Introduction to unitary t-designs

Artem Kaznatcheev

McGill University

March 25, 2010

Outline

Outline

Preliminaries: $U(d)$

- $U(d)$ is the topologically compact and connected group of norm preserving (unitary) operators on $\mathbb{C}^d$.

Preliminaries: $U(d)$

- $U(d)$ is the topologically compact and connected group of norm preserving (unitary) operators on $\mathbb{C}^d$.
- We can introduce the Haar measure and use it to integrate functions f of $U \in U(d)$ to find their averages:

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

- For convenience we normalize integration by assuming that $\int_{U(d)} dU = 1$.

Preliminaries: $U(d)$

- $U(d)$ is the topologically compact and connected group of norm preserving (unitary) operators on $\mathbb{C}^d$.
- We can introduce the Haar measure and use it to integrate functions f of $U \in U(d)$ to find their averages:

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

- For convenience we normalize integration by assuming that $\int_{U(d)} dU = 1$.
- The goal of unitary t-designs is to evaluate averages of polynomials via a finite sum.

Preliminaries: $\mathrm{Hom}(r, s)$

Definition

$\mathrm{Hom}(r, s)$ is the set of polynomials homogeneous of degree r in entries of $U \in U(d)$ and homogeneous of degree s in U^*.

Preliminaries: $\mathrm{Hom}(r, s)$

Definition

$\mathrm{Hom}(r, s)$ is the set of polynomials homogeneous of degree r in entries of $U \in U(d)$ and homogeneous of degree s in U^*.

Examples

$$
\begin{aligned}
U, V &\mapsto U^* V^* UV && \in Hom(2,2) \\
U &\mapsto U^* V^* UV && \in Hom(1,1)
\end{aligned}
$$

Preliminaries: $\mathrm{Hom}(r, s)$

Definition

$\mathrm{Hom}(r, s)$ is the set of polynomials homogeneous of degree r in entries of $U \in U(d)$ and homogeneous of degree s in U^*.

Examples

$$\begin{aligned}
U, V &\mapsto U^* V^* UV && \in Hom(2,2) \\
U &\mapsto U^* V^* UV && \in Hom(1,1) \\
U &\mapsto \frac{tr(U^* U)}{d} && \in Hom(1,1)
\end{aligned}$$

Preliminaries: $\mathrm{Hom}(r, s)$

Definition

$\mathrm{Hom}(r, s)$ is the set of polynomials homogeneous of degree r in entries of $U \in U(d)$ and homogeneous of degree s in U^*.

Examples

$$
\begin{array}{rcll}
U, V & \mapsto & U^*V^*UV & \in Hom(2,2) \\
U & \mapsto & U^*V^*UV & \in Hom(1,1) \\
U & \mapsto & \dfrac{tr(U^*U)}{d} & \in Hom(1,1) \\
U, V & \mapsto & tr(U^*V)U^2 + VU^*VU & \in Hom(3,1) \\
U & \mapsto & \underbrace{tr(U^*V)U^2}_{Hom(2,1)} + \underbrace{VU^*VU}_{Hom(1,1)} & \notin Hom(2,1)
\end{array}
$$

Functional definition of unitary t-designs

Definition

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

Functional definition of unitary t-designs

Definition

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

Definition

A tuple (X,w) with finite $X \subset U(d)$ and weight function w on X is a unitary t-design if

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

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

Functional definition of unitary t-designs

Definition

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

Definition

A tuple (X,w) with finite $X \subset U(d)$ and weight function w on X is a unitary t-design if

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

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

Definition

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 $U \in X$).

Functional definition is general enough

Proposition

Every t-design is a $(t-1)$-design.

Functional definition is general enough

Proposition

Every t-design is a $(t-1)$-design.

Proposition

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

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

Lemma

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

Strengths and shortcomings of the functional definition

Strengths:

- Average of any polynomial with degrees in U and U^* less than t can be evaluated one summand at a time.
- Multi-variable polynomials can be evaluated:

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

$$= \sum_{U_1 \in X} ... \sum_{U_n \in X} w(U_1)...w(U_n) f(U_1, ..., U_n).$$

Strengths and shortcomings of the functional definition

Strengths:

- Average of any polynomial with degrees in U and U^* less than t can be evaluated one summand at a time.
- Multi-variable polynomials can be evaluated:

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

$$= \sum_{U_1 \in X} ... \sum_{U_n \in X} w(U_1)...w(U_n) f(U_1, ..., U_n).$$

Shortcomings:

- Not clear how to test if a given (X, w) is a t-design.
- If (X, w) is not a design, then how far away is it?

Tensor product definition of unitary t-designs

Definition

A tuple (X,w) with finite $X \subset U(d)$ and weight function w on X is a unitary t-design if

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

Tensor product definition of unitary t-designs

Definition

A tuple (X,w) with finite $X \subset U(d)$ and weight function w on X is a unitary t-design if

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

- More tractable for checking if an arbitrary (X, w) is a t-design.
- Literature has explicit formula for the RHS for many choices of d and t [Col03, CS06].
- Still not metric.

ϵ-approximate unitary t-designs

Definition

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

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

ϵ-approximate unitary t-designs

Definition

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

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

- A glaring omission is a specification of which norm to use in the definition.

ϵ-approximate unitary t-designs

Definition

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

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

- A glaring omission is a specification of which norm to use in the definition.
- There are many choices of operator norms, important ones in QIT are Schatten norms. In particular the trace, Frobenius, and spectral norms.

ϵ-approximate unitary t-designs

Definition

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

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

- A glaring omission is a specification of which norm to use in the definition.
- There are many choices of operator norms, important ones in QIT are Schatten norms. In particular the trace, Frobenius, and spectral norms.
- By modifying the definition slightly, we can also study super-operator norms. In particular, the diamond norm (most useful from a cryptographic and experimental point of view).

Outline

The trace double sum inequality

Theorem

A tuple (X, w) is an ϵ-approximate unitary t-design (with respect to the Frobenius norm) if and only if

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

- Proved earlier in the non-approximate case by Scott [Sco08].

The trace double sum inequality

Theorem

A tuple (X, w) is an ϵ-approximate unitary t-design (with respect to the Frobenius norm) if and only if

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

- Proved earlier in the non-approximate case by Scott [Sco08].
- The integral is the number of permutations of $\{1, ..., t\}$ with no increasing subsequences of order greater than d [DS94, Rai98]. We will call this number σ.
- If $d \geq t$ then σ is $t!$.

The trace double sum inequality

Theorem

A tuple (X, w) is an ϵ-approximate unitary t-design (with respect to the Frobenius norm) if and only if

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

- Proved earlier in the non-approximate case by Scott [Sco08].
- The integral is the number of permutations of $\{1, ..., t\}$ with no increasing subsequences of order greater than d [DS94, Rai98]. We will call this number σ.
- If $d \geq t$ then σ is $t!$.
- Limitation: no one really cares about the Frobenius norm. -_-

Metric definition of unitary t-designs

Definition

A weight function w is an optimal weight function on X if for all other choices of weight function w' on X, we have:

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

The trace double sum is a function Σ defined for finite $X \subset U(d)$ as:

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

Definition

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

$$\Sigma(X) = \langle |tr(U)|^{2t} \rangle$$

Outline

Four symmetries of t-designs

Proposition

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 $\phi_1, ..., \phi_n \in [0, 2\pi]$.

Four symmetries of t-designs

Proposition

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* $\phi_1, ..., \phi_n \in [0, 2\pi]$.

Proposition

If X *is a t-design then* $X^* = \{U^* : U \in X\}$ *is also a t-design.*

Four symmetries of t-designs

Proposition

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 $\phi_1, ..., \phi_n \in [0, 2\pi]$.

Proposition

If X is a t-design then $X^* = \{U^* : U \in X\}$ is also a t-design.

Proposition

If $X \subset U(d)$ is a t-design then $\forall M \in U(d)$, $MX = \{MU : U \in X\}$ and $XM = \{UM : U \in X\}$ are also a t-design.

Minimal designs

Lemma

If X, Y are two t-designs then so is $X \cup Y$.

- Designs can be arbitrarily large

Minimal designs

Lemma

If X, Y are two t-designs then so is $X \cup Y$.

- Designs can be arbitrarily large
- We are interested in smaller designs

Definition

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

Characterization of minimal t-designs

Theorem

A t-design X is minimal if and only if it has a unique optimal weight function w.

Characterization of minimal t-designs

Theorem

A t-design X is minimal if and only if it has a unique optimal weight function w.

- Useful tool for proving minimality.

Characterization of minimal t-designs

Theorem

A t-design X is minimal if and only if it has a unique optimal weight function w.

- Useful tool for proving minimality.
- Sadly, minimal designs are not necessarily minimum.
- Still working on finding correspondences between minimal and minimum designs.

Outline

Orthonormal bases for $\mathbb{C}^{d\times d}$

Goal: find an orthonormal basis $|E_1\rangle, \ldots, |E_{d^2}\rangle$ of $\mathbb{C}^{d\times d}$ such that each $E_i \in U(d)$

Orthonormal bases for $\mathbb{C}^{d\times d}$

Goal: find an orthonormal basis $|E_1\rangle, \ldots, |E_{d^2}\rangle$ of $\mathbb{C}^{d\times d}$ such that each $E_i \in U(d)$

Definition

$X \subset U(d)$ is pairwise traceless if for every $U, V \in X$ with $U \neq V$ we have $tr(U^* V) = 0$.
A pairwise traceless $X \subset U(d)$ is maximum pairwise traceless if $|X| = d^2$.

Orthonormal bases of unitaries for $\mathbb{C}^{d\times d}$ are maximum pairwise traceless sets.

Orthonormal bases for $\mathbb{C}^{d\times d}$

Goal: find an orthonormal basis $|E_1\rangle, ..., |E_{d^2}\rangle$ of $\mathbb{C}^{d\times d}$ such that each $E_i \in U(d)$

Definition

$X \subset U(d)$ is pairwise traceless if for every $U, V \in X$ with $U \neq V$ we have $tr(U^* V) = 0$.
A pairwise traceless $X \subset U(d)$ is maximum pairwise traceless if $|X| = d^2$.

Orthonormal bases of unitaries for $\mathbb{C}^{d\times d}$ are maximum pairwise traceless sets.

Proposition

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

Very brief introduction to MUBs

Definition

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 $1 \leq i, j \leq d$.

Very brief introduction to MUBs

Definition

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 $1 \leq i, j \leq d$.

- Open question: determine the maximum number $\mathfrak{M}(d)$ of pairwise mutually unbiased bases for $\mathbb{C}^d$.

Very brief introduction to MUBs

Definition

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 $1 \leq i, j \leq d$.

- Open question: determine the maximum number $\mathfrak{M}(d)$ of pairwise mutually unbiased bases for $\mathbb{C}^d$.
- If we write the prime decomposition of $d = p_1^{n_1} \ldots p_k^{n_k}$ such that $p_i^{n_i} \leq p_{i+1}^{n_{i+1}}$ then $p_1^{n_1} \leq \mathfrak{M}(d) \leq d + 1$.

Very brief introduction to MUBs

Definition

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 $1 \leq i, j \leq d$.

- Open question: determine the maximum number $\mathfrak{M}(d)$ of pairwise mutually unbiased bases for $\mathbb{C}^d$.
- If we write the prime decomposition of $d = p_1^{n_1} \ldots p_k^{n_k}$ such that $p_i^{n_i} \leq p_{i+1}^{n_{i+1}}$ then $p_1^{n_1} \leq \mathfrak{M}(d) \leq d + 1$.

Important features for us:

- $\mathfrak{M}(d) \geq 2$ for $d \geq 1$.
- Without loss of generality, can assume one of the bases to be the standard basis.

Example

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}, \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}, \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ +i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\}$$

Maximum pairwise traceless set construction

- Let $|e_1\rangle ... |e_d\rangle$ be an orthonormal basis of $\mathbb{C}^d$ that is mutually unbiased with the standard basis.
- Define $I_i = \sqrt{d}\mathrm{diag}(|e_i\rangle)$ for $1 \leq i \leq d$.

Maximum pairwise traceless set construction

- Let $|e_1\rangle ... |e_d\rangle$ be an orthonormal basis of $\mathbb{C}^d$ that is mutually unbiased with the standard basis.
- Define $I_i = \sqrt{d}\,\mathrm{diag}(|e_i\rangle)$ for $1 \le i \le d$.
- Consider the cyclic permutation group of order d, represented as d-by-d matrices: $C^1 ... C^d$ where $C^d = C^0 = I$.
- Define $C_i^m = C^m I_i$

Maximum pairwise traceless set construction

- Let $|e_1\rangle ... |e_d\rangle$ be an orthonormal basis of $\mathbb{C}^d$ that is mutually unbiased with the standard basis.
- Define $I_i = \sqrt{d}\mathrm{diag}(|e_i\rangle)$ for $1 \leq i \leq d$.
- Consider the cyclic permutation group of order d, represented as d-by-d matrices: $C^1 ... C^d$ where $C^d = C^0 = I$.
- Define $C_i^m = C^m I_i$

For any tuple $1 \leq i, j, m, n \leq d$ we have:

$$tr((C_i^m)^* C_j^n) = tr(I_i^* C^{d-m+n} I_j) = \begin{cases} d & \text{if } i = j \text{ and } m = n \\ 0 & \text{otherwise} \end{cases}$$

Outline

The center of t-designs is trivial

Lemma

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

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

The center of t-designs is trivial

Lemma

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

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

Proposition

If $X \subset U(d)$ is a minimal t-design then there is at most one element that commutes with all elements of X. In other words, $Z(X)$ is trivial.

Some other structural observations

Proposition

Every t-design of dimension d spans $\mathbb{C}^{d \times d}$.

Some other structural observations

Proposition

Every t-design of dimension d spans $\mathbb{C}^{d \times d}$.

A group t-design is a unitary t-design that also happens to have group structure. Group designs were defined by Gross, Audenaert, and Eisert [GAE07], and all known constructions are via group designs.

Some other structural observations

Proposition

Every t-design of dimension d spans $\mathbb{C}^{d \times d}$.

A group t-design is a unitary t-design that also happens to have group structure. Group designs were defined by Gross, Audenaert, and Eisert [GAE07], and all known constructions are via group designs.

Proposition

Every unitary irreducible representation of a finite group is a group 1-design and vice versa.

A simple lower bound on the size of t-designs

Proposition

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

A simple lower bound on the size of t-designs

Proposition

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

- Best known bounds are by Roy and Scott [RS08]: $|X| \geq \binom{d^2+t-1}{t}$
- Asymptotically, for large d and fixed t, both bounds are $\Theta(d^{2t})$

A simple lower bound on the size of t-designs

Proposition

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

- Best known bounds are by Roy and Scott [RS08]: $|X| \geq \binom{d^2+t-1}{t}$
- Asymptotically, for large d and fixed t, both bounds are $\Theta(d^{2t})$
- By taking note of some structural observations, we can do a little better:

Proposition

If $X \subset U(d)$ is a t-design then $|X| \geq \frac{d^{2t}}{\sigma} + \frac{1}{2d^t}(\frac{\sigma}{2d^{2t}})^{2(t-1)}$.

Conjecture

Conjecture

If X is a unitary t-design with $t \geq 2$, then for any $W \in X$ there exists some $Y \subset X - \{W\}$ such that Y is a $t-1$-design.

Conjecture

Conjecture

If X is a unitary t-design with $t \geq 2$, then for any $W \in X$ there exists some $Y \subset X - \{W\}$ such that Y is a $t-1$-design.

If true, this conjecture can significantly improve our lower bounds:

Theorem

If $(X \subset U(d), w)$ is a unitary t-design and the conjecture is true, then:

$$|X| \geq \frac{d^{2t}}{\sigma_t}\left(1 + 2\frac{\sigma_t}{d^{2t}}\sigma_{t-1}^{\frac{t}{t-1}}\right)$$

Outline

Concluding remarks

- Introduces 3 definitions of unitary t-designs and one for approximate ones.
- Showed the trace double sum inequality: $\Sigma(X) - \langle |tr(U)|^{2t} \rangle < \epsilon^2$ with equality if and if X is a ϵ approximate t-design with respect to the Frobenius norm.

Concluding remarks

- Introduces 3 definitions of unitary t-designs and one for approximate ones.
- Showed the trace double sum inequality: $\Sigma(X) - \langle |tr(U)|^{2t} \rangle < \epsilon^2$ with equality if and if X is a ϵ approximate t-design with respect to the Frobenius norm.
- Used an orthonormal basis of $\mathbb{C}^{d \times d}$ as a 1-design.
- Evaluated the average commutator on $U(d)$: $\langle [\,\cdot\,, V] \rangle = \frac{tr(V^*)}{d} V$
- Showed that t-designs are non-commuting

Concluding remarks

- Introduces 3 definitions of unitary t-designs and one for approximate ones.
- Showed the trace double sum inequality: $\Sigma(X) - \langle |tr(U)|^{2t} \rangle < \epsilon^2$ with equality if and if X is a ϵ approximate t-design with respect to the Frobenius norm.
- Used an orthonormal basis of $\mathbb{C}^{d \times d}$ as a 1-design.
- Evaluated the average commutator on $U(d)$: $\langle [\,\cdot\,, V] \rangle = \frac{tr(V^*)}{d} V$
- Showed that t-designs are non-commuting
- Discussed symmetries of designs: phase, X^*, MX, and XM.
- Classified minimal designs: a t-design is minimal if and only if it has a unique proper weight function.

Concluding remarks

- Introduces 3 definitions of unitary t-designs and one for approximate ones.
- Showed the trace double sum inequality: $\Sigma(X) - \langle |tr(U)|^{2t} \rangle < \epsilon^2$ with equality if and only if X is a ϵ approximate t-design with respect to the Frobenius norm.
- Used an orthonormal basis of $\mathbb{C}^{d \times d}$ as a 1-design.
- Evaluated the average commutator on $U(d)$: $\langle [\,\cdot\,, V] \rangle = \frac{tr(V^*)}{d} V$
- Showed that t-designs are non-commuting
- Discussed symmetries of designs: phase, X^*, MX, and XM.
- Classified minimal designs: a t-design is minimal if and only if it has a unique proper weight function.
- Mentioned some useful observations about the structure of designs
- Derived lower bounds on the size of t-designs: $X \geq \frac{d^{2t}}{\sigma}$.

Concluding remarks

- Introduces 3 definitions of unitary t-designs and one for approximate ones.
- Showed the trace double sum inequality: $\Sigma(X) - \langle |tr(U)|^{2t} \rangle < \epsilon^2$ with equality if and if X is a ϵ approximate t-design with respect to the Frobenius norm.
- Used an orthonormal basis of $\mathbb{C}^{d\times d}$ as a 1-design.
- Evaluated the average commutator on $U(d)$: $\langle [\,\cdot\,, V] \rangle = \frac{tr(V^*)}{d} V$
- Showed that t-designs are non-commuting
- Discussed symmetries of designs: phase, X^*, MX, and XM.
- Classified minimal designs: a t-design is minimal if and only if it has a unique proper weight function.
- Mentioned some useful observations about the structure of designs
- Derived lower bounds on the size of t-designs: $X \geq \frac{d^{2t}}{\sigma}$.

Thank you for listening!

References I

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.

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.

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

D. Gross, K. Audenaert, and J. Eisert.
Evenly distributed unitaries: on the structure of unitary designs.
Journal of Mathematical Physics, 48, 2007.

References II

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

A. Roy and A. J. Scott.
Unitary designs and codes.
2008.

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