' - U\| = \epsilon$ then the resulting design will be ϵ^{2t}-approximate.*

Here, we assume that the norm of $\|U' - U\|$ and definition 2.11 are the same and fixed. We provide a sketch of the derivation:

Proof The first step is to consider what $\|U' - U\| \leq \epsilon$ means for ${U'}^{\otimes t} \otimes ({U'}^*)^{\otimes t}$:

$$\begin{aligned}\|{U'}^{\otimes t} \otimes ({U'}^*)^{\otimes t} - U^{\otimes t} \otimes (U^*)^{\otimes t}\| &\leq \|(U' - U)^{\otimes t} \otimes ((U' - U)^*)^{\otimes t}\| \\ &\leq \|U' - U\|^{2t} \\ &\leq \epsilon^{2t}\end{aligned}$$

Now, we can consider the whole design:

$$\begin{aligned}\| \sum_{U \in X} w(U)(U^{\otimes t} \otimes (U^*)^{\otimes t} + {U'}^{\otimes t} \otimes ({U'}^*)^{\otimes t} - U^{\otimes t} \otimes (U^*)^{\otimes t}) - \int_{U(d)} U^{\otimes t} \otimes (U^*)^{\otimes t} dU\| \\ \leq \| \sum_{U \in X} w(U)({U'}^{\otimes t} \otimes ({U'}^*)^{\otimes t} - U^{\otimes t} \otimes (U^*)^{\otimes t})\| \\ \leq \epsilon^{2t}\end{aligned}$$

Where the first inequality comes from the triangle inequality and the assumption that (X, w) is a t-design. ∎

Proposition 2.12 allows us to bound the error of the implemented design based on the error of our implementation of the individual components.

3 Trace $2p$-sum inequality

A candidate for a metric classification is the trace double sum. In this section we will prove a general theorem relating the trace $2p$-sum of an arbitrary finite $X \subset U(d)$ and an integral with a direct combinatorial interpretation. This theorem generalized the previous trace double sum inequality [Wel74, Sco08, Kaz09].

Theorem 3.1 (Trace $2p$-sum inequality) *A tuple (X, w) is an ϵ-approximate unitary t-design (with respect to the Schatten $2p$-norm) if and only if*

$$\int_{U(d)} |tr(U)|^{2t}\, dU \leq \sum_{U_1,V_1,\ldots,U_p,V_p \in X} w(U_1)w(V_1)...w(U_p)w(V_p)|tr(U_1^* V_1 ... U_p^* V_p)|^{2t} \leq \int_{U(d)} |tr(U)|^{2t}\, dU + \epsilon^{2p}$$

Proof Consider an arbitrary finite $X \subset U(d)$ with a weight function w, define matrices S and Σ as:

$$S = \sum_{U \in X} w(U) U^{\otimes t} \otimes (U^*)^{\otimes t}$$
$$\Sigma = \int_{U(d)} U^{\otimes t} \otimes (U^*)^{\otimes t} dU$$

Now, consider the matrix $D = S - \Sigma$; observe that $D = 0$ if and only if X is a t-design and $\|D\|_{2p} \leq \epsilon$ if X is an ϵ-approximate t-design with respect to the Schatten $2p$-norm. If we consider the definition of the Schatten norm, we can see that for the even cases, we have:

$$\|D\|_{2p} = \sqrt[2p]{tr((D^* D)^p)}$$

Expanding:

$$\begin{aligned} tr((D^* D)^p) &= tr(((S^* - \Sigma^*)(S - \Sigma))^p) \\ &= tr((S^* S - \Sigma^* S - S^* \Sigma + \Sigma^* \Sigma)^p) \end{aligned} \tag{10}$$

Look at the four summands individually. For instance the fourth term in eq. 10 reduces to:

$$\begin{aligned} \Sigma^* \Sigma &= (\int_{U(d)} U^{\otimes t} \otimes (U^*)^{\otimes t} dU)^* (\int_{U(d)} V^{\otimes t} \otimes (V^*)^{\otimes t} dV) \\ &= \int_{U(d)} \int_{U(d)} ((U^*)^{\otimes t} \otimes U^{\otimes t})(V^{\otimes t} \otimes (V^*)^{\otimes t})\, dU dV \\ &= \int_{U(d)} \int_{U(d)} (UV^*)^{\otimes t} \otimes (U^* V)^{\otimes t}\, dU dV \end{aligned} \tag{11}$$

In general, the summands/integrands of all four terms in eq. 10 are the same as the integrand in eq. 11. However, instead of two integrals we have two sums (for the $\Sigma^* \Sigma$ term) or a sum and an integral (for the other two terms). A nice trick can be done with any term containing an integral, we will illustrate this with the $\Sigma^* \Sigma$ term. Define f as

$$f(V) = \int_{U(d)} (UV^*)^{\otimes t} \otimes (U^* V)^{\otimes t}\, dU$$

Clearly, $f(V)$ is the inner integral of eq. 11. No matter which unitary is selected for V the product $U^* V$ and UV^* will still equal each element of $U(d)$ exactly once as U varies through the whole group. This is easy to see since for every W in the group we have exactly one $U = VW$. Thus $f(U) = f(V)$ for all $V \in U(d)$. Hence, we have:

$$\begin{aligned}\Sigma^*\Sigma &= \int_{U(d)} f(V)dV \\ &= f(I)\int_{U(d)} dV \\ &= \int_{U(d)} U^{\otimes t}\otimes (U^*)^{\otimes t}\, dU \\ &= \Sigma\end{aligned}$$

We can repeat a similar argument for $\Sigma^* S$ and $S^*\Sigma$. Observe that by definition of weight function $\sum_{U\in X} w(U) = 1$, thus $f(I)\sum_{U\in X} w(U) = f(I)$. In general, this argument can be used to reduce the product of one or more Σ (or Σ^*) and any number of S (or S^*) to a single Σ. With this in mind, eq. 11 becomes:

$$\begin{aligned}tr((D^*D)^p) &= tr((S^*S-\Sigma)^p) \\ &= tr((S^*S)^p + \sum_{k=1}^{p}(-1)^k\binom{p}{k}\Sigma)) \\ &= tr((S^*S)^p) - tr(\Sigma) \end{aligned} \tag{12}$$

Noting that trace is linear, we see that:

$$\begin{aligned}tr(\Sigma) &= \int_{U(d)} tr(U^{\otimes t}\otimes (U^*)^{\otimes t})\, dU \\ &= \int_{U(d)} tr(U)^t tr(U^*)^t\, dU \\ &= \int_{U(d)} |tr(U)|^{2t} \end{aligned} \tag{13}$$

Similarly, we can expand the first term of eq. 12 as:

$$\begin{aligned}tr((S^*S)^p) &= \sum_{U_1,V_1,\ldots,U_p,V_p\in X} w(U_1)w(V_1)...w(U_p)w(V_p)tr(((U_1V_1^*)^{\otimes t}\otimes (U_1^*V_1)^{\otimes t})...((U_pV_p^*)^{\otimes t}\otimes (U_p^*V_p)^{\otimes t})) \\ &= \sum_{U_1,V_1,\ldots,U_p,V_p\in X} w(U_1)w(V_1)...w(U_p)w(V_p)tr((U_1V_1^*...U_pV_p^*)^{\otimes t}\otimes (U_1^*V_1...U_p^*V_p)^{\otimes t}) \\ &= \sum_{U_1,V_1,\ldots,U_p,V_p\in X} w(U_1)w(V_1)...w(U_p)w(V_p)|tr(U_1^*V_1...U_p^*V_p)|^{2t} \end{aligned} \tag{14}$$

■

To conclude the proof, we combine equations 12, 13 and 14, that the choice of X is arbitrary, $tr((D^*D)^p) \geq 0$ for all choices of X, and $tr((D^*D)^p) \leq \epsilon^{2p}$ iff X is an ϵ-approximate unitary t-design with respect to the $2p$-norm.

3.1 Metric definition and minimal unitary t-designs

As a corollary of theorem 3.1 we recover the trace double-sum inequality [Sco08, Kaz09] as the simplest case of $p = 1$ or the Frobenius norm:

Corollary 3.2 (Metric definition of unitary t-designs) *For all finite $X \subset U(d)$ we have*

$$\sum_{U,V\in X} w(U)w(V)|tr(U^*V)|^{2t} \geq \int_{U(d)} |tr(U)|^{2t}\, dU \tag{15}$$

With equality if and only if X is a t-design.

At first it might seem that corollary 3.2 is not much more tractable than definition 2.7. However, the RHS of the inequality 15 has a relatively simple combinatorial interpretation. We know that the RHS is the number of permutations of $\{1, ..., t\}$ with no increasing subsequences of order greater than d [DS94, Rai98]. Thus for $d \geq t$ it has a particularly simple form of $t!$. In general, we will call this number $\sigma_{(t,d)}$, σ_t, or just σ depending on the context.

Corollary 3.2 suggests an important definition:

Definition 3.3 *Given a finite $X \subset U(d)$ we call w a* minimal weight function *if for all other choices of weight function w' on X, we have:*

$$\sum_{U,V \in X} w(U)w(V)|tr(U^*V)|^{2t} \leq \sum_{U,V \in X} w'(U)w'(V)|tr(U^*V)|^{2t}$$

.

This allows us to introduce a third definition of unitary t-designs that eliminates the need of thinking of designs as tuples:

Definition 3.4 *A finite $X \subset U(d)$ is a* unitary t-design *if*

$$\sum_{U,V \in X} w(U)w(V)|tr(U^*V)|^{2t} = \int_{U(d)} |tr(U)|^{2t} \, dU$$

Where w is the minimal weight function on X.

X is called an unweighted t-design if the minimal weight function on X is the uniform distribution. In general, minimal weight functions are not unique unless we only consider minimal designs.

Definition 3.5 *A* minimal *(unweighted) t-design X is a t-design such that all $Y \subset X$ are not (unweighted) t-designs.*

This definition is particularly friendly since the property of minimality can be tested algorithmically. One approach is to considering all subsets of X and the minimal weight functions on them. A second (analytic) approach is possible by noticing an important relationship between minimal designs and minimal weight functions:

Theorem 3.6 (Equivalence of minimal designs and unique weight functions) *A t-design X is minimal if and only if it has a unique minimal weight function w.*

Proof ($\Rightarrow$) To prove the forward direction, we will consider the contrapositive: if there are two distinct minimal weight functions w and w' on X then X is not a minimal t-design. Let:

$$\alpha = \min_{U \in X} \frac{w'(U)}{w(U)}.$$

Let $Z = \{U \in X : w'(U) - \alpha w(U) = 0\}$. We know that $|Z| \geq 1$ since for $V = \text{argmin}_{U \in X} w'(U)/w(U)$ we will have $w'(V) - \alpha w(V) = 0$. Thus, $Y = X - Z \subset X$. We will now show that

$$w'' = \frac{w' - \alpha w}{1 - \alpha}$$

is a minimal weight function on Y. First, we check that w'' is indeed a weight function. Clearly, by our choice of α and Y we have $w(U) > 0$ for all $U \in Y$, and

$$\begin{aligned} \sum_{U \in Y} w''(U) &= \sum_{U \in X} \frac{w' - \alpha w}{1 - \alpha} \\ &= \frac{1}{1 - \alpha}\left(\sum_{U \in X} w' - \alpha \sum_{U \in X} w\right) \\ &= \frac{1 - \alpha}{1 - \alpha} = 1 \end{aligned}$$

By letting $\langle f \rangle_X^w$ be the average of $f \in \text{Hom}(t,t)$ over X with weight function w (the LHS of equation) we can show that for arbitrary $f \in \text{Hom}(t,t)$:

$$\begin{aligned}\langle f \rangle_Y^{w''} &= \frac{\langle f \rangle_X^{w'} - \alpha \langle f \rangle_X^w}{1-\alpha} \\ &= \frac{\langle f \rangle - \alpha \langle f \rangle}{1-\alpha} \\ &= \langle f \rangle\end{aligned}$$

Thus, (Y, w'') is a t-design. Since $Y \subset X$, X is not a minimal t-design.

($\Leftarrow$) For the other direction we will prove that if $(X,w), (Y,w')$ are t-designs such that $Y \subset X$ then there are infinitely many minimal weight functions on X.

Assuming that $w'(U) = 0$ for $U \notin Y$, let $w'' = pw + (1-p)w'$ for any choice of $p \in (0,1)$. Clearly, w'' is a minimal weight function on X. ∎

Thus, an analytic test is to show that there is only one minimum for the LHS of equation 15 as you optimize over w.

Sadly, a minimal t-design is not necessarily the minimum one mentioned in corollary 2.10. It is important to understand if there is a simple correspondence between minimal and minimum designs. In particular, if the two are one and the same, then minimum designs are as easy to find as arbitrary t-designs. In the more likely case where no simple correspondence exists, it is not even clear if there is an upper bound on the size of minimal designs for a given d and t.

Combining minimal weight functions and corollary 3.2 we can characterize unweighted t-designs in a particularly salient way. For shorthand, we introduce some notation:

Definition 3.7 *The* trace double sum *is a function* $\Sigma_2 : \mathbb{F}(U(d)) \mapsto \mathbb{R}^+$ *defined for finite* $X \subset U(d)$ *as:*

$$\Sigma_2(X) = \sum_{U,V \in X} w(U)w(V)|tr(U^*V)|^{2t}$$

Further, we introduce notation for the internal sum:

Definition 3.8 *The* contribution of U to X *is a function* $S : U(d) \times \mathbb{F}(U(d)) \mapsto \mathbb{R}^+$ *defined as:*

$$S(U;X) = \sum_{V \in X} w(V)|tr(U^*V)|^{2t}$$

This definition is useful since there exists a simple relation between S and Σ_2 given by:

$$\Sigma_2(X) = \sum_{U \in X} w(U)S(U;X) \tag{16}$$

It is easy to see that $S(U;X) \geq 0$ for all choices of U and X. For a set with a minimal weight function w, we can also derive a relation between S and w:

Lemma 3.9 *For a set* $X \subset U(d)$ *with minimal weight function* w*, and any pair of elements* $U, V \in X$*, if* $w(U) \geq w(V)$ *then* $S(U; X - \{U,V\}) \leq S(V; X - \{U,V\})$.

Proof Assume that $w(U) \geq w(V)$. Consider $\Sigma_2(X)$:

$$\Sigma_2(X) = w^2(U)d^{2t} + 2w(U)w(V)|tr(U^*V)|^{2t} + 2w(U)S(U;X-\{U,V\}) \tag{17}$$

$$= w^2(V)d^{2t} + 2w(V)w(U)|tr(V^*U)|^{2t} + 2w(V)S(V;X-\{U,V\}) \tag{18}$$

Now consider $\Sigma_2'(X)$ which uses an alternative weight function w' with the weights of U and V permuted:

$$\Sigma_2'(X) = w^2(V)d^{2t} + 2w(V)w(U)|tr(U^*V)|^{2t} + 2w(V)S(U; X - \{U, V\}) \tag{19}$$
$$= w^2(U)d^{2t} + 2w(U)w(V)|tr(V^*U)|^{2t} + 2w(U)S(V; X - \{U, V\}) \tag{20}$$

Since w was a minimal weight function on X, $\Sigma_2'(X) \geq \Sigma_2(X)$, taking the difference of equation 19 + 20 and equation 17 + 18, we have:

$$\begin{aligned}\Sigma_2'(X) - \Sigma_2(X) &= w(V)S(U; X - \{U, V\}) + w(U)S(V; X - \{U, V\}) \\ &\quad - w(U)S(U; X - \{U, V\}) - w(V)S(V; X - \{U, V\}) \\ &= (w(U) - w(V))S(V; X - \{U, V\}) \\ &\quad - (w(U) - w(V))S(U; X - \{U, V\}) \\ &\geq 0\end{aligned}$$

Thus, we can conclude that $S(U; X - \{U, V\}) \leq S(V; X - \{U, V\})$ ∎

This provides an important corollary for unweighted sets:

Proposition 3.10 *For a set $X \subset U(d)$ for which the uniform distribution is a minimal weight function, and all elements $U, V \in X$, $S(U; X) = S(V; X) \geq \int_{U(d)} |tr(U)|^{2t}\, dU$ with equality if and only if X is a t-design.*

Proof Consider any pair $U, V \in X$, since $w(U) \geq w(V)$ and $w(V) \geq w(U)$ by Lemma 3.9 we have $S(U; X - \{U, V\} = S(V; X - \{U, V\})$. Thus, we have:

$$\begin{aligned}S(U; X) &= \frac{1}{|X|}(d^{2t} + |tr(U^*V)|^{2t} + S(U; X - \{U, V\})) \\ &= \frac{1}{|X|}(d^{2t} + |tr(V^*U)|^{2t} + S(V; X - \{U, V\})) \\ &= S(V; X)\end{aligned}$$

By using eq. 16, cor. 3.2, and the fact we just observed, we have:

$$\begin{aligned}\Sigma_2(X) &= \frac{1}{|X|}\sum_{W \in X} S(W; X) \\ &= \frac{1}{|X|}\sum_{W \in X} S(U; X) \\ &= S(U; X) \\ &\geq \int_{U(d)} |tr(U)|^{2t}\, dU\end{aligned}$$

With equality if and only if X is a t-design. ∎

This allows the simpler definition:

Definition 3.11 (Metric definition for unweighted unitary t-designs) *A finite set $X \subset U(d)$ is an* unweighted unitary t-design *if*

$$\frac{1}{|X|}\sum_{U \in X} |tr(U)|^{2t} = \int_{U(d)} |tr(U)|^{2t}\, dU$$

Where we implicitly assumed that without loss of generality a design contains the identity element (this is verified by proposition 3.17).

3.2 Three basic symmetries of unitary t-designs

When studying any novel mathematical object it is often enlightening to understand the group of symmetries corresponding to the object. Symmetries often allow us to simplify proofs or make WLOG assumptions. In this subsection we study the symmetries of t-designs and how they can be used to expand designs.

Proposition 3.12 *If $X = \{U_1, ..., U_n\}$ is a t-design then $Y = \{e^{i\phi_1}U_1, ..., e^{i\phi_n}U_n\}$ is also a t-design for all $\phi_1, ..., \phi_n \in [0, 2\pi]$.*

This proposition can be seen as a consequence of Lemma 2.5 for all $f \in Hom(t, t)$, or we can prove it from definition 2.7:

Proof Consider the sum in equation 5 for Y:

$$\begin{aligned} S &= \sum_{k=1}^{n} w(U_k)(e^{i\phi_k}U_k)^{\otimes t} \otimes (e^{-i\phi_k}U_k^*)^{\otimes t} \\ &= \sum_{k=1}^{n} (e^{i\phi_k})^t (e^{-i\phi_k})^t w(U_k) U_k^{\otimes t} \otimes (U_k^*)^{\otimes t} \\ &= \sum_{k=1}^{n} w(U_k) U_k^{\otimes t} \otimes (U_k^*)^{\otimes t} \end{aligned} \tag{21}$$

Clearly, equation 21 is just the sum in equation 5 for X. ∎

If we chose $(e^{i\phi_k})^d = \overline{det(U_k)}$ then we have a map $U(d) \to SU(d)$. In general, we can also simply define an equality class over phase, giving us a map $U(d) \to PU(d)$. This gives us an important corollary:

Corollary 3.13 *If we have a t-design X then we can always assume $X \subset PU(d) \subset SU(d) \subset U(d)$.*

For shorthand, we will represent rotating the k-th element of a set X by a phase θ as $P_{\theta,k}(X)$.

Proposition 3.14 *If (X, w) is a t-design then $(X^* = \{U^* : U \in X\}, w)$ is also a t-design.*

Proof Consider the sum in inequality 15 for the set X^*:

$$\begin{aligned} S &= \sum_{U,V \in X^*} w(U)w(V)|tr(U^*V)|^{2t} \\ &= \sum_{U^*,V^* \in X} w(U)w(V)|tr(U^*V)|^{2t} \\ &= \sum_{U,V \in X} w(U)w(V)|tr(UV^*)|^{2t} \\ &= \sum_{V,U \in X} w(V)w(U)|tr(V^*U)|^{2t} \end{aligned} \tag{22}$$

Clearly, equation 22 is the sum over X in inequality 15. ∎

Shorthand for inverting every element in a set X will be $\mathrm{Inv}(X)$.

Since trace is invariant under transpose, the above proof also shows that t-designs are invariant under complex conjugate. Combining this with the phase property, we can define a complex field transformation.

Definition 3.15 *A* reflection through θ *is a transformation $R_\theta : \mathbb{C} \to \mathbb{C}$ for $\theta \in [0, 2\pi]$ such that $R_\theta(re^{i\phi}) = re^{i(\theta+(\theta-\phi))}$*

We can abuse the above notation by writing $R_\theta(U)$ for a matrix U as shorthand for applying $R_\theta(U_{ij})$ to each element of U and $R(X)$ for a set X of matrices as applying R_θ (with arbitrary θ) to the elements of X.

Corollary 3.16 *If (X, w) is a t-design then so is $(R(X), w)$*

Proposition 3.17 *If $(X \subset U(d), w)$ is a t-design then $\forall M \in U(d), MX = \{MU : U \in X\}$ is also a t-design with the minimal weight function $w'(U) = w(M^{-1}U)$.*

PROOF Consider the sum over MX in inequality 15:

$$\begin{aligned} S &= \sum_{U,V \in MX} w'(U)w'(V)|tr(U^*V)|^{2t} \\ &= \sum_{U,V \in X} w'(MU)w'(MV)|tr((MU)^*(MV))|^{2t} \\ &= \sum_{U,V \in X} w(U)w(V)|tr(U^*V)|^{2t} \end{aligned} \tag{23}$$

Clearly, equation 23 is the sum over X in the inequality 15. ∎

A similar argument can be used for multiplication on the right.

Proposition 3.18 *If $X \subset U(d)$ is a t-design then $\forall M \in U(d), XM = \{UM : U \in X\}$ is also a t-design with the same proper weight function w.*

Combining both left and right multiplication of a set X we can write ${}_UM_V(X)$ for UXV. Using $U = P^*$ and $V = P$ we get the change of basis:

Corollary 3.19 *If $X \subset U(d)$ is a t-design then $\forall P \in U(d), [X]_P = \{P^*UP : U \in X\}$ is also a t-design with the same proper weight function w.*

We can also combine Proposition 3.14 and 3.17 to draw a curious corollary.

Corollary 3.20 *If $X \subset U(d)$ is a t-design then $\forall M \in U(d), X_M = \{U : V \in X,\ UV = M\}$ is a t-design with the same proper weight function w.*

PROOF An equivalent definition of X^* from Proposition 3.14 is $X^* = \{U : V \in X,\ UV = I\}$. Now, consider MX^* which we can define as:

$$\begin{aligned} MX^* &= \{MU : V \in X,\ UV = I\} \\ &= \{U : V \in X,\ UV = M\} \\ &= X_M \end{aligned}$$

∎

Together, the symmetries we found form a group H generated by $\langle R_{\theta,k}, {}_UM_V, \text{Inv}\rangle$. A more elegant, albeit more sophisticated, approach to finding H is possible. We can see Proposition 3.12 as a consequence of Lemma 2.5 - a property of all $f \in \text{Hom}(t, t)$. Propositions 3.14, 3.17, and 3.18 can be seen as a consequence of the compactness of $U(d)$. In particular, by a significantly more sophisticated argument in representation theory, we can conclude that for a Haar measure μ on a compact group G, any measurable $S \subseteq G$, and any $g \in G$ we have $\mu(S) = \mu(gS) = \mu(Sg) = \mu(S^{-1})$. Regardless of the approach, an important question is if there is a strictly larger group G such that for all t-designs X and $g \in G$ the set $g(X)$ is also a t-design. Stated in a simpler form: is H the complete set of symmetries for t-designs?

Even without an answer to this question we can expand beyond corollary 2.10 and use the above symmetries to constructively show that t-designs are not unique and can be arbitrarily large.

Lemma 3.21 *If $(X, w_X), (Y, w_Y)$ are two t-designs then so is $X \cup Y$ with some proper weight function w.*

PROOF Let $Z = X \cap Y$, $X' = X - Z$, and $Y' = Y - Z$. From equation 5 we have:

$$
\begin{aligned}
S &= \int_{U(d)} U^{\otimes t} \otimes (U^*)^{\otimes t} dU \\
&= \sum_{U \in X'} w_X(U) U^{\otimes t} \otimes (U^*)^{\otimes t} + \sum_{U \in Z} w_X(U) U^{\otimes t} \otimes (U^*)^{\otimes t} \\
&= \sum_{U \in Y'} w_Y(U) U^{\otimes t} \otimes (U^*)^{\otimes t} + \sum_{U \in Z} w_Y(U) U^{\otimes t} \otimes (U^*)^{\otimes t}
\end{aligned}
$$

and thus we can choose an arbitrary $p \in (0,1)$ and generate a new proper weight function w:

$$
w(U) = \begin{cases} p w_X(U) & \text{if} U \in X' \\ (1-p) w_Y(U) & \text{if} U \in Y' \\ p w_X(U) + (1-p) w_Y(U) & \text{if} U \in Z \end{cases}
$$

Clearly, this will complete our new design. ∎

In the special case of two unweighted designs X, Y such that $X \cap Y = \emptyset$, we can select $p = \frac{|X|}{|X|+|Y|}$ to make a new unweighted design $X \cup Y$.

The symmetries in the section alongside lemma 3.21 concretize the results of corollary 2.10 and show that t-designs can be arbitrarily large.

3.3 Group t-designs

Another approach to working with theorem 3.1 is to simplify it by considering group designs.

Definition 3.22 (Group t-design) *A pair (G, ρ) with a finite group G and unitary representation ρ of G is a* group t-design *if $\rho(G)$ is a t-design.*

The interest in group designs stemps from a practical consideration: most designs that have been found are group designs [RS09]. Definition 3.22 can be made stricter, in particular it is easy to show that if this definition holds, then we can assume that $\rho(G)$ is an unweighted t-design.

Proposition 3.23 *If (G, ρ) is a t-design then $\rho(G)$ is an unweighted unitary t-design.*

Proof Assume that $(\rho(G), w)$ is not an unweighted design. Then there exists two $U, V \in \rho(G)$ such that $w(U) < \frac{1}{|\rho G|} < w(V)$. Consider the set $X = VU^{-1}\rho(G)$, by prop. 3.17 we know that X is a t-design with weight function $w'(W) = w(UV^{-1}W)$. However, since $\rho(G)$ forms a group, we know that $X = \rho(G)$, thus we have the same set with two weight functions w and w'. Using the same arguments as in the proof of thm. 3.6 we can see that $w'' = pw + (1-p)w'$ is also a minimal weight function for any $p \in [0,1]$. Since $w(U) < \frac{1}{|\rho(G)|} < w'(U)$ we can chose a p such that $w''(U) = \frac{1}{|\rho(G)|}$. The choice of U,V,w, and w' was arbitrary, so we can repeat until we have the uniform weight function. ∎

This allows us to simplify the $2p$-sum to a single sum and use it as a definition that extends to approximate designs with respect to $2p$-norm:

Definition 3.24 (Approximate group t-design) *A pair (G, ρ) with a finite group G and unitary representation ρ of G is an* ϵ-approximate group t-design *with respect to the Schatten $2p$-norm if*

$$
\sigma \leq \frac{1}{|G|} \sum_{g \in G} |\chi_\rho(g)|^{2t} \leq \sigma + \epsilon^{2p} \tag{24}
$$

This definition provides a nice simplification of theorem 3.1 for the case of group designs. However the validity of equation 24 and thus equivalence of definitions 3.22 and 3.24 must be proved:

PROOF Since ρ is a homomorphism, we know that $|G| = |\text{Ker}(\rho)||\rho(G)|$ and for every $U \in \rho(G)$ we have exactly $|\text{Ker}(\rho)|$ many $g \in G$ such that $\rho(g) = U$. Noting that χ_ρ is tr, we can rewrite the summation in the middle of eq. 24 as:

$$\frac{1}{|\text{Ker}(\rho)||\rho(G)|} \sum_{U \in \rho(G)} |\text{Ker}(\rho)||tr(U)|^{2t} = \frac{1}{|\rho(G)|} \sum_{U \in \rho(G)} |tr(U)|^{2t} \tag{25}$$

Now, let us apply thm. 3.1 to def. 3.22 assuming that $\rho(G)$ is an unweighted design by prop. 3.23:

$$\int_{U(d)} |tr(U)|^{2t}\, dU \leq \frac{1}{|\rho(G)|^{2p}} \sum_{U_1, V_1, \ldots, U_p, V_p \in \rho(G)} |tr(U_1^* V_1 ... U_p^* V_p)|^{2t} \leq \int_{U(d)} |tr(U)|^{2t}\, dU + \epsilon^{2p} \tag{26}$$

Consider the inner-most sum (over $V_p \in \rho(G)$) with $U_1, V_1 ..., U_p$ fixed. Let $W = U_1^* V_1 ... U_p^*$ Since all the elements are in $\rho(G)$, so is W. The inner sum becomes:

$$\sum_{V_p \in \rho(G)} |tr(W V_p)|^{2p}$$

Since $W \in \rho(G)$ the sum is the same for all choices of W we can rewrite the middle term of eq. 26 as:

$$\frac{|\rho(G)|^{2p-1}}{|\rho(G)|^{2p}} \sum_{V_p} |tr(V_p)|^{2p}$$

This is the same as eq. 25 and thus eq. 24 and def. 3.24 follow. ∎

A nice feature about definition 3.24 is that it allows us to show that ρ has to be an irreducible representation:

Proposition 3.25 *If (G, ρ) is a group design then ρ is irreducible representation and if ρ is an irreducible unitary representation of a finite group G then (G, ρ) is a 1-design.*

PROOF This results follows from a lemma in representation theory (see, for instance theorem A2.3 in [NC00]) that states that ρ is an irreducible representation of G if and only if:

$$\frac{1}{|G|} \sum_{g \in G} |\chi_\rho(g)|^2 = 1 \tag{27}$$

This also happens to be the condition for G being a 1-design concluding the reverse direction. For the forward direction, note that by prop. 2.4 every t-design is a 1-design. ∎

4 Structure of unitary t-designs

In this section we study the structure of unitary t-design and the implications of these structures for lower bounds. We classify 1-designs and show a relation between t-design and bases of specific spaces. We report a novel conjecture and its implications for lower bounds.

4.1 Simple lower bounds for the Frobenius norm

In this subsection we generalize our earlier lower bounds [Kaz09] to the case of ϵ-approximate unitary t-designs with respect to the Frobenius norm. We present our proof in a much more compact form, without resorting to convoluted 'greedy algorithms' that we relied on earlier.

Proposition 4.1 (Simple lower bounds) *If $(X \subset U(d), w)$ is an ϵ-approximate unitary t-design with respect to the Frobenius norm, then $|X| \geq \frac{d^{2t}}{\sigma+\epsilon^2}$.*

Proof To prove this theorem we will consider how quickly we can reduce Σ_2 below $\sigma + \epsilon^2$. By cor. 3.2 we know that if $\Sigma_2(X) > \sigma + \epsilon^2$ then X is not an ϵ-approximate design with respect to the Frobenius norm. Let's use this:

$$\begin{aligned} \Sigma_2(X) &= \sum_{U \in X} w(U) S(U; X) \\ &\geq \sum_{U \in X} (w(U))^2 d^{2t} \end{aligned} \tag{28}$$

Clearly, eq.

is minimized by the uniform distribution, so we can conclude:

$$\Sigma_2(X) \geq \frac{d^{2t}}{|X|} > \sigma + \epsilon^2$$

Thus, X is definitely not a t-design if $|X| < \frac{d^{2t}}{\sigma+\epsilon^2}$. ∎

The bounds of proposition 4.1 look too high to be meaningful, but this is mostly due to the fact that the Frobenius norm is very sensitive to the dimensionality of the space. In particular, to be more realistic, we would have to account for the fact that ϵ^2 goes as the dimensionality of the space, d^{2t}, and thus, a more realistic way to write down the bound is:

$$|X| \geq \frac{d^{2t}}{\sigma + \varepsilon^2 d^{2t}}$$

For fixed t and large d this bound is approximately $\frac{1}{\varepsilon^2}$. The independence from dimension and t-ness suggests that the Frobenius norm is not the best norm to use for approximate designs.

4.2 Orthonormal bases for $\mathbb{C}^{d\times d}$ are 1-designs

Let $\mathbb{C}^{d\times d}$ be the space of all d-by-d matrices with complex entries. Clearly, this is a vector space over $\mathbb{C}$. To make it into an inner product space, we will define the trace inner product:

$$\langle M|N\rangle = \frac{tr(M^* N)}{d}$$

With this definition, it is clear that all unitaries have norm 1. Our goal becomes to find an orthonormal basis $|E_1\rangle, ..., |E_{d^2}\rangle$ of $\mathbb{C}^{d\times d}$ such that each $E_i \in U(d)$.

At first it might not seem obvious that we can find *any* basis of unitaries; but we can easily dispel such thoughts. Consider the standard basis $\{|E^{ij}\rangle\}$ of matrices that are 0 everywhere except a 1 in the i-th row and j-th column. These are clearly not unitary.

Let P^{ij} be the matrix that permutes the i-th and j-th columns of the identity. In a similar fashion, let P^{-ij} be P^{ij} with the entry in the $j-th$ column changed to a -1. Both P^{ij} and P^{-ij} are unitary

matrices and $E^{ij} = \frac{P^{ij} - P^{-ij}}{2}$. Thus $\{P^{ij}, P^{-ij} : 1 \leq i, j \leq d\} \subset U(d)$ spans $\mathbb{C}^{d\times d}$. By eliminating the linearly dependent ones we form a basis of unitaries. This is not the only basis possible, but it shows that it is not hard to find some basis - now, we just want to find an orthonormal one. The importance of unitary orthonormal bases is in their relation to 1-designs:

Proposition 4.2 *For any $X \subset U(d)$, X is a unitary orthonormal basis of $\mathbb{C}^{d\times d}$ if and only if X is a minimum unweighted 1-design.*

PROOF ($\Rightarrow$) X is a unitary orthonormal basis of $\mathbb{C}^{d\times d}$, consider the contribution of each $U \in X$ to X:

$$S(U; X) = \frac{1}{|X|} \sum_{V \in X} |tr(U^* V)|^2$$

Since X is orthonormal basis, for all $U \neq V$ the trace is zero. Thus, $S(U; X) = \frac{d^2}{|X|}$. From this we can calculate $\Sigma(X) = \frac{d^2}{|X|}$ by equation 16 or Proposition 3.10. We get $\Sigma(X) = 1$ and by cor. 3.2 X is a 1-design. Further, by the bounds in Proposition 4.1 X is a minimum unweighted 1-design.

($\Leftarrow$) If X is a minimum unweighted 1-design then by Proposition 3.10 we have $S(U; X) = 1$ for all $U \in X$. Rewriting the definition of $S(U; X)$ in a more suggestive form:

$$S(U; X) = \frac{1}{|X|} |tr(U^* U)|^2 + S(U; X - \{U\}) = 1$$

By the $\Rightarrow$ part of this proof we know Proposition 4.1 is tight for 1-designs. Thus $|X| = d^2$ and $S(U; X - \{U\}) = 0$. Since every term in $S(U; X - \{U\})$ is greater than or equal to zero, we must have each term equal to zero. Thus, $tr(U^* V) = 0$ for all $U, V \in X$ with $U \neq V$ and $|X| = d^2$. ∎

Proposition 4.2 provides an interesting relationship between minimum 1-designs and orthonormal bases of $\mathbb{C}^{d\times d}$, supporting the intuitive notion that the elements of a t-design must be evenly/well 'spread' out.

A subtle part of Proposition 4.2 is that it is prefaced on the existence of unitary orthonormal bases. It might seem obvious since *a priori* we know that there must be some orthonormal bases of $\mathbb{C}^{d\times d}$. However, our basis is restricted to elements from $U(d)$, thus we have to prove that there exist such sets for every d. Here, we present more than a proof - a simple construction - for the existence of such bases. For our construction, we need to introduce the basic ideas of mutually unbiased bases (MUBs).

Definition 4.3 (Mutually unbiased bases) *Two orthonormal bases $\{|e_i\rangle : 1 \leq i \leq d\}$ and $\{|e'_i\rangle : 1 \leq i \leq d\}$ of $\mathbb{C}^d$ are* mutually unbiased *if $|\langle e_i | e'_j \rangle|^2 = \frac{1}{d}$ for all $1 \leq i, j \leq d$.*

A current open question is to determine the maximum number $\mathfrak{M}(d)$ of pairwise mutually unbiased bases for $\mathbb{C}^d$. If we write the prime decomposition of $d = p_1^{n_1} ... p_k^{n_k}$ such that $p_i^{n_i} \leq p_{i+1}^{n_{i+1}}$ then $p_1^{n_1} + 1 \leq \mathfrak{M}(d) \leq d + 1$. In particular, for our purposes it is important that $\mathfrak{M}(d) \geq 2$ for all $d \geq 1$ and that without loss of generality, we can assume one of the bases to be the standard basis.

Theorem 4.4 (Construction for 1-designs) *For every $d \geq 1$ there is an orthonormal bases $X \subset U(d)$ of $\mathbb{C}^{d\times d}$.*

PROOF Let $|e_1\rangle ... |e_d\rangle$ be an orthonormal basis of $\mathbb{C}^d$ that is mutually unbiased with the standard basis. Thus, for every entry e_{ij} of $|e_i\rangle$ we have $|e_{ij}|^2 = \frac{1}{d}$. Let $I_i = \sqrt{d}\ \mathrm{diag}(|e_i\rangle)$ be a diagonal matrix with diagonal entries corresponding to the elements of $\sqrt{d}|e_i\rangle$. Since I_i is diagonal and every entry has norm 1 we have a unitary matrix. Further, we have:

$$tr(I_i^* I_j) = d\langle e_i | e_j \rangle \tag{29}$$

Now, consider the cyclic permutation group of order d, represented as d-by-d matrices: $C^1 ... C^d$ where $C^d = C^0 = I$. Since the cyclic permutation matrices are all unitary, we have $(C^m)^* = C^{d-m}$ for all $1 \leq m \leq d$. Now, define $C_i^m = C^m I_i$. For any tuple $1 \leq i, j, m, n \leq d$ we have:

$$(C_i^m)^* C_j^n = I_i^* C^{d-m+n} I_j$$

If $m = n$ then this simplifies to $I_i^* I_j$. By equation 29 we know that that the trace is not equal to zero only if $i = j$.

If $m \neq n$ then $C^{d-m+n} = C^r$ for some $1 \leq r < d$. Since the cyclic permutations have no fixed points, we know that the diagonal entries of C^r will be zero. Thus trace will always be zero.

If we set $X = \{C_i^m : 1 \leq i, m \leq d\}$ then we have an orthonormal basis of unitaries. ∎

As an example, we can consider $\mathbb{C}^{2\times 2}$. One choice of a basis of $\mathbb{C}^2$ unbiased with the standard basis is:

$$\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$$

This generates basis:

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\} \tag{30}$$

4.3 Spaces spanned by t-designs

In this section we generalize the relationship between designs and vector spaces suggested by proposition 4.2. To do so, we first provide the evaluation of a special integral as a lemma:

Lemma 4.5 *For any $V \in U(d)$ and a fixed $c \in \mathbb{C}$ independent of V, we have:*

$$\int_{U(d)} tr(U^{*\otimes t} V^{\otimes t}) U^{\otimes t} dU = cV^{\otimes t}$$

with $|c| \geq d^t$.

Proof Consider the following integral:

$$\int_{U(d)} tr(U^{*\otimes t} V^{\otimes t}) U^{\otimes t} V^{*\otimes t} dU = \int_{U(d)} tr((VU^*)^{\otimes t})(UV^*)^{\otimes t} dU$$

By the simple substitution $UV^* \mapsto U$ the integral simplifies to:

$$\int_{U(d)} tr(U^{*\otimes t}) U^{\otimes t} dU \tag{31}$$

Now, consider an arbitrary $W \in U(d)$ and conjugate eq. 31 by $W^{\otimes t}$:

$$\begin{aligned} W^{\otimes t} \int_{U(d)} tr(U^{*\otimes t}) U^{\otimes t} dU \; W^{*\otimes t} &= \int_{U(d)} tr(U^{*\otimes t} W^{*\otimes t} W^{\otimes t}) W^{\otimes t} U^{\otimes t} dU \; W^{*\otimes t} \\ &= \int_{U(d)} tr(W^{\otimes t} U^{*\otimes t}) U^{\otimes t} W^{*\otimes t} dU \\ &= \int_{U(d)} tr(U^{*\otimes t}) U^{\otimes t} dU \end{aligned}$$

Thus, the integral in eq. 31 commutes with all $W \in U(d)$ and must be proportional to the identity where the constant of proportionality c is independent of V. Further, note that if we used the inner-product $\langle M|N\rangle = \frac{tr(M^* N)}{d^t}$ then $U^{\otimes t}$ would have norm 1 and then the projection onto all the $U^{\otimes t}$ would have norm greater than or equal to 1. Thus $|c| \geq d^t$. ∎

We are pretty sure that the constant of proportionality is d^t but that specificity is irrelevant to the main result:

Theorem 4.6 (Spaces spanned by t-designs) *If X is a t-design then* $\text{span}(X) = \text{span}(\{U^{\otimes t} | U \in U(d)\})$.

PROOF Consider any $W \in \text{span}(\{U^{\otimes t} | U \in U(d)\})$. We can rewrite W as:

$$W = c_1 V_1^{\otimes t} + ... + c_n V_n^{\otimes t}$$

Where each $V_i \in U(d)$. By linearity, and lem. 4.5 we have:

$$\int_{U(d)} tr(U^{*\otimes t} W) U^{\otimes t} \, dU = cW \tag{32}$$

Since X is a t-design, we can replace the integral by a sum over the design:

$$\sum_{U \in X} w(U) tr(U^{*\otimes t} W) U^{\otimes t} = cW \tag{33}$$

Thus, any $W \in \text{span}(\{U^{\otimes t} | U \in U(d)\})$ is a linear combination of elements $U \in X$ with weights $c_U^W = \frac{w(U)}{c} tr(U^{*\otimes t} W)$. ∎

Note that this space is larger than $\mathbb{C}^{d \times d}$ since in general $U^{\otimes t} + V^{\otimes t} \neq (U+V)^{\otimes t}$. However, the space is smaller than $(\mathbb{C}^{d \times d})^{\otimes t}$ since $\text{span}(\{U^{\otimes t} | U \in U(d)\})$ has an extra symmetry that the larger space lacks. In particular, the standard basis for $(\mathbb{C}^{d \times d})^{\otimes t}$ cannot be generated. If we knew the dimensionality of $\text{span}(\{U^{\otimes t} | U \in U(d)\})$ then we would have another source of lower bounds. However, even without this knowledge we can use theorem 4.6 to produce fun corollaries. For instance, by combining proposition 3.25 with the restriction of theorem 4.6 to 1-designs we have a result for group designs:

Corollary 4.7 *Every unitary irreducible representation ρ of a finite group spans $\mathbb{C}^{d_\rho \times d_\rho}$.*

In general, we believe that analogous to proposition 4.2 there exist generalizations of 'orthonormal' bases to the space $\text{span}(\{U^{\otimes t} | U \in U(d)\})$ such that these bases are t-designs. Thus, our conjecture is:

Conjecture 4.8 ($|X| = \dim(\text{span}(\{U^{\otimes t} | U \in U(d)\}))$) *For a minimum t-design $X \subset U(d)$ we have $|X| = \dim(\text{span}(\{U^{\otimes t} | U \in U(d)\}))$.*

We can take the ideas of theorem 4.6 and use them to look at spaces spanned by subsets of designs:

Proposition 4.9 *If X is a unitary $(t+1)$-design, then for any $V \in X$ $\text{span}(X - \{V\}) = \text{span}(\{U^{\otimes t} | U \in U(d)\})$.*

PROOF Consider eq. 32 and 33 from before, except instead of having W arbitrary, use the $W = V^{\otimes t}$ from the theorem statement. From proposition 2.4 we know that X can serve as a t-design and hence replace the integral. Now, expand the sum:

$$\frac{d^t w(U)}{c} V^{\otimes t} + \sum_{U \in X - \{V\}} c_U^W U^{\otimes t} = W \tag{34}$$

By lem. 4.5 $|c| \geq d^t$ and $w(U) < 1$, thus $|\frac{d^t w(U)}{c}| < 1$ and $\sum_{U \in X - \{W\}} c_U^W U = \alpha W$ for some non-zero α. Thus, W is not linearly independent from $X - \{V\}$. ∎

Although proposition 4.9 only holds for unweighted designs, we are confident that the result can be generalized to weighted ones. In fact, our intuition is that a much stronger result holds:

Conjecture 4.10 (t-designs contain $(t-1)$-designs) *If X is a unitary t-design (with $t \geq 2$), then for any $V \in X$ there exists some $Y \subset X - \{V\}$ such that Y is a $(t-1)$-design.*

We still lack the mechanisms to relate subsets directly to $(t-1)$-designs. The missing step is showing that an appropriate type of basis for $\text{span}(\{U^{\otimes t} | U \in U(d)\})$ forms a t-designs. Of course, this result is far from trivial, and by itself provides a perfect characterization of t-designs (via conjecture 4.8). An alternative, would be to prove the conjecture directly, without making the basis connection.

5 Conclusion

Throughout this note, we introduced tools for working with and finding t-designs. We provided many definitions of designs, including the functional, tensor, and metric definition. We also studied approximate and group designs stressing connections to linear algebra. In applications, 2-designs are currently generating the most interest [Dan05, Sco08, DCEL09]. No applications are known for arbitrary t-designs. We outlined several directions in our current research. In particular, our primary goal is to study the connection between bases for spaces like $\text{span}(\{U^{\otimes t} | U \in U(d)\})$, t-designs, and the applications to lower bounds.

An important focus for future research is finding applications for arbitrary t-designs. We are confident that as researchers become more comfortable with random unitaries we will see more and more applications of t-designs to randomized quantum algorithms and codes. To help with this, it is important to find simple constructions for designs with any choice of t and d. The final goal, though, is a simple classification (if possible) of minimum designs.

References

[AE07] Andris Ambainis and Joseph Emerson. Quantum t-designs: t-wise independence in the quantum world. *Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity*, pages 129–140, 2007, arXiv:quant-ph/0701126.

[Col03] B. Collins. Moments and cumulants of polynomial random variables on unitary groups, the Itzykson-Zuber integral, and free probability. *International Mathematics Research Notices*, pages 953–982, 2003.

[CS06] B. Collins and P. Śniady. Integration with respect to the haar measure on unitary, orthogonal and symplectic group. *Communications in Mathematical Physics*, 264:773–795, 2006.

[Dan05] Christoph Dankert. Efficient simulation of random quantum states and operators. Master's thesis, University of Waterloo, 2005.

[DCEL09] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Physical Review A*, 80, 2009.

[DLT02] D.P. DiVincenzo, Debbie Leung, and B.M. Terhal. Quantum data hiding. *IEEE transactions on information theory*, 48, 2002.

[DS94] P. Diaconis and M. Shahshahani. On the eigenvalues of random matrices. *Journal of Applied Probability*, 31A:49–62, 1994.

[EWS+03] Joseph Emerson, Y.S. Weinstein, Marcos Saraceno, Seth Lloyd, and D.G. Cory. Psudo-random unitary operators for quantum information processing. *Science*, 303:2098–2100, 2003.

[HLSW04] Patrick Hayden, Debbie Leung, P.W. Shor, and Andreas Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics*, 250(2):371–391, 2004.

[Kaz09] Artem Kaznatcheev. Unitary t-designs. `http://www.cs.mcgill.ca/~akazna/AK_UnitaryDesigns20090929.pdf`, 2009.

[Kit97] A.Y. Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52:1191–1249, 1997.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2000.

[Rai98] E. M. Rains. Increasing subsequences and the classical groups. *Electronic Journal of Combinatorics*, 5:Research Paper 12, 9 pp., 1998.

[RS09] Aidan Roy and A.J. Scott. Unitary designs and codes. *Designs, Codes and Cryptography*, 53, 2009, arXiv:0809.3813v1.

[Sco08] A. J. Scott. Optimizing quantum process tomography with unitary 2-designs. *Journal of Physics A: Mathematical and Theoretical*, 41:055308 (26 pp.), 2008.

[SZ84] P.D. Seymour and T. Zaslavsky. Averaging sets: a generalization of mean values and spherical designs. *Advances in Mathematics*, 52:213–240, 1984.

[Wel74] W. Welch. Lower bounds on the maximum cross correlation of signals. *IEEE Transactions on Information Theory*, 20:397–399, 1974.