Necessary condition for existence of conditional SIC-POVM

Hiromichi Ohno * †

Department of Mathematics, Faculty of Engineering, Shinshu University, 4-17-1 Wakasato, Nagano 380-8553, Japan

1 Introduction

This paper is an announcement of our result and the detailed version will be submitted to somewhere. (See [2].)

POVMs (positive operator valued measure) on quantum systems are considered as a measurement in quantum physics. If POVMs have a good condition, then we can determine a state by results of a measurement. In this case, the POVM is called informationally complete and the process is called quantum state tomography.

First, we introduce SIC-POVMs (symmetric informationally complete POVM). SIC-POVMs is generated by vectors in \mathbb{C}^n whose the absolute values of inner products of each vectors are same. Zauner conjectured that there exist such n^2 vectors in \mathbb{C}^n for any n. But the existence is only proved when $n \leq 15$ and n = 19, 24, 35, 48 [5, 8].

Next, we introduce conditional SIC-POVMs. A state of a quantum system is a density matrix which has several parameters. When a few parameters are known, then SIC-POVM is not the best measurement to determine the state. Hence we need another POVM and it is a conditional SIC-POVM. Conditional SIC-POVMs are also generated by vectors in \mathbb{C}^n . But the existence of conditional SIC-POVMs depends on the system. We will discuss the details in Sect. 4.

2 Preliminaries

Definition 2.1 $\rho \in M_n(\mathbb{C})$ is called a density matrix (or state) if $\rho \geq 0$ and

$$Tr(\rho) = 1.$$

For any density matrix ρ , we can define a state $\hat{\rho}$ by

$$\hat{\rho}(X) = \text{Tr}(\rho X).$$

Conversely, any state is written by the above form. Therefore, there exists a one-to-one correspondence between density matrices and states.

Definition 2.2 A set of positive operators $\{P_i\}_{i=1}^k \subset M_n(\mathbb{C})$ is called a positive operator valued measure (POVM) if $P_i \geq 0$ $(1 \leq i \leq k)$ and

$$\sum_{i=1}^k P_i = I.$$

If P_i is a projection, then $\{P_i\}_{i=1}^k$ is called a projection valued measure (PVM).

^{*}The author is supported partially by JSPS KAKENHI Grant Number 25800061.

[†]E-mail: h_ohno@shinshu-u.ac.jp

For a POVM $\{P_i\}_{i=1}^k$, we can consider a measurement device by using this POVM:

$$\begin{array}{ccc}
\hline{\rho} & \xrightarrow{input} & & & \\
\hline
& & \\
& \xrightarrow{output} & & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\
& & \\$$

This means that we can know $\text{Tr}(\rho P_i)$ for all $(1 \leq i \leq k)$, if we have many copies of ρ . Therefore, if a POVM $\{P_i\}_{i=1}^k$ has a good condition, then we can determine the quantum state ρ by $\text{Tr}(\rho P_i)$. This is called **quantum state tomography**.

Definition 2.3 A POVM $\{P_i\}_{i=1}^k$ is called informationally complete if for density matrices $\rho \neq \sigma$, there exists P_i such that

$$\operatorname{Tr}(\rho P_i) \neq \operatorname{Tr}(\sigma P_i).$$

If a POVM $\{P_i\}_{i=1}^k$ is informationally complete, then we can determine the quantum state ρ by $\text{Tr}(\rho P_i)$. If ρ is a state in $M_n(\mathbb{C})$, then the following statement holds.

Theorem 2.4 A POVM $\{P_i\}_{i=1}^k \subset M_n(\mathbb{C})$ is informationally complete if and only if

$$\operatorname{span}\{P_i\}_{i=1}^k = M_n(\mathbb{C}).$$

In particular, we can determine the quantum state ρ by $\text{Tr}(\rho P_i)$.

Example 2.5 For small $\varepsilon > 0$. Let

$$P_{1} = \frac{1}{2+2\varepsilon^{2}} \begin{bmatrix} 1 & \varepsilon \\ \varepsilon & \varepsilon^{2} \end{bmatrix}, P_{2} = \frac{1}{2+2\varepsilon^{2}} \begin{bmatrix} 1 & -\varepsilon \\ -\varepsilon & \varepsilon^{2} \end{bmatrix},$$

$$P_{3} = \frac{1}{2+2\varepsilon^{2}} \begin{bmatrix} \varepsilon^{2} & \varepsilon i \\ -\varepsilon i & 1 \end{bmatrix}, P_{4} = \frac{1}{2+2\varepsilon^{2}} \begin{bmatrix} \varepsilon^{2} & -i\varepsilon \\ i\varepsilon & 1 \end{bmatrix}.$$

Then $\{P_i\}_{i=1}^4$ is an informationally complete POVM. For a state ρ in $M_n(\mathbb{C})$, by equations

$$(2 + 2\varepsilon^{2}) \operatorname{Tr}(\rho P_{1}) = \rho_{11} + \varepsilon \rho_{12} + \varepsilon \rho_{21} + \varepsilon^{2} \rho_{22}$$

$$(2 + 2\varepsilon^{2}) \operatorname{Tr}(\rho P_{2}) = \rho_{11} - \varepsilon \rho_{12} - \varepsilon \rho_{21} + \varepsilon^{2} \rho_{22}$$

$$(2 + 2\varepsilon^{2}) \operatorname{Tr}(\rho P_{3}) = \varepsilon^{2} \rho_{11} - i\varepsilon \rho_{12} + i\varepsilon \rho_{21} + \rho_{22}$$

$$(2 + 2\varepsilon^{2}) \operatorname{Tr}(\rho P_{4}) = \varepsilon^{2} \rho_{11} + i\varepsilon \rho_{12} - i\varepsilon \rho_{21} + \rho_{22},$$

we have

$$\rho = \operatorname{Tr}(\rho P_{1}) \begin{bmatrix}
\frac{1}{1-\varepsilon^{2}} & \frac{1}{4\varepsilon(1+\varepsilon^{2})} \\
\frac{1}{4\varepsilon(1+\varepsilon^{2})} & \frac{-\varepsilon^{2}}{1-\varepsilon^{2}}
\end{bmatrix} + \operatorname{Tr}(\rho P_{2}) \begin{bmatrix}
\frac{1}{1-\varepsilon^{2}} & \frac{-1}{4\varepsilon(1+\varepsilon^{2})} \\
\frac{-1}{4\varepsilon(1+\varepsilon^{2})} & \frac{-\varepsilon^{2}}{1-\varepsilon^{2}}
\end{bmatrix} + \operatorname{Tr}(\rho P_{2}) \begin{bmatrix}
\frac{1}{1-\varepsilon^{2}} & \frac{-1}{4\varepsilon(1+\varepsilon^{2})} \\
\frac{-1}{4\varepsilon(1+\varepsilon^{2})} & \frac{-\varepsilon^{2}}{1-\varepsilon^{2}}
\end{bmatrix} + \operatorname{Tr}(\rho P_{4}) \begin{bmatrix}
\frac{-\varepsilon^{2}}{1-\varepsilon^{2}} & \frac{-i}{4\varepsilon(1+\varepsilon^{2})} \\
\frac{i}{4\varepsilon(1+\varepsilon^{2})} & \frac{1}{1-\varepsilon^{2}}
\end{bmatrix}.$$

Hence we can determine a state ρ . But this is not a good POVM to detect ρ . Since

$$\rho_{12} = \frac{1}{4\varepsilon(1+\varepsilon^2)} \left(\operatorname{Tr}(P_1\rho) - \operatorname{Tr}(P_2\rho) - i \left(\operatorname{Tr}(P_3\rho) - \operatorname{Tr}(P_4\rho) \right) \right),$$

a small error causes a big difference.

If a POVM is informationally complete, then we can determine a state ρ by $\{\operatorname{Tr}(\rho P_i)\}_{i=1}^k$. But by ℓ experiments, we can only obtain approximate values of $\{\operatorname{Tr}(\rho P_i)\}_{i=1}^k$. Let the candidate generated by these approximate values be $\hat{\rho}$. A POVM is called optimal, if the expected value of

$$\|\rho - \hat{\rho}\|_2$$

is the minimum among all candidates generated by any POVM and ℓ experiments. If a POVM is optimal, then it satisfies the following condition.

Theorem 2.6 [4] A POVM in $M_n(\mathbb{C})$ with rank one positive operators $\{\frac{n}{k}P_i\}_{i=1}^k$ are optimal POVM if and only if

$$\sum_{i=1}^{k} \frac{n}{k} |P_i\rangle\langle P_i| = \frac{1}{n+1} \left(\mathrm{id}_{M_n(\mathbb{C})} + |I\rangle\langle I| \right),$$

where $|P_i\rangle\langle P_i|$ is a superoperator $M_n(\mathbb{C})\to M_n(\mathbb{C})$ with $A\mapsto \operatorname{Tr}(AP_i)P_i$.

3 SIC-POVM

In this section, we introduce a SIC-POVM (symmetric informationally complete positive operator valued measure) which is an optimal POVM.

Definition 3.1 A set of vectors $\{\xi_i\}_{i=1}^{n^2} \subset \mathbb{C}^n$ is called symmetric informationally complete POVM (SIC-POVM) if

$$|\langle \xi_i, \xi_j \rangle| = \frac{1}{\sqrt{n+1}}.$$

A POVM generated by the above vectors

$$\left\{\frac{1}{n}|\xi_i\rangle\langle\xi_i|\right\}_{i=1}^{n^2}$$

is also called a SIC-POVM, where $|x\rangle\langle y|z=\langle y,z\rangle x$ for all $x,y,z\in\mathbb{C}^n$.

A SIC-POVM is informationally complete. Indeed, if we assume

$$\sum_{i=1}^{n^2} a_i |\xi_i\rangle\langle\xi_i| = 0,$$

then for all $1 \le j \le n^2$ we have

$$0 = \operatorname{Tr}\left(\sum_{i=1}^{n^2} a_i |\xi_i\rangle\langle\xi_i| \cdot |\xi_j\rangle\langle\xi_j|\right) = a_j + \frac{1}{n+1} \sum_{i \neq j} a_i.$$

So it is easy to see that $\{|\xi_i\rangle\langle\xi_i|\}_{i=1}^{n^2}$ is linearly independent. Moreover, for all $1 \leq j \leq n^2$,

$$\operatorname{Tr}\left(\sum_{i=1}^{n^2} \frac{1}{n} |\xi_i\rangle\langle\xi_i| \cdot |\xi_j\rangle\langle\xi_j|\right) = \frac{1}{n} + \sum_{i\neq j} \frac{1}{n(n+1)} = 1.$$

Hence $\sum_{i=1}^{n^2} \frac{1}{n} |\xi_i\rangle \langle \xi_i| = I$.

Example 3.2 In \mathbb{C}^2 ,

$$\xi_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \xi_2 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ \sqrt{2} \end{bmatrix}, \xi_3 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ \lambda\sqrt{2} \end{bmatrix}, \xi_4 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ \bar{\lambda}\sqrt{2} \end{bmatrix}$$

is a SIC-POVM, where $\lambda = e^{2\pi i/3} = \frac{-1 + \sqrt{3}i}{2}$. In \mathbb{C}^3 ,

$$\xi_{1} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \xi_{2} = \frac{1}{2} \begin{bmatrix} 1 \\ \sqrt{3} \\ 0 \end{bmatrix}, \xi_{3} = \frac{1}{2} \begin{bmatrix} 1 \\ -\sqrt{3} \\ 0 \end{bmatrix},$$

$$\xi_{4} = \frac{1}{2} \begin{bmatrix} 1 \\ i \\ \sqrt{2} \end{bmatrix}, \xi_{5} = \frac{1}{2} \begin{bmatrix} 1 \\ i \\ \sqrt{2}\lambda \end{bmatrix}, \xi_{6} = \frac{1}{2} \begin{bmatrix} 1 \\ i \\ \sqrt{2}\bar{\lambda} \end{bmatrix},$$

$$\xi_{7} = \frac{1}{2} \begin{bmatrix} 1 \\ -i \\ \sqrt{2} \end{bmatrix}, \xi_{8} = \frac{1}{2} \begin{bmatrix} 1 \\ -i \\ \sqrt{2}\lambda \end{bmatrix}, \xi_{9} = \frac{1}{2} \begin{bmatrix} 1 \\ -i \\ \sqrt{2}\bar{\lambda} \end{bmatrix},$$

is a SIC-POVM, where $\lambda = e^{2\pi i/3}$.

It is known that a SIC-POVM exists if $n \le 15$ or n = 19, 24, 35, 48. Numerical solutions have been found when $n \le 67$. But for other cases, the existence is an open problem. The following is conjectured by G. Zauner in 1999 [7].

Let

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

where $\lambda = \exp \frac{2\pi i}{n}$. $\{W^k S^\ell\}_{k,\ell=1}$ are called generalized Pauli matrices.

Definition 3.3 A unit vector ξ is called a fiducial vector if

$$\{W^k S^\ell \xi\}_{k,\ell=1}^n$$

is a SIC-POVM.

Conjecture (Zauner's conjecture [7]) A fiducial vector exists in \mathbb{C}^n for all $n \geq 2$. In particular, a SIC-POVM exists in \mathbb{C}^n .

4 Conditional SIC-POVM

Recently, SIC-POVMs in arbitrary subspace of $M_n(\mathbb{C})$ are also considered. Let $M_n(\mathbb{C})$ be decomposed as

$$M_n(\mathbb{C}) = \mathbb{C}I \oplus \mathcal{A} \oplus \mathcal{B}$$

and $\rho \in M_n(\mathbb{C})$ be a density matrix. Let P_A and P_B be projections onto A and B. Assume we know $P_A \rho$. Then we want to know an optimal POVM which determines ρ . Since we already know $P_A \rho$, SIC-POVM is not suitable.

Let dim $\mathcal{A}=m$ then dim $\mathcal{B}=n^2-m-1$ and let $N=n^2-m$. For rank one informationally complete POVM $\{\frac{n}{k}P_i\}_{i=1}^k$, let

$$\mathcal{F} = \frac{n}{k} |P_i\rangle\langle P_i|.$$

Then the following theorem holds.

Theorem 4.1 [3] Rank one informationally complete POVM $\{\frac{n}{N}P_i\}_{i=1}^N$ is optimal if and only if

$$\mathcal{F} = |I\rangle\langle I| + \frac{n-1}{N-1}P_{\mathcal{B}}.$$

In this case,

$$\sum_{i=1}^{k} P_i = \frac{N}{n} I, \qquad \operatorname{Tr}(P_i P_j) = \frac{N-n}{n(N-1)}.$$

Such POVM is called a conditional SIC-POVM. Examples of conditional SIC-POVMs are following.

Example 4.2 If we do not have any information a priory about the state $(m = 0, N = n^2)$, then

$$\operatorname{Tr} P_i P_j = \frac{1}{n+1} \quad (i \neq j)$$

so the optimal POVM is the well-known SIC-POVM (if it exists).

Example 4.3 If we know the off-diagonal elements of the state, and we want to estimate the diagonal entries $(m = n^2 - n, N = n)$, then from Theorem 4.1 it follows that the optimal POVM has the properties

$$\operatorname{Tr} P_i P_j = 0 \quad (i \neq j), \quad \sum_{i=1}^n P_i = I, \quad \text{ and } \quad P_i \text{ is diagonal.}$$

So the diagonal matrix units form an optimal POVM.

Example 4.4 If we know the diagonal elements of the state, and we want to estimate the off-diagonal entries $(m = n - 1, N = n^2 - n + 1)$, then from Theorem 4.1 it follows that the optimal POVM has the properties

$$\operatorname{Tr} P_i P_j = \frac{n-1}{n^2} \quad (i \neq j), \quad \sum_{i=1}^n P_i = \frac{n^2 - n + 1}{n} I$$

and P_i has a constant diagonal.

The existence is not clear generally, but if n-1 is a prime power then it can be constructed. Details are written in [3].

Next, we present a necessary condition for existence of a conditional SIC-POVM.

Lemma 4.5 Let $\{P_i\}_{i=1}^N$ be a conditional SIC-POVM in $A \oplus C$ and let

$$Q_{i} = \sqrt{\frac{n(N-1)}{N(n-1)}} \left(P_{i} - \frac{1}{n} \left(1 + \sqrt{\frac{n-1}{N-1}} \right) I \right). \tag{1}$$

Then $\{Q_i\}_{i=1}^N$ is an orthonormal basis of $A \oplus C$.

Proof. For any $1 \le i \le N$, we have

$$\operatorname{Tr}\left(\left(P_{i} - \frac{1}{n}\left(1 + \sqrt{\frac{n-1}{N-1}}\right)I\right)^{2}\right)$$

$$= \operatorname{Tr}\left(P_{i} - \frac{2}{n}\left(1 + \sqrt{\frac{n-1}{N-1}}\right)P_{i} + \frac{1}{n^{2}}\left(1 + \sqrt{\frac{n-1}{N-1}}\right)^{2}I\right)$$

$$= 1 - \frac{2}{n}\left(1 + \sqrt{\frac{n-1}{N-1}}\right) + \frac{1}{n}\left(1 + 2\sqrt{\frac{n-1}{N-1}} + \frac{n-1}{N-1}\right)$$

$$= 1 - \frac{1}{n} + \frac{n-1}{n(N-1)}$$

$$= \frac{N(n-1)}{n(N-1)}.$$

Moreover, for any $1 \le i < j \le N$,

$$\operatorname{Tr}\left(\left(P_{i} - \frac{1}{n}\left(1 + \sqrt{\frac{n-1}{N-1}}\right)I\right)\left(P_{j} - \frac{1}{n}\left(1 + \sqrt{\frac{n-1}{N-1}}\right)I\right)\right)$$

$$= \frac{N-n}{n(N-1)} - \frac{2}{n}\left(1 + \sqrt{\frac{n-1}{N-1}}\right) + \frac{1}{n}\left(1 + 2\sqrt{\frac{n-1}{N-1}} + \frac{n-1}{N-1}\right)$$

$$= \frac{N-n}{n(N-1)} - \frac{1}{n} + \frac{n-1}{n(N-1)} = 0.$$

These equations imply $\langle Q_i, Q_j \rangle = \text{Tr}(Q_i^*Q_j) = \delta_{ij}$ so that $\{Q_i\}_{i=1}^N$ is an orthonormal basis of $A \oplus C$.

Theorem 4.6 If there exists a conditional SIC-POVM in $A \oplus C$, then for any $X \in B$ and any orthonormal basis $\{R_i\}_{i=1}^m$ of B,

$$\sum_{i=1}^m R_i^* X R_i = \frac{N-n}{n(n-1)} X.$$

Proof. Let $\{P_i\}_{i=1}^N$ be a conditional SIC-POVM in $A \oplus C$ and define $\{Q_i\}_{i=1}^N$ by (1). Then from the previous lemma, $\{Q_1, \ldots, Q_N, R_1, \ldots R_m\}$ is an orthonormal basis of $M_n(\mathbb{C})$. It is well known that

$$\sum_{i=1}^{N} Q_{i}^{*} X Q_{i} + \sum_{i=1}^{m} R_{i}^{*} X R_{i} = \text{Tr}(X).$$

B is orthogonal to $A = \mathbb{C}I$ so that Tr(X) = 0. Hence we will calculate $\sum_{i=1}^{N} Q_i^* X Q_i$. Since P_i is a rank one projection, $P_i X P_i = t P_i$ for some $t \in \mathbb{C}$. But $\text{Tr}(P_i X P_i) = t P_i$

 $\langle P_i, X \rangle = 0$ implies t = 0. Therefore $P_i X P_i = 0$. From the equation

$$\sum_{i=1}^{N} P_i = \frac{N}{n} I,$$

we have

$$\begin{split} &\frac{N(n-1)}{n(N-1)} \sum_{i=1}^{N} Q_{i}^{*} X Q_{i} \\ &= \sum_{i=1}^{N} \left(P_{i} - \frac{1}{n} \left(1 + \sqrt{\frac{n-1}{N-1}} \right) \right) X \left(P_{i} - \frac{1}{n} \left(1 + \sqrt{\frac{n-1}{N-1}} \right) \right) \\ &= \sum_{i=1}^{N} \left(P_{i} X P_{i} - \frac{1}{n} \left(1 + \sqrt{\frac{n-1}{N-1}} \right) (X P_{i} + P_{i} X) + \frac{1}{n^{2}} \left(1 + \sqrt{\frac{n-1}{N-1}} \right)^{2} X \right) \\ &= \left(-\frac{1}{n} \left(1 + \sqrt{\frac{n-1}{N-1}} \right) (X \sum_{i=1}^{N} P_{i} + \sum_{i=1}^{N} P_{i} X) + \frac{N}{n^{2}} \left(1 + \sqrt{\frac{n-1}{N-1}} \right)^{2} X \right) \\ &= \left(-\frac{2N}{n^{2}} \left(1 + \sqrt{\frac{n-1}{N-1}} \right) + \frac{N}{n^{2}} \left(1 + 2\sqrt{\frac{n-1}{N-1}} + \frac{n-1}{N-1} \right) \right) X \\ &= \frac{N}{n^{2}} \left(-1 + \frac{n-1}{N-1} \right) X = \frac{N(n-N)}{n^{2}(N-1)} X. \end{split}$$

This implies the assertion.

Example 4.7 Now we consider $M_4(\mathbb{C}) = M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$. A density matrix

$$ho = \left[egin{array}{ccccc} a_{11} & a_{12} & a_{13} & a_{14} \ a_{21} & a_{22} & a_{23} & a_{24} \ a_{31} & a_{32} & a_{33} & a_{34} \ a_{41} & a_{42} & a_{43} & a_{44} \end{array}
ight]$$

has reduced densities:

$$\rho_1 = \left[\begin{array}{ccc} a_{11} + a_{22} & a_{13} + a_{24} \\ a_{31} + a_{42} & a_{33} + a_{44} \end{array} \right], \qquad \rho_2 = \left[\begin{array}{ccc} a_{11} + a_{33} & a_{12} + a_{34} \\ a_{21} + a_{43} & a_{22} + a_{44} \end{array} \right].$$

The condition $\rho_1 = \rho_2$ implies

$$a_{22} = a_{33}$$
 and $a_{13} + a_{24} = a_{12} + a_{34}$.

Let

$$R_1 = \frac{1}{\sqrt{2}}(e_{22} - e_{33}), \quad R_2 = \frac{1}{2}(e_{12} - e_{13} - e_{24} + e_{34}), \quad R_3 = \frac{1}{2}(e_{21} - e_{31} - e_{42} + e_{43}),$$

and $B = \text{span}\{R_1, R_2, R_3\}$, then

$$ho = \left[egin{array}{ccccc} a_{11} & a_{12} & a_{13} & a_{14} \ a_{12}^* & b & a_{23} & c - a_{13} \ a_{13}^* & a_{23}^* & b & c - a_{12} \ a_{14}^* & c^* - a_{13}^* & c^* - a_{12}^* & a_{44} \end{array}
ight]$$

is orthogonal to B. But a conditional SIC-POVM for this ρ does not exist. Indeed, the equations

$$R_1^*R_1R_1 = \frac{1}{2}R_1, \quad R_2^*R_1R_2 = 0, \quad R_3^*R_1R_3 = 0$$

imply $\sum_{i=1}^{3} R_i^* R_1 R_i = \frac{1}{2} R_1$ and this is in contradict to the condition in Theorem 4.6.

References

- [1] I. D. Ivanovic, Geometrical description of quantum state determination, J. Phys. A, Math. Gen. 14, 3241 (1981).
- [2] H. Ohno, D. Petz, some problems from state estimations, preprint.
- [3] D. Petz, L. Ruppert and A. Szántó, Conditional SIC-POVMs, arXiv:1202.5741.
- [4] A. J. Scott, Tight informationally complete quantum measurements, J. Phys. A: Math. Gen. **39**, 13507 (2006).
- [5] A. J. Scott and M. Grassl, SIC-POVMs: A new computer study, J. Math. Phys. 51, 042203 (2010).
- [6] W. K. Wootters and B. D. Fields, Optimal state determination by mutually unbiased measurements, Ann. Phys., 191, 363-381 (1989).
- [7] G. Zauner, Quantendesigns Grundzüge einer nichtkommutativen Designtheorie, PhD thesis (University of Vienna, 1999).
- [8] H. Zhu, SIC POVMs and Clifford groups in prime dimensions, J. Phys. A: Math. Theor. 43, 305305 (2010).