Unitary t-designs

Artem Kaznatcheev

September 29, 2009

Abstract

Unitary t-designs provide a method to simplify integrating polynomials of degree less than t over $U(d)$. We prove a classic result - the trace double sum inequality - and use it to derive the fundamental symmetries of t-designs. As an alternate approach to deriving an asymptotically tight lower bound on the size of t-designs, we introduce a greedy algorithm for constructing designs. Unfortunately, we also show that the most naive version of the algorithm cannot converge to an unweighted t-design. We observe the correspondence between unitary orthonormal bases for $\mathbb{C}^{d\times d}$ and 1-designs. As a sample application of 1-designs we evaluate the average of $U \mapsto U^*V^*UV$ for fixed $V \in U(d)$ and use it to prove that t-designs are non-commuting.

Contents

1 Introduction

In quantum mechanics, we represent a particle's state as a vector $|\psi\rangle \in \mathbb{C}^d$. 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 a particle 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 change a particle's state (with time for instance) 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. $U(d)$ 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 the remainder of the introduction we elaborate on what we mean by 'polynomials' and introduce our first two definitions of unitary t-designs. To show the generality of our first definition, we prove some basic facts about homogeneous polynomials. In section 2, we present a proof of the trace double-sum inequality, and use it to introduce a metric definition of t-designs. We further use the trace double-sum in section 3 to find symmetries of t-designs. We culminate the section with the definition of minimal designs and a classification of them in terms of their proper weight functions. Section 4 introduces a computation flavor by considering greedy 'algorithms' for constructing t-designs. We use our notion of greedy algorithms to find asymptotically tight lower bounds on the size of designs. Unfortunately, we conclude the section by proving that the most naive greedy algorithm can not converge to an unweighted t-design. Finally, in section 5 we synthesize some of our results in a sample application. We show that orthonormal bases for $C^{d\times d}$ are 1-designs and use a mutually unbiased basis of the standard basis in C^d to construct a 1-design. We resolve the section by evaluating the average commutator on $U(d)$ and using it to prove that t-designs are non-commuting.

1.1 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.

1.2 Two definitions of unitary t-designs

First we introduce an important component of designs:

Definition 1.1. 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 a simple definitions for designs:

Definition 1.2. 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 1.3. 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 1.4. *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 1.5. *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 1.6. *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 1.5 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 1.4 or set to zero by Proposition 1.6. 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 1.6.

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:

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

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 1.2 is general enough for applications.

However, the downside of definition 1.2 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 1.7. 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 [1, 2]. 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.

2 Trace double sum inequality

A candidate for a metric classification is the trace double sum. In this section we will prove an important theorem relating the trace double sum of an arbitrary finite $X \subset U(d)$ and an integral with a direct combinatorial interpretation.

Theorem 2.1. *For all finite $X \subset U(d)$ we have*

$$\sum_{U,V \in X} w(U)w(V)|tr(U^*V)|^{2t} \geq \int_{U(d)} |tr(U)|^{2t}\, dU \tag{6}$$

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

The proof is based on a bound of Welch [7] and the theorem has been proved earlier by Scott [6]. We include a more detailed proof:

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. Further D^*D will be positive semidefinite and thus $tr(D^*D) \geq 0$ with equality if and only if $D = 0$. This provides us with a nice notion (the Frobenius norm squared) of how far a given set X is from being a t-design. Expand:

$$\begin{aligned} tr(D^*D) &= tr((S^* - \Sigma^*)(S - \Sigma)) \\ &= tr(S^*S) - tr(\Sigma^*S) - tr(S^*\Sigma) + tr(\Sigma^*\Sigma) \end{aligned} \tag{7}$$

Since trace is linear it can be brought inside the sums and integrals (and past the weights) inside each summand. Further, since $tr(AB) = tr(BA)$ for all A and B, the traces inside the terms become identical functions f of the two matrices U and V, in particular they are:

$$\begin{aligned} f(U,V) &= tr((U^{\otimes t} \otimes (U^*)^{\otimes t})^* (V^{\otimes t} \otimes (V^*)^{\otimes t})) \\ &= tr((U^*V)^{\otimes t} \otimes (UV^*)^{\otimes t}) \\ &= tr((U^*V)^{\otimes t}) tr((UV^*)^{\otimes t}) \\ &= tr(U^*V)^t tr(UV^*)^t \\ &= |tr(U^*V)|^{2t} \end{aligned}$$

Consider the fourth summand $tr(\Sigma^*\Sigma)$:

$$tr(\Sigma^*\Sigma) = \int_{U(d)} \int_{U(d)} |tr(U^*V)|^{2t} dV\, dU$$

Let $f(U) = \int_{U(d)} |tr(U^*V)|^{2t} dV$ be the inner integral. No matter which unitary is selected for U the product U^*V will still equal each element of $U(d)$ exactly once as V varies through the whole group. This is easy to see since for every W in the group we have exactly one $V = UW$. Thus $f(U) = f(I)$ for all $U \in U(d)$. Hence, we have:

$$
\begin{aligned}
tr(\Sigma^*\Sigma) &= \int_{U(d)} f(U)dU \\
&= \int_{U(d)} f(I)dU \\
&= f(I)\int_{U(d)} dU \\
&= \int_{U(d)} |tr(V)|^{2t} dV
\end{aligned}
$$

We can repeat a similar argument for $tr(\Sigma^* S)$ and $tr(S^*\Sigma)$. Observe that by definition of weight function, $\sum_{U\in X} w(U) = 1$. Thus $f(I)\sum_{U\in X} w(U) = f(I)$. We conclude that $tr(\Sigma^* S) = tr(S^*\Sigma) = tr(\Sigma^*\Sigma)$. By combining equation 7 and the fact that $tr(D^*D) \geq 0$ we have:

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

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

At first it might seem that theorem 2.1 is not much more tractable than definition 1.7. However, the RHS of the inequality 6 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 [3, 4]. Thus for $d \geq t$ it has a particularly simple form of $t!$.

Theorem 2.1 suggests an important definition:

Definition 2.2. A tuple (X, w) with finite $X \subset U(d)$ and weight function w on X is a *proper pair* if for all other choices of weight function w' on X, we have:

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

.

In other words, to have a proper pair for a finite $X \subset U(d)$ we need to choose a weight function w such that the LHS of equation 6 is minimized. Equivalently:

Definition 2.3. A weight function w is a *proper weight function on* X if (X, w) is a proper pair.

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

Definition 2.4. 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 proper weight function on X.

X is called an unweighted t-design if the proper weight function on X is the uniform distribution.

3 Symmetries and minimal 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 section we study the symmetries of t-designs and how they can be used to expand designs. We conclude with a definition of minimal designs and a classification of them according to the uniqueness of their proper weight functions.

3.1 Three basic symmetries of t-designs

Proposition 3.1. *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 1.5 for all $f \in Hom(t, t)$, or we can prove it from definition 1.7:

Proof. Consider the sum in equation 5 for Y:

$$\begin{aligned} S &= \sum_{k=1}^{n} w(U_k)(e^{i\phi_k}U_k)^{\otimes t} \otimes (e^{-i\phi_k}U_k^*)^{\otimes t} \\ &= \sum_{k=1}^{n} (e^{i\phi_k})^t (e^{-i\phi_k})^t w(U_k) U_k^{\otimes t} \otimes (U_k^*)^{\otimes t} \\ &= \sum_{k=1}^{n} w(U_k) U_k^{\otimes t} \otimes (U_k^*)^{\otimes t} \end{aligned} \tag{8}$$

Clearly, equation 8 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 3.2. *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 3.3. *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 6 for the set X^*:

$$\begin{aligned} S &= \sum_{U,V \in X^*} w(U)w(V)|tr(U^*V)|^{2t} \\ &= \sum_{U^*,V^* \in X} w(U)w(V)|tr(U^*V)|^{2t} \\ &= \sum_{U,V \in X} w(U)w(V)|tr(UV^*)|^{2t} \\ &= \sum_{V,U \in X} w(V)w(U)|tr(V^*U)|^{2t} \end{aligned} \tag{9}$$

Clearly, equation 9 is the sum over X in inequality 6. □

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 3.4. 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 3.5. *If (X, w) is a t-design then so is $(R(X), w)$*

Proposition 3.6. *If $X \subset U(d)$ is a t-design then $\forall M \in U(d), MX = \{MU : U \in X\}$ is also a t-design with the same proper weight function w.*

Proof. Consider the sum over MX in inequality 6:

$$\begin{aligned} S &= \sum_{U,V \in MX} w(U)w(V)|tr(U^*V)|^{2t} \\ &= \sum_{U,V \in X} w(U)w(V)|tr((MU)^*(MV))|^{2t} \\ &= \sum_{U,V \in X} w(U)w(V)|tr(U^*V)|^{2t} \end{aligned} \tag{10}$$

Clearly, equation 10 is the sum over X in the inequality 6. □

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

Proposition 3.7. *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 3.8. *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 3.3 and 3.6 to draw a curious corollary.

Corollary 3.9. *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 3.3 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 3.1 as a consequence of Lemma 1.5 - a property of all $f \in \text{Hom}(t, t)$. Propositions 3.3, 3.6, and 3.7 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?

3.2 Growing non-minimal designs

However, even without an answer to this question we can use the above symmetries to show that t-designs are not unique.

Lemma 3.10. *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 3.10 show that t-designs can be arbitrarily large. This suggests an important definition:

Definition 3.11. 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 proper weight function on them. A second (analytic) approach is possible by noticing an important relationship between minimal designs and proper weight functions:

Theorem 3.12. *A t-design X is minimal if and only if it has a unique proper weight function w.*

Proof. ($\Rightarrow$) To prove the forward direction, we will consider the contrapositive: if there are two distinct proper 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 proper 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

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

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 proper 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 proper weight function on X. □

Thus, an analytic test is to show that there is only one minimum for the LHS of equation 6 as you optimize over w.

Sadly, a minimal t-design is not necessarily a minimum one. 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.

4 Greedy algorithms for building designs

To provide an alternate viewpoint on t-designs, we can try to tackle them from a more algorithmic framework. We can try to build designs by adding unitaries one at a time to a set until we reach equality in theorem 2.1. It is clear that there is *some* way to do this, the question becomes on how much we have to keep track of the as we progress. In particular, we can try to find a greedy algorithm that only considers the next element to add.

Due to the extensive amount of arithmetic in this section, we will define several convenient shorthands. We will also use some standard, but less common notation, such as $\mathbb{F}(X)$ - the set of all finite subsets of X.

Definition 4.1. The *trace double sum* is a function $\Sigma : \mathbb{F}(U(d)) \mapsto \mathbb{R}^+$ defined for finite $X \subset U(d)$ as:

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

The analogous concept for all of $U(d)$ can be defined as the integral $\int_{U(d)} |tr(U)|^{2t} dU$. From section 2, we know that this is simply the number of permutations of $\{1, ..., t\}$ with no increasing subsequences of order greater than d; thus for $d \geq t$ it has a particularly nice form of $t!$. We will call this limit σ for arbitrary d and t.

With this notation, we can succinctly rephrase theorem 2.1 as: for all finite $X \subset U(d)$, $\Sigma(X) \geq \sigma$ with equality iff X is a t-design.

This notation, also allows us to making the following observation (which we present as a lemma):

Lemma 4.2. *A finite $X \subset U(d)$ is a t-design if and only if for all finite $Y \subset U(d)$, $\Sigma(X) \leq \Sigma(X \cup Y)$*

Although the forward direction is obvious, for the reverse direction it is not obvious that any set can be extended to a t-design. Since such extensions are vital for greedy algorithms we include extension as a lemma.

Lemma 4.3. *For every finite $X \subset U(d)$ there is some t-design Z such that $X \subseteq Z$*

Proof. Let $Y \subset U(d)$ be some t-design (WLOG containing the identity matrix - by Proposition 3.6). Now consider the following set:

$$Z = \bigcup_{U \in X} UY$$

Clearly $X \subseteq Z$ and Z is a t-design by Proposition 3.6 and Lemma 3.10. □

However, for a greedy algorithm, it is impractical to consider all possible finite subsets. Thus, it would be more useful to classify t-designs in terms of the contributions of single unitaries.

Definition 4.4. 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 given by:

$$\Sigma(X) = \sum_{U \in X} w(U)S(U; X) \tag{11}$$

It is easy to see that $S(U; X) \geq 0$ for all choices of U and X.

4.1 A lower bound on the size of t-designs

If $U \in X$ then $S(U; X) \geq w(U)d^{2t}$ since then there must be a term $|tr(U^*U)|^{2t} = |tr(I)|^{2t} = d^{2t}$. This allows us to find a simple lower bound on the size of unweighted t-designs. From equation 11 and theorem 2.1 we have:

$$\sigma = \frac{1}{|X|}\sum_{U\in X} S(U;X)$$
$$\geq \frac{d^{2t}}{|X|}$$

Thus, we have a simple lower bound:

Lemma 4.5. *If $X \subset U(d)$ is an unweighted t-design then $|X| \geq \frac{d^{2t}}{\sigma}$*

The total amount a given unitary $U \in X$ contributes to $\Sigma(X)$ can be given by:

$$d^{2t} + 2S(U; X - \{U\})$$

Where the d^{2t} term comes from the $tr(U^*U)$ term. This suggests a tempting greedy 'algorithm'. For each set X that is not yet a t-design, select a $U \in U(d)$ that minimizes $S(U;X)$ and let $X' = X \cup \{U\}$ with $w'(U) = p$ and for $V \in X$, $w'(V) = (1-p)w(V)$. Then the new trace double sum is:

$$\Sigma(X') = (1-p)^2\Sigma(X) + p^2 d^{2t} + 2p(1-p)S(U;X)$$

To minimize $\Sigma(X')$ we need:

$$p = \frac{\Sigma(X) - S(U;X)}{\Sigma(X) - 2S(U;X) + d^{2t}} \tag{12}$$

Thus, we can express $\Sigma(X')$ in terms of $\Sigma(X)$ and $S(U;X)$ as:

$$\begin{aligned}\Sigma(X') &= \Big(\frac{d^{2t} - S(U;X)}{\Sigma(X) - 2S(U;X) + d^{2t}}\Big)^2 \Sigma(X) \\ &\quad + \Big(\frac{\Sigma(X) - S(U;X)}{\Sigma(X) - 2S(U;X) + d^{2t}}\Big)^2 d^{2t} \\ &\quad + 2\frac{(d^{2t} - S(U;X))(\Sigma(X) - S(U;X))}{(\Sigma(X) - 2S(U;X) + d^{2t})^2} S(U;X) \\ &= \frac{d^{2t}\Sigma(X) - S^2(U;X)}{\Sigma(X) - 2S(U;X) + d^{2t}}\end{aligned} \tag{13}$$

The danger with this scheme is that the weight function w' might not be a proper weight function for X'. Although it optimizes the contribution of $S(U;X)$ by adjusting weights in w we might be able to lower the value of $S(U;X)$ at the expense of raising the value of $\Sigma(X)$ instead. However, if we assume the minimal value of $S(U;X) = 0$ then this problem disappears and w' is a proper weight function. It is clear that any t-design will have at least as many elements as one where all contributions $S(U;X)$ in our algorithm are zero. We can use this observation to generalize Lemma 4.5:

Proposition 4.6. *If $X \subset U(d)$ is a t-design then $|X| \geq \frac{d^{2t}}{\sigma}$.*

Proof. Consider our algorithm with the best case of $S(U_k; X_k) = 0$ for every time step k:

$$\Sigma(X_{k+1}) = \frac{d^{2t}\Sigma(X_k)}{\Sigma(X_k) + d^{2t}}$$

With $\Sigma(X_1) = d^{2t}$ since $\Sigma(X) = d^{2t}$ for any singleton X. Rewriting this recurrence with simpler variables:

$$v_{k+1} = \frac{Dv_k}{v_k + D}$$

With $v_1 = D$. Consider $y_k = kv_k$ with $D_y = cD$ and $y_1 = cD$ then

$$\begin{aligned} y_{k+1} &= \frac{cDy_k}{y_k + cD} \\ &= \frac{c^2 D v_k}{c(v_k + D} \\ &= cv_{k+1} \end{aligned}$$

Thus, we can rescale the recurrence by any constant c while leaving it essentially unchanged. We select $c = \frac{1}{D}$ to get the simple recurrence $x(1) = 1$ and:

$$x(k+1) = \frac{x(k)}{x(k)+1}$$

We want to find an analytic form for this recurrence. Consider $x(k) = \frac{1}{k}$, then $x(1) = 1$ and:

$$\begin{aligned} x(k+1) &= \frac{\frac{1}{k}}{\frac{1}{k}+1} \\ &= \frac{1}{k+1} \end{aligned}$$

Until $d^{2t}x(k)$ falls below the value σ we know that there is no possible way to construct a t-design X with $|X| \leq k$. Thus, we can conclude that $|X| \geq \frac{d^{2t}}{\sigma}$. □

Although this approach does not significantly extend the results of the simple Lemma 4.5 it does give us a hint at the potential power of thinking about greedy constructions of t-designs. Further, the results of Proposition 4.6 for fixed t agree asymptotically with the best known results of $|X| \in \Omega(d^{2t})$ [5].

4.2 Limitations of greedy algorithms

For a proper set (such that the choice of weights minimizes $\Sigma(X)$), we can also derive a relation between S and w.

Lemma 4.7. *For a proper $X \subset U(d)$, 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 $\Sigma(X)$:

$$\begin{aligned} \Sigma(X) &= w^2(U)d^{2t} + 2w(U)w(V)|tr(U^*V)|^{2t} + 2w(U)S(U; X - \{U, V\}) && (14) \\ &= w^2(V)d^{2t} + 2w(V)w(U)|tr(V^*U)|^{2t} + 2w(V)S(V; X - \{U, V\}) && (15) \end{aligned}$$

Now consider $\Sigma'(X)$ which permutes the weights of U and V:

$$\begin{aligned} \Sigma'(X) &= w^2(V)d^{2t} + 2w(V)w(U)|tr(U^*V)|^{2t} + 2w(V)S(U; X - \{U, V\}) && (16) \\ &= w^2(U)d^{2t} + 2w(U)w(V)|tr(V^*U)|^{2t} + 2w(U)S(V; X - \{U, V\}) && (17) \end{aligned}$$

Since X was proper, $\Sigma'(X) \geq \Sigma(X)$, taking the difference of equation 16 + 17 and equation 14 + 15, we have:

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

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

This provides an important corollary for proper unweighted sets.

Proposition 4.8. *For a proper unweighted $X \subset U(d)$, and all elements $U, V \in X$, $S(U;X) = S(V;X) \geq \sigma$ 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 4.7 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 equation 11, theorem 2.1, and the fact we just observed, we have:

$$\begin{aligned} \Sigma(X) &= \frac{1}{|X|}\sum_{W \in X} S(W;X) \\ &= \frac{1}{|X|}\sum_{W \in X} S(U;X) \\ &= S(U;X) \\ &\geq \sigma \end{aligned}$$

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

However, there are downsides to the greedy approach that must be overcome. In particular, it is very unlikely that the greedy algorithm as presented above (with only p adjustment and no w adjustment) can actually construct t-designs.

Theorem 4.9. *A p-adjustment greedy algorithm cannot construct an unweighted t-design.*

Proof. At the k-th time step, in order to produce an unweighted design, we must have $p = \frac{1}{k+1}$. Thus, using equation 12, we have the equality:

$$k + 1 = \frac{\Sigma(X_k) - 2S(U_k; X_k) + d^{2t}}{\Sigma(X_k) - S(U_k; X_k)}$$

At the next time step, we will have:

$$\begin{aligned} k + 2 &= \frac{\Sigma(X_{k+1}) - 2S(U_{k+1}; X_{k+1}) + d^{2t}}{\Sigma(X_{k+1}) - S(U_{k+1}; X_{k+1})} \\ &= \frac{2\Sigma(X_k) - 3S(U_k; X_k) + d^{2t}}{\Sigma(X_k) - S(U_k; X_k)} \end{aligned}$$

Solving for $S(U_{k+1}; X_{k+1})$ we get:

$$\frac{\Sigma(X_{k+1})(\Sigma(X_k) + 2d^{2t} - 2S(U_k; X_k)) - d^{2t}(\Sigma(X) - S(U_k; X_k))}{\Sigma(X_k) + d^{2t} - 2S(U_k; X_k)} \tag{18}$$

Combining equation 13 and 18, we can simplify:

$$S(U_{k+1}; X_{k+1}) = \frac{d^{2t}S(U_k; X_k) - S^2(U_k; X_k)}{\Sigma(X_k) + d^{2t} - 2S(U_k; X_k)} \tag{19}$$

Using the same rescaling tricks as in prop 4.6, we can rewrite the recurrences in equation 13 and 19 in a simpler form. We start with $x(1) = 1$ and $y(1) = q$ with $0 < q < 1$ and follow the two coupled recurrences:

$$x(k+1) = \frac{x(k) - y^2(k)}{x(k) - 2y(k) + 1}$$

$$y(k+1) = \frac{y(k) - y^2(k)}{x(k) - 2y(k) + 1}$$

There recurrences are related to our more familiar variables by $x(k) = \frac{\Sigma(X_k)}{d^{2t}}$ and $y(k) = \frac{S(U_k;X_k)}{d^{2t}}$. Thus, by Proposition 4.8 we know that for a proper t-design X_k we must have $x(k) = y(k)$. Define $z(k) = x(k) - y(k)$:

$$z(k+1) = \frac{z(k)}{z(k) - y(k) + 1}$$

Clearly, for our choice of initial parameters, $z(k)$ will be zero only in the limit as $k \to \infty$. □

Although it is disappointing that we cannot use such a simple greedy algorithm to build t-designs, the framework is still promising and merits further exploration.

5 Sample application

In this section we will introduce the concept of pairwise traceless sets, their connection to 1-designs, and bases of the space of d-by-d matrices. We will use 1-designs to evaluate the commutator we introduced equation 2 for arbitrary d. Lastly, we will use the commutator to prove that all the unitaries of a t-design can not commute.

5.1 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 can be 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 $\{P^{ij}, P^{-ij} : 1 \le i, j \le d\} \subset U(d)$ 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.

Definition 5.1. $X \subset U(d)$ is *pairwise traceless* if for every $U, V \in X$ with $U \neq V$ we have $tr(U^*V) = 0$

Since $\dim(\mathbb{C}^{d\times d}) = d^2$, any pairwise traceless X with $|X| = d^2$ will form an orthonormal basis for $\mathbb{C}^{d\times d}$. Further, since any pairwise traceless X is an orthonormal basis for some subspace of $\mathbb{C}^{d\times d}$, we have an important property of pairwise traceless sets:

Lemma 5.2. *For any pairwise traceless $X \subset U(d)$, $|X| \le d^2$.*

This allows a notion of maximality:

Definition 5.3. A pairwise traceless $X \subset U(d)$ is *maximum pairwise traceless* if $|X| = d^2$.

The importance of maximum pairwise traceless sets is in their relation to 1-designs:

Proposition 5.4. *For any $X \subset U(d)$, X is maximum pairwise traceless if and only if X is a minimum unweighted 1-design.*

Proof. ($\Rightarrow$) If X is maximum pairwise traceless, 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 pairwise traceless 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 11 or Proposition 4.8. Since X is maximum pairwise traceless, we get $\Sigma(X) = 1$ and by theorem 2.1 X is a 1-design. Further, by the bounds in Proposition 4.6 X is a minimum unweighted 1-design.

($\Leftarrow$) If X is a minimum unweighted 1-design then by Proposition 4.8 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 4.6 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 5.4 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.

5.2 MUBs and maximum pairwise traceless sets

A subtle part of Proposition 5.4 is that it is prefaced on the existence of maximum pairwise traceless sets. It might seem obvious since *a priori* we know that there must be some orthonormal bases of $\mathbb{C}^{d\times d}$. However, maximum pairwise traceless sets are restricted to subsets of $U(d)$, 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 maximum pairwise traceless sets.

For our construction, we need to introduce the basic ideas of mutually unbiased bases (MUBs).

Definition 5.5. 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 5.6. *For every $d \geq 1$ there is a maximum pairwise traceless $X \subset U(d)$.*

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:

$$tr(I_i^* I_j) = d\langle e_i|e_j\rangle \tag{20}$$

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 20 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 a maximum pairwise traceless set. □

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 the maximum pairwise traceless set:

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\} \tag{21}$$

5.3 Evaluating the average commutator over $U(d)$

As an application of 1-designs, we will evaluate the average of the commutator from equation 2 for unitary V. To simplify our work a little, we will observe that since V is constant, we have:

$$\int_{U(d)} U^* V^* U V \, dU = \Big[\int_{U(d)} U^* V^* U \, dU \Big] V \tag{22}$$

We will use 1-designs to evaluate the average of $f(U) = U^* D U$ for a fixed diagonal $D = \mathrm{diag}(|\psi\rangle)$. As an example, consider evaluating it for $d = 2$ with the 1-design X in equation 21. For this example, we will let $D = \mathrm{diag}(x, y)$. Since X_1 and X_2 are diagonal (and thus commute with D), we have $f(X_1) = f(X_2) = D$. However, for X_3 and X_4 (which we will call X_+ and X_-, respectively) we have:

$$
\begin{aligned}
f(X_{\pm}) &= \begin{bmatrix} 0 & \pm 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \begin{bmatrix} 0 & 1 \\ \pm 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} 0 & \pm y \\ x & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ \pm 1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} y & 0 \\ 0 & x \end{bmatrix}
\end{aligned}
$$

Thus, the average in $U(2)$ is given by:

$$
\begin{aligned}
\langle f \rangle &= \frac{f(X_1) + f(X_2) + f(X_3) + f(X_4)}{4} \\
&= \frac{x+y}{2} I
\end{aligned}
$$

From this, we can see that the average of the commutator in $U(2)$ with $V = \mathrm{diag}(x, y)$ is:

$$
\int_{U(2)} U^* V^* U V \, dU = \frac{1}{2} \begin{bmatrix} x(\bar{x} + \bar{y}) & 0 \\ 0 & y(\bar{x} + \bar{y}) \end{bmatrix} \tag{23}
$$

We will prove that the simplest generalization of equation 23 to arbitrary d is in fact accurate.

Theorem 5.7. *For any $V \in U(d)$ and $[U, V] = U^* V^* U V$ we have:*

$$
\langle [\,\cdot\,, V] \rangle = \frac{tr(V^*)}{d} V
$$

Proof. As in our example, we will use a 1-design to evaluate the average of $f(U) = U^* D U$ for diagonal D. Consider a 1-design X as in theorem 5.6.

$$
f(C_i^m) = I_i^* (C^m)^* D C^m I_i
$$

The inside term is simply a change of basis on D. Since C^m is the matrix representation of a cyclic permutation c^m and $D = \mathrm{diag}(y_1, ..., y_d)$ we have:

$$
(C^m)^* D C^m = \mathrm{diag}(y_{c^m(1)}, ..., y_{c^m(d)})
$$

Since the cyclic permutations have no fixed points, every element $y_1 ... y_d$ will appear in each entry of the diagonal matrix for exactly one cyclic permutation. Thus:

$$
\begin{aligned}
\langle f \rangle &= \frac{1}{d^2} \sum_{i,m=1}^{d} f(C_i^m) \\
&= \frac{1}{d^2} \sum_{i=1}^{d} I_i^* \Big(\sum_{m=1}^{d} (C^m)^* D C^m \Big) I_i \\
&= \frac{tr(D)}{d^2} \sum_{i=1}^{d} I_i^* I I_i \\
&= \frac{tr(D)}{d} I
\end{aligned}
$$

To evaluate $\langle [\,\cdot\,, V] \rangle$ we use equation 22 and observe that V is unitary, thus there is some unitary change of basis such that $V^* = P^* D P$ for a diagonal matrix D:

$$
\Big[\int_{U(d)} U^* V^* U \, dU \Big] V = \Big[\int_{U(d)} U^* P^* D P U \, dU \Big] V
$$

By Corollary 3.8 we know that we can send $U \leftarrow P^*UP$ without changing the integral. Thus, we can simplify further:

$$\Big[\int_{U(d)} U^*P^*VPU\ dU\Big]V = P^*\Big[\int_{U(d)} U^*DU\ dU\Big]PV$$

Now observing that trace is invariant under change of basis, i.e. $tr(D) = tr(V^*)$ we have:

$$\begin{aligned}\langle[\,\cdot\,, V]\rangle &= P^*\langle f\rangle PV \\ &= P^*\frac{tr(V^*)}{d}IPV \\ &= \frac{tr(V^*)}{d}V\end{aligned}$$

□

5.4 t-designs are non-commuting

The overarching goal of this section is to prove that t-designs are non-commuting. For this to make sense, we have to first define non-commuting sets.

Definition 5.8. $X \subset U(d)$ is a *non-commuting* if there is some $U, V \in X$ such that $[U, V] \neq I$.

This allows us to state the main result of this section.

Theorem 5.9. *For all $d \geq 2$ if $X \subset U(d)$ is a t-design then X is non-commuting.*

Proof. Consider a t-design X' such that for all $U, V \in X'$ we have $[U, V] = I$. Since all $U \in X'$ commute, we know that there is some basis P in which all $U \in X'$ are diagonal. By Corollary 3.8 we know that $X = [X']_P$ must also be a t-design. Further, by Proposition 3.1 we can assume that $X \subset PU(d)$.

Take any $V \in X$ that is not the identity matrix. We know this is possible, since X is non-singular by Proposition 4.6 for $d \geq 2$. By repeated applications of Proposition 1.4 we know that every t-design is a 1-design. Thus by def. 1.2:

$$\frac{1}{|X|^2}\sum_{U\in X}[U, V] = \langle[\,\cdot\,, V]\rangle$$

Since for every $U \in X$, $[U, V] = I$ by Theorem 5.7 we have $I = \frac{tr(V^*)}{d}V$. This is only possible if $V = e^{i\theta}I$, which in $PU(d)$ is the identity - a contradiction. □

Of course, the reverse direction of Theorem 5.9 is not true. Easiest way to see this is to consider the non-commuting set:

$$\left\{\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}, \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\right\}$$

This is clearly not a t-design.

6 Conclusion

Throughout this paper, we introduced tools for working with and finding t-designs. Studying the symmetries of t-designs provides a classical, but before unexplored, tool for better understanding how designs behave and transform. Greedy algorithms provide a novel method for studying designs and how to find them in practice. Sadly, with theorem 4.9 we showed that the most naive approach for building unweighted designs will not converge. However, we are optimistic of further research in greedy algorithms. In particular, it is important to understand if we can improve Lemma 4.2 to only consider the addition of a single unitary, instead of all possible finite subsets of $U(d)$. Hopefully, the study of symmetries and greedy algorithms can improve our understanding of unitary t-designs and how to apply them.

In applications, 2-designs are currently generating the most interest. No applications are known for arbitrary t-designs. Our sample application does no better by only using properties of a 1-design. However, the proofs in our sample application are still enlightening. They provide connections between 1-designs and general linear algebra, and introduce a (rather superficial) tie between MUBs and 1-designs. Further, Proposition 5.4 and Theorem 5.9 support our intuition that the elements of a design are 'spread out'.

An important focus for future research is finding applications for arbitrary t-designs. To help with this, it is important to find simple constructions for designs with any choice of t and d. The first steps to making experimental applications of designs were made in this paper by exploring symmetry. The three fundamental symmetries of t-designs allow us to adjust the unitaries in a design to a more experiment friendly form (by change of basis or rotation for instance). A promising second step is to generalize the ideas behind the greedy construction of designs to work with approximate t-designs. The final goal, though, is a simple classification (if possible) of minimum designs.

References

[1] 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.

[2] 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.

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

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

[5] A. Roy and A. J. Scott. Unitary designs and codes. 2008, arXiv:0809.3813v1.

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

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