G2C2 Lecture No. 7. The explicit constructions of unitary t-designs

Eiichi Bannai

August 15, 2024

References

[1] Roy-Scott: Unitary designs and codes, Des. Codes Cryptogr. (2009).

[2] Bannai-Nakata-Okuda-Zhao: Explicit construction of exact unitary designs, Advances in Math. (2022).

We give more references later.

Plan of this talk.

(1) The concept of unitary t-design.

(2) The Classification of unitary t-groups (Bannai-Navarro-Rizo-Tiep).

(3) Explicit constructions of unitary 4-designs in $U(4)$. (Bannai-Nakahara-Zhao-Zhu).

(4) Explicit constructions of unitary t-designs in $U(d)$ for any t and any d (Bannai-Nakata-Okuda-Zhao).

(5) Another approach. (Bannai-Okuda-Xiang-Zhao).

(6) Final Remarks.

The concept of unitary t-designs.

The purpose of design theory is, for a given space M, try to find finite subsets that approximate the space M well. There are various design theories for various spaces M. Unitary t-designs are when $M = U(d)$ (the unitary group $U(d)$).

Definition (unitary t-design). A finite subset X of the unitary group $U(d)$ is called a unitary t-design, if

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

for any $f(U) \in Hom(U(d), t, t)$. (Here we are normalizing $|U(d)| = 1$.)

Here, $Hom(U(d), r, s)$ = the space of polynomials that are homogeneous of degree r in the matrix entries of U, and homogeneous of degree s in the complex conjugates of the matrix entries of U.

This definition is known to be equivalent to the following definition.
Definition. A finite subset X of $U(d)$ is called a unitary t-design if

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

where dU denotes the unit Haar measure on $U(d)$.

Another equivalent definition of unitary t-design follows from the following theorem.

Theorem. For any finite subset X of $U(d)$,

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

with equality if and only if X is a unitary t-design.

Further equivalent definition will be explained later.

History of the study of unitary t-designs.
(The concept was started in physics.)

(1) D. Gross, K. Andenaert and J. Eisert : Evenly distributed unitaries: On the structure of unitary designs, J. Math. Physics (2007),
(2) A. J. Scott : Optimizing quantum process tomography with unitary 2-designs, J. Physics A (2008),
(3) A. Roy and A. J. Scott : On unitary designs and codes, Designs, Codes and Cryptography (2009),
(4) H. Zhu, R. Kueng, M. Grassl and D. Gross : The Clifford group fails gracefully to be unitary 4-design, arXiv:1609.08172v1.

What are known on unitary t-designs ?

- Unitary t-designs in $U(d)$ exist for any t and any d (Seymour-Zaslavsky).

- On the other hand, the explicit constructions of them are not easy in general. (We will come back to this question.)

- We can consider Fisher type lower bound for $|X|$ and tight unitary t-designs. (But the classification of tight unitary t-designs are still open. We will not discuss this topic today.)

Review on Irreducible representations of $U(d)$.
(Cf. Roy-Scott (2009) in most cases below.)

The irreducible representations of $U(d)$ are parametrized by the non-increasing length-d integer sequences:
$\mu = (\mu_1, \mu_2, \ldots, \mu_d)$ with $\forall \mu_i \in \mathbb{Z},\ \mu_1 \geq \mu_2 \geq \ldots \geq \mu_d$.

The degree of the representation μ is given by

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

(Note that $d_{(1,0,\ldots,0)} = d$.)

• Let $V = \mathbb{C}^d$ be the space on which $U(d)$ acts naturally. Then the irreducible representations of $U(d)$ appearing in $V^{\otimes r} \otimes (V^*)^{\otimes s}$ are those $\mu = (\mu_1, \mu_2, \ldots, \mu_d)$ with
$|\mu| = \mu_1 + \mu_2 + \cdots + \mu_d = r - s$ and $\mu_+ \leq r$,
where μ_+ =the sum of those positive μ_i's.

• $\dim(\mathrm{Hom}(U(d), r, s)) = D(d, r, s)$

$$= \sum_{|\mu|=r-s,\ \mu_+ \leq r} d_\mu^2.$$

$$D(d,0,0) = 1,$$
$$D(d,1,1) = (d^2-1)^2 + 1 = d^4 - 2d^2 + 2,$$
$$D(d,2,2) = \frac{1}{4}(d^8 - 6d^6 + 25d^4 - 28d^2 + 16),$$
$$D(d,3,3) = \frac{1}{36}(d^{12} - 12d^{10} + 103d^8 - 378d^6 + 778d^4 - 600d^2 + 252),$$

Fisher type inequalities for unitary t-designs.

• $X \subset U(d)$ is a $2e$-design $\Longrightarrow |X| \geq D(d,e,e)(\approx \frac{d^{4e}}{(e!)^2})$.

We call $X \subset U(d)$ to be a unitary tight $2e$-design, if X is a $2e$-design with $|X| = D(d,e,e)$.

• For odd $t = 2e+1$, Fisher type lower bound becomes $|X| \geq D(d,e+1,e)(\approx \frac{d^{4e+2}}{(e+1)!e!})$.

Also, a $(2e+1)$-design X is called a tight unitary $(2e+1)$-design if $|X| = D(d,e+1,e)$.

(The classification of tight unitary t-designs, as well as how Fisher type inequality is close to the reality is still open.)

The classification of Unitary t-groups

- Unitary t-designs in $U(d)$ exist for any t and d.
- But the explicit constructions are difficult in general.

Definition (unitary t-group). If a unitary t-design X in $U(d)$ is itself a group, then such X is called a unitary t-group in $U(d)$. (We sometimes denote X by G.)

- Let χ be the natural representation $U(d)$ of degree d. It is known that G is a unitary t-group in $U(d)$, if and only if the decomposition of $\chi^{\otimes t}$ into the irreducible representations of G is the same as the decomposition into the irreducible representations of $U(d)$.

- Also, G is a unitary t-group in $U(d)$, if and only if

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

Namely, $G\subset U(d)$ is a unitary t-group, if and only if

$$M_{2t}(G,V)=M_{2t}(U(d),V).$$

where the LHS

$$M_{2t}(G,V)=(\chi^t,\chi^t)_G=\frac{1}{|G|}\sum_{g\in G}\chi^t(g)\overline{\chi^t(g)}=\frac{1}{|G|}\sum_{g\in G}|tr(g)|^{2t},$$

where χ is the character of the natural representation of $U(d)$.
The RHS is

$$M_{2t}(U(d),V)=(\chi^t,\chi^t)_{U(d)}=\int_{U\in U(d)}|tr(U)|^{2t}dU.$$

Remarks.

- For $d = 2$, there are some unitary 5-groups. For example, $G = SL(2, 5)$ of order 120. (On the other hand, there is no unitary 6-group in $U(2)$.)

- In Physics community, it seems that, for some $d \geq 3$, some unitary 3-groups were known (see the list in the next page). But no unitary 4-groups in $U(d)$ were known for all $d \geq 3$.

The following unitary 3-groups have been known.

- **The Clifford group $G = \mathbb{Z}_4 * 2_+^{1+2m} \cdot Sp(2m, 2)$ is known to be a unitary 3-group in $U(2^m)$, but cannot be a unitary 4-group.**

- **The following sporadic examples of unitary 3-groups for $U(d)$ ($d \geq 3$) have been known.**

(i) $d = 3$, $G = 3A_6$,
(ii) $d = 4$, $G = 6A_7$, $Sp(4, 3)$,
(iii) $d = 6$, $G = 6L_3(4) \cdot 2_1$, $6_1U_4(3)$,
(iv) $d = 12$, $G = 6Suz$,
(v) $d = 18$, $G = 3J_3$.

The classification of unitary t-groups.

Bannai-Navarro-Rizo-Tiep[BNRT]: Unitary t-groups, (J. Math. Soc. Japan, 2020), gave the following answer.

(i) We [BNRT] pointed out that the paper [GT] by Robert M. Guralnick and Pham Huu Tiep, "Decompositions of small tensor powers and Larsen's conjecture". Representation Theory, 9 (2005), 138-208.
already gave the non-existence of unitary t-groups in $U(d)$ for $t \geq 4$ (at least for $d \geq 5$.) Also, [GT] gives the complete classification of unitary t groups in $U(d)$ for all $t \geq 2$ and all $d \geq 5$.

(ii) We [BNRT] gave the complete classification of unitary t-groups (for all $t \geq 2$) for the remaining cases $d = 2, 3, 4$. The classifications for $d = 2, 3, 4$ are also very interesting, as finite unitary reflection groups (complex reflection groups) play very important roles.

Explicit Constructions: unitary 4-designs in $U(4)$

It seems that the explicit constructions of unitary 4-designs in $U(4)$ had not been made before. We answered this question by
Eiichi Bannai, Mikio Nakahara, Da Zhao, Yan Zhu [BNZZ]. "On the explicit constructions of certain unitary t-designs", J. Phys. A, 2019.

The rough method is as follows.

Theorem. Let χ be the natural representation of $U(d)$. Suppose that G is a unitary t-group in $U(d)$, and that

$$(\chi^{t+1}, \chi^{t+1})_G = (\chi^{t+1}, \chi^{t+1})_{U(d)} + 1.$$

Then there exist a non-trivial (unique up to scalar multiplication) $f \in Hom(U(d), t+1, t+1)^{G \times G}$. Let $x_0 \in U(d)$ be a zero of f. Then the orbit X of x_0 by the action of $G \times G$ on $U(d)$ becomes a unitary $(t+1)$-design in $U(d)$.

We [BNZZ] found explicit unitary 4-designs in $U(4)$ coming from the unitary 3-design $G = Sp(4, 3)$, (with $t = 3, d = 4$) based on the Theorem mentioned above. Exactly speaking, we can describe such examples numerically with the errors as small as we want.

(The size of the smallest unitary 4-designs in $U(4)$ thus constructed is $|Sp(4, 3)|^2/6 = 447897600$.)

§6 Explicit Constructions of exact unitary t-designs in $U(d)$ for any t and d.

Theorem (Bannai-Nakata-Okuda-Zhao, Advances in Math. vol. 405, 2022, Article ID 108457) For each pair of t and d, we can explicitly construct unitary t-designs in $U(d)$.

Idea of Proof. (1) Induction on d.
(2) We need a new concept of strong unitary t-design in $U(d)$ in order to use the induction.
(3) For any representation ρ of $U(d)$ (or any compact Lie group G), we say that a subset X in $U(d)$ is a ρ-design if

$$\frac{1}{|X|}\sum_{U\in X}\rho(U) = \int_{U\in G=U(d)}\rho(U)dU\text{............}(\star)$$

.

As we discussed before, irreducible representation of $U(n)$ are parametrized by non-increasing integer sequences:
$\lambda = (\lambda_1, \lambda_2, ..., \lambda_n)$. As before, let λ_+ be the sum of positive λ_i's and λ_- be the $-$ of the sum of negative λ_i's. We set

$$\Phi_n^{t,t} = \{\lambda \mid \lambda_+ = \lambda_- \leq t\}$$

and

$$\Psi_n^{t,t} = \{\lambda \mid \lambda_+ \leq t, \lambda_- \leq t\}$$

We define $X \subset U(n)$ to be a strong unitary t-design if the equality $(\star)$ holds for any irreducible representation $\rho_\lambda \in \Psi_n^{t,t}$.
Recall that $X \subset U(n)$ is a unitary t-design if the equality $(\star)$ hold for any irreducible representation $\rho_\lambda \in \Phi_n^{t,t}$. So, since $\Phi_n^{t,t} \subset \Psi_n^{t,t}$, a strong unitary t-design is a unitary t-design.

Let $G = U(n)$ and $K = U(m) \times U(n-m)$. (Then G/K is the Grassmanian space $G_{m,n}$. In particular, if $m = 1$, then it is the complex projective space.)
(1) We can easily construct strong unitary t-design in $U(1)$.
(2) Let X_m be a strong unitary t-design in $U(m)$ and X_{n-m} be a strong unitary t-design in $U(n-m)$. Then

$$X_{m,n-m} = \left\{ \begin{bmatrix} g & 0 \\ 0 & h \end{bmatrix} \,\middle|\, g \in X_m,\ h \in X_{n-m} \right\}$$

is a $\rho_\lambda |_K$-design in $K = U(m) \times U(n-m)$. (Namely, ρ-design for any irred. rep. ρ appearing in $\rho_\lambda |_K$.)
(3)Let $f_1, f_2, ..., f_\ell$ be all the zonal spherical functions on G/K and in $\Psi_n^{t,t}$. Let z_j be a zero of f_j for each $j = 1, 2, \ldots, \ell$. Then we can find elements $g_j \in G = U(n)$ whose action of g_j on G/K is the same as z_j.

(4) Then

$$\boldsymbol{X} = \boldsymbol{X}_n = \boldsymbol{X}_{m,n-m} \prod_{j=1}^{\ell} (\boldsymbol{g}_j \boldsymbol{X}_{m,n-m})$$

becomes a strong unitary t-design in $U(d)$.

Hence this gives explicit constructions of many unitary t-designs in $U(d)$ for any t and d.

Remark. This idea also gives explicit constructions of spherical t-designs in S^{n-1} by induction on n, by using $O(n)$ instead of $U(n)$.

Final Remark. **Our theorem was already applied to experimental physics in quantum information theory. Please see:**

Quantum circuits for exact unitary t-designs and applications to higher-order randomized benchmarking, PRX Quantum 2, 030339 (2021)

Authors: Yoshifumi Nakata, Da Zhao, Takayuki Okuda, Eiichi Bannai, Yasunari Suzuki, Shiro Tamiya, Kentaro Heya, Zhiguang Yan, Kun Zuo, Shuhei Tamate, Yutaka Tabuchi, Yasunobu Nakamura.

Another approach.

Here, we describe another (but similar) approach for the explicit construction of unitary t-designs in $U(n)$ by induction on n.

Let G be a compact Lie group, and let K be a closed subgroup of G. Let $\mu_G, \mu_K, \mu_{G/K}$ be the Haar measures on $G, K, G/K$ respectively with total measure normalized to be 1. For any representation of G, a finite set X of G is called a ρ-design, if

$$\frac{1}{|X|}\sum_{x\in X}\rho(x) = \int_G \rho(g)d\mu_g.$$

We use the following result of Okuda first obtained in his Ph.D thesis in 2013.

Theorem (Okuda). Let Y be a ρ-design on G/K, and let Γ be a ρ-design on K. Fix a map $s : Y \to G$ such that $\pi \circ s = id_Y$. Consider the following set

$$X(Y, s, \Gamma) = \{s(y)\gamma \mid y \in Y, \gamma \in \Gamma\} \subset G.$$

Then $X(Y, s, \Gamma)$ is a ρ-design on G.

The irreducible representations of $U(n)$ are parametrized by the dominant weight $\lambda = (\lambda_1, \lambda_2, ..., \lambda_n)$ of non-increasing integers. We denote by λ^+ the sum of positive integers of λ and by λ^- the sum of absolute value of negative entries in λ.

Now we define three subsets of the irreducible representations of $U(n)$.

$$\mathcal{T}_{\square}(n,t) := \{\lambda = (\lambda_1, \lambda_2, ..., \lambda_n) \mid \lambda^+, \lambda^- \leq t\},$$

$$\mathcal{T}_{/}(n,t) := \{\lambda = (\lambda_1, \lambda_2, ..., \lambda_n) \mid \lambda^+ = \lambda^- \leq t\},$$

$$\mathcal{T}_{\triangle}(n,t) := \{\lambda = (\lambda_1, \lambda_2, ..., \lambda_n) \mid \lambda^+ + \lambda^- \leq t\}.$$

Remark. $\mathcal{T}_{/}(n,t)$-design on $U(n)$ is nothing but the classical unitary t-design on $U(n)$. The strong unitary t-design (introduced before) is exactly unitary $\mathcal{T}_{\square}(n,t)$-design on $U(n)$. Since $\mathcal{T}_{/}(n,t), \mathcal{T}_{\triangle}(n,t) \subset \mathcal{T}_{\square}(n,t)$ and $\mathcal{T}_{/}(n,t) \subset \mathcal{T}_{\square}(n,t) \subset \mathcal{T}_{\triangle}(n,2t)$, we have the following fact.

(1) Any strong unitary t-design on $U(n)$ is a unitary t-design and a $\mathcal{T}_{\triangle}(n,t)$-design.

(2) Any $\mathcal{T}_{\triangle}(n,2t)$-design on $U(n)$ is a unitary t-design and a strong unitary t-design.

Consider the representation $\rho_\Lambda = \bigoplus_{\rho \in \mathcal{T}_{\triangle}(n,t)} \rho$ of $U(n)$. We want to apply the previous theorem to the case of $G = U(n), K = U(n-1)$, and $\rho = \rho_\Lambda$.

Note that $U(n)/U(n-1)$ is isomorphic to the complex sphere $\Omega(n)$ in ^{n}. Now we want to study the subspace $\mathcal{H}_{U(n-1)}^{\rho_\Lambda}$ and $\mathcal{H}_{\Omega(n)}^{\rho_\Lambda}$.

The subspace $\mathcal{H}_{U(n-1)}^{\rho_\Lambda}$ can be determined by the following theorem.

Theorem (see Bump, Theorem 41.1).
Let $\lambda = (\lambda_1, \lambda_2, ..., \lambda_n)$ $\mu = (\mu_1, \mu_2, ..., \mu_{n-1})$. Then the restriction of ρ_λ to $U(n-1)$ contains a copy of ρ_μ if and only if λ and μ interlace. The restriction of ρ_λ is multiplicity-free. Moreover, if λ and μ interlace, then we have $\mu^+ + \mu^- \leq \lambda^+ + \lambda^-$. Therefore, supp $\rho_\Lambda|_{U(n-1)} = \mathcal{T}_\triangle(n-1, t)$. Hence we determine the subspace $\mathcal{H}_{U(n-1)}^{\rho_\Lambda}$.

$$\mathcal{H}_{U(n-1)}^{\rho_\Lambda} = \mathcal{H}_{U(n-1)}^{T_\triangle(n-1,t)}.$$

Next, we determine the subspace $\mathcal{H}_{\Omega(n)}^{\rho_\Lambda}$.

Definition. For a fixed dimension n and non-negative integers p and q, $H_n(p, q)$ is the vector space of all harmonic homogeneous polynomials om $\mathbb{C}^n$ that have total degree p in the variables $z_1, z_2, ..., z_n$ and total degree q in the variables $\bar{z_1}, \bar{z_2}, ..., \bar{z_n}$.

It is known that these $H_n(p,q)$ are minimal unitary invariant spaces on $\Omega(n)$.

Note that X is a $\mathcal{T}_{\triangle}(n,t)$-design on $U(n)$ if and only if

$$\frac{1}{|X|}\sum_{U\in X} U^{\otimes r}\otimes (U^{\dagger})^{\otimes s} = \int_G U^{\otimes r}\otimes (U^{\dagger})^{\otimes s} d\mu(U)$$

holds for every nonnegative integers r and s suchthat $r+s\leq t$. Take $gK=U_zK$, where U_z is a unitary matrix with last column $z\in\Omega(n)$ and $K=\langle [M,0;0,1], M\in U(n-1)\rangle$. Observe that the functions appearing in $\mathcal{H}^{\rho_\Lambda}_{U(n)/U(n-1)}$ are in $\otimes_{p+q\leq t} H_n(p,q)$.

Recall that X is a complex spherical t-design on $\Omega(n)$ if and only if

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

holds for every $f\in\otimes_{p+q\leq t} H(p,q)$.

Now, $\mathcal{H}^{\rho_\Lambda}_{U(n-1)}$ and $\mathcal{H}^{\rho_\Lambda}_{\Omega(n)}$ are determined, we are ready to apply the previous theorem with $G=U(n), K=U(n-1)$, and $\rho|\rho_\Lambda$.

Corollary. Let Y be a complex spherical t-design on $\Omega(n) \cong U(n)/U(n-1)$, and let Γ be a $\mathcal{T}_{\triangle}(n-1,t)$-design on $U(n-1)$. Fix map $s : Y \to U(n)$ such that $\pi \circ s = id_Y$. Consider the following set

$$X(Y, s, \Gamma); = \{s(y)\gamma \mid y \in Y, \gamma \in \Gamma\} \subset U(n).$$

Then $X(Y, s, \Gamma)$ is a $\mathcal{T}_{\triangle}(n,t)$-design on $U(n)$.

By induction construction, we obtain the following Corollary.

Corollary. Let $Y_1, Y_2, ..., Y_n$ be complex spherical $2t$-designs on $\Omega(1), \Omega(2), , ..., \Omega(n)$ respectively. Then we can construct a $\mathcal{T}_{\triangle}(n, 2t)$-design on $U(n)$ inductively via the previous Corollary. In particular, it is a (strong) unitary t-design on $U(n)$.

Finally, we reduce complex spherical designs to real spherical designs.

Consider the following map $\phi : \mathbb{C}^d \to \mathbb{R}^{2d}$:

$$\phi(z_1, z_2, ..., z_d) = (Re(z_1), Im(z_1), Re(z_2), Im(z_2), ..., Re(z_d), Im(z_d)).$$

Note that ϕ maps points in the complex unit sphere $\Omega(d)$ to points in the real unit sphere S^{2d-1}.

Theorem. Let t, d be positive integers. Let t, d be positive integers. Let X be a subset of the complex sphere $\Omega(d)$. Then the followings are equivalent.

(1) The set X is a complex spherical t-design on $\Omega(d)$.

(2) The set $\phi(X)$ is a real spherical t-design on S^{2d-1}.

Corollary. Let $Y_1, Y_2, ..., Y_n$ be real spherical $2t$-design on $S^1, S^3, ..., S^{2n-1}$ respectively. Then we can construct a $\mathcal{T}_{\triangle}(n, 2t)$-design on $U(n)$ respectively via The previous Corollary and the above Theorem just mentioned. In particular, it is a (strong) unitary t-design on $U(n)$.

Thank You