

Quasi-orthogonal subalgebras of matrix algebras

Hironichi Ohno
Graduate School of Mathematics,
Kyushu University

The motivation of this work comes from the algebraic or matrix formalism of finite quantum systems. An n -level system is described by the algebra $M_n = M_n(\mathbb{C})$ of $n \times n$ complex matrices. The matrix algebra of a composite system consisting of an n -level and an m -level system is $M_n \otimes M_m \simeq M_{nm}$. A subalgebra of M_k corresponds to a subsystem of a k -level quantum system.

In this lecture, subalgebras contain the identity and closed under the adjoint operation of matrices, that is, they are unital $*$ -subalgebras. The algebra M_k can be endowed by the inner product $\langle A, B \rangle = \text{Tr}(A^*B)$ and it becomes a Hilbert space. Two subalgebras \mathcal{A}_1 and \mathcal{A}_2 are called quasi-orthogonal if $\mathcal{A}_1 \ominus \mathbb{C}I \perp \mathcal{A}_2 \ominus \mathbb{C}I$.

The aim of this lecture is to show the maximal number of (pairwise) quasi-orthogonal subalgebras which are isomorphic to M_d in M_{d^n} with some special d .

1 Preliminaries

\mathcal{A} is a finite dimensional C^* -algebra with usual trace Tr and is considered as a Hilbert space under the inner product

$$\langle A, B \rangle = \text{Tr}(A^*B)$$

for any $A, B \in \mathcal{A}$.

Definition 1.1 Two subalgebras \mathcal{A}_1 and \mathcal{A}_2 are called *quasi-orthogonal* (MQOA) if

$$\mathcal{A}_1 \ominus \mathbb{C}I \perp \mathcal{A}_2 \ominus \mathbb{C}I.$$

The equivalent conditions of this definition are following:

(i) For any $A_1 \in \mathcal{A}_1$ and $A_2 \in \mathcal{A}_2$,

$$\text{Tr}(A_1 A_2) = \frac{\text{Tr}(A_1)\text{Tr}(A_2)}{\text{Tr}(I)}.$$

(ii) For any $A_1 \in \mathcal{A}_1$ and $A_2 \in \mathcal{A}_2$ with $\text{Tr}(A_1) = \text{Tr}(A_2) = 0$,

$$\text{Tr}(A_1 A_2) = 0.$$

If e, f, g are vectors of a Hilbert space, then the linear operator $|e\rangle\langle f|$ acts as $|e\rangle\langle f|g := \langle f, g\rangle e$.

Theorem 1.2 *Let E_i be an orthonormal basis in M_n and let $W = \sum_i E_i \otimes W_i \in M_n \otimes M_m$ be a unitary. The subalgebra $W(I \otimes M_m)W^*$ is quasi-orthogonal to $I \otimes M_m$ if and only if*

$$\frac{m}{n} \sum_k |W_k\rangle\langle W_k|$$

is the identity mapping on M_m . This condition cannot hold if $m < n$ and in the case $n = m$ the condition means that $\{W_k : 1 \leq k \leq n^2\}$ is an orthonormal basis in M_m .

Proof. Assume that $A, B \in M_m$ and $\text{Tr}B = 0$. Then the condition

$$W(I \otimes A^*)W^* \perp (I \otimes B)$$

is equivalently written as

$$\text{Tr}(W(I \otimes A)W^*(I \otimes B)) = \sum_{k,l} \text{Tr}(E_k E_l^*) \text{Tr}(W_k A W_l^* B) = \sum_k \text{Tr}(W_k A W_k^* B) = 0.$$

Putting $B - \text{Tr}(B)I_m/m$ in place of B , we get

$$\sum_k \text{Tr}(W_k A W_k^* B) = \frac{\text{Tr}B}{m} \sum_k \text{Tr}(W_k A W_k^*).$$

for every $B \in M_m$. Let $\mathcal{E}_2 : M_n \otimes M_m \rightarrow M_m$ be the linear mapping defined as

$$\mathcal{E}_2(K \otimes L) = \frac{\text{Tr}K}{n} L.$$

Since \mathcal{E}_2 is unit-preserving and W is a unitary,

$$I_m = \mathcal{E}_2(W^*W) = \mathcal{E}_2\left(\sum_{k,l} E_k^* E_l \otimes W_k^* W_l\right) = \frac{1}{n} \sum_{k,l} \text{Tr}(E_k^* E_l) W_k^* W_l = \frac{1}{n} \sum_k W_k^* W_k,$$

and we arrive at the relation

$$\sum_k \text{Tr}W_k A W_k^* B = \frac{n}{m} \text{Tr}A \text{Tr}B. \quad (1)$$

We can transform this into another equivalent condition in terms of the left multiplication, right multiplication and $|W_k\rangle\langle W_k|$ operators.

For $A, B \in M_m$, the operator R_A is the right multiplication by A and the operator L_B is the left multiplication by B : $R_A, L_B : M_m \rightarrow M_m$, $R_A X = XA$, $L_B X = BX$. If λ_i 's are the eigenvalues of A and μ_j 's are the eigenvalues of B , then $\lambda_i \mu_j$'s are the eigenvalues of $R_A L_B$. Therefore

$$\text{Tr}R_A L_B = \left(\sum_i \lambda_i\right) \left(\sum_j \mu_j\right) = \text{Tr}A \text{Tr}B.$$

We have

$$\begin{aligned} \sum_k \text{Tr}|W_k\rangle\langle W_k|R_AL_B &= \sum_k \langle W_k, R_AL_B W_k \rangle = \sum_k \text{Tr}W_k^* B W_k A \\ &= \frac{n}{m} \text{Tr}A \text{Tr}B = \frac{n}{m} \text{Tr}R_AL_B \end{aligned}$$

for every $A, B \in M_m$. Since the operators R_AL_B linearly span the space of all linear operators on M_m , we have

$$\frac{m}{n} \sum_k |W_k\rangle\langle W_k| = I_{m^2}.$$

This is our statement. □

2 Quasi-orthogonal subalgebras in the case $d = 2$

In this section, we consider the quasi-orthogonal subalgebras in $M_4 = M_2 \otimes M_2$ which are isomorphic to M_2 . A natural orthogonal basis of M_2 consists of the Pauli matrices:

$$\sigma_0 := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_1 := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_2 := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

It is easy to construct four pairwise quasi-orthogonal subalgebras by using the Pauli matrices. For example:

$$\begin{aligned} &\text{span}\{I, \sigma_1 \otimes \sigma_0, \sigma_2 \otimes \sigma_0, \sigma_3 \otimes \sigma_0\}, & \text{span}\{I, \sigma_0 \otimes \sigma_1, \sigma_1 \otimes \sigma_2, \sigma_1 \otimes \sigma_3\} \\ &\text{span}\{I, \sigma_2 \otimes \sigma_1, \sigma_0 \otimes \sigma_2, \sigma_2 \otimes \sigma_3\}, & \text{span}\{I, \sigma_3 \otimes \sigma_1, \sigma_3 \otimes \sigma_2, \sigma_0 \otimes \sigma_3\}. \end{aligned}$$

Next, we prove that the maximal number of such quasi-orthogonal subalgebras is 4.

Theorem 2.1 *Let $I \otimes M_2$ and \mathcal{A} be quasi-orthogonal subalgebras of M_4 which are isomorphic to M_2 . Then the intersection $M_2 \otimes I \cap \mathcal{A}$ is an at least two dimensional subspace of M_4 .*

Proof. The 4×4 matrices

$$C = \begin{bmatrix} a & 0 & 0 & b \\ 0 & c & d & 0 \\ 0 & d & c & 0 \\ b & 0 & 0 & a \end{bmatrix}$$

form a commutative algebra \mathcal{C} . Since

$$\sum_{i=0}^3 c_i \sigma_i \otimes \sigma_i = \begin{bmatrix} c_0 + c_3 & 0 & 0 & c_1 - c_2 \\ 0 & c_0 - c_3 & c_1 + c_2 & 0 \\ 0 & c_1 + c_2 & c_0 - c_3 & 0 \\ c_1 - c_2 & 0 & 0 & c_0 + c_3 \end{bmatrix},$$

\mathcal{C} is the linear span of the matrices $\sigma_i \otimes \sigma_i$, $0 \leq i \leq 3$. (These are the matrices which are diagonal in the so-called Bell basis.)

The algebra \mathcal{C} plays a special role. Any unitary in M_4 can be written in the form

$$(L_1 \otimes L_2)N(L_3 \otimes L_4), \quad (2)$$

where L_1, L_2, L_3, L_4 are 2×2 unitaries and the unitary N is in \mathcal{C} . This is called Cartan decomposition, see equation (11) in [7] or [3].

There is a unitary $W \in M_4$ such that

$$W(I \otimes M_2)W^* = \mathcal{A}.$$

W has a Cartan decomposition (2). Since the subalgebra $W(I \otimes M_2)W^*$ does not depend on L_3 and L_4 , we may assume that $L_3 = L_4 = I$. Moreover, the quasi-orthogonality of $W(I \otimes M_2)W^*$ and $I \otimes M_2$ does not depend on L_1 and L_2 . The quasi-orthogonality is determined by the factor $N \in \mathcal{C}$. Since the matrices $E_i = \sigma_i/\sqrt{2}$ form a basis in M_2 , Theorem 1.2 is conveniently applied for the unitary $N = \sum_{i=0}^3 c_i \sigma_i \otimes \sigma_i$, choose W_i as $c_i \sqrt{2} \sigma_i$. The theorem gives that

$$2 \sum_{i=0}^3 |c_i|^2 |\sigma_i\rangle \langle \sigma_i|$$

is the identity mapping on M_2 which implies $|c_i|^2 = 1/4$ ($0 \leq i \leq 3$). In a trigonometric approach, let

$$\begin{aligned} c_0 &= \cos \alpha \cos \beta \cos \gamma + i \sin \alpha \sin \beta \sin \gamma, \\ c_1 &= \cos \alpha \sin \beta \sin \gamma + i \sin \alpha \cos \beta \cos \gamma, \\ c_2 &= \sin \alpha \cos \beta \sin \gamma + i \cos \alpha \sin \beta \cos \gamma, \\ c_3 &= \sin \alpha \sin \beta \cos \gamma + i \cos \alpha \cos \beta \sin \gamma. \end{aligned}$$

In order to get a proper unitary, two of the values of $\cos^2 \alpha$, $\cos^2 \beta$ and $\cos^2 \gamma$ equal $1/2$ and the third one may be arbitrary. Let \mathcal{N} be the set of all matrices such that the parameters α, β and γ satisfy the above condition, in other words two of the three values are of the form $\pi/4 + k\pi/2$. (k is an integer.) Let

$$\mathcal{N}_1 := \{N \in \mathcal{N} : \alpha \text{ is arbitrary, } \beta = \pi/4 + k_1\pi/2, \text{ and } \gamma = \pi/4 + k_2\pi/2\} \quad (3)$$

and define \mathcal{N}_2 and \mathcal{N}_3 similarly. ($\mathcal{N} = \mathcal{N}_1 \cup \mathcal{N}_2 \cup \mathcal{N}_3$.) Since the subalgebra $N(I \otimes M_2)N^*$ does not depend on the integers k_1 and k_2 , we simply take $k_1 = k_2 = 0$. This makes computations a bit more convenient. One computes that

$$N_i(I \otimes \sigma_i)N_i^* = \pm \sigma_i \otimes I$$

for $N_i \in \mathcal{N}_i$. It follows that

$$(L_1 \otimes L_2)N_i(I \otimes \sigma_i)N_i^*(L_1^* \otimes L_2^*) = \pm L_1 \sigma_i L_1^* \otimes I$$

for every unitary $N_i \in \mathcal{N}_i$. Therefore $L_1 \sigma_i L_1^* \otimes I \in \mathcal{A}(0)' \cap \mathcal{B}$. \square

The theorem immediately gives that the maximal number of pairwise quasi-orthogonal subalgebras isomorphic to M_2 is at most 4.

3 Quasi-orthogonal subalgebras in M_{2^n}

Next we consider the pairwise quasi-orthogonal subalgebras $\mathcal{A}_i \simeq M_2$ in M_{2^n} . Let $m(n)$ be the maximal number of pairwise quasi-orthogonal subalgebras of M_{2^n} which are isomorphic to M_2 . The question is their maximal number $m(n)$.

The traceless subspaces of M_2 and M_{2^n} are a 3-dimensional space and a $(4^n - 1)$ -dimensional space, respectively. Therefore,

$$m(n) \leq \frac{4^n - 1}{3} =: N_n.$$

Below, we construct $N_n - 1$ pairwise quasi-orthogonal subalgebras. We conjecture that this is the true value of $m(n)$.

The Hilbert space M_{2^n} has a natural orthogonal basis

$$\sigma_{i_1} \otimes \sigma_{i_2} \otimes \cdots \otimes \sigma_{i_n} =: (i_1, i_2, \dots, i_n),$$

where $i_j = 0, 1, 2, 3$ and $1 \leq j \leq n$. We put

$$P_n = \{(i_1, i_2, \dots, i_n) : 0 \leq i_j \leq 3, 1 \leq j \leq n\} \setminus \{I\}.$$

A triplet $(A_1, A_2, A_3) \in P_n^3$ is called a weak Pauli triplet if $A_1 A_2 = \pm i A_3$. and $(A_1, A_2, A_3) \in P_n^3$ is a commuting triplet if $A_1 A_2 = \pm A_3$. The linear span of elements of a weak Pauli triplet and I is a subalgebra isomorphic to M_2 .

Assume that $A = (A_1, A_2, A_3) \in P_n^3$ is a commuting triplet. Then we can construct three pairwise disjoint weak Pauli triplets: $\hat{A}^{(1)} := (\sigma_1 \otimes A_1, \sigma_2 \otimes A_2, \sigma_3 \otimes A_3)$ and $\hat{A}^{(2)} := (\sigma_2 \otimes A_1, \sigma_3 \otimes A_2, \sigma_1 \otimes A_3)$ and $\hat{A}^{(3)} := (\sigma_3 \otimes A_1, \sigma_1 \otimes A_2, \sigma_2 \otimes A_3)$ in P_{n+1}^3 . Therefore, to construct pairwise quasi-orthogonal subalgebras isomorphic to M_2 , it is useful to consider weak Pauli triplets and commuting triplets.

Example 3.1 *There are 5 pairwise disjoint commuting triplets in P_2^3 . Indeed,*

$$\begin{aligned} &((0, 1), (1, 0), (1, 1)), \quad ((0, 2), (2, 0), (2, 2)), \quad ((0, 3), (3, 0), (3, 3)), \\ &((1, 2), (2, 3), (3, 1)), \quad ((1, 3), (2, 1), (3, 2)). \end{aligned}$$

There are 21 pairwise disjoint commuting triplets in P_3^3 . Indeed,

$$\begin{aligned} &((1, 0, 1), (2, 0, 3), (3, 0, 2)), \quad ((1, 0, 2), (2, 0, 1), (3, 0, 3)), \quad ((0, 1, 1), (0, 2, 3), (0, 3, 2)), \\ &((0, 1, 3), (0, 1, 0), (0, 0, 3)), \quad ((0, 2, 2), (0, 2, 0), (0, 0, 2)), \quad ((0, 3, 1), (0, 3, 0), (0, 0, 1)), \\ &((3, 2, 1), (3, 0, 0), (0, 2, 1)), \quad ((2, 1, 2), (2, 0, 0), (0, 1, 2)), \quad ((1, 3, 3), (1, 0, 0), (0, 3, 3)), \\ &((3, 3, 1), (2, 3, 2), (1, 0, 3)), \quad ((3, 1, 1), (1, 1, 3), (2, 0, 2)), \quad ((2, 2, 2), (1, 2, 3), (3, 0, 1)), \\ &((1, 1, 1), (2, 2, 1), (3, 3, 0)), \quad ((1, 2, 1), (2, 3, 1), (3, 1, 0)), \quad ((1, 3, 1), (2, 1, 1), (3, 2, 0)), \\ &((1, 1, 2), (2, 2, 0), (3, 3, 2)), \quad ((1, 2, 2), (2, 3, 0), (3, 1, 2)), \quad ((1, 3, 2), (2, 1, 0), (3, 2, 2)), \\ &((1, 1, 0), (2, 2, 3), (3, 3, 3)), \quad ((1, 2, 0), (2, 3, 3), (3, 1, 3)), \quad ((1, 3, 0), (2, 1, 3), (3, 2, 3)). \end{aligned}$$

We show that P_n can be decomposed into commuting triplets.

Theorem 3.2 For each $n \geq 2$, there is a family of commuting triplets

$$\{A^{(i)} = (A_1^{(i)}, A_2^{(i)}, A_3^{(i)})\}_{i=1}^{N_n} \subset P_n^3$$

such that

$$\bigcup_{i=1}^{N_n} A^{(i)} = P_n.$$

Proof. In the case $n = 2$ and $n = 3$, it is already proven above. Assume it is proven in the case $n = k$, and we consider the case $n = k + 2$. Let $\{A^{(i)}\}_{i=1}^5$ and $\{B^{(j)}\}_{j=1}^{N_k}$ be the family of commuting triplets satisfying the theorem in the case of $n = 2$ and $n = k$, respectively. Then, for each $A^{(i)} = (A_1^{(i)}, A_2^{(i)}, A_3^{(i)})$ and $B^{(j)} = (B_1^{(j)}, B_2^{(j)}, B_3^{(j)})$, we can construct three commuting triplets in P_{k+2}^3 , that is, $(A_1^{(i)} \otimes B_1^{(j)}, A_2^{(i)} \otimes B_2^{(j)}, A_3^{(i)} \otimes B_3^{(j)})$ and $(A_1^{(i)} \otimes B_2^{(j)}, A_2^{(i)} \otimes B_3^{(j)}, A_3^{(i)} \otimes B_1^{(j)})$ and $(A_1^{(i)} \otimes B_3^{(j)}, A_2^{(i)} \otimes B_1^{(j)}, A_3^{(i)} \otimes B_2^{(j)})$. Moreover, we have other commuting triplets, i.e., $(A_1^{(i)} \otimes I_k, A_2^{(i)} \otimes I_k, A_3^{(i)} \otimes I_k)$ and $(I_2 \otimes B_1^{(j)}, I_2 \otimes B_2^{(j)}, I_2 \otimes B_3^{(j)})$. Consequently, we have $5 + N_k + 3 \cdot 5 \cdot N_k = N_{k+2}$ commuting triplets. Since $\bigcup_{i=1}^5 A^{(i)} = P_2$ and $\bigcup_{j=1}^{N_k} B^{(j)} = P_k$, $\{A_1^{(i)}, A_2^{(i)}, A_3^{(i)}\}_{i=1}^5$ and $\{B_1^{(j)}, B_2^{(j)}, B_3^{(j)}\}_{j=1}^{N_k}$ are distinct. Hence, we obtain the union of the above N_{k+2} commuting triplets is P_{k+2} . \square

The good point of this construction is that it is easy to use the induction.

Theorem 3.3 There exist $N_n - 1$ quasi-orthogonal subalgebras in M_{2^n} .

Proof. The case $n = 2$ is already proven in Theorem 3. Assume it is proven for $n = k$, and we consider the case $n = k + 1$.

From Theorem 3.2, let $\{A^{(i)} = (A_1^{(i)}, A_2^{(i)}, A_3^{(i)})\}_{i=1}^{N_k}$ be commuting triplets in P_k^3 such that $\bigcup_{i=1}^{N_k} A^{(i)} = P_k$. Then we have $3N_k$ pairwise disjoint weak Pauli triplets, that is, $(\sigma_1 \otimes A_1^{(i)}, \sigma_2 \otimes A_2^{(i)}, \sigma_3 \otimes A_3^{(i)})$ and $(\sigma_2 \otimes A_1^{(i)}, \sigma_3 \otimes A_2^{(i)}, \sigma_1 \otimes A_3^{(i)})$ and $(\sigma_3 \otimes A_1^{(i)}, \sigma_1 \otimes A_2^{(i)}, \sigma_2 \otimes A_3^{(i)})$. Furthermore, we obtain another weak Pauli triplet $(\sigma_1 \otimes I_k, \sigma_2 \otimes I_k, \sigma_3 \otimes I_k)$. These $3N_k + 1$ weak Pauli triplets are pairwise disjoint. Moreover, the complement space of above $3N_k + 1$ Pauli triplets is $I \otimes M_{2^k}$. Indeed, since $\bigcup_{i=1}^{N_k} A^{(i)} = P_k$, we have

$$\begin{aligned} & \{(\sigma_1 \otimes A_1^{(i)}, \sigma_2 \otimes A_2^{(i)}, \sigma_3 \otimes A_3^{(i)}), (\sigma_2 \otimes A_1^{(i)}, \sigma_3 \otimes A_2^{(i)}, \sigma_1 \otimes A_3^{(i)}), \\ & (\sigma_3 \otimes A_1^{(i)}, \sigma_1 \otimes A_2^{(i)}, \sigma_2 \otimes A_3^{(i)}), (\sigma_1 \otimes I_k, \sigma_2 \otimes I_k, \sigma_3 \otimes I_k) \mid 1 \leq i \leq N_k\} \\ & = \{\sigma_i \otimes \sigma_{j_1} \otimes \cdots \otimes \sigma_{j_k} \mid i = 1, 2, 3, j_l = 0, 1, 2, 3, 1 \leq l \leq k\}. \end{aligned}$$

Therefore, the complement space is $I \otimes M_{2^k}$ spanned by

$$\{\sigma_0 \otimes \sigma_{j_1} \otimes \cdots \otimes \sigma_{j_k} \mid j_l = 0, 1, 2, 3, 1 \leq l \leq k\}.$$

Now we use the assumption that there are $N_k - 1$ pairwise disjoint weak Pauli triplets $B^{(i)} = (B_1^{(i)}, B_2^{(i)}, B_3^{(i)})$ in M_{2^k} ($1 \leq i \leq N_k - 1$). Then

$$(\sigma_0 \otimes B_1^{(i)}, \sigma_0 \otimes B_2^{(i)}, \sigma_0 \otimes B_3^{(i)})$$

give pairwise disjoint weak Pauli triplets in P_{k+1}^3 . Summing up, we have $3N_k + 1 + N_k - 1 = 4N_k = N_{k+1} - 1$ pairwise disjoint weak Pauli triplets. \square

Similarly, we can prove the following. If there exist N_n pairwise quasi-orthogonal subalgebras in M_{2^n} for some n , then there exist N_k pairwise quasi-orthogonal subalgebras in M_{2^k} for all $k \geq n$.

4 Quasi-orthogonal subalgebras: d is prime

In this section, we consider the quasi-orthogonal subalgebras in $M_{p^2} = M_p \otimes M_p$ which are isomorphic to M_p , where p is a prime number with $p \geq 3$. In this case, we can construct $p^2 + 1$ pairwise quasi-orthogonal subalgebras.

Define the unitary operators W and S in M_p by

$$W = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & 0 & \cdots & 0 \\ 0 & 0 & \lambda^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda^{p-1} \end{bmatrix}, \quad S = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix},$$

where $\lambda = e^{2\pi i/p}$. A natural orthogonal basis of M_p consists of $\{S^i W^j\}_{0 \leq i, j \leq p-1}$. Since $SW = \lambda^{-1}WS$, we have

$$S^{k_1} W^{l_1} S^{k_2} W^{l_2} = \lambda^{l_1 k_2} S^{k_1+k_2} W^{l_1+l_2}. \quad (4)$$

Therefore $S^{k_1} W^{l_1}$ and $S^{k_2} W^{l_2}$ commute if and only if $k_1 l_2 = k_2 l_1 \pmod{p}$. We consider this commutativity condition in the context of a vector space over the finite field Z_p . Let $Z_p^4 = \{(k_1, l_1, k_2, l_2) \mid k_1, l_1, k_2, l_2 \in Z_p\}$ and define a natural homomorphism π (up to scalar multiple) from Z_p^4 to $M_p \otimes M_p$ by

$$\pi(k_1, l_1, k_2, l_2) = S^{k_1} W^{l_1} \otimes S^{k_2} W^{l_2}.$$

We denote a *symplectic product* by

$$u \circ u' = k_1 l'_1 - k'_1 l_1 + k_2 l'_2 - k'_2 l_2 \pmod{p},$$

where $u = (k_1, l_1, k_2, l_2)$ and $u' = (k'_1, l'_1, k'_2, l'_2)$. From (4),

$$\pi(u)\pi(u') = \lambda^{-u \circ u'} \pi(u')\pi(u). \quad (5)$$

Hence $\pi(u)$ and $\pi(u')$ commute if and only if their symplectic product equals zero.

Lemma 4.1 *If $\pi(u)$ and $\pi(u')$ are not commutative for $u = (k_1, l_1, k_2, l_2)$, $u' = (k'_1, l'_1, k'_2, l'_2) \in Z_p^4$, then the algebra \mathcal{A} generated by $\pi(u)$ and $\pi(u')$ is isomorphic to M_p .*

Proof. From the assumption, $u \circ u' \neq 0$. We define a map ρ from $\{S, W^{u \circ u'}\}$ to \mathcal{A} by

$$\rho(S) = \pi(u), \quad \rho(W^{u \circ u'}) = \pi(u').$$

From (5) and $SW^{u \circ u'} = \lambda^{-u \circ u'} W^{u \circ u'} S$, the commutativity condition of $\pi(u)$, $\pi(u')$ and that of S , $W^{u \circ u'}$ are same. Therefore ρ can be extended to a isomorphism from M_p generated by S and $W^{u \circ u'}$ to \mathcal{A} . \square

From this lemma, we need to find such u and u' . Let D be a non-zero interger in Z^p with the requirement that $D \neq k^2 \pmod p$ for all k in Z_p , i.e. D is not a quadratic residue of p . For any $a_0, a_1 \in Z_p$, we define subgroups of Z_p^4 by

$$C_{a_0, a_1} = \{b_0(1, a_1, 0, a_0) + b_1(0, a_0, -1, a_1 D) \mid b_0, b_1 \in Z_p\},$$

where scalar multiplication and addition are defined by a natural way. Moreover define

$$C_\infty = \{b_0(0, 1, 0, 0) + b_1(0, 0, 0, 1) \mid b_0, b_1 \in Z_p\}.$$

Lemma 4.2 *The only vector common to any pair of above subgroups is $(0, 0, 0, 0)$. In particular, the subgroups partition $Z_p^4 \setminus \{(0, 0, 0, 0)\}$.*

Proof. Since there are p^2+1 subgroups and each subgroup has p^2 elements, it is enough to prove that the intersection of any two subgroups is $\{(0, 0, 0, 0)\}$. It is easy to see $C_{a_0, a_1} \cap C_\infty = \{(0, 0, 0, 0)\}$. Therefore we prove that $C_{a_0, a_1} \cap C_{a'_0, a'_1} = \{(0, 0, 0, 0)\}$ if $a_0 \neq a'_0$ or $a_1 \neq a'_1$.

Assume $b_0(1, a_1, 0, a_0) + b_1(0, a_0, -1, a_1 D) = b'_0(1, a'_1, 0, a'_0) + b'_1(0, a'_0, -1, a'_1 D)$, then from the first and third components we have $b_0 = b'_0$ and $b_1 = b'_1$. Similary, from the second and fourth components we are led to the equations

$$\begin{aligned} a_1 b_0 + a_0 b_1 &= a'_1 b_0 + a'_0 b_1 \\ a_0 b_0 + a_1 b_1 D &= a'_0 b_0 + a'_1 b_1 D. \end{aligned}$$

These equations can be rewritten as a matrix equation

$$\begin{bmatrix} b_1 & b_0 \\ b_0 & b_1 D \end{bmatrix} \begin{bmatrix} a_0 - a'_0 \\ a_1 - a'_1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

If $b_0 = b_1 = 0$, then the element is $(0, 0, 0, 0)$. Therefore we assume $b_0 \neq 0$ or $b_1 \neq 0$. Then the above matrix is invertible, indeed

$$\begin{bmatrix} b_1 & b_0 \\ b_0 & b_1 D \end{bmatrix}^{-1} = (b_1^2 D - b_0^2)^{-1} \begin{bmatrix} b_1 D & -b_0 \\ -b_0 & b_1 \end{bmatrix}.$$

Here we use that $b_1^2 D \neq b_0^2 \pmod p$ from the assumption of D . This implies $a_0 = a'_0$ and $a_1 = a'_1$ which is a contradiction. \square

Since $(1, a_1, 0, a_0) \circ (0, a_0, -1, a_1 D) = 2a_0$, if $a_0 \neq 0$ then

$$\text{span}\{\pi(C_{a_0, a_1})\} \simeq M_p$$

by Lemma 4.1. But if $a_0 = 0$, the algebra is commutative and hence $\text{span}\{\pi(C_{a_0, a_1})\} \simeq \mathbb{C}^{p^2}$. Therefore we need reconstruct subgroups in the case $a_0 = 0$.

For any $a \in Z_p$, define subgroups by

$$\begin{aligned} D_a &= \{b_0(1, 1, -a, aD) + b_1(1, 2, -a, 2aD) \mid b_0, b_1 \in Z_p\}, \\ D_\infty &= \{b_0(0, 0, 1, 0) + b_1(0, 0, 0, 1) \mid b_0, b_1 \in Z_p\}. \end{aligned}$$

Lemma 4.3 *The only vector common to any pair of above subgroups is $(0, 0, 0, 0)$. Moreover we have*

$$\bigcup_{a \in Z_p} D_a \cup D_\infty = \bigcup_{a_1 \in Z_p} C_{0, a_1} \cup C_\infty.$$

Proof. It is easy to see the first assertion. Therefore to show the second assertion, it is enough to prove $D_a, D_\infty \subset \bigcup_{a_1 \in Z_p} C_{0, a_1} \cup C_\infty$.

First consider the element $(0, 0, b_0, b_1)$ in D_∞ . If $b_0 = 0$, then $(0, 0, 0, b_1) \in C_\infty$. If $b_0 \neq 0$, then

$$(0, 0, b_0, b_1) = -b_0(0, 0, -1, -b_0^{-1}b_1D^{-1}D) \in C_{0, -b_0^{-1}b_1D^{-1}}.$$

Hence $D_\infty \subset \bigcup_{a_1 \in Z_p} C_{0, a_1} \cup C_\infty$. Next we consider the element $b_0(1, 1, -a, aD) + b_1(1, 2, -a, 2aD)$ in D_a . If $b_0 + b_1 = 0$, then $b_0(1, 1, -a, aD) + b_1(1, 2, -a, 2aD) = (0, b_0 + 2b_1, 0, ab_0D + 2ab_1D) \in C_\infty$. If $b_0 + b_1 \neq 0$, then

$$\begin{aligned} & b_0(1, 1, -a, aD) + b_1(1, 2, -a, 2aD) \\ &= (b_0 + b_1) (1, (b_0 + b_1)^{-1}(b_0 + 2b_1), 0, 0) \\ & \quad + a(b_0 + b_1) (0, 0, -1, (b_0 + b_1)^{-1}(b_0 + 2b_1)D) \\ & \in C_{0, (b_0 + b_1)^{-1}(b_0 + 2b_1)}. \end{aligned}$$

Therefore we obtain $D_a \subset \bigcup_{a_1 \in Z_p} C_{0, a_1} \cup C_\infty$. □

Since $(1, 1, -a, aD) \circ (1, 2, -a, 2aD) = 1 - a^2D \neq 0$ by the assumption of D and $(0, 0, 1, 0) \circ (0, 0, 0, 1) = 1$, we obtain

$$\begin{aligned} \text{span}\{\pi(D_a)\} &\simeq M_p \\ \text{span}\{\pi(D_\infty)\} &\simeq M_p \end{aligned}$$

by Lemma 4.1. Consecntly we have the next theorem.

Theorem 4.4 *There are $p^2 + 1$ pairwise quasi-orthogonal subalgebras of M_{p^2} which are isomorphic to M_p .*

References

- [1] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury and F. Vatan, A new proof for the existence of mutually unbiased bases, *Algoritmica* **34**, 512–528, 2002.
- [2] P.O Boykin, M. Sitharam, P.H. Tiep and P. Wocjan, Mutually unbiased bases and orthogonal decompositions of Lie algebras, arXiv:quant-ph/0506089, 2005.
- [3] D. D'Alessandro and F. Albertini, Quantum symmetries and Cartan decompositions in arbitrary dimensions, quant-ph/0504044, 2005.
- [4] H. Ohno, D. Petz and A. Szántó, Quasi-orthogonal subalgebras of 4×4 matrices, *Linear Alg. Appl.* **425**, 109-118, 2007.
- [5] D. Petz, Complementarity in quantum systems, preprint, 2006, to be published in *Rep. Math. Phys.*
- [6] D. Petz and J. Kahn, Complementary reductions for two qubits, *J. Math. Phys.* **48**(2007), 012107.
- [7] J. Zhang, J. Vala, K.B. Whaley and S. Sastry, A geometric theory of non-local two-qubit operations, *Phys. Rev.* **A67**(2003), 042313.