Title: Unitary design: bounds on their size

Date: Oct 27, 2008 11:30 AM

URL: http://pirsa.org/08100071

Abstract: As a means of exactly derandomizing certain quantum information processing tasks, unitary designs have become an important concept in quantum information theory. A unitary design is a collection of unitary matrices that approximates the entire unitary group, much like a spherical design approximates the entire unit sphere. We use irreducible representations of the unitary group to find a general lower bound on the size of a unitary t-design in U(d), for any d and t. The tightness of these bounds is then considered, where specific unitary 2-designs are introduced that are analogous to SIC-POVMs and complete sets of MUBs in the complex projective case. Additionally, we catalogue the known constructions of unitary t-designs and give an upper bound on the size of the smallest weighted unitary t-design in U(d). This is joint work with Aidan Roy (Calgary): \'Unitary designs and codes,\' arXiv:0809.3813.

Unitary designs: bounds on their size

Andrew Scott

Centre for Quantum Computer Technology
Centre for Quantum Dynamics, Griffith University

Joint work with

Aidan Roy

Institute for Quantum Information Science
University of Calgary

A. Roy and A. J. Scott, Unitary designs and codes, arXiv:0809.3813.

Unitary designs

- The literature is so small we can list all the papers:

Dankert. MSc thesis (2005). [arXiv:quant-ph/0512217]

Dankert, Cleve, Emerson and Livine. Exact and approximate unitary 2-designs: Constructions and applications. [arXiv:quant-ph/0606161]

Gross, Audenaert and Eisert. Evenly distributed unitaries: On the structure of unitary designs. J Math Phys 48, 052104 (2007). [arXiv:quant-ph/0611002]

AJS. Optimizing quantum process tomography with unitary 2-designs. J Phys A 41, 055308 (2008). [arXiv:0711.1017]

Harrow and Low. Random quantum circuits are approximate 2-designs. [arXiv: 0802.1919]

Roy and AJS. Unitary designs and codes. [arXiv:0809.3813]

Unitary designs

- Unitary designs are like spherical designs, except that members of the design are elements of the unitary group $\mathrm{U}(d)$ rather than points on the sphere S^{d-1}:

Let $X \subset \mathrm{U}(d)$ be finite. Then X is called a unitary t-design if

$$\frac{1}{|X|}\sum_{U\in X} U^{\otimes t}\otimes\overline{U}^{\otimes t} = \int_{\mathrm{U}(d)} U^{\otimes t}\otimes\overline{U}^{\otimes t}\,\mathrm{d}U$$

- $\mathrm{d}U$ – unit Haar measure.
- RHS can be evaluated explicitly in terms of the so-called Weingarten function (see papers of Collins and Śniady for details); but this is complicated!
- U and $e^{i\phi}U$ are effectively the same point, ie. the current type of unitary design might be better defined as a subset of $\mathrm{PU}(d)$; but we will follow tradition.

Unitary designs

- Let $\mathrm{Hom}(r,s) = \mathrm{Hom}(\mathrm{U}(d),r,s)$ denote the polynomials that are homogeneous of degree r in the matrix entries of U and homogeneous of degree s in the entries of $\overline{U}$.

  Eg. $f(U) = U_{11}U_{33}\overline{U_{23}} + 2(U_{22})^2\overline{U_{31}} \in \mathrm{Hom}(2,1)$

- The traditional definition: X is a t-design if, for every $f \in \mathrm{Hom}(t,t)$,

$$\frac{1}{|X|}\sum_{U\in X} f(U) = \int_{\mathrm{U}(d)} f(U)\,\mathrm{d}U$$

  (former definition is just a compact way of expressing this in terms of monomials)

- Note that if $(\mathrm{tr}(U^\dagger U)/d)f \in \mathrm{Hom}(t,t)$ then $f \in \mathrm{Hom}(t-1,t-1)$.
  And since $\mathrm{tr}(U^\dagger U)/d = 1$ on $\mathrm{U}(d)$,

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

Unitary designs

- Unitary designs are like spherical designs, except that members of the design are elements of the unitary group $\mathrm{U}(d)$ rather than points on the sphere S^{d-1}:

Let $X \subset \mathrm{U}(d)$ be finite. Then X is called a unitary t-design if

$$\frac{1}{|X|}\sum_{U \in X} U^{\otimes t} \otimes \overline{U}^{\otimes t} = \int_{\mathrm{U}(d)} U^{\otimes t} \otimes \overline{U}^{\otimes t} \, \mathrm{d}U$$

- $\mathrm{d}U$ – unit Haar measure.

- RHS can be evaluated explicitly in terms of the so-called Weingarten function (see papers of Collins and Śniady for details); but this is complicated!

- U and $e^{i\phi}U$ are effectively the same point, ie. the current type of unitary design might be better defined as a subset of $\mathrm{PU}(d)$; but we will follow tradition.

Unitary designs

- Let $\text{Hom}(r,s) = \text{Hom}(\text{U}(d), r, s)$ denote the polynomials that are homogeneous of degree r in the matrix entries of U and homogeneous of degree s in the entries of $\overline{U}$.

  Eg. $f(U) = U_{11}U_{33}\overline{U_{23}} + 2(U_{22})^2\overline{U_{31}} \in \text{Hom}(2,1)$

- The traditional definition: X is a t-design if, for every $f \in \text{Hom}(t,t)$,

$$\frac{1}{|X|}\sum_{U\in X} f(U) = \int_{\text{U}(d)} f(U)\,\mathrm{d}U$$

  (former definition is just a compact way of expressing this in terms of monomials)

- Note that if $(\text{tr}(U^\dagger U)/d)f \in \text{Hom}(t,t)$ then $f \in \text{Hom}(t-1,t-1)$.
  And since $\text{tr}(U^\dagger U)/d = 1$ on $\text{U}(d)$,

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

Unitary designs

- As t is increased, functions with an increasingly finer sieve (higher nonlinearity) cannot distinguish unitaries drawn from X, from those drawn from $\mathrm{U}(d)$.

- Weighted unitary designs (ie. cubature formulas for $\mathrm{U}(d)$) are a generalisation:

> Let $X \subset \mathrm{U}(d)$ be finite and let $w : X \to \mathbb{R}$ be a positive normalized weight function. Then (X, w) is called a weighted unitary t-design if
>
> $$\sum_{U \in X} w(U)\, U^{\otimes t} \otimes \overline{U}^{\otimes t} = \int_{\mathrm{U}(d)} U^{\otimes t} \otimes \overline{U}^{\otimes t}\, \mathrm{d}U$$

- $w > 0$ so that it can be interpreted as a probability density on X.

- Every t-design is a weighted t-design with weight function $w(U) := 1/|X|$.

- Weighted t-designs are generally much easier to find!

Unitary designs

- Testing whether a weighted set (X, w) forms a t-design can be difficult without the following third characterization in terms of the inner product values:

Theorem

For any finite $X \subset \mathrm{U}(d)$ and positive normalized weight function w on X,

$$\sum_{U,V \in X} w(U)w(V) \left|\mathrm{tr}(U^\dagger V)\right|^{2t} \geq \int_{\mathrm{U}(d)} |\mathrm{tr}(U)|^{2t} \, \mathrm{d}U$$

with equality if and only if (X, w) is a weighted t-design.

- RHS can be evaluated explicitly: it is the number of permutations of $(1, \ldots, t)$ that have no increasing subsequence of length greater than d,

$$\int_{\mathrm{U}(d)} |\mathrm{tr}(U)|^{2t} \, \mathrm{d}U = \begin{cases} t! & d \geq t, \\ t! - 1 & d = t - 1, \\ \vdots & \\ \frac{(2t)!}{t!(t+1)!} & d = 2, \end{cases}$$

Diaconis and Shahshahani (1994)
Rains (1998)

Unitary designs

- This theorem is analogous to one by Welch (1974) for complex vectors, and has a simple proof:

Proof of Theorem:

Consider $D := \sum_{U \in X} w(U)\, U^{\otimes t} \otimes \overline{U}^{\otimes t} - \int_{\mathrm{U}(d)} U^{\otimes t} \otimes \overline{U}^{\otimes t}\, \mathrm{d}U$. Then

$$\mathrm{tr}(D^\dagger D) = \sum_{U,V \in X} w(U)w(V)\, \left|\mathrm{tr}(U^\dagger V)\right|^{2t} - 2\int_{\mathrm{U}(d)} \sum_{V \in X} w(V)\, \left|\mathrm{tr}(U^\dagger V)\right|^{2t} \mathrm{d}U$$
$$+ \iint_{\mathrm{U}(d)} \left|\mathrm{tr}(U^\dagger V)\right|^{2t} \mathrm{d}U \mathrm{d}V$$
$$= \sum_{U,V \in X} w(U)w(V)\, \left|\mathrm{tr}(U^\dagger V)\right|^{2t} - \int_{\mathrm{U}(d)} \left|\mathrm{tr}(U)\right|^{2t} \mathrm{d}U$$

But $\mathrm{tr}(D^\dagger D) \geq 0$ with equality if and only if $D = 0$, ie. (X, w) is a t-design.

Why designs?

- Randomness is expensive. It is hard to fake classically and costly to share secretly. At any point where we can reduce the randomness required for a task, we should.

- Designs allow $\mathrm{U}(d)$ to be replaced by a small set X, reducing the required number of random bits to $\log|X|$:

  1-designs depolarize: $\sum_{U\in X} w(U)\, U\rho U^\dagger = \int_{\mathrm{U}(d)} U\rho U^\dagger\, \mathrm{d}U = I/d$

  2-designs twirl: $\sum_{U\in X} w(U)\, U^\dagger\mathcal{E}(U\rho U^\dagger)U = \int_{\mathrm{U}(d)} U^\dagger\mathcal{E}(U\rho U^\dagger)U\, \mathrm{d}U$

- The hope is also that members of X will be easier to implement on a quantum computer than arbitrary unitaries, which require exponentially many gates.

- In the context of state estimation, for example, designs reduce the optimal covariant measurement to a simpler one:

  $\mathbb{C}^d$ t-designs realize optimal measurements for the Massar-Popescu state estimation problem [Hayashi et al (2005)]

  $\mathbb{C}^d/\mathrm{U}(d)$ 2-designs realize optimal measurements for state/process tomography [AJS (2006,2008), Roy and AJS (2007)]

How big does X need to be?

Outline

1. Unitary designs.

1.5. Primer: Complex projective designs.

2. Lower bounds.

3. Tight designs?

   – SIC-POVMs for maximally entangled states?

   – MUU(nitary)Bs?

4. Upper bounds.

5. Constructions.

   – Designs from unitary representations of finite groups.

   – $\mathrm{U}(2)$ designs $= \mathrm{P}\mathbb{R}^4$ designs.

Primer: Complex projective designs

(Standard methods dating to Delsarte, Goethels and Seidel (1977), then generalised by Neumaier (1981), Godsil (1986), and Levenshtein (1998), then debased by me to make them understandable)

- A weighted complex projective t-design (X, w), $X \subset \mathbb{C}^d$, satisfies

$$\sum_{v \in X} w(v)\, v^{\otimes t} \otimes \overline{v}^{\otimes t} = \int_{\mathbb{C}^d} v^{\otimes t} \otimes \overline{v}^{\otimes t}\, \mathrm{d}v$$

or, reshaping the vector $v^{\otimes t} \otimes \overline{v}^{\otimes t}$ into an outer product, for any $r + s = t$,

$$\sum_{v \in X} w(v)\, |v^{\otimes r} \otimes \overline{v}^{\otimes s}\rangle\langle v^{\otimes r} \otimes \overline{v}^{\otimes s}| = \int_{\mathbb{C}^d} |v^{\otimes r} \otimes \overline{v}^{\otimes s}\rangle\langle v^{\otimes r} \otimes \overline{v}^{\otimes s}|\, \mathrm{d}v$$

- The span of the vectors $v^{\otimes r} \otimes \overline{v}^{\otimes s}$ is therefore independent of whether v is drawn from X or $\mathbb{C}^d$: it is the support of the above positive operator.

$\Rightarrow$ $|X|$ must be bigger than the dimension of this support

Primer: Complex projective designs

- The dimension of $\mathrm{span}\{v^{\otimes r} \otimes \overline{v}^{\otimes s}\}_{v \in \mathbb{C}^d}$ is known in terms of its dual space, $\mathrm{Hom}(\mathbb{C}^d, r, s)$, the space of polynomials that are homogeneous of degree r in the matrix entries of v and homogeneous of degree s in the entries of $\overline{v}$:

  For any weighted t-design (X, w), and $r + s = t$,

$$|X| \geq \dim(\mathrm{Hom}(\mathbb{C}^d, r, s)) = \binom{d+r-1}{r}\binom{d+s-1}{s}$$

  The optimal choices, $r = \lceil t/2 \rceil$ and $s = \lfloor t/2 \rfloor$, recover the standard bound.

- An upper bound follows from convexity arguments (folklore?):

  There is a weighted t-design (X, w) with

$$|X| \leq \dim(\mathrm{Hom}(\mathbb{C}^d, t, t)) = \binom{d+t-1}{t}^2$$

- Eg. there is a weighted 2-design with $d^2 \leq |X| \leq d^2(d+1)^2/4$.

Lower bounds

- Use the same tricks: A weighted unitary t-design (X, w) satisfies, for $r + s = t$,

$$\sum_{U \in X} w(U)\, |U^{\otimes r} \otimes \overline{U}^{\otimes s}\rangle\langle U^{\otimes r} \otimes \overline{U}^{\otimes s}| = \int_{\mathrm{U}(d)} |U^{\otimes r} \otimes \overline{U}^{\otimes s}\rangle\langle U^{\otimes r} \otimes \overline{U}^{\otimes s}| \,\mathrm{d}U =: \mathcal{B}$$

where $|A\rangle = \mathrm{Vec}(A)$ and $\langle A| = \mathrm{Vec}(A)^\dagger$ so that $\langle A|B\rangle := \mathrm{tr}(A^\dagger B)$.

Therefore,

$$|X| \;\geq\; \mathrm{rank}(\mathcal{B}) \;=\; \dim(\mathrm{span}\{U^{\otimes r} \otimes \overline{U}^{\otimes s}\}_{U \in \mathrm{U}(d)}) \;=\; \dim(\mathrm{Hom}(\mathrm{U}(d), r, s))$$

- An easy rough bound: Let $b_1, \ldots, b_n > 0$ be the nonzero eigenvalues of $\mathcal{B}$.

$$\frac{t!}{n} \geq \frac{\int |\mathrm{tr}(U)|^{2t}\,\mathrm{d}U}{n} = \frac{\mathrm{Tr}(\mathcal{B}^2)}{n} = \frac{1}{n}\sum_k b_k{}^2 \geq \left(\frac{1}{n}\sum_k b_k\right)^2 = \frac{\mathrm{Tr}(\mathcal{B})^2}{n^2} = \frac{d^{2t}}{n^2}$$

$$\Rightarrow \qquad \mathrm{rank}(\mathcal{B}) \;=\; n \;\geq\; \frac{d^{2t}}{t!}$$

Lower bounds

- A better bound from representation theory: Let R take the $\mathrm{U}(d)$-representation $U^{\otimes r} \otimes \overline{U}^{\otimes s}$ to its irreducible decomposition:

$$R\big(U^{\otimes r} \otimes \overline{U}^{\otimes s}\big)R^\dagger = \bigoplus_\mu \rho_\mu(U) \otimes I_{m_\mu}$$

where each irrep $\rho_\mu : \mathrm{U}(d) \to \mathrm{U}(V_\mu)$ has dimension $\dim V_\mu = d_\mu$ and occurs with multiplicity m_μ. Now define $\mathcal{R}$ by the action $\mathcal{R}|A\rangle = |RAR^\dagger\rangle$ and consider

$$\mathcal{R}\mathcal{B}\mathcal{R}^\dagger = \int \Big| \bigoplus_\mu \rho_\mu(U) \otimes I_{m_\mu} \Big\rangle \Big\langle \bigoplus_\nu \rho_\nu(U) \otimes I_{m_\nu} \Big| \mathrm{d}U$$

- Let $E^\mu_{ij} := |e^\mu_i\rangle\langle e^\mu_j|$ be the matrix component basis for $\mathrm{End}(V_\mu)$, then by Schur orthogonality of the matrix components of irreps,

$$\int \langle E^\mu_{ij}|\rho_\mu(U)\rangle\langle\rho_\nu(U)|E^\nu_{kl}\rangle \,\mathrm{d}U = \int \langle e^\mu_i|\rho_\mu(U)|e^\mu_j\rangle \overline{\langle e^\nu_k|\rho_\nu(U)|e^\nu_l\rangle}\,\mathrm{d}U = \frac{\delta_{\mu\nu}\delta_{ik}\delta_{jl}}{d_\mu}$$

Lower bounds

This means $$\int |\rho_\mu(U)\rangle\langle\rho_\nu(U)|\,\mathrm{d}U = \frac{\delta_{\mu\nu}}{d_\mu}\sum_{ij}|E^\mu_{ij}\rangle\langle E^\mu_{ij}| =: \frac{\delta_{\mu\nu}}{d_\mu}\mathbf{I}_{d_\mu^2}$$

where $\mathbf{I}_{d_\mu^2}$ is the ${d_\mu}^2 \times {d_\mu}^2$ identity on $\mathrm{End}(V_\mu)$.

- The result is $$\mathcal{RBR}^\dagger = \bigoplus_\mu \frac{\mathbf{I}_{d_\mu^2}}{d_\mu} \otimes |I_{m_\mu}\rangle\langle I_{m_\mu}|$$

  from which we can read off the rank:

$$\boxed{\mathrm{rank}(\mathcal{B}) = \sum_\mu {d_\mu}^2}$$

- (Another formula also: $\int |\mathrm{tr}(U)|^{2t}\,\mathrm{d}U = \mathrm{Tr}(\mathcal{B}^2) = \mathrm{Tr}((\mathcal{RBR}^\dagger)^2) = \sum_\mu {m_\mu}^2$)
- But how does $U^{\otimes r} \otimes \overline{U}^{\otimes s}$ decompose? Luckily, this has already been worked out

Lower bounds

- The irreps of $\mathrm{U}(d)$ are labeled by nonincreasing integer partitions of length d:

$$\mu = (\mu_1, \ldots, \mu_d), \qquad \mu_i \geq \mu_{i+1}, \qquad \mu_i \in \mathbb{Z}$$

- The dimension of the irrep (ρ_μ, V_μ) is

$$d_\mu = \dim V_\mu = \prod_{1 \leq i < j \leq d} \frac{\mu_i - \mu_j + j - i}{j - i} \qquad \text{(Weyl's dimension formula)}$$

- Let μ_+ be the subsequence of μ of positive integers. Let $|\mu| = \sum_i \mu_i$.

eg. $\mu = (1, 1, 0, -1, -2)$, $\quad |\mu| = -1$, $\quad \mu_+ = (1, 1)$, $\quad |\mu_+| = 2$

- Theorem [Stembridge (1987,1989), Benkart et al (1994)]: The irreducible representations that occur in $U^{\otimes r} \otimes \overline{U}^{\otimes s}$ are precisely those with

$$|\mu| = r - s \qquad \text{and} \qquad |\mu_+| \leq r$$

Lower bounds

- And finally, our lower bound:

Theorem

Let (X, w) be a weighted t-design for $\mathrm{U}(d)$. Then for any $r + s = t$,

$$|X| \geq \dim(\mathrm{Hom}(\mathrm{U}(d), r, s)) = \sum_{\substack{|\mu| = r - s \\ |\mu_+| \leq r}} {d_\mu}^2$$

where the sum is over nonincreasing, length-d integer sequences μ, and

$$d_\mu = \prod_{1 \leq i < j \leq d} \frac{\mu_i - \mu_j + j - i}{j - i}$$

Lower bounds

- The best bounds come from the choices $r = \lceil t/2 \rceil$ and $s = \lfloor t/2 \rfloor$:

$$|X| \geq \dim(\mathrm{Hom}(\lceil t/2 \rceil, \lfloor t/2 \rfloor)) = \textstyle\sum_\mu {d_\mu}^2$$

which, for small t, are

$t = 1: \quad |X| \geq d^2,$

$t = 2: \quad |X| \geq d^4 - 2d^2 + 2,$ – originally due to Gross, Audenaert, Eisert (200

$t = 3: \quad |X| \geq d^2(d^4 - 3d^2 + 6)/2,$

$$t = 4: \quad |X| \geq \begin{cases} 35, & d = 2 \\ (d^8 - 6d^6 + 25d^4 - 28d^2 + 16)/4, & d \geq 3 \end{cases}$$

$$t = 5: \quad |X| \geq \begin{cases} 56, & d = 2 \\ 2835, & d = 3 \\ d^2(d^8 - 8d^6 + 47d^4 - 88d^2 + 84)/12, & d \geq 4 \end{cases}$$

Lower bounds

- Another rough bound comes from the choices $r = t$ and $s = 0$:

$$\begin{aligned} |X| &\geq \dim(\mathrm{Hom}(\mathrm{U}(d), t, 0)) \\ &= \dim(\mathrm{Hom}(\mathbb{C}^{d^2}, t, 0)) \\ &= \binom{d^2 + t - 1}{t} \end{aligned}$$

from which the asymptotics easily follow:

$$|X| = \Omega(d^{2t}) \qquad \text{for fixed } t$$

$$|X| = \Omega(t^{d^2-1}) \qquad \text{for fixed } d$$

(constructions meeting the second are known for $\mathrm{U}(2)$)

Tight designs?

- Are these lower bounds achievable? A design that meets a bound is called tight:

$$|X| = \dim(\mathrm{Hom}(\lceil t/2 \rceil, \lfloor t/2 \rfloor)) = \textstyle\sum_\mu {d_\mu}^2$$

- These are interesting because considerable structure is then enforced:

  Let $\{|e_U\rangle\}_{U\in X}$ be an orthonormal basis for $\mathbb{C}^{|X|}$ and construct another:

$$|f^\mu_{ij}\rangle := \sum_{U\in X} \sqrt{w(U)}\, f^\mu_{ij}(U)\, |e_U\rangle$$

  where the polynomials $f^\mu_{ij}(U) := \sqrt{d_\mu}\langle e^\mu_i|\rho_\mu(U)|e^\mu_j\rangle$ form an orthonormal basis for $\mathrm{Hom}(\lceil t/2 \rceil, \lfloor t/2 \rfloor)$, by Schur orthogonality. Thus $\{|f^\mu_{ij}\rangle\}$ is an orthonormal basis for $\mathbb{C}^{|X|}$:

$$\langle f^\mu_{ij}|f^\nu_{kl}\rangle = \sum_{U\in X} w(U)\overline{f^\mu_{ij}(U)} f^\nu_{kl}(U) = \int_{\mathrm{U}(d)} \overline{f^\mu_{ij}(U)} f^\nu_{kl}(U)\mathrm{d}U = \delta_{\mu\nu}\delta_{ik}\delta_{jl}$$

  since (X, w) is a t-design and $\overline{f^\mu_{ij}(U)} f^\nu_{kl}(U) \in \mathrm{Hom}(t, t)$.

Tight designs?

- Now since $\{|f_{ij}^{\mu}\rangle\}$ is an orthonormal basis for $\mathbb{C}^{|X|}$: $\displaystyle\sum_{i,j,\mu} |f_{ij}^{\mu}\rangle\langle f_{ij}^{\mu}| = I_{|X|}$

Or

$$\begin{aligned}
\delta_{UV} = \langle e_U|e_V\rangle &= \sum_{i,j,\mu} \langle e_U|f_{ij}^{\mu}\rangle\langle f_{ij}^{\mu}|e_V\rangle \\
&= \sqrt{w(U)w(V)} \sum_{i,j,\mu} \overline{f_{ij}^{\mu}(U)} f_{ij}^{\mu}(V) \\
&= \sqrt{w(U)w(V)} \sum_{i,j,\mu} d_\mu \langle e_j^{\mu}|\rho_\mu(U)^\dagger|e_i^{\mu}\rangle\langle e_i^{\mu}|\rho_\mu(V)|e_j^{\mu}\rangle \\
&= \sqrt{w(U)w(V)} \sum_{\mu} d_\mu \,\mathrm{tr}[\rho_\mu(U)^\dagger \rho_\mu(V)] \\
&= \sqrt{w(U)w(V)} \sum_{\mu} d_\mu \,\mathrm{tr}[\rho_\mu(U^\dagger V)] \\
&= \sqrt{w(U)w(V)} \sum_{\mu} d_\mu \chi_\mu(U^\dagger V)
\end{aligned}$$

where the characters $\chi_\mu := \mathrm{tr}\,\rho_\mu$ are known in terms of Schur polynomials.

Tight designs?

- Choosing $U = V$ we obtain $1 = w(U)\sum_\mu d_\mu \chi_\mu(I) = w(U)\sum_\mu {d_\mu}^2 = w(U)|X|$.

  ie. tight designs are necessarily unweighted: $w(U) = 1/|X|$

- The other tightness conditions are: $$\sum_\mu d_\mu \chi_\mu(U^\dagger V) = 0, \quad U \neq V \in X$$

- These are in fact both necessary and sufficient conditions for any (X, w) to be a t-design when $|X| = \sum_\mu {d_\mu}^2$.

- Tight 1-designs: The sum contains only the standard irrep $\mu = (1, 0, \ldots, 0)$,

$$d_{(1,0,\ldots,0)}\chi_{(1,0,\ldots,0)}(U^\dagger V) = d\,\mathrm{tr}(U^\dagger V) = 0, \quad U \neq V \in X$$

  ie. tight 1-designs are unitary operator bases (and thus exist in every dimension).

Tight designs?

- Tight 2-designs: The sum contains two irreps,

$$d_{(0,\ldots,0)}\chi_{(0,\ldots,0)}(U^\dagger V) \;+\; d_{(1,0,\ldots,0,-1)}\chi_{(1,0,\ldots,0,-1)}(U^\dagger V)$$
$$= \quad 1\cdot 1 \quad + \quad (d^2-1)\cdot\left(\left|\mathrm{tr}(U^\dagger V)\right|^2 - 1\right) \quad = \quad 0$$

ie. tight 2-designs are equiangular: $\left|\mathrm{tr}(U^\dagger V)\right|^2 = 1 - \frac{1}{d^2-1}, \quad U \neq V \in X$

- Tight unitary 2-designs, if they were to exist, would define "SIC-POVMs" that are informationally complete on the (operator) subspace defined by taking convex combinations of maximally entangled (mixed) states. Such POVMs would be optimal for ancilla-assisted process tomography of unital channels [AJS (2008)].

- But it is proven that they do not exist for $\mathrm{U}(2)$, ie. $|X| > d^4 - 2d^2 + 2 = 10$ for $d = 2$, and computer searches suggest that they do not exist in general.

- Tight t-designs: ... complicated, but we think they don't exist for $t > 1$ anyway.

Tight designs?

- If we cannot achieve $|X| = \sum_\mu {d_\mu}^2$, can we at least find a construction with $|X| = O(d^{2t})$, thus implying our bounds are asymptotically optimal.

- Asymptotically tight 2-designs:

  So far, the most efficient construction of a unitary 2-design that we know of is the projective Clifford group: $|X| = |\mathbb{F}_d^2 \rtimes \mathrm{Sp}(2,d)| = d^5 - d^3$ $(d = p^n)$.

  But the bound is a factor of d lower: $|X| \geq d^4 - 2d^2 + 2$!

- Open problem: Find a family of unitary 2-designs with $|X| = O(d^4)$.

- In the $\mathbb{C}^d$ case the lower bound $|X| \geq d^2$ is saturated asymptotically by complete sets of MUBs: $|X| = d^2 + d$ $(d = p^n)$.

- Do there exist complete sets of mutually unbiased unitary bases (MUUBs)?

Two bases $\{U_k\}$ and $\{V_k\}$ are mutually unbiased if $|\,\mathrm{tr}({U_j}^\dagger V_k)| = 1$ for all j, k.

Tight designs?

- Tight 2-designs: The sum contains two irreps,

$$
\begin{aligned}
& d_{(0,\ldots,0)}\chi_{(0,\ldots,0)}(U^\dagger V) \;+\; d_{(1,0,\ldots,0,-1)}\chi_{(1,0,\ldots,0,-1)}(U^\dagger V) \\
= \quad & 1\cdot 1 \qquad\qquad\qquad + \quad (d^2-1)\cdot\left(\left|\mathrm{tr}(U^\dagger V)\right|^2-1\right) \quad = \quad 0
\end{aligned}
$$

ie. tight 2-designs are equiangular: $\left|\mathrm{tr}(U^\dagger V)\right|^2 = 1 - \frac{1}{d^2-1}, \quad U \neq V \in X$

- Tight unitary 2-designs, if they were to exist, would define "SIC-POVMs" that are informationally complete on the (operator) subspace defined by taking convex combinations of maximally entangled (mixed) states. Such POVMs would be optimal for ancilla-assisted process tomography of unital channels [AJS (2008)].

- But it is proven that they do not exist for $\mathrm{U}(2)$, ie. $|X| > d^4 - 2d^2 + 2 = 10$ for $d = 2$, and computer searches suggest that they do not exist in general.

- Tight t-designs: ... complicated, but we think they don't exist for $t > 1$ anyway.

Tight designs?

- If we cannot achieve $|X| = \sum_\mu {d_\mu}^2$, can we at least find a construction with $|X| = O(d^{2t})$, thus implying our bounds are asymptotically optimal.

- Asymptotically tight 2-designs:

  So far, the most efficient construction of a unitary 2-design that we know of is the projective Clifford group: $|X| = |\mathbb{F}_d^2 \rtimes \mathrm{Sp}(2,d)| = d^5 - d^3$ $(d = p^n)$.

  But the bound is a factor of d lower: $|X| \geq d^4 - 2d^2 + 2$!

- Open problem: Find a family of unitary 2-designs with $|X| = O(d^4)$.

- In the $\mathbb{C}^d$ case the lower bound $|X| \geq d^2$ is saturated asymptotically by complete sets of MUBs: $|X| = d^2 + d$ $(d = p^n)$.

- Do there exist complete sets of mutually unbiased unitary bases (MUUBs)?

> Two bases $\{U_k\}$ and $\{V_k\}$ are mutually unbiased if $|\operatorname{tr}({U_j}^\dagger V_k)| = 1$ for all j, k.

Tight designs?

- There can be at most d^2-1 pairwise mutually unbiased bases in $\mathrm{U}(d)$:

Define the embedding $\vartheta : \mathrm{U}(d) \hookrightarrow \mathbb{R}^{(d^2-1)^2}$ by

$$\vartheta(U) \;:=\; |U\rangle\langle U| - I/d^2 \;=\; \sum_{j,k=1}^{d^2-1} r_{jk}\,\lambda_j \otimes \lambda_k\,, \qquad r \in \mathbb{R}^{(d^2-1)^2}$$

where $|U\rangle := (I\otimes U)\frac{1}{\sqrt{d}}\sum_k |k\rangle\otimes|k\rangle$ and $\{\lambda_k\}$ is a basis for traceless Hermitians. A basis $\{U_k\}$ then specifies the vertices of a regular simplex in the (d^2-1)-dimensional subspace of $\mathbb{R}^{(d^2-1)^2}$ spanned:

$$\frac{d^2}{d^2-1}\,\mathrm{tr}[\vartheta(U_j)\vartheta(U_k)] = \frac{d^2}{d^2-1}\,|\langle U_j|U_k\rangle|^2 - \frac{1}{d^2-1} = \begin{cases} 1, & j=k \\ -1/(d^2-1) & j\neq k \end{cases}$$

Mutually unbiased bases, $\{U_k\}$ and $\{V_k\}$, correspond to orthogonal subspaces:

$$\mathrm{tr}[\vartheta(U_j)\vartheta(V_k)] = |\langle U_j|V_k\rangle|^2 - 1/d^2 = |\,\mathrm{tr}(U_j{}^\dagger V_k)|^2/d^2 - 1/d^2 = 0\,,$$

of which, there can be at most $(\dim \mathbb{R}^{(d^2-1)^2})/(d^2-1) = d^2-1$ many.

Tight designs?

- The union of d^2-1 MUUBs is an unweighted 2-design (of size $|X| = d^4 - d^2$). Use the inner-product test:

$$\frac{1}{|X|^2}\sum_{U,V\in X}\left|\mathrm{tr}(U^\dagger V)\right|^4 = \frac{1}{d^4(d^2-1)^2}\Big[\underbrace{(d^2-1)d^2\cdot d^4}_{U=V} + \underbrace{(d^2-1)(d^2-2)d^4\cdot 1}_{U,V \text{ from different bases}}\Big] = 2 \checkmark$$

- These are the unique minimal 2-designs that consist entirely of unitary bases:

  Theorem: Suppose $X \subseteq \mathrm{U}(d)$ is the union of a family of m unitary operator bases. If (X, w) is a weighted 2-design, where w is constant across members of the same basis, then $m \geq d^2 - 1$ with equality only if X is the union of a complete set of MUUBs and $w(U) = 1/|X|$. [AJS (2008)]

- Do there exist complete sets of MUUBs? Yes! Well... at least in some dimensions: They are known for $d = 2, 3, 5, 7, 11$ as special subgroups of the projective Clifford group that were discovered by Chau (2005).

- Open problem: Find more MUUBs (if they exist).

Upper bounds

- The general theorem of Seymour and Zaslavsky (1984) on averaging sets applies to unitary designs:

  For any t and d, and all large enough n, there exists an unweighted unitary t-design in $\mathrm{U}(d)$ of size $|X| = n$.

- Relaxing to weighted designs allows us to bound the size of the smallest:

  Theorem

  For any t and d, there exists a weighted t-design in $\mathrm{U}(d)$ of size

$$|X| \leq \dim(\mathrm{Hom}(\mathrm{U}(d), t, t)) = O(d^{4t})$$

Upper bounds

- Proof:

Let $A := \int U^{\otimes t} \otimes \overline{U}^{\otimes t} \mathrm{d}U$. Then $\int |U^{\otimes t} \otimes \overline{U}^{\otimes t} - A\rangle \mathrm{d}U = 0$ and thus

$$0 \in \mathrm{conv}\{|U^{\otimes t} \otimes \overline{U}^{\otimes t} - A\rangle\}_{U \in \mathrm{U}(d)}$$

By Carathéodory's theorem, there exists a finite $X \subset \mathrm{U}(d)$ such that

$$0 \in \mathrm{conv}\{|U^{\otimes t} \otimes \overline{U}^{\otimes t} - A\rangle\}_{U \in X}$$

$\Rightarrow \exists\ w(U) > 0$ such that $\sum_{U \in X} w(U) |U^{\otimes t} \otimes \overline{U}^{\otimes t} - A\rangle = 0$

$\Rightarrow (X, w)$ is a t-design

Again by Carathéodory's theorem, X can be chosen with size

$$\begin{aligned} |X| &\leq \dim_{\mathbb{R}} \left(\mathrm{span}_{\mathbb{R}}\{|U^{\otimes t} \otimes \overline{U}^{\otimes t} - A\rangle\}_{U \in \mathrm{U}(d)}\right) + 1 \\ &= \dim(\mathrm{Hom}(t,t)) - 1 + 1 \\ &= \dim(\mathrm{Hom}(t,t)) \end{aligned}$$

Constructions

- Group designs (Gross et al, 2007): Let ρ be a unitary representation of a finite group G. Since $\rho(g)^\dagger \rho(h) = \rho(g^{-1}h)$ we can test whether the image of ρ is a t-design in terms of the character $\chi := \operatorname{tr}\rho$ alone:

  Corollary ("inner-product test" translated for group designs)

  Let G be a finite group and $\rho : G \to \mathrm{U}(d)$ a representation with character χ. Then $X = \{\rho(g) : g \in G\}$ is a unitary t-design if and only if

  $$\frac{1}{|G|}\sum_{g\in G} |\chi(g)|^{2t} = \int_{\mathrm{U}(d)} |\mathrm{tr}(U)|^{2t}\, dU.$$

- X is a 1-design iff ρ is irreducible: $\sum_\mu m_\mu^2 = \frac{1}{|G|}\sum_g |\chi(g)|^2 = \int |\mathrm{tr}(U)|^2 \mathrm{d}U = 1$

  We can therefore restrict to irreducible representations, in which case $\rho(g) \propto I$ for all $g \in Z(G)$, by Schur's lemma, and the size of the design can be reduced to $|G/Z(G)|$ by ignoring the $|Z(G)|$ different phase factors.

- We can now harvest unitary designs from the known character tables ...

d	t	lower bound	$\|X\| = \|H\|$	$H = G/Z(G)$	G {χ no.}
q	2	$q^4 - 2q^2 + 2$	$q^5 - q^3$	$\mathbb{F}_q^2 \rtimes \mathrm{Sp}(2,q)$	
2	2	10	12	$\mathbb{F}_2^2 \rtimes H'_{C2} \cong A_4$	SL(2,3) {4}
2	3	20	24	$\mathbb{F}_2^2 \rtimes \mathrm{Sp}(2,2) \cong S_4$	GL(2,3) {4}
2	5	56	60	A_5	SL(2,5) {2}
3	2	65	72	$\mathbb{F}_3^2 \rtimes H'_{C3}$	2^3.L3(2) {2}
3	3	270	360	A_6	3.A6 {8}
4	3	1 712	2 520	A_7	6.A7 {10}
5	2	577	600	$\mathbb{F}_5^2 \rtimes H'_{C5}$	5^1+2.2A4 {9}
6	2	1 226	2 520	A_7	6.A7 {31}
6	3	21 492	40 320		6.L3(4).2_1 {49}
7	2	2 305	2 352	$\mathbb{F}_7^2 \rtimes H'_{C7}$	
8	2	3 970	20 160		4_1.L3(4) {19}
9	2	6 401	12 960	$\mathbb{F}_3^4 \rtimes H'_{GAE}$	
10	2	9 802	95 040		2.M12 {16}
11	2	14 401	14 520	$\mathbb{F}_{11}^2 \rtimes H'_{C11}$	
12	3	1 462 320	448 345 497 600		6.Suz {153}
14	2	38 026	87 360		Sz(8).3 {4}
18	3	16 849 620	50 232 960		3.J3 {22}
21	2	193 601	9 196 830 720		3.U6(2) {47}
26	2	455 626	17 971 200		2F4(2)' {2}
28	2	613 090	145 926 144 000		2.Ru {37}
45	2	4 096 577	10 200 960		M23 {3}
342	2	13 680 343 370	460 815 505 920		3.ON {31}
1333	2	$3.157.. \times 10^{12}$	$8.677.. \times 10^{19}$		J4 {2}

(mostly stolen from Gross et al (2007))

Constructions

- U(2) t-designs: These are equivalent to $\mathbb{PR}^4$ t-designs through the isomorphism

$$e^{i\phi}U = r_0 I + i(r_1 X + r_2 Y + r_3 Z), \quad (r_0, r_1, r_2, r_3) \in \mathbb{R}^4$$

- From the known constructions of real projective designs:

t	standard lower bound	known better bound	construction
1	4	-	4
2	10	11	11
3	20	21	23
4	35	37	43
5	56	60	60
6	84	89	
7	120	134	264
8	165	180	
9	220	250	360
10	286	318	

- The optimal U(2) 2-design is necessarily weighted.

- Shamisiev (2006) has constructions with $|X| = O(t^3)$ for all t, which is optimal.

Conclusions and open questions

- Unitary designs are new and there is still much to be discovered.
- The lower bound method of Delsarte, Goethels and Seidel has now been extended to this case:

  A. Roy and A. J. Scott, Unitary designs and codes, arXiv:0809.3813.
- But efficient constructions of unitary designs remain elusive.
- Have all examples of complete sets of MUUBs already been discovered?
- Is there a family of unitary 2-designs with sizes $|X| = O(d^4)$?