彼此正交非凡超方的构造与彼此无偏基

程晓雅^{1,2}, 尚云^{1,3,4*}

1. 中国科学院数学与系统科学研究院, 北京 100190;

2. 中国科学院大学数学科学学院, 北京 100049;

3. 国家数学与交叉科学中心, 北京 100190;

4. 管理决策与信息系统重点实验室, 北京 100190

*联系人, E-mail: shangyun@amss.ac.cn

收稿日期: 2018-01-25; 接受日期: 2018-03-07; 网络出版日期: 2018-08-08

国家科技攻关计划(编号: 2016YFB1000902)、国家自然科学基金(编号: 61472412)和国家自然科学基金创新群体(编号: 61621003)资助

摘要 本文研究了彼此正交非凡超方(Extraordinary Supersquares)与彼此无偏基(Mutually Unbiased Bases)的关系. 首先我们将 Ghiu 等人定义的非凡超方扩展到任意阶 d . 对阶 $d = p^a$ 为素数幂, 构造出 $d+1$ 个彼此正交的非凡超方; 对任意阶 d , 构造了 $p_1^{a_1} + 1$ 个彼此正交的非凡超方, 其中 $p_1^{a_1}$ 是整除 d 的最小素数幂. 进一步, 对任意 d 建立了彼此正交的非凡超方与彼此无偏基的联系. 进而给出彼此无偏基现有下界的另一种新的证明.

关键词 非凡超方, 彼此正交的非凡超方, 彼此无偏基

PACS: 02.10.Hh, 02.10.Ud, 02.10.Ox, 03.67.-a, 03.65.Aa

1 引言

彼此无偏基是量子信息中一个重要的概念, 在 d 维希尔伯特空间 $\mathbb{C}^d$ 中, 两组正交基 $\mathcal{B}_1 = \{|\phi_i\rangle\}_{i=1}^d$ 和 $\mathcal{B}_2 = \{|\psi_j\rangle\}_{j=1}^d$ 称为彼此无偏正交基, 如果对于任意 $(1 \leq i, j \leq d)$, 有 $|\langle\phi_i|\psi_j\rangle| = \frac{1}{\sqrt{d}}$. $\mathbb{C}^d$ 上的正交基集合 $\{\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_m\}$ 称为一个彼此无偏基组, 若集合中每一对 $\mathcal{B}_i, \mathcal{B}_j$ ($1 \leq i \neq j \leq d$) 都是彼此无偏的. 彼此无偏基在量子信息处理中有着广泛的应用, 比如它可以应用于量子纠错码^[1]、量子层析^[2,3]、量子密钥分配^[4]、密码协议^[4,5]、量子隐形传态和量子超密编码^[6-8]等协议中.

到目前为止, 科学家们发现彼此无偏基的最大个数不会超过 $d+1$. 当空间维数 d 是素数或单个素数幂时, 彼此无偏基的最大个数可以取到最大值 $d+1$ ^[9]. 而对于一般的 $d \geq 2$, 有 $p_1^{a_1} + 1 \leq N(d) \leq d+1$ ($d = p_1^{a_1} \cdots p_n^{a_n}$ 且 $p_1^{a_1} \leq \cdots \leq p_n^{a_n}$), 其中 $N(d)$ 表示在 d 维希尔伯特空间中彼此无偏基的最大个数^[10]. 然而对于任意维数的希尔伯特空间到底存在多少个彼此无偏基仍然是个公开问题.

目前, 存在很多不同的方法构造彼此无偏基. 其中一种方法是构造酉算子类, 每一类酉算子的公共特征向量组成一组基, 任意两个不同酉算子类得到的基是彼此无偏基^[11]. 在 2004 年, Wootters^[12]

引用格式: 程晓雅, 尚云. 彼此正交非凡超方的构造与彼此无偏基. 中国科学: 物理学 力学 天文学, 2018, 48: 110301

Cheng X Y, Shang Y. Construction of orthogonal extraordinary supersquares and mutually unbiased bases (in Chinese). Sci Sin-Phys Mech Astron, 2018, 48: 110301, doi: 10.1360/SSPMA2018-00022

和 Gibbons 等人^[13] 利用彼此无偏基与离散相空间的相关性给出一种几何方法来构造彼此无偏基. 同年, Klappenecker 等人^[14] 基于有限域上的 Weil 和以及 Galois 环上的指数和, 分别研究了奇素数幂和偶素数幂上的彼此无偏基. 在 2004 以后, Wooters^[12], Durt 等人^[10] 和 Cheng 等人^[15] 用彼此正交的 Latin 方来研究彼此无偏基. 此外在 2014 年, Ghiu 等人^[16,17] 对阶是素数或单个素数幂提出了一个新的概念非凡超方并发现了彼此正交的非凡超方与彼此无偏基具有一定的对应关系. 由此给出了对维数为素数或单个素数幂时构造彼此无偏基的另一种新方法. 但 Ghiu 等人^[17] 给出的这种新方法只适用于维数为素数或单个素数幂. 因此我们想是否这个新方法能推广到任意维, 由此得到适用于任意维希尔伯特空间中彼此无偏基构造的新方法.

本文给出了任意阶彼此正交的非凡超方的构造并建立了彼此正交非凡超方与彼此无偏基之间的对应关系, 进而给出彼此无偏基现有下界的一种新的证明. 首先, 对任意阶的方阵, 我们定义新的迹映射, 将 Ghiu 等人定义的非凡超方扩展到任意阶 (注意文献^[16] 中阶为素数幂). 接着, 为了建立任意 d 阶彼此正交的非凡超方与彼此无偏基的关系, 我们证明由彼此正交的非凡超方产生的酉算子类与彼此无偏基具有一致性, 而这些酉算子类必须满足: 所有酉算子是彼此正交的; 每一类酉算子是由 d 个可交换酉算子构成; 任意两类酉算子相交为恒等算子. 为此, 我们构造任意阶上的平移算子使得它满足以上条件. 从而我们将 Ghiu 等人^[16] 定义的非凡超方推广到任意阶并且建立了彼此正交的非凡超方与彼此无偏基的关系. 因此研究任意维的彼此无偏基的个数问题转化为研究任意阶的彼此正交非凡超方的个数问题.

在构造中, 为了使得到的方阵是彼此正交的非凡超方, 我们将方阵的性质转化为群的结构来研究, 这些群需要满足三个条件: 首先, 子群必须是生成子群 (超方); 其次, 子群是非凡的 (这种子群对解决彼此无偏基问题是一个关键因素, 因为它产生一个包含 $d-1$ 个可交换算子集); 最后, 这些子群两两相交为零 (正交性). 基于这些构造条件, 当 $d = p^a$ 为素数幂时, 本文构造了阶为 d 的完备的彼此正交的非

凡超方集, 从而可得完备的彼此无偏基; 当 d 是任意数时, 本文构造了 $p_1^{a_1} + 1$ 个彼此正交的阶为 d 的非凡超方, 从而可得到 $p_1^{a_1} + 1$ 个彼此无偏基, 其中 $p_1^{a_1}$ 是整除 d 的最小素数幂. 这是对任意维现有彼此无偏基个数的最好下界的另一种新的证明, 从而我们提供了研究彼此无偏基的新方法. 在文章的最后, 通过两个例子 $d = 9$ 和 $d = 36$, 具体说明了如何构造彼此正交的非凡超方集.

本文结构如下, 第2节给出一些基本概念、定义、定理和一些基本结果. 第3节证明了对阶为素数幂 q 时, 可以构造 $q + 1$ 个彼此正交的非凡超方. 第4节致力于重新定义迹映射以得到任意 d 阶非凡超方的定义并构造新的平移算子, 使得对于每一对彼此正交的非凡超方都可以构造出一对彼此无偏基. 给出当 $d = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ (其中 $p_1^{a_1} \leq p_2^{a_2} \leq \cdots \leq p_n^{a_n}$) 时可以构造 $p_1^{a_1} + 1$ 个彼此正交的非凡超方. 第5节分别给出当阶为 9 和 36 时, 彼此正交的非凡超方的构造过程. 第6节给出结论以及下一步工作.

2 预备知识

本节回顾了文献^[11,16] 中的一些定义和定理. 在本节中 M 表示阶为 d 的阿贝尔群. 设 $\mathbb{M}_d(\mathbb{C})$ 是 $\mathbb{C}^d$ 上 $d \times d$ 的所有复矩阵组成的集合.

定义1^[11] 矩阵 $A, B \in \mathbb{M}_d(\mathbb{C})$ 是正交的当且仅当 $\langle A, B \rangle = \text{Tr}(A^\dagger B) = 0$.

设 $\mathcal{B} = \{U_1, U_2, \dots, U_d\}$ 是酉矩阵 $\mathbb{M}_d(\mathbb{C})$ 的一组基. 假设 $U_1 = \mathbf{I}_d$ (阶为 d 的单位阵). 若 $\mathcal{B}$ 能被划分为

$$\mathcal{B} = \{\mathbf{I}_d\} \cup \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_{d+1},$$

其中每一个 $\mathcal{C}_i$, $i = 1, 2, \dots, d+1$ 都由 $d-1$ 个可交换矩阵组成, 基 $\mathcal{B}$ 称为 $\mathbb{M}_d(\mathbb{C})$ 上一个最大可交换基.

定理1^[11] 当阶为素数 p 时, 如果存在一个正交酉矩阵的最大可交换基, 则存在 $p+1$ 个彼此无偏基.

定理2^[11] 对维数为素数 p , 设 $\mathcal{B}_1, \dots, \mathcal{B}_m$ 是 $\mathbb{C}^p$ 上一组彼此无偏基. 那么存在 m 类 $\mathcal{C}_1, \dots, \mathcal{C}_m$,

每一类 C_i 都是由 p 个可交换酉矩阵组成, 使得 $C_1 \cup \cdots \cup C_m$ 中的所有矩阵都是两两正交的.

对 $(x, y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, $x = (x_{e_1}, \cdots, x_{e_n})$, $y = (y_{f_1}, \cdots, y_{f_n})$, 令

$$T_{(x,y)} = X^{x_{e_1}} Z^{y_{f_1}} \otimes \cdots \otimes X^{x_{e_n}} Z^{y_{f_n}},$$

其中 p^n 表示单个素数幂 [17].

定理3 [11] 设 $(x_1, y_1), (x_2, y_2) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$. 若 $T_{(x_1, y_1)} \neq T_{(x_2, y_2)}$ (这等价于 $(x_1, y_1) \neq (x_2, y_2)$), 则算子 $T_{(x_1, y_1)}$ 和 $T_{(x_2, y_2)}$ 是正交的.

定义2 [16] 一个阶为 d 的方阵是 $M \times M$ 的一个划分, 记为 $S = \{A_1, A_2, \cdots, A_d\}$, 每个子集 A_i 的元素个数为 d . 我们分配数 i 给子集 A_i 的所有元素: 每个 A_1 的元素 $\rightarrow 1$, 每个 A_2 的元素 $\rightarrow 2$,
...
每个 A_d 的元素 $\rightarrow d$.

定义3 (超方 [16]) 设 $S = \{A_1, A_2, \cdots, A_d\}$ 是一个 d 阶方阵. S 是一个阶为 d 的超方 (Supersquare) 如果 A_1 是 $M \times M$ 的一个含有 d 个元素的子群并且 $S = M \times M / A_1$ 是一个商集合. 子集 A_i 如下:

$$A_1 = \hat{0};$$

$$A_2 = a_2 + A_1 = \hat{a}_2;$$

...

$$A_d = a_d + A_1 = \hat{a}_d,$$

这里 $a_i \in M \times M$, $i = 2, 3, \cdots, d$, 且 A_1 叫做超方的生成子群.

我们将文献 [16] 命题 3.3 中的 $\mathbb{F}_q \times \mathbb{F}_q$ 换成 $M \times M$ 结论仍然成立, 证明完全类似文献 [16] 中命题 3.3 的证明, 从而得到下面命题.

命题1 假设 A_1 和 B_1 都是含有 d 个元素的 $M \times M$ 的子群并且 $S_1 = M \times M / A_1$, $S_2 = M \times M / B_1$. S_1 和 S_2 是正交的当且仅当 $A_1 \cap B_1 = \{0\}$.

3 阶为单个素数幂时, 彼此正交的非凡超方的构造

在文献 [16] 中, Ghiu 等人只证明当阶为素数 p

(或 2^n) 时, 可以构造 $p+1$ (或 2^n+1) 个彼此正交的非凡超方. 对于阶为 $q = p^n$ (p 为任意素数) 的情况, Ghiu 等人未给出相应的构造. 所以本节将主要研究在阶为 q 的情况下所构造的彼此正交的非凡超方的个数. 在给出构造之前, 我们首先给出一些基本定义和结论. 在本文中 q 表示单个素数幂.

设 $v_1 = (x_1, y_1)$, $v_2 = (x_2, y_2) \in \mathbb{F}_q \times \mathbb{F}_q$ 并且 $q = p^n$, p 是一个素数. $\begin{vmatrix} v_1 & v_2 \end{vmatrix}$ 表示如下行列式:

$$\begin{vmatrix} v_1 & v_2 \end{vmatrix} = \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}.$$

对 $\alpha \in \mathbb{F}_q$, α 的迹定义为

$$\text{tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}}.$$

用 K 表示 $\mathbb{F}_q$ 的子群并且 $K = \{\alpha \in \mathbb{F}_q \mid \text{tr}(\alpha) = 0\}$.

定义4 (非凡的 [16]) 子群 $G \in \mathbb{F}_q \times \mathbb{F}_q$ 称为非凡的 (Extraordinary), 如果对 $\forall g_1, g_2 \in G$ 都有 $\begin{vmatrix} g_1 & g_2 \end{vmatrix} \in K$.

下面我们给出一个阶为 4 的彼此正交的非凡超方的例子 (参见文献 [16] 中图 6).

例1

4	1	3	2
3	2	4	1
2	3	1	4
1	4	2	3

3	2	2	3
4	1	1	4
2	3	3	2
1	4	4	1

1	2	1	2
3	4	3	4
3	4	3	4
1	2	1	2

4	2	3	1
1	3	2	4
4	2	3	1
1	3	2	4

2	2	4	4
2	2	4	4
1	1	3	3
1	1	3	3

这 5 个非凡超方中只有第一个是 Latin 方 (阶为 d 的 Latin 方是一个 $d \times d$ 的方阵, 在这种方阵里恰好有 d 个不同的元素, 每一种不同的元素在同一行和同一列中都只出现一次).

定义5 [16] 一个阶为 q 的方阵 $S = \{A_1, A_2, \cdots, A_q\}$ 称为非凡的, 如果存在 $i \in \{1, 2, \cdots, q\}$ 使得 A_i 是 $\mathbb{F}_q \times \mathbb{F}_q$ 的一个非凡子群.

定义6 (非凡超方 [16]) 一个超方 S 是非凡超方, 如果它的生成子群是非凡的.

定理4 设 $q = p^n$ 是一个素数幂. 则 $\mathbb{F}_q \times \mathbb{F}_q$ 上有 $q+1$ 个线性子空间, 其中每个线性子空间都含有 q 个元素. 由此可以构造出 $q+1$ 个彼此正交的非凡超方.

证明 设 $\{v', v''\}$ 是 $\mathbb{F}_q \times \mathbb{F}_q$ 上的一组基, 定义下列含有 q 个元素的子群:

$$A_1^{(i)} = \mathbb{F}_q(v' + x_i v''), \quad i = 0, 1, \dots, q-1,$$

$$A_1^{(q)} = \mathbb{F}_q v'',$$

其中 $x_i \in \mathbb{F}_q$ 且 $\forall i \neq j$ 都有 $x_i \neq x_j$. 令 $S^{(i)} = \mathbb{F}_q \times \mathbb{F}_q / A_1^{(i)}, i = 0, 1, \dots, q$. 显然以上子群都是 $\mathbb{F}_q \times \mathbb{F}_q$ 的线性子空间, 由线性子空间的性质可知每两个线性子空间相交为零. 即, $A_1^{(i)} \cap A_1^{(j)} = 0, \forall i \neq j, i, j \in \{0, 1, \dots, q\}$. 由定义 3 和命题 1 可知 $\{S^{(i)}\}_{i=0}^q$ 是彼此正交的超方. 设 $v_1, v_2 \in A_1^{(i)}, i = 0, 1, 2, \dots, q$, 由于每个 $A_1^{(i)}$ 是一维线性子空间, 故 $|v_1 \ v_2| = 0$. 即, $\text{tr}(0) = 0$. 由定义 9 得 $S^{(i)} = \mathbb{F}_q \times \mathbb{F}_q / A_1^{(i)}, i \in \{0, 1, \dots, q\}$ 是彼此正交的非凡超方.

定理5 [18–20] 设 $v_1 = (x_1, y_1), v_2 = (x_2, y_2) \in \mathbb{F}_q \times \mathbb{F}_q$, 其中 $q = p^n$ 或 $q = p$ (p 是一个素数). 若 $\text{tr}(x_1 y_2 - x_2 y_1) = 0$, 则平移算子 $T_{(x_1, y_1)}, T_{(x_2, y_2)}$ 是可交换的.

由定理 4 和 5 我们得到了 $q+1$ 个彼此正交的非凡超方. 而定理 1 对素数幂 q 也成立 [17]. 因此我们得到在希尔伯特空间 $\mathbb{C}^q$ 中存在 $q+1$ 个彼此无偏基, 这提供了该结论的一种新的证明.

4 对任意 d 阶的非凡超方的定义及构造

在文献 [16] 中, Ghiu 等人对阶为素数或素数幂定义了新的概念 (非凡超方), 并证明了存在多少个彼此正交的非凡超方就可以构造相应个数的彼此无偏基. 这显然对维数为素数或素数幂的彼此无偏基的构造提供了一种新的方法. 由于 Ghiu 等人的方法对维数有限制, 本节我们将研究当阶为任意数时如何定义非凡超方, 使得彼此正交的非凡超方与彼此无偏基的关系仍然成立.

设 $d \geq 2, d = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, 其中 $p_1^{a_1} \leq p_2^{a_2} \leq \cdots \leq p_n^{a_n}, q_i = p_i^{a_i}$ 并且 $R = \mathbb{F}_{q_1} \oplus \cdots \oplus \mathbb{F}_{q_n}$ 是一个交

换环, 其中每一个 $p_i, i = 1, 2, \dots, n$ 是不同的素数.

由定义 3 可知, 对任意阶 d , 超方的定义已经给出, 接下来我们给出相应的非凡的定义.

这里, 用 R 代替 M , 则 $M \times M = R \times R$ 是一个 R 模.

设 $v_1 = (x_1, y_1), v_2 = (x_2, y_2) \in R \times R. |v_1 \ v_2|$ 表示如下行列式:

$$|v_1 \ v_2| = \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}.$$

对 $\alpha_i \in \mathbb{F}_{q_i}, \text{tr}_{\mathbb{F}_{q_i}/\mathbb{F}_{p_i}}$ 是一个从 $\mathbb{F}_{q_i}$ 映射到 $\mathbb{F}_{p_i}$ 的迹映射, 即 $\text{tr}_{\mathbb{F}_{q_i}/\mathbb{F}_{p_i}}(\alpha_i) = \alpha_i + \alpha_i^{p_i} + \alpha_i^{p_i^2} + \cdots + \alpha_i^{p_i^{q_i-1}}$. 则我们定义 $\alpha = (\alpha_1, \dots, \alpha_n) \in R$ 的迹 $\text{tr}(\alpha) = (\text{tr}_{\mathbb{F}_{q_1}/\mathbb{F}_{p_1}}(\alpha_1), \dots, \text{tr}_{\mathbb{F}_{q_n}/\mathbb{F}_{p_n}}(\alpha_n))$. 用 K 表示 R 的子环并且 $K = \{\alpha \in R \mid \text{tr}(\alpha) = 0\}$, 其中 $0 = (0, \dots, 0) \in R$.

由以上的定义我们给出一般的非凡的定义, 如下:

定义7 (非凡的) 子群 $G \in R \times R$ 称为非凡的如果对 $\forall g_1, g_2 \in G$ 都有 $|g_1 \ g_2| \in K$.

定义8 一个阶为 d 的方阵 $S = \{A_1, A_2, \dots, A_d\}$ 称为非凡的, 如果存在 $i \in \{1, 2, \dots, d\}$ 使得 A_i 是 $R \times R$ 的一个非凡子群.

类似地, 我们定义非凡超方.

定义9 (非凡超方) 一个超方 S 是非凡超方 (Extraordinary Supersquare), 如果它的生成子群是非凡的.

我们已经将 Ghiu 等人 [16] 的非凡超方定义推广到任意 d 阶. 接下来, 我们将证明彼此正交非凡超方与彼此无偏基之间的对应关系. 首先, 证明由彼此正交的非凡超方所得到的酉算子类满足:

- (a) 所有的酉算子都是彼此正交的;
- (b) 任意两类酉算子除恒等算子外无其他公共元素;
- (c) 每一类酉算子都是由 d 个可交换的酉算子构成.

其次证明满足上述条件的正交酉算子类的个数与彼此无偏基的个数等价.

定义10 对 $(x, y) \in R \times R$, $x = (x_1, x_2, \dots, x_n)$, $y = (y_1, y_2, \dots, y_n) \in R$ 定义

$$T_{(x,y)} := T_{(x_1,y_1)} \otimes T_{(x_2,y_2)} \otimes \cdots \otimes T_{(x_n,y_n)},$$

其中 $\forall i \in \{1, 2, \dots, n\}$,

$$T_{(x_i,y_i)} = X^{x_{ie_1}} Z^{y_{if_1}} \otimes \cdots \otimes X^{x_{ie_{a_i}}} Z^{y_{if_{a_i}}}.$$

下面我们证明由彼此正交的非凡超方所得到的酉算子类满足(a)和(b)两个条件.

由定理 3 可知对于阶为单个素数幂时, 如果 $(x_j^{(1)}, y_j^{(1)}) \neq (x_j^{(2)}, y_j^{(2)}) \in \mathbb{F}_q \times \mathbb{F}_q$, 则 $T_{(x_j^{(1)}, y_j^{(1)})}$ 和 $T_{(x_j^{(2)}, y_j^{(2)})}$ 是正交的. 再由 $\text{Tr}(M \otimes N) = \text{Tr}(M)\text{Tr}(N)$ (其中 $M, N \in \mathbb{M}_d(\mathbb{C})$) 以及 $T_{(x_1,y_1)}$ 和 $T_{(x_2,y_2)}$ 的定义可知 $T_{(x_1,y_1)}$ 和 $T_{(x_2,y_2)}$ 是正交的. 设 $\{S^{(i)} = R \times R/A_1^{(i)}\}_i^m$ 是彼此正交的非凡超方. 由彼此正交的非凡超方的定义, 可知 $\forall A_1^{(i)}, i = 1, 2, \dots, m$ 是含有 d 个元素的生成子群且 $\forall i \neq j \in \{1, 2, \dots, m\}, A_1^{(i)} \cap A_1^{(j)} = 0$. 由 $\forall i \neq j \in \{1, 2, \dots, m\}, A_1^{(i)} \cap A_1^{(j)} = 0$. 故将两两正交的酉算子划分为 m 类, 且任意两类酉算子只有公共的单位阵无其他公共元素. 即对所有 $1, 2, \dots, m$ 中不相等的 i 和 j , 我们有 $C_i \cap C_j = \mathbf{I}_d$.

接下来, 我们证明由彼此正交的非凡超方所得到的酉算子类也满足条件(c). 为此, 我们只需要证明定理 5 的结果对任意阶仍然成立.

引理1 设 $v_1 = (x_1, y_1), v_2 = (x_2, y_2) \in R \times R$. 若 $\text{tr}(x_1 y_2 - x_2 y_1) = 0$, 则平移算子 $T_{(x_1,y_1)}$ 和 $T_{(x_2,y_2)}$ 是可交换的.

证明 设对 $i = 1, 2$,

$$x_i = (x_1^{(i)}, x_2^{(i)}, \dots, x_n^{(i)}), \quad y_i = (y_1^{(i)}, y_2^{(i)}, \dots, y_n^{(i)}) \in R.$$

由以上的定义, 可得

$$\begin{aligned} \text{tr}(x_1 y_2 - x_2 y_1) &= (\text{tr}_{\mathbb{F}_{q_j}/\mathbb{F}_{p_j}}(x_j^{(1)} y_j^{(2)} - x_j^{(2)} y_j^{(1)}))_j \\ &= (0, \dots, 0), \end{aligned}$$

即 $\text{tr}_{\mathbb{F}_{q_j}/\mathbb{F}_{p_j}}(x_j^{(1)} y_j^{(2)} - x_j^{(2)} y_j^{(1)}) = 0, j = 1, 2, \dots, n$. 由定理 5 可得 $T_{x_j^{(1)}, y_j^{(1)}}$ 和 $T_{x_j^{(2)}, y_j^{(2)}}$ 是可交换的. 由于 $T_{(x_1,y_1)}$ 和 $T_{(x_2,y_2)}$ 的每一项 $T_{x_j^{(1)}, y_j^{(1)}}$ 和 $T_{x_j^{(2)}, y_j^{(2)}}$ 都是可交换的, 可得 $T_{(x_1,y_1)}$ 和 $T_{(x_2,y_2)}$ 是可交换算子.

到此我们证明了由彼此正交的非凡超方所得到的酉算子类满足上述所有条件.

最后, 我们证明满足上述条件的正交酉算子类的个数与彼此无偏基的个数等价. 事实上, 我们可以将定理 1 和 2 推广到任意阶数 d , 其证明类似于文献 [11] 中定理 3.2 和 3.4 的证明.

引理2 对任意阶 d , 如果两两正交的酉算子划分为 m 类, 每一类含有 d 个元素, 任意两类相交只有单位阵且每类中西算子都是可交换的, 则存在 m 个彼此无偏基.

引理3 对任意维数 $d, \mathbb{C}^d$ 中存在 m 个彼此无偏基. 则存在两两正交的酉算子划分为 m 类, 每一类含有 d 个元素, 任意两类相交只有单位阵且每类中西算子都是可交换的.

由引理 2 和 3 可知满足上述条件的正交酉算子类的个数与彼此无偏基的个数等价. 由以上分析我们可以得到如下定理:

定理6 对任意 d , 若存在 m 个 d 阶彼此正交的非凡超方, 则 $\mathbb{C}^d$ 中彼此无偏基所组成的集合中最大元素个数大于等于 m .

接下来由定理 6 可知为了构造彼此无偏基, 可以先构造彼此正交的非凡超方. 构造彼此正交的非凡超方需要满足三个条件. 首先, 构造的方阵必须是超方. 即, 要找模 $R \times R$ 上的子模且每个子模含有 d 个元素. 其次, 任意两个子模只有公共的零元素无其他公共元素(正交性). 最后, 对每个子模中的任意两个向量的行列式的值求迹必须为零(非凡的).

命题2 设 $d \geq 2$ 且环 $R = \mathbb{F}_{q_1} \oplus \cdots \oplus \mathbb{F}_{q_n}$, 其中 $d = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ 是 d 的素数幂分解并且 $p_1^{a_1} \leq p_2^{a_2} \leq \cdots \leq p_n^{a_n}$, 每个 $p_i, i = 1, 2, \dots, n$ 是不同的素数. 令 $q_i = p_i^{a_i}$. 则 $R \times R$ 中存在 $p_1^{a_1} + 1$ 个含有 d 个元素的子模, 且任意两个子模相交为零.

证明 对所有的 $i > 1$ 都有 $q_i - 1 \geq q_1 - 1$, 其中 $q_i = p_i^{a_i}$. 对每一个 $i > 1$, 给定一个单射 $\iota_i: \mathbb{F}_{q_1}^* \rightarrow \mathbb{F}_{q_i}^*$. 定义

$$R_1 = \{(u, \iota_2(u), \dots, \iota_n(u)) \in R^* \mid u \in \mathbb{F}_{q_1}^*\}.$$

显然, R_1 是 R^* (R^* 是 R 的所有可逆元) 的一个子

集且对任意 $a \neq b \in R_1$ 都有 $a - b \in R^*$ 并且集合 R_1 的元素个数是 $p_1^{a_1} - 1$. 由此可以构造 $R \times R$ 上含有 d 个元素的子模, 如 $R(0, 1)$, $R(1, 0)$ 以及 $R(1, a)$, $a \in R_1$, 其中 $(0, 1)$, $(1, 0)$ 以及 $(1, a) \in R \times R$. 故得到 $p_1^{a_1} + 1$ 个子模.

下面证明以上构造的子模任意两个相交都为零. 首先, 显然 $R(0, 1) \cap R(1, 0) = 0$ 且对所有 $a \in R_1$, $R(0, 1) \cap R(1, a) = 0$. 接着, 由 $a \in R_1$, R_1 是 R^* 的子集可知 a 可逆, 故对所有 $a \in R_1$, 有 $R(1, 0) \cap R(1, a) = 0$. 最后, 证明 $\forall a \neq b \in R_1$, $R(1, b) \cap R(1, a) = 0$. 假设存在 $v \neq 0$ 且 $v \in R(1, b) \cap R(1, a)$, 则存在 $x, y \in R$ 使得 $x(1, a) = y(1, b) = v$, 故 $(x - y, xa - yb) = 0$, 由此推出 $x = y$ 且 $(a - b)x = 0$, 再由 R_1 的构造以及 $a \neq b \in R_1$, 得 $a - b \in R^*$. 故可得 $v = 0$ 与假设相矛盾. 因此 $R(1, b) \cap R(1, a) = 0$. 证毕.

由命题 2 可知, 存在 $p_1^{a_1} + 1$ 个彼此正交超方 (参见命题 1). 然后对 $\forall v_1, v_2 \in R(0, 1)$ (类似地对 $R(1, 0)$, $R(1, a)$ 也一样), 易得 $|v_1 \ v_2| = 0$, 所以 $\text{tr}(0) = 0$. 由定义 7, 可以构造 $p_1^{a_1} + 1$ 个彼此正交的非平凡超方. 最后, 由定理 6 可得到 $p_1^{a_1} + 1$ 个彼此无偏基. 我们给出了现有彼此无偏基个数的最好下界的一种新的证明.

5 阶分别为 9 和 36 的彼此正交非凡超方的构造

本节给出两个彼此正交的非平凡超方的构造例子. 首先, 在阶为 $d = 3^2$ 的情况下, 取本原多项式 $x^2 + 2x + 2$, $\mathbb{F}_9 = \{0, 1, x, x^2, x^3, x^4, x^5, x^6, x^7\}$. 由定理 4 可知彼此正交非凡超方的完备集由 10 个方阵组成, 且非凡超方的生成子群为

$$A_1^{(i)} = \mathbb{F}_q(v' + x_i v''), \quad i = 2, \dots, 10,$$

$$A_1^{(1)} = \mathbb{F}_q v'',$$

其中 $x_i \in \mathbb{F}_q$ 且 $\forall i \neq j$ 都有 $x_i \neq x_j$. $\{v', v''\}$ 是 $\mathbb{F}_q \times \mathbb{F}_q$ 上的一组基, 这里我们取 $v' = (1, 0)$, $v'' = (0, 1)$ 可得下列含有 9 个元素的生成子群:

$$A_1^{(1)} = \mathbb{F}_9(0, 1) = \{(0, 0), (0, 1), (0, x), (0, x^2), (0, x^3), (0, x^4), (0, x^5), (0, x^6), (0, x^7)\};$$

$$A_1^{(2)} = \mathbb{F}_9(1, 0) = \{(0, 0), (1, 0), (x, 0), (x^2, 0),$$

$$(x^3, 0), (x^4, 0), (x^5, 0), (x^6, 0), (x^7, 0)\};$$

$$A_1^{(3)} = \mathbb{F}_9(1, 1) = \{(0, 0), (1, 1), (x, x), (x^2, x^2),$$

$$(x^3, x^3), (x^4, x^4), (x^5, x^5), (x^6, x^6), (x^7, x^7)\};$$

$$A_1^{(4)} = \mathbb{F}_9(1, x) = \{(0, 0), (1, x), (x, x^2), (x^2, x^3),$$

$$(x^3, x^4), (x^4, x^5), (x^5, x^6), (x^6, x^7), (x^7, 1)\};$$

$$A_1^{(5)} = \mathbb{F}_9(1, x^2) = \{(0, 0), (1, x^2), (x, x^3), (x^2, x^4),$$

$$(x^3, x^5), (x^4, x^6), (x^5, x^7), (x^6, 1), (x^7, x)\};$$

$$A_1^{(6)} = \mathbb{F}_9(1, x^3) = \{(0, 0), (1, x^3), (x, x^4), (x^2, x^5),$$

$$(x^3, x^6), (x^4, x^7), (x^5, 1), (x^6, x), (x^7, x^2)\};$$

$$A_1^{(7)} = \mathbb{F}_9(1, x^4) = \{(0, 0), (1, x^4), (x, x^5), (x^2, x^6),$$

$$(x^3, x^7), (x^4, 1), (x^5, x), (x^6, x^2), (x^7, x^3)\};$$

$$A_1^{(8)} = \mathbb{F}_9(1, x^5) = \{(0, 0), (1, x^5), (x, x^6), (x^2, x^7),$$

$$(x^3, 1), (x^4, x), (x^5, x^2), (x^6, x^3), (x^7, x^4)\};$$

$$A_1^{(9)} = \mathbb{F}_9(1, x^6) = \{(0, 0), (1, x^6), (x, x^7), (x^2, 1),$$

$$(x^3, x), (x^4, x^2), (x^5, x^3), (x^6, x^4), (x^7, x^5)\};$$

$$A_1^{(10)} = \mathbb{F}_9(1, x^7) = \{(0, 0), (1, x^7), (x, 1), (x^2, x),$$

$$(x^3, x^2), (x^4, x^3), (x^5, x^4), (x^6, x^5), (x^7, x^6)\}.$$

可知对 $\forall i \neq j \in \{1, 2, \dots, 10\}$, 都有 $A_1^{(i)} \cap A_1^{(j)} = (0, 0) = 0$. 并且对所有 $i = 1, 2, \dots, 10$ 以及 $v_1, v_2 \in A_1^{(i)}$, 有 $|v_1 \ v_2| = 0$, 可得 $\text{tr}(0) = 0$. 设 $\mathbf{S}^{(i)} = \mathbb{F}_9 \times \mathbb{F}_9 / A_1^{(i)}$, $i = 1, 2, \dots, 10$, 可以得到 10 个阶为 9 的彼此正交的非平凡超方, 再由定理 6 可以构造 10 组彼此无偏基.

下面给出一个非凡超方的具体形式.

由生成子群得到的非凡超方不是唯一的, 与所选的代表元有关. 在此, 我们给出一种选法. 以 $\mathbf{S}^{(3)}$ 为例, $\mathbf{S}^{(3)} = \mathbb{F}_9 \times \mathbb{F}_9 / A_1^{(3)}$, 类似地可得其他非凡超方. 这里取 $A_1^{(2)} \setminus (0, 0)$ 中的元素作为代表元, 可得

$$A_2^{(3)} = (1, 0) + A_1^{(3)} = \{(1, 0), (x^4, 1), (x^2, x), (x^7, x^2),$$

$$(x^6, x^3), (0, x^4), (x^3, x^5), (x^5, x^6), (x, x^7)\};$$

$$A_3^{(3)} = (x, 0) + A_1^{(3)} = \{(x, 0), (x^2, 1), (x^5, x), (x^3, x^2),$$

$$(1, x^3), (x^7, x^4), (0, x^5), (x^4, x^6), (x^6, x^7)\};$$

$$A_4^{(3)} = (x^2, 0) + A_1^{(3)} = \{(x^2, 0), (x^7, 1), (x^3, x), (x^6, x^2),$$

$$(x^4, x^3), (x, x^4), (1, x^5), (0, x^6), (x^5, x^7)\};$$

$$A_5^{(3)} = (x^3, 0) + A_1^{(3)} = \{(x^3, 0), (x^6, 1), (1, x), (x^4, x^2), (x^7, x^3), (x^5, x^4), (x^2, x^5), (x, x^6), (0, x^7)\};$$

$$A_6^{(3)} = (x^4, 0) + A_1^{(3)} = \{(x^4, 0), (0, 1), (x^7, x), (x, x^2), (x^5, x^3), (1, x^4), (x^6, x^5), (x^3, x^6), (x^2, x^7)\};$$

$$A_7^{(3)} = (x^5, 0) + A_1^{(3)} = \{(x^5, 0), (x^3, 1), (0, x), (1, x^2), (x^2, x^3), (x^6, x^4), (x, x^5), (x^7, x^6), (x^4, x^7)\};$$

$$A_8^{(3)} = (x^6, 0) + A_1^{(3)} = \{(x^6, 0), (x^5, 1), (x^4, x), (0, x^2), (x, x^3), (x^3, x^4), (x^7, x^5), (x^2, x^6), (1, x^7)\};$$

$$A_9^{(3)} = (x^7, 0) + A_1^{(3)} = \{(x^7, 0), (x, 1), (x^6, x), (x^5, x^2), (0, x^3), (x^2, x^4), (x^4, x^5), (1, x^6), (x^3, x^7)\}.$$

可得方阵 $S^{(3)}$ 具体的数学表达式

x^7	5	8	2	6	9	7	4	3	1
x^6	4	9	5	8	6	3	2	1	7
x^5	3	4	7	5	2	9	1	6	8
x^4	2	6	4	9	8	1	5	7	3
x^3	9	3	8	7	1	4	6	2	5
x^2	8	7	6	1	3	5	9	4	2
x	7	5	1	2	4	8	3	9	6
1	6	1	9	3	7	2	8	5	4
0	1	2	3	4	5	6	7	8	9
	0	1	x	x^2	x^3	x^4	x^5	x^6	x^7

下面讨论 $d = 36 = 2^2 3^2$ 的情况, 由命题 2 可知存在 5 个子模(每个子模含有 36 个元素). 设 $A_1^{(i)}$, $i = 1, 2, \dots, 5$ 表示子模. 取 $\mathbb{F}_9$ 和 $\mathbb{F}_4$ 的本原多项式分别为 $x^2 + 2x + 2$ 和 $\mu^2 + \mu + 1$,

$$\mathbb{F}_9 = \{0, 1, x, x^2, x^3, x^4, x^5, x^6, x^7\},$$

$$\mathbb{F}_9^* = \{1, x, x^2, x^3, x^4, x^5, x^6, x^7\},$$

$$\mathbb{F}_4 = \{0, 1, \mu, \mu^2\}, \quad \mathbb{F}_4^* = \{1, \mu, \mu^2\},$$

$$R = \mathbb{F}_4 \oplus \mathbb{F}_9 = \{(0, 0), \dots, (0, x^7), (1, 0), \dots, (1, x^7), (\mu, 0), \dots, (\mu, x^7), (\mu^2, 0), \dots, (\mu^2, x^7)\},$$

其中 x, μ 分别是 $\mathbb{F}_9$ 和 $\mathbb{F}_4$ 的生成元. 给定一个单射 $\iota: \mathbb{F}_4^* \rightarrow \mathbb{F}_9^*$. 定义

$$R_1 = \{(u, \iota(u)) \in R^* \mid u \in \mathbb{F}_4^*\}.$$

显然 R_1 是 R^* 的一个子集且对任意的 $a \neq b \in R_1$ 都有 $a - b \in R^*$. 这里, 令

$$\iota(u) = \begin{cases} 1 & u = 1, \\ x & u = \mu, \\ x^2 & u = \mu^2, \end{cases}$$

则 $R_1 = \{(1, 1), (\mu, x), (\mu^2, x^2)\}$. 子模构造如下:

$$A_1^{(1)} = R((0, 0), (1, 1)) = \{((0, 0), (0, 0)), \dots, ((0, 0), (0, x^7)), ((0, 0), (1, 0)), \dots, ((0, 0), (1, x^7)), ((0, 0), (\mu, 0)), \dots, ((0, 0), (\mu, x^7)), ((0, 0), (\mu^2, 0)), \dots, ((0, 0), (\mu^2, x^7))\};$$

$$A_1^{(2)} = R((1, 1), (0, 0)) = \{((0, 0), (0, 0)), \dots, ((0, x^7), (0, 0)), ((1, 0), (0, 0)), \dots, ((1, x^7), (0, 0)), ((\mu, 0), (0, 0)), \dots, ((\mu, x^7), (0, 0)), ((\mu^2, 0), (0, 0)), \dots, ((\mu^2, x^7), (0, 0))\};$$

$$A_1^{(3)} = R((1, 1), (1, 1)) = \{((0, 0), (0, 0)), \dots, ((0, x^7), (0, x^7)), ((1, 0), (1, 0)), \dots, ((1, x^7), (1, x^7)), ((\mu, 0), (\mu, 0)), \dots, ((\mu, x^7), (\mu, x^7)), ((\mu^2, 0), (\mu^2, 0)), \dots, ((\mu^2, x^7), (\mu^2, x^7))\};$$

$$A_1^{(4)} = R((1, 1), (\mu, x)) = \{((0, 0), (0, 0)), \dots, ((0, x^7), (0, 1)), ((1, 0), (\mu, 0)), \dots, ((1, x^7), (\mu, 1)), ((\mu, 0), (\mu^2, 0)), \dots, ((\mu, x^7), (\mu^2, 1)), ((\mu^2, 0), (1, 0)), \dots, ((\mu^2, x^7), (1, 1))\};$$

$$A_1^{(5)} = R((1, 1), (\mu^2, x^2)) = \{((0, 0), (0, 0)), \dots, ((0, x^7), (0, x)), ((1, 0), (\mu^2, 0)), \dots, ((1, x^7), (\mu^2, x)), ((\mu, 0), (1, 0)), \dots, ((\mu, x^7), (1, x)), ((\mu^2, 0), (\mu, 0)), \dots, ((\mu^2, x^7), (\mu, x))\}.$$

对 $\forall i \neq j \in \{1, 2, \dots, 5\}$, 都有 $A_1^{(i)} \cap A_1^{(j)} = 0$. 并且对所有 $i = 1, 2, \dots, 5$ 和 $\forall v_1, v_2 \in A_1^{(i)}$, 有 $|v_1 v_2| = 0$,

则 $\text{tr}(0) = 0$. 设 $S^{(i)} = R \times R/A_1^{(i)}, i = 1, 2, \dots, 5$, 由此可得存在 5 个阶为 36 的彼此正交非凡超方, 再由定理 6 可以构造 5 组彼此无偏基.

下面给出一个非凡超方的具体形式 (其他的非凡超方类似可得), 这里取 $A_1^{(2)} \setminus (0, 0)$ 中的元素作为代表元, 可得

$$\begin{aligned}
 A_2^{(1)} &= ((0, 1), (0, 0)) + A_1^{(1)} = \{((0, 1), (0, 0)), \\
 &((0, 1), (0, 1)), ((0, 1), (0, x)), \dots, ((0, 1), (0, x^7)) \\
 &((0, 1), (1, 0)), ((0, 1), (1, 1)), ((0, 1), (1, x)), \dots, \\
 &((0, 1), (1, x^7)), ((0, 1), (\mu, 0)), ((0, 1), (\mu, 1)), \\
 &((0, 1), (\mu, x)), \dots, ((0, 1), (\mu, x^7)), ((0, 1), (\mu^2, 0)), \\
 &((0, 1), (\mu^2, 1)), ((0, 1), (\mu^2, x)), \\
 &\dots, ((0, 1), (\mu^2, x^7))\}; \\
 A_3^{(1)} &= ((0, x), (0, 0)) + A_1^{(1)} = \{((0, x), (0, 0)), \\
 &((0, x), (0, 1)), ((0, x), (0, x)), \dots, ((0, x), \\
 &(0, x^7)), ((0, x), (1, 0)), ((0, x), (1, 1)), ((0, x), (1, x)), \\
 &\dots, ((0, x), (1, x^7)), ((0, x), (\mu, 0)), ((0, x), (\mu, 1)), \\
 &((0, x), (\mu, x)), \dots, ((0, x), (\mu, x^7)), ((0, x), \\
 &(\mu^2, 0)), ((0, x), (\mu^2, 1)), ((0, x), (\mu^2, x)), \\
 &\dots, ((0, x), (\mu^2, x^7))\}; \\
 A_4^{(1)} &= ((0, x^2), (0, 0)) + A_1^{(1)} = \{((0, x^2), (0, 0)), \\
 &((0, x^2), (0, 1)), ((0, x^2), (0, x)), \dots, ((0, x^2), \\
 &(0, x^7)), ((0, x^2), (1, 0)), ((0, x^2), (1, 1)), ((0, x^2), \\
 &(1, x)), \dots, ((0, x^2), (1, x^7)), ((0, x^2), (\mu, 0)), ((0, x^2), \\
 &(\mu, 1)), ((0, x^2), (\mu, x)), \dots, ((0, x^2), (\mu, x^7)), \\
 &((0, x^2), (\mu^2, 0)), ((0, x^2), (\mu^2, 1)), ((0, x^2), \\
 &(\mu^2, x)), \dots, ((0, x^2), (\mu^2, x^7))\}; \\
 &\vdots \\
 A_{36}^{(1)} &= ((\mu^2, x^7), (0, 0)) + A_1^{(1)} = \{((\mu^2, x^7), \\
 &(0, 0)), ((\mu^2, x^7), (0, 1)), ((\mu^2, x^7), (0, x)), \dots, \\
 &((\mu^2, x^7), (0, x^7)), ((\mu^2, x^7), (1, 0)), ((\mu^2, x^7),
 \end{aligned}$$

$$\begin{aligned}
 &(1, 1)), ((\mu^2, x^7), (1, x)), \dots, ((\mu^2, x^7), (1, x^7)), \\
 &((\mu^2, x^7), (\mu, 0)), ((\mu^2, x^7), (\mu, 1)), ((\mu^2, x^7), \\
 &(\mu, x)), \dots, ((\mu^2, x^7), (\mu, x^7)), ((\mu^2, x^7), (\mu^2, 0)), \\
 &((\mu^2, x^7), (\mu^2, 1)), ((\mu^2, x^7), (\mu^2, x)), \dots, \\
 &((\mu^2, x^7), (\mu^2, x^7))\};
 \end{aligned}$$

可得方阵 $S^{(1)}$ 具体的数学表达式

1	2	...	36
1	2	...	36
$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	2	...	36

6 结论

本文主要研究对于任意阶彼此正交的非凡超方与彼此无偏基的关系. 从而给出构造任意维希尔伯特空间中彼此无偏基的一种新方法. 首先, 我们定义了任意阶的非凡超方 (文献[16] 中的定义仅限于阶为素数幂). 其次, 证明对任意阶由彼此正交的非凡超方导出的酉算子类满足一定条件, 使得导出的酉算子类与彼此无偏基等价. 从而建立了彼此正交的非凡超方与彼此无偏基的关系. 故我们提供了另一种新方法来研究任意维彼此无偏基. 由此得到当阶为素数幂 ($d = p^a$) 时, 可以构造完备的彼此正交的非凡超方集, 从而可得完备的彼此无偏基. 当阶是任意数 d 时, 我们证明可以构造 $p_1^{a_1} + 1$ 个彼此正交的非凡超方, 从而可得 $p_1^{a_1} + 1$ 个彼此无偏基, 其中 $p_1^{a_1}$ 是整除 d 的最小素数幂. 最后我们给出具体构造彼此正交的非凡超方集的两个例子. 虽然本文用彼此正交的非凡超方来构造彼此无偏基得到的结果与前人一样, 但是我们引入了新的方法来构造彼此无偏基, 从而我们提供基于这种新方法来构造更多彼此无偏基的可能. 未来的工作, 我们将考虑对任意阶用非凡超方是否能构造出比现有下界更多的彼此无偏基, 或者是否能证明对任意维 $p_1^{a_1} + 1$ 已经是上界了.

参考文献

- 1 Pawłowski M, Żukowski M. Entanglement-assisted random access codes. *Phys Rev A*, 2010, 81: 042326
- 2 Ivonovic I D. Geometrical description of quantal state determination. *J Phys A-Math Gen*, 1981, 14: 3241–3245
- 3 Wootters W K, Fields B D. Optimal state-determination by mutually unbiased measurements. *Ann Phys*, 1989, 191: 363–381
- 4 Cerf N J, Bourennane M, Karlsson A, et al. Security of quantum key distribution using d-level systems. *Phys Rev Lett*, 2002, 88: 127902
- 5 Brierley S. Quantum key distribution highly sensitive to eavesdropping. 2009, 1–19, arXiv: 0910.2578.
- 6 Durt T. If $1 = 2 + 3$, then $1 = 2 \cdot 3$: Bell states, finite groups, and mutually unbiased bases, a unifying approach. 2004, 1–24, arXiv: quant-ph/0401046.
- 7 Revzen M. Maximally entangled states via mutual unbiased collective bases. *Phys Rev A*, 2010, 81: 012113
- 8 Sangare D, Adler P M. Continuum percolation of isotropically oriented circular cylinders. *Phys Rev E*, 2009, 79: 052101
- 9 Calderbank A, Cameron P, Kantor W, et al. $\mathbb{Z}_4$ -kerdock codes, orthogonal spreads, and extremal euclidean line-sets. *Proc London Math Soc*, 1997, 75: 436–480
- 10 Durt T, Englert B G, Bengtsson I, et al. On mutually unbiased bases. *Int J Quantum Inform*, 2010, 8: 535–640
- 11 Bandyopadhyay S, Boykin B O, Roychowdhury V, et al. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 2002, 34: 512–528
- 12 Wootters W K. Picturing qubits in phase space. *IBM J Res Dev*, 2004, 48: 99–110
- 13 Gibbons K S, Hoffman M J, Wootters W K. Discrete phase space based on finite fields. *Phys Rev A*, 2004, 70: 062101
- 14 Klappenecker A, Rötteler M. Constructions of mutually unbiased bases. In: *Finite Fields and Applications*. Berlin: Springer, 2004. 137–144
- 15 Cheng X Y, Shang Y. New bounds of mutually unbiased maximally entangled bases in $\mathbb{C}^d \otimes \mathbb{C}^{kd}$. 2017, arXiv: 1710.07458.
- 16 Ghiu C, Ghiu I. Construction of the mutually orthogonal extraordinary supersquares. *Open Math*, 2014, 12: 337–348
- 17 Ghiu I, Ghiu C. The correspondence between mutually unbiased bases and mutually orthogonal extraordinary supersquares. *Rep Math Phys*, 2014, 73: 49–63
- 18 Ghiu I. A new method of construction of all sets of mutually unbiased bases for two-qubit systems. *J Phys-Conf Ser*, 2012, 338: 012008
- 19 Ghiu I. Generation of all sets of mutually unbiased bases for three-qubit systems. *Phys Scr*, 2013, 2013: 014027, arXiv: 1205.6276
- 20 Klimov A B, Romero J L, Björk G, et al. Geometrical approach to mutually unbiased bases. *J Phys A-Math Theor*, 2007, 40: 3987–3998

Construction of orthogonal extraordinary supersquares and mutually unbiased bases

CHENG XiaoYa^{1,2} & SHANG Yun^{1,3,4*}

¹*Institute of Mathematics, Academy of Mathematics and System Science, Chinese Academy of Sciences, Beijing 100190, China;*

²*School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China;*

³*National Center for Mathematics and Interdisciplinary Sciences, Beijing 100190, China;*

⁴*Key Laboratory of Management, Decision and Information Systems, Beijing 100190, China*

This article studies the connection between mutually orthogonal extraordinary supersquares and mutually unbiased bases. Firstly, we generalize extraordinary supersquares defined by Ghiu et al. to arbitrary order d . For order $d = p^a$ being a single prime power, we construct $d + 1$ mutually orthogonal extraordinary supersquares; for arbitrary order d , we construct $p_1^{a_1} + 1$ mutually orthogonal extraordinary supersquares, where $p_1^{a_1}$ is the minimal prime power dividing d . In addition, this article sets up the connection between mutually orthogonal extraordinary supersquares and mutually unbiased bases for arbitrary d . Then we provide a new proof for the known lower bound of mutually unbiased bases.

extraordinary supersquares, mutually orthogonal extraordinary supersquares, mutually unbiased bases

PACS: 02.10.Hh, 02.10.Ud, 02.10.Ox, 03.67.-a, 03.65.Aa

doi: 10.1360/SSPMA2018-00022