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

$$\text{Tr}(\rho) = 1.$$  

For any density matrix $\rho$, 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:

\[
\begin{array}{c}
\rho \\
\rightarrow \\
\text{Measurement device by } \{P_i\}_{i=1}^{k} \\
\rightarrow \\
\{ \\
1 \text{ with probability } \text{Tr}(\rho P_1) \\
2 \text{ with probability } \text{Tr}(\rho P_2) \\
\vdots \\
k \text{ with probability } \text{Tr}(\rho P_k) \\
\end{array}
\]

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

\[ \text{Tr}(\rho P_i) \neq \text{Tr}(\sigma P_i). \]

If a POVM \( \{P_i\}_{i=1}^{k} \) is informationally complete, then we can determine the quantum state \( \rho \) by \( \text{Tr}(\rho P_i) \). If \( \rho \) 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

\[ \text{span}\{P_i\}_{i=1}^{k} = M_n(\mathbb{C}). \]

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

**Example 2.5** For small \( \epsilon > 0 \). Let

\[
P_1 = \frac{1}{2 + 2\epsilon^2} \begin{bmatrix} 1 & \epsilon \\ \epsilon & \epsilon^2 \end{bmatrix}, \quad P_2 = \frac{1}{2 + 2\epsilon^2} \begin{bmatrix} 1 & -\epsilon \\ -\epsilon & \epsilon^2 \end{bmatrix},
\]

\[
P_3 = \frac{1}{2 + 2\epsilon^2} \begin{bmatrix} \epsilon^2 & \epsilon i \\ -\epsilon i & 1 \end{bmatrix}, \quad P_4 = \frac{1}{2 + 2\epsilon^2} \begin{bmatrix} \epsilon^2 & -i\epsilon \\ i\epsilon & 1 \end{bmatrix}.
\]

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

\[
\begin{align*}
(2 + 2\epsilon^2)\text{Tr}(\rho P_1) &= \rho_{11} + \epsilon\rho_{12} + \epsilon\rho_{21} + \epsilon^2\rho_{22} \\
(2 + 2\epsilon^2)\text{Tr}(\rho P_2) &= \rho_{11} - \epsilon\rho_{12} - \epsilon\rho_{21} + \epsilon^2\rho_{22} \\
(2 + 2\epsilon^2)\text{Tr}(\rho P_3) &= \epsilon^2\rho_{11} - i\epsilon\rho_{12} + i\epsilon\rho_{21} + \rho_{22} \\
(2 + 2\epsilon^2)\text{Tr}(\rho P_4) &= \epsilon^2\rho_{11} + i\epsilon\rho_{12} - i\epsilon\rho_{21} + \rho_{22},
\end{align*}
\]
we have

\[
\rho = \text{Tr}(\rho P_1) + \text{Tr}(\rho P_2) + \text{Tr}(\rho P_3) + \text{Tr}(\rho P_4) \bigg[ \begin{array}{cc}
\frac{1}{1-\epsilon^2} & \frac{1}{4\epsilon(1+\epsilon^2)} \\
\frac{-\epsilon^2}{1-\epsilon^2} & \frac{i}{4\epsilon(1+\epsilon^2)} \\
\frac{1-\epsilon^2}{4\epsilon(1+\epsilon^2)} & \frac{1}{1-\epsilon^2}\end{array} \bigg] + \text{Tr}(\rho P_3) + \text{Tr}(\rho P_4) \bigg[ \begin{array}{cc}
\frac{1}{1-\epsilon^2} & \frac{-1}{4\epsilon(1+\epsilon^2)} \\
\frac{-\epsilon^2}{1-\epsilon^2} & \frac{-i}{4\epsilon(1+\epsilon^2)} \\
\frac{1-\epsilon^2}{4\epsilon(1+\epsilon^2)} & \frac{1}{1-\epsilon^2}\end{array} \bigg].
\]

Hence we can determine a state \( \rho \). But this is not a good POVM to detect \( \rho \). Since

\[
\rho_{12} = \frac{1}{4\epsilon(1+\epsilon^2)} \left( \text{Tr}(P_1 \rho) - \text{Tr}(P_2 \rho) - i \left( \text{Tr}(P_3 \rho) - \text{Tr}(P_4 \rho) \right) \right),
\]

a small error causes a big difference.

If a POVM is informationally complete, then we can determine a state \( \rho \) by \( \{\text{Tr}(\rho P_i)\}_{i=1}^{k} \). But by \( \ell \) experiments, we can only obtain approximate values of \( \{\text{Tr}(\rho P_i)\}_{i=1}^{k} \). 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 \( \ell \) 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 \( \{P_i\}_{i=1}^{k} \) are optimal POVM if and only if

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

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

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 \(|x\rangle \langle y|z = (y, z)x\) 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 \(1 \leq j \leq n^2\) we have
\[ 0 = \text{Tr} \left( \sum_{i=1}^{n^2} a_i |\xi_i\rangle \langle \xi_i| \cdot |\xi_j\rangle \langle \xi_j| \right) = a_j + \frac{1}{n+1} \sum_{i \neq j} a_i. \]
So it is easy to see that \(\left\{ |\xi_i\rangle \langle \xi_i| \right\}_{i=1}^{n^2}\) is linearly independent. Moreover, for all \(1 \leq j \leq n^2\),
\[ \text{Tr} \left( \sum_{i=1}^{n^2} \frac{1}{n} |\xi_i\rangle \langle \xi_i| \cdot |\xi_j\rangle \langle \xi_j| \right) = \frac{1}{n} + \sum_{i \neq j} \frac{1}{n(n+1)} = 1. \]
Hence \(\sum_{i=1}^{n^2} \frac{1}{n} |\xi_i\rangle \langle \xi_i| = I.\)

Example 3.2 In \(\mathbb{C}^2\),
\[ \xi_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \xi_2 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ \sqrt{2} \end{bmatrix}, \xi_3 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \lambda \sqrt{2} \\ 0 \end{bmatrix}, \xi_4 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \lambda \sqrt{2} \\ 0 \end{bmatrix} \]
is a SIC-POVM, where \(\lambda = e^{2\pi i/3} = \frac{-1 + \sqrt{3}i}{2}\).

In \(\mathbb{C}^3\),
\[ \xi_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \xi_2 = \frac{1}{2} \begin{bmatrix} 1 \\ \sqrt{3} \\ 0 \end{bmatrix}, \xi_3 = \frac{1}{2} \begin{bmatrix} 1 \\ -\sqrt{3} \\ 0 \end{bmatrix}, \xi_4 = \frac{1}{2} \begin{bmatrix} i \\ \sqrt{2} \\ 0 \end{bmatrix}, \xi_5 = \frac{1}{2} \begin{bmatrix} i \\ -\sqrt{2} \lambda \\ 0 \end{bmatrix}, \xi_6 = \frac{1}{2} \begin{bmatrix} 1 \\ \sqrt{2} \lambda \\ 0 \end{bmatrix}, \xi_7 = \frac{1}{2} \begin{bmatrix} 1 \\ -i \sqrt{2} \\ 0 \end{bmatrix}, \xi_8 = \frac{1}{2} \begin{bmatrix} 1 \\ -i \sqrt{2} \lambda \\ 0 \end{bmatrix}, \xi_9 = \frac{1}{2} \begin{bmatrix} 1 \\ -i \sqrt{2} \lambda \\ 0 \end{bmatrix} \]
is a SIC-POVM, where \(\lambda = e^{2\pi i/3}\).
It is known that a SIC-POVM exists if $n \leq 15$ or $n = 19, 24, 35, 48$. Numerical solutions have been found when $n \leq 67$. But for other cases, the existence is an open problem. The following is conjectured by G. Zauner in 1999 [7].

Let

\[ W = \begin{bmatrix}
1 & 0 & 0 & \ldots & 0 \\
0 & \lambda & 0 & \ldots & 0 \\
0 & 0 & \lambda^2 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \ldots & \lambda^{n-1}
\end{bmatrix}, \quad S = \begin{bmatrix}
0 & 0 & 0 & \ldots & 0 & 1 \\
1 & 0 & 0 & \ldots & 0 & 0 \\
0 & 1 & 0 & \ldots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & 1 & 0
\end{bmatrix}, \]

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

**Definition 3.3** A unit vector $\xi$ is called a fiducial vector if

\(\{W^kS^\ell\xi\}_{k,\ell=1}^{n}\) 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

\[ M_n(\mathbb{C}) = CI \oplus A \oplus B \]

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 $\rho$. Since we already know $P_A \rho$, SIC-POVM is not suitable.

Let $\dim A = m$ then $\dim B = n^2 - m - 1$ 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

\[ \mathcal{F} = |I \rangle \langle I| + \frac{n-1}{N-1} P_B. \]

In this case,

\[ \sum_{i=1}^{k} P_i = \frac{N}{n} I, \quad \text{Tr}(P_i P_j) = \frac{N-n}{n(N-1)}. \]
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

\[
\text{Tr}P_iP_j = \frac{1}{n+1} \quad (i \neq j)
\]

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

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

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

\[
\text{Tr}P_iP_j = \frac{n-1}{n^2} \quad (i \neq j), \quad \sum_{i=1}^{n} P_i = \frac{n^2-n+1}{n} I
\]

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

\[
Q_i = \sqrt{\frac{n(N-1)}{N(n-1)}} \left( P_i - \frac{1}{n} \left( 1 + \sqrt{\frac{n-1}{N-1}} \right) I \right)
\]  

Then \(\{Q_i\}_{i=1}^{N}\) is an orthonormal basis of \(A \oplus C\).
Proof. For any $1 \leq i \leq N$, we have
\[
\text{Tr} \left( \left( P_i - \frac{1}{n} \left( 1 + \sqrt{\frac{n-1}{N-1}} \right) I \right)^2 \right) = \text{Tr} \left( P_i - \frac{2}{n} \left( 1 + \sqrt{\frac{n-1}{N-1}} \right) P_i + \frac{1}{n^2} \left( 1 + \sqrt{\frac{n-1}{N-1}} \right)^2 I \right) = 1 - \frac{2}{n} \left( 1 + \sqrt{\frac{n-1}{N-1}} \right) + \frac{1}{n} \left( 1 + 2 \sqrt{\frac{n-1}{N-1}} + \frac{n-1}{N-1} \right) = 1 - \frac{1}{n} + \frac{n-1}{n(N-1)} = \frac{N(n-1)}{n(N-1)}.
\]
Moreover, for any $1 \leq i < j \leq N,$
\[
\text{Tr} \left( \left( P_i - \frac{1}{n} \left( 1 + \sqrt{\frac{n-1}{N-1}} \right) I \right) \left( P_j - \frac{1}{n} \left( 1 + \sqrt{\frac{n-1}{N-1}} \right) I \right) \right) = \frac{N-n}{n(N-1)} - \frac{2}{n} \left( 1 + \sqrt{\frac{n-1}{N-1}} \right) + \frac{1}{n} \left( 1 + 2 \sqrt{\frac{n-1}{N-1}} + \frac{n-1}{N-1} \right) = \frac{N-n}{n(N-1)} - \frac{1}{n} + \frac{n-1}{n(N-1)} = 0.
\]
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 $\text{Tr}(X) = 0$. 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 $\text{Tr}(P_i X P_i) = \text{Tr}(t P_i) = \text{Tr}(P_i) = \frac{1}{n}$. Therefore,
\[
\sum_{i=1}^N Q_i^* X Q_i = \text{Tr}(X) = 0.
\]
\(\langle P_i, X \rangle = 0\) implies \(t = 0\). Therefore \(P_iXP_i = 0\). From the equation

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

we have

\[
\begin{align*}
\frac{N(n-1)}{n(N-1)} \sum_{i=1}^{N} Q_i^{*} X Q_i &= \sum_{i=1}^{N} \left( P_i - \frac{1}{n} \left( 1 + \sqrt{\frac{n-1}{N-1}} \right) \right) X \left( P_i - \frac{1}{n} \left( 1 + \sqrt{\frac{n-1}{N-1}} \right) \right) \\
&= \left( -\frac{1}{n} \left( 1 + \sqrt{\frac{n-1}{N-1}} \right) \right) \left( \sum_{i=1}^{N} P_i + \sum_{i=1}^{N} P_i X \right) + \frac{N}{n^2} \left( 1 + \sqrt{\frac{n-1}{N-1}} \right)^2 X \\
&= \frac{N}{n^2} \left( -1 + \frac{n-1}{N-1} \right) X = \frac{N(n-N)}{n^2(N-1)} X.
\end{align*}
\]

This implies the assertion. \(\square\)

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

\[
\rho = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\
 a_{21} & a_{22} & a_{23} & a_{24} \\
 a_{31} & a_{32} & a_{33} & a_{34} \\
 a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}
\]

has reduced densities:

\[
\rho_1 = \begin{bmatrix} a_{11} + a_{22} & a_{13} + a_{24} \\
 a_{31} + a_{42} & a_{33} + a_{44} \end{bmatrix}, \quad \rho_2 = \begin{bmatrix} a_{11} + a_{33} & a_{12} + a_{34} \\
 a_{21} + a_{43} & a_{22} + a_{44} \end{bmatrix}.
\]

The condition \(\rho_1 = \rho_2\) implies

\[a_{22} = a_{33} \quad \text{and} \quad a_{13} + a_{24} = a_{12} + a_{34}.\]

Let

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

where \(e_{ij}\) denotes the elementary matrix.
and $B = \text{span}\{R_1, R_2, R_3\}$, then
\[
\rho = \begin{bmatrix}
a_{11} & a_{12} & a_{13} & a_{14} \\
a_{12}^* & b & a_{23} & c - a_{13} \\
a_{13}^* & a_{23}^* & b & c - a_{12} \\
a_{14}^* & c^* - a_{13}^* & c^* - a_{12}^* & a_{44}
\end{bmatrix}
\]
is orthogonal to $B$. But a conditional SIC-POVM for this $\rho$ does not exist. Indeed, the equations
\[
R_1^* R_1 R_1 = \frac{1}{2} R_1, \quad R_2^* R_1 R_2 = 0, \quad R_3^* R_1 R_3 = 0
\]
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