(This is basically the exact copy of the slides of my talk.)

Unitary t-designs and unitary t-groups

Eiichi Bannai

(Professor Emeritus of Kyushu University)

Dec. 11, 2018 at RIMS, Kyoto, Japan

This talk is based on the paper [BNRT] : Eiichi Bannai, Gabriel Navarro, Noelia Rizo, Pham Huu Tiep, "Unitary t-groups", arXiv:1810.02507.

The purpose of "design theory" is, for a given space M, to find good finite subsets X that approximate the whole space M well.

1

Unitary t-designs are finite subsets X of the unitary group U(d) that approximate U(d) well.

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

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

for any $f(U) \in Hom(U(d), t, t)$.

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 matrix entries of U^* . History of the study of unitary t-designs.

(1) Gross-Andenaert-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) Roy-Scott : On unitary designs and codes, Designs, Codes and Cryptography (2009),

(4) Zhu-Kueng-Grassl-Gross : The Clifford group fails gracefully to be unitary 4-design, arXiv:1609.08172v1.

• Unitary t-designs in U(d) exist for any t and d.

But the explicit constructions are difficult in general. (There is some work by Takayuki Okuda.)

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

• It is known that G is a unitary t-group in U(d), if and only if

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

and also if and only if the decomposition of $U(d)^{\otimes t}$ into the irreducible representations of U(d) is the same as the decomposition into the irreducible representation of G.

 $\mathbf{2}$

3

 $\mathbf{4}$

Equivalently, $G \subset U(d)$ is a unitary *t*-design, if and only if

$$M_{2t}(G,V)=M_{2t}(\mathcal{G},V).$$

where the LHS

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

where χ is the natural representation of $G \hookrightarrow U(d)$ and $\chi^t = \chi \otimes \cdots \otimes \chi$ (t imes). The RHS $M_{2t}(\mathcal{G}, V)$ is the corresponding inner product

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

• Unitary *t*-groups have been studied in physics.

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

• For $d \ge 3$, some unitary 3-groups were known, but no unitary 4-groups were known.

The purpose of this talk is to clarify this situation.

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 is known not to be a unitary 4-group.

• The following sporadic examples of unitary 3-groups for U(d) $(d \ge 3)$ 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 following unitary 2-groups have been known (in addition to those already mentioned to be 3-groups). Note that this is not the complete list.

(i) Lie type case. (a) $G = PSp(2n, 3), d = \frac{3^n \pm 1}{2}$ (Weil representation) (b) $G = U_n(2), d = \frac{2^n - (-1)^n}{3}$ (Weil representation) (ii) Extra special case. (Clifford groups.) Let $d = p^m$ (p is a prime). $E = p_+^{1+2m}$ (p is odd prime), or $E = \mathbb{Z}_4 * 2_+^{1+2m}$ (for p = 2). Let H be a subgroup of Sp(2m, p) such that H acts transitively on $\mathbb{F}_p^{2m} - \{0\}$. Then $G = E \cdot H$ becomes a unitary 2-group in $U(p^m)$. Such H are basically classified by Hering in his determination of 2-transitive perm. groups.

 $\mathbf{5}$

6

$$egin{aligned} d &= 6 \; G = 6 A_7, \ d &= 8, \, G = 4_1 L_3(4), \ d &= 10, \, G = 2 M_{12}, \ d &= 10, \, G = 2 M_{22}, \ d &= 14, \, G = ^2 B_2(8) \cdot 3, \ d &= 26, \, G = ^2 F_4(2), \ d &= 28, \, G = 2 R u, \ d &= 45, \, G = M_{23}, \ d &= 45, \, G = M_{24}, \ d &= 342, \, G = 3 O' N, \ d &= 1333, \, G = J_4. \end{aligned}$$

8

The paper: Guralnick and Tiep, Decompositions of small tensor powers and Larsen's conjecture, Representation Theory 9 (2005), 138-208,

essentially obtained the following results.

(i) There is no unitary 4-groups in U(d) for $d \ge 5$.

(ii) The unitary 2-groups (and unitary 3-groups) are basically classified for $d \ge 5$.

(Basically those mentioned already.)

The exact statements will be mentioned later in the Appendix. Our joint paper [BNRT] arXiv: 1810.02507 also settles the remaining cases d = 2, 3, 4.

How I was involved in this work?

First, I noticed the paper of Tiep: Finite groups admitting grassmannian 4-designs, J. of Algebra 306 (2006), 227-243, which proved the following result :

Let G be a finite subgroup of O(d), and let χ be the natural embedding of $G \hookrightarrow O(d)$. Suppose that $sym^2\chi - 1$ is irreducible (as G-modules). Then such G are classified. (The list is very complicated.) Then I noticed that his method can be used to show that :

If χ is the embedding of $G \hookrightarrow U(d)$, and if $\chi \otimes \chi^* - 1$ is irreducible (as *G*-module), then *G* can be classified. (Then this in turn gives the classification of unitary 2-groups.)

So, I wrote to Tiep. Then I got his reply that this was already done by the Guralnick-Tiep paper (2005), although Tiep did not know this is related to the concept of unitary t-groups, being interested in physics.

Tiep was recently working on the explicit classification of $H \subset Sp(2m, p)$ acting transitively on $\mathbb{F}_p^{2m} - \{0\}$ together with Gabriel Navarro and Noelia Rizo.

Moreover, we were able to give the complete classification of unitary t-groups for U(d) for remaining cases d = 2, 3, 4. (The list is fairly involved, and is available below in the Appendix.)

This finally led to the joint paper [BNRT] with the 4 authors: Unitary t-groups, arXiv: 1810.02507.

9

10

Appendix.

Corollary 2 in [BNRT]. Let G < U(d) be a finite group and $d \ge 2$. Then G is a unitary t-group for some $t \ge 4$ if and only if d = 2, t = 4 or 5, and $G = \mathbb{Z}(G)SL_2(5)$.

Next, we obtain the following consequences of [Theorems 1.5, 1.6 in [GT], where $F^*(G) = F(G)E(G)$ denotes the generalized Fitting subgroup of any finite group G (respectively, F(G) is the Fitting subgroup and E(G) is the layer of G); furthermore, we follow the notation of [Atlas] for various simple groups. We also refer the reader to [GMST] and [TZ2] for the definition and basic properties of Weil representations of (certain) finite classical groups.

Theorem 3 of [BNRT](=[GT]).

Let $V = \mathbb{C}^d$ with $d \geq 5$ and let $\mathcal{G} = GL(V)$. For any finite subgroup $G < \mathcal{G}$, set $\overline{S} = S/Z(S)$ for $S := F^*(G)$. Then $M_4(G, V) = M_4(\mathcal{G}, V)$ if and only if one of the following conditions holds.

(i) (Lie-type case) One of the following holds.

(a) $\overline{S} = PSp_{2n}(3), n \ge 2, G = S$, and $V \downarrow_S$ is a Weil module of dimension $(3^n \pm 1)/2$.

(b) $\overline{S} = U_n(2), n \ge 4, [G:S] = 1 \text{ or } 3$, and $V \downarrow_S$ is a Weil module of dimension $(2^n - (-1)^n)/3$.

(ii) (Extraspecial case) $d = p^a$ for some prime p and $F^*(G) = F(G) = Z(G)E$, where $E = p_+^{1+2a}$ is an extraspecial p-group of order p^{1+2a} and type +. Furthermore, G/Z(G)E is a subgroup of $Sp(W) \cong Sp_{2a}(p)$ that acts transitively on $W - \{0\}$ for W = E/Z(E), and so is listed in Theorem 5 (below). If p > 2 then $E \triangleleft G$; if p = 2 then $F^*(G)$ contains a normal subgroup $E_1 \triangleleft G$, where $E_1 = C_4 * E$ is a central product of order 2^{2a+2} of $Z(E_1) = C_4 \leq Z(G)$ with E.

(iii) (Exceptional cases) $S = Z(G)[G^*, G^*]$, and $(\dim(V), \overline{S}, G^*)$ is as listed in Table I. Furthermore, in all but lines 2–6 of Table I, $G = Z(G)G^*$. In lines 2–6, either G = S or [G:S] = 2 and G induces on \overline{S} the outer automorphism listed in the fourth column of the table.

In particular, $G < \mathcal{H} = U(V)$ is a unitary 2-group if and only if G is as described in (i)–(iii).

(i)

(ii)

Table I. Exceptional examples in $\mathcal{G} = GL_d(\mathbb{C})$ with $d \ge 5$

d	\boldsymbol{S}	G^*	Outer	The largest $2k$ with	$M_{2k+2}(G.V) \ vs.$
u	N	ŭ	Outer	$M_{2k}(G,V)=M_{2k}(\mathcal{G},V)$	$M_{2k+2}(\mathcal{G}.V)$
6	A_7	$6A_7$		4	$21 \ vs. \ 6$
6	$L_{3}(4)$ (*)	$6L_3(4)\cdot 2_1$	2_1	6	$56 \ vs. \ 24$
6	$U_4(3)^{(*)}$	$6_1 \cdot U_4(3)$	2_2	6	$25 \ vs. \ 24$
8	$L_4(3)$	$4_1 \cdot L_3(4)$	2_3	4	$17 \ vs. \ 6$
10	M_{12}	$2M_{12}$	2	4	$15 \ vs. \ 6$
10	M_{22}	$2M_{22}$	2	4	$7 \ vs. \ 6$
12	$Suz^{(*)}$	6Suz		6	$25 \ vs. \ 24$
14	$^{2}B_{2}(8)$	$^{2}B_{2}(8) \cdot 3$		4	$90 \ vs. \ 6$
18	$J_3^{(st)}$	$3J_3$		6	$238 \ vs. \ 24$
26	$^{2}F_{4}(2)'$	$^{2}F_{4}(2)'$		4	$26 \ vs. \ 6$
28	Ru	2Ru		4	$7 \ vs. \ 6$
45	M_{23}	M_{23}		4	$817 \ vs. \ 6$
45	M_{24}	M_{24}		4	42 vs. 6
342	$O'\overline{N}$	3O'N		4	$3480 \ vs. \ 6$
1333	J_4	J_4		4	$8 \ vs. \ 6$

Note that in Table I, the data in the sixth column is given when we take $G = G^*$.

(iv) Theorem 4 in [BNRT]. Let $V = \mathbb{C}^d$ with $d \ge 5$ and let $\mathcal{G} = GL(V)$. Assume G is a finite subgroup of \mathcal{G} . Then $M_6(G, V) = M_6(\mathcal{G}, V)$ if and only if one of the following two conditions holds. (i) (Extraspecial case) $d = 2^a$ for some a > 2, and $G = Z(G)E_1 \cdot Sp_{2a}(2)$,

where $E \cong 2_{+}^{1+2a}$ is extraspecial and of type + and $E_1 = C_4 * E$ with $C_4 \leq \overline{Z}(G)$.

(ii) (Exceptional cases) Let $\overline{S} = S/\overline{Z}(S)$ for $S = F^*(G)$. Then

$$ar{S} \in \{L_3(4), U_4(3), Suz, J_3\},$$

and $(\dim(V), \overline{S}, G^*)$ is as listed in the lines marked by (\star) in Table I. Furthermore, either $G = \overline{Z}(G)G^*$, or $\overline{S} = U_4(3)$ and $S = \overline{Z}(G)G^*$.

In particular, $G < \mathcal{H} = U(V)$ is a unitary 3-group if and only if G is as described in (i), (ii).

(v)

Theorem 5 in [BNRT]. Let p be a prime and let $W = \mathbb{F}_p^{2n}$ be endowed with a non-degenerate symplectic form. Assume that a subgroup $H \leq Sp(W)$ acts transitively on $W - \{0\}$. Then (H, p, 2n)is as in one of the following cases.

(A) (Infinite classes):

 $\text{(i)} \ n=bs \text{ for some integers } b,s\geq 1 \text{, and } Sp_{2b}(p^s)' \lhd H \leq Sp_{2b}(p^s) \rtimes C_s.$

(ii) p = 2, n = 3s for some integer $s \ge 2$; and $G_2(2^s) \triangleleft H \le G_2(2^s) \rtimes C_s$. (B) (Small cases):

(i) (2n, p) = (2, 3), and $H = Q_8$.

(ii) (2n, p) = (2, 5), and $H = SL_2(3)$.

(iii) (2n, p) = (2, 7), and $H = SL_2(3).C_2 = \text{SmallGroup}(48, 28)$.

(iv) (2n, p) = (2, 11), and $H = SL_2(5)$.

(v) (2n, p) = (4, 3), and H = SmallGroup(160, 199), SmallGroup(320, 1581), 2.S₅, $SL_2(9)$, $SL_2(9) \rtimes C_2 = \text{SmallGroup}(1440, 4591)$, or $C_2 \cdot ((C_2 \times C_2 \times C_2 \times C_2) \rtimes A_5) = \text{SmallGroup}(1920, 241003)$.

(to be continued to the next page)

 $(ext{vi})$ $(ext{vi})$ $(2n, p) = (6, 2), ext{ and } H = SL_2(8), SL_2(8) \rtimes C_3, SU_3(3), SU_3(3) \rtimes C_2.$ $(ext{vii})$ $(2n, p) = (6, 3) ext{ and } H = SL_2(13).$

The case d = 4.

Next we complete the classification of unitary *t*-groups in dimension 4. First we introduce some key groups for this classification, where we use the notation of GAP for SmallGroup(64, 266) and PerfectGroup(23040, 2).

Notation. Consider an irreducible subgroup $E_4 = C_4 * 2^{1+4}_+ = ext{SmallGroup}(64, 266) ext{ of order } 2^6 ext{ of } GL(V),$ where $V = \mathbb{C}^4$, and let $\Gamma_4 := N_{GL(V)}(E_4).$

Next, we recall three complex reflection groups G_{29} , G_{31} , and G_{32} in dimension 4, namely, the ones listed on lines 29, 31, and 32 of [Table VII in Shephard-Todd]. A direct calculation using the computer packages GAP3 and Chevie shows that each of these 3 groups G, being embedded in $\mathcal{H} = U_4(\mathbb{C})$, is a unitary 2-group. Also,

$$F(G_{29})\cong F(G_{31})\cong ext{SmallGroup}(64,266),\; F(G_{32})=Z(G_{32})\cong C_6,$$

and

$$G_{29}/F(G_{29})\cong S_5,\;G_{31}/F(G_{31})\cong S_6,\;G_{32}\cong C_3 imes Sp_4(3).$$

In what follows, we will identify $F(G_{29})$ and $F(G_{31})$ with the subgroup E_4 defined just before. Let us denote the derived subgroup of G_k by G'_k for $k \in \{29, 31, 32\}$. With this notation, we can give a complete classification of unitary 2-groups and unitary 3-groups in the following statement.

(viii) Theorem 7 in [BNRT]. Let $V = \mathbb{C}^4$, $\mathcal{G} = GL(V)$, and let $G < \mathcal{G}$ be any finite subgroup. Then the following statements hold. (A) With E_4 , Γ_4 and L as defined before, we have that $[\Gamma_4, \Gamma_4] = L = G'_{31}$ and $\Gamma_4 = Z(\Gamma_4)G_{31}$. Furthermore, $M_4(G, V) = M_4(\mathcal{G}, V)$ if and only if one of the following conditions holds

(A1) G = Z(G)H, where $H \cong 2A_7$ or $H \cong Sp_4(3) \cong G'_{32}$.

(A2) $L = [G, G] \le G < \Gamma_4$.

(A3) $E_4 \triangleleft G < \Gamma_4$, and, after a suitable conjugation in Γ_4 ,

$$G_{29}'=[G,G]\leq G\leq Z(\Gamma_4)G_{29}.$$

In particular, $G < \mathcal{H} = U(V)$ is a unitary 2-group if and only if G is as described in (A1)–(A3).

(B) $M_6(G, V) = M_6(\mathcal{G}, V)$ if and only if G is as described in (A1)–(A2). In particular, G < U(V) is a unitary 3-group if and only if G is as described in (A1)–(A2).

(C) $M_8(G, V) > M_8(\mathcal{G}, V)$. In particular, no finite subgroup of $U_4(\mathbb{C})$ can be a unitary 4-group.

(vii)

The cases d = 3 and d = 2.

Now we recall three complex reflection groups $G_4 \cong SL_2(3)$, $G_{12} \cong GL_2(3)$, and $G_{16} \cong C_5 \times SL_2(5)$ in dimension d = 2, listed on lines 4, 12, and 16 of [Table VII in Shephard-Todd], and three complex reflection groups $G_{24} \cong C_2 \times SL_3(2)$, $G_{25} \cong 3^{1+2}_+ \rtimes SL_2(3)$, and $G_{27} \cong C_2 \times 3A_6$ in dimension d = 3, listed on lines 24, 25, and 27 of [Table VII in S-T]. As above, for any of these 6 groups G_k , G'_k denotes its derived subgroup. A direct calculation using the computer packages GAP3 and Chevie shows that each of these 6 groups G, being embedded in $\mathcal{H} = U_d(\mathbb{C})$, is a unitary 2-group; furthermore, G_{12} , G'_{16} , and G'_{27} are unitary 3-groups. One can check that $F(G_4) \cong F(G_{12})$ is a quaternion group $Q_8 = 2^{1+2}_-$, and we will identify them with an irreducible subgroup $E_2 \cong Q_8$ of $GL_2(\mathbb{C})$. Also, $E_3 := F(G_{25}) \cong 3^{1+2}_+$ is an extraspecial 3-group of order 27 and exponent 3, which is an irreducible subgroup of $GL_3(\mathbb{C})$. Let $\Gamma_d := N_{GL_d(\mathbb{C})}(E_d)$ for d = 2, 3. Now we can give a complete classification of unitary t-groups in dimensions 2 and 3.

(x) Theorem 9 in [BNRT]. Let $V = \mathbb{C}^d$ with d = 2 or 3, $\mathbb{G} = GL(V)$, and let $G < \mathbb{G}$ be any finite subgroup. Then the following statements hold.

- (A) Suppose d = 2. Then $M_4(G, V) = M_4(\mathcal{G}, V)$ if and only if one of the following conditions holds
 - (A1) G = Z(G)H, where $H = G'_{16} \cong SL_2(5)$.
 - (A2) $E_2 \triangleleft G < \Gamma_2$ and $Z(\mathcal{G})G = Z(\mathcal{G})H$, where $H = G_{12} \cong GL_2(3)$.
 - (A3) $E_2 \triangleleft G < \Gamma_2$ and $Z(\mathcal{G})G = Z(\mathcal{G})H$, where $H = G_4 \cong SL_2(3)$.

In particular, $G < \mathcal{H} = U(V)$ is a unitary 2-group if and only if G is as described in (A1)-(A3). Furthermore, $G < \mathcal{H} = U(V)$ is a unitary 3-group if and only if G is as described in (A1)-(A2). Moreover, such a subgroup G can be a unitary *t*-group for some $t \geq 4$ if and only if $4 \leq t \leq 5$ and G is as described in (A1).

(to be continued to the next page)

- (B) Suppose d = 3. Then $M_4(G, V) = M_4(\mathcal{G}, V)$ if and only if one of the following conditions holds
 - (B1) G = Z(G)H, where $H = G'_{27} \cong 3A_6$.
 - (B2) G = Z(G)H, where $H = G'_{24} \cong SL_3(2)$.
 - (B3) $E_3 \triangleleft G < \Gamma_3$. Moreover, either $Z(\mathcal{G})G = Z(\mathcal{G})G'_{25}$, or $Z(\mathcal{G})G = Z(\mathcal{G})G_{25}$.

In particular, $G < \mathcal{H} = U(V)$ is a unitary 3-group if and only if G is as described in (B1), and no finite subgroup of U(V) can be a unitary 4-group.

Further development. This part was added after the talk.

It seems that the explicit constructions of (exact) unitary 4-designs in U(4) has been an open problem in the physics community. We want to answer to this question. This is an ongoing joint work with Da Zhao, Yan Zhu, Mikio Nakahara.

Theorem. Let G be a finite subgroup of U(d), and let $\chi: G \hookrightarrow U(d)$ be the natural embedding. 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) $f \in Harm(U(d), t+1, t+1)^{G \times G}$. 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). Remarks. (i) For any character (or representation) ϕ of $(\phi,\phi)_G = rac{1}{|G|} \sum_{x \in G} \phi(x) \overline{\phi(x)}.$ G, the inner product (ii) $\chi^i = \chi^{\otimes i}$. (iii) If $d \ge t$, then it is known that $(\chi^i, \chi^i)_{U(d)} = i!$. (iv) Examples of unitary t-groups $G \subset U(d)$ that satisfy $(\chi^{t+1},\chi^{t+1})_G = (\chi^{t+1},\chi^{t+1})_{U(d)} + 1.$ (a) For t = 3, (We assume $d \ge 3$.) d = 4, G = Sp(4, 3), $d=6, G=6_1U_4(3),$ d = 12, G = 6Suz.(b) For t = 2, (We assume d > 3.) d = 3, G = SL(3, 2) = PSL(2, 7), $d = 10, G = M_{22},$ d = 28, G = Rd, $d = (3^m \pm 1)/2, G = PSp(2m, 3), Sp(2m, 3).$ (Cf. Section 4 of a new version of [BNRT].)

(c)

Let us conclude my talk by mentioning that Da Zhao and Yan Zhu found explicit unitary 3-designs in U(3) coming from t = 2, d = 2, G = SL(3, 2), and unitary 4-designs in U(4) coming from t = 3, d = 4, G = Sp(4, 3), based on the Theorem mentioned above. Exactly speaking, we can describe such examples numerically with the errors as small as we want.

The Problem is (a) to find $G \times G$ -invariant f in Harm(U(d), t+1, t+1)explicitly, (b) to find a zero $x_0 \in U(d)$ of the polynomial f on U(d), (c) to describe the orbit X of x_0 by the action of $G \times G$ on U(d).

(b)

(extra page)

The following problem is still open and interesting.

Let G be a subgroup of O(d), $(d \ge 3)$. Let χ_i be the irreducible representation of O(d) on $Harm_i(\mathbb{R}^d)$. Then G acts on the space $Harm_i(\mathbb{R}^d)$. (The paper of Tiep (2006) classifies those G with $\chi_1 \downarrow_G$ and $\chi_2 \downarrow_G$ being irreducible.

Can we classify those $G \subset O(d)$ with $(1, \chi_i)_G = 0$ for i = 1, 2, ..., k.?

In particular, is there any finite G such that this holds for k = 12? No example is known, but the non-existence is still an open problem.) (Note that $\chi_i \downarrow_G$ are irreducible for i = 1, 2, ..., s implies that $(1, \chi_i)_G = 0$ for i = 1, 2, ..., 2s, but the converse does not necessarily hold.

Thank You