Thus,

$$\langle e_j \star e^i, M_{b,k} \rangle = \langle e_j \star e^i, M_k \rangle. \tag{113}$$

If $\|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})} > 1$, then

$$\begin{aligned}
\langle g \star \rho, M_{b,k} \rangle &= \langle g \star \rho, M_{k,1} \rangle \\
&= \int_{T_\rho P} g(x) \operatorname{tr}_{\mathcal{H}}(M_{b,k}(\, dx)\rho) \\
&= \int_{T_\rho P} g(\|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})} \cdot x) \operatorname{tr}_{\mathcal{H}}(\frac{1}{\|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})}} \cdot M_k(\, dx)\rho) \\
&= \int_{T_\rho P} \|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})} \cdot g(x) \operatorname{tr}_{\mathcal{H}}(M_k(\, dx)\rho) \\
&= \|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})} \langle g \star \rho, M_k \rangle.
\end{aligned}$$

Thus,

$$\langle g \star \rho, M_{b,k} \rangle = \|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})} \langle g \star \rho, M_k \rangle.$$

If $\|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})} \leq 1$, then

$$\langle g \star \rho, M_{b,k} \rangle = \langle g \star \rho, M_{k,1} \rangle = \langle g \star \rho, M_k \rangle.$$

Because $\|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})} \to 1$ and $\{\langle g \star \rho, M_k \rangle\}$ is a Cauchy sequence ,

$$\lim_{k\to\infty} \langle g \star \rho, M_{b,k} \rangle = \lim_{k\to\infty} \langle g \star \rho, M_k \rangle.$$

Let $b_k := (\mathcal{C} \times \mathcal{A})(M_{b,k})$, then $\lim_{k\to\infty} a_k = \lim_{k\to\infty} b_k$. The proof is complete. □
From the preceding lemmas, we obtain the following theorem.

Theorem 11 *$(\mathcal{A}, \mathcal{B}, \mathcal{C})$ is normal.*

We obtain Theorem 6 from this theorem, Theorem 10, the equation (94) and the equation (99).

References

[1] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North_Holland, Amsterdam, 1982).

[2] H. P. Yuen and M. Lax, IEEE trans. **IT-19**, 740 (1973).

[3] H. Nagaoka, Trans. Jap. Soci. Ind. App. Math., **1**, 305 (1991)(in Japanese).

[4] K. Matsumoto, to be published.

[5] R. M. Van Style and R. J. B. Wets, J. Math. Anal. Appl., **22**, 679 (1968).

[6] A. S. Holevo, Rep. Math. Phys., **12**, 251 (1977).

[7] M. Hayashi, Masters Thesis, Dep. Math., Kyoto University, (1996)(in Japanese).

[8] H. P. Yuen, M. Lax and R. S. Kennedy, IEEE, **IT-21**, 125 (1975).

[9] R. Hartley Siam J. Appl. Math. **34**, 211 (1978).

[10] A. Fujiwara and H. Nagaoka, in *Quantum coherence and decoherence*, edited by K. Fujikawa and Y. A. Ono, (Elsevier, Amsterdam, 1996), pp. 303.

[11] A. Fujiwara and H. Nagaoka, Phys. Lett. A 201 (1995) 119-124.

And

$$\begin{aligned} & \int_{T_\rho P} \frac{m-1}{m} g(\frac{m}{m-1} \cdot x) \, \mathrm{tr}_{\mathcal{H}}(M_{k(m)}(\, dx)\rho) \\ = & \int_{T_\rho P} \frac{m}{m-1} g(x) \, \mathrm{tr}_{\mathcal{H}}(M_{k(m)}(\, dx)\rho) \\ = & \frac{m}{m-1} \cdot \langle g \star \rho, M_{k(m)} \rangle. \end{aligned}$$

Thus,

$$\langle g \star \rho, M_{m,1} \rangle = \frac{m}{m-1} \cdot \langle g \star \rho, M_{k(m)} \rangle$$

As $\{\langle g \star \rho, M_{k(m)} \rangle\}$ is a Cauchy sequence,

$$\langle g \star \rho, M_{m,1} \rangle - \langle g \star \rho, M_{k(m)} \rangle \to 0 \ (\text{ as } m \to \infty).$$

We obtain that $\lim_{m\to\infty} b_m = \lim_{m\to\infty} a_{k(m)}$. The proof is complete. □

Lemma 23 *We obtain*

$$\overline{\mathcal{F} \cap \mathcal{G}} = \overline{\mathcal{F}} \cap \mathcal{G}.$$

Proof It suffices to prove that for a Cauchy sequence $\{a_k\} \subset \mathcal{F}$ such that $\lim_{k\to\infty} a_k \in \mathcal{G}$ there exists a Cauchy sequence $\{b_k\} \subset \mathcal{F} \cap \mathcal{G}$ such that $\lim_{k\to\infty} a_k = \lim_{k\to\infty} b_k \in \mathcal{G}$. The component of a_k is denoted by $a_k = d_k \times a_{k,j}^i \times X_k \in \mathbf{R} \times \mathrm{End}(T_\rho P) \times \mathcal{B}_{sa}(\mathcal{H})$. For $M_k \in (\mathcal{C} \times \mathcal{A})^{-1}(a_k) \subset \mathcal{M}(T_\rho P, \mathcal{H}, g)$, $M_{k,1}(B)$ is defined in the following:

$$M_{k,1}(B) := \begin{cases} M_k(B) & (\|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})} \leq 1) \\ \frac{1}{\|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})}} \cdot M_k(\frac{1}{\|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})}} \cdot B) & (\|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})} > 1) \end{cases} \quad \text{for } B \in \mathcal{B}(T_\rho P).$$

Notice that $M_k(T_\rho P) = X_k$. $M_{b,k}$ is defined in the following way:

$$M_{b,k} := M_{k,1} + \delta_0(\mathrm{Id}_{\mathcal{H}} - M_{k,1}(T_\rho P)).$$

If $\|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})} > 1$, then

$$\begin{aligned} \langle e_j \star e^i, M_{b,k} \rangle &= \langle e_j \star e^i, M_{k,1} \rangle \\ &= \int_{T_\rho P} x_j \, \mathrm{tr}_{\mathcal{H}}(M_{b,k}(\, dx) e^i) \\ &= \int_{T_\rho P} \|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})} \cdot x_j \, \mathrm{tr}_{\mathcal{H}}(\frac{1}{\|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})}} \cdot M_k(\, dx) e^i) \\ &= \int_{T_\rho P} x_j \, \mathrm{tr}_{\mathcal{H}}(M_k(\, dx) e^i) \\ &= \langle e_j \star e^i, M_k \rangle. \end{aligned}$$

If $\|X_k\|_{\mathcal{B}_{sa}(\mathcal{H})} \leq 1$, then

$$\langle e_j \star e^i, M_{b,k} \rangle = \langle e_j \star e^i, M_{k,1} \rangle = \langle e_j \star e^i, M_k \rangle.$$

Therefore,

$$\begin{aligned}
& \int_{T_\rho P} e_j(x) M_{m,2}(\,dx) \\
= & \int_{T_\rho P} x_j M_{m,2}(\,dx) \\
= & \sum_{i=1}^{n} (m \cdot d \cdot (\delta_j^i - a^i_{k(m),j}) \cdot \frac{1}{m \cdot d} \cdot D_i^+ + m \cdot d \cdot (-\delta_j^i + a^i_{k(m),j}) \cdot \frac{1}{m \cdot d} \cdot D_i^-) \\
= & \sum_{i=1}^{n} ((\delta_j^i - a^i_{k(m),j}) \cdot D_i^+ + (-\delta_j^i + a^i_{k(m),j}) \cdot D_i^-) \\
= & \sum_{i=1}^{n} (\delta_j^i - a^i_{k(m),j}) \cdot (D_i^+ - D_i^-).
\end{aligned}$$

Thus,

$$\begin{aligned}
\langle e_j \star e^i, M_{m,2} \rangle &= \mathrm{tr}_{\mathcal{H}}(\sum_{l=1}^{n} (\delta_j^l - a^l_{k(m),j}) \cdot (D_i^+ - D_i^-) e^i) \\
&= \delta_j^i - a^i_{k(m),j}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
\langle e_j \star e^i, M_{b,m} \rangle &= \langle e_j \star e^i, M_{m,1} + M_{m,2} \rangle \\
&= a^i_{k(m),j} + \delta_j^i - a^i_{k(m),j} \\
&= \delta_j^i.
\end{aligned}$$

b_m denotes $\mathcal{C} \times \mathcal{A}(M_{b,m}) \in \mathcal{E}$. Then it suffices to prove that $\lim_{m\to\infty} b_m = \lim_{m\to\infty} a_{k(m)}$.

$$\begin{aligned}
& \langle g \star \rho, M_{m,2} \rangle \\
= & \sum_{i=1}^{n} g(m \cdot d \cdot \sum_{j=1}^{n} (\delta_j^i - a^i_{k(m),j}) e^j) \cdot \mathrm{tr}_{\mathcal{H}}(\frac{1}{m \cdot d} \cdot D_i^+ \rho) \\
& + \sum_{i=1}^{n} g(m \cdot d \cdot \sum_{j=1}^{n} (-\delta_j^i + a^i_{k(m),j}) e^j) \cdot \mathrm{tr}_{\mathcal{H}}(\frac{1}{m \cdot d} \cdot D_i^- \rho) \\
= & (\max_{|x|=1} g(x)) \cdot \frac{1}{m \cdot d} \cdot \mathrm{tr}_{\mathcal{H}}((\sum_{i=1}^{n} D_i^+ + D_i^-) \rho) \\
\to & \ 0 \ (as \ m \to \infty).
\end{aligned}$$

And

$$\begin{aligned}
& \langle g \star \rho, M_{m,1} \rangle \\
= & \int_{T_\rho P} g(x) \, \mathrm{tr}_{\mathcal{H}}(M_{m,1}(\,dx) \rho) \\
= & \int_{T_\rho P} \frac{m-1}{m} g(\frac{m}{m-1} \cdot x) \, \mathrm{tr}_{\mathcal{H}}(M_{k(m)}(\,dx) \rho).
\end{aligned}$$

Proof Let $e^1, \ldots, e^n$ be bases of $T_\rho P$, and let $e_1, \ldots, e_n$ the dual bases of $e^1, \ldots, e^n$. Linear functionals $e_i \star e^j$, $g \star \rho$ on $\mathcal{X}(T_\rho P, \mathcal{H}, g)$ are defined in the following way:

$$\begin{array}{rccc} e_i \star e^j : & \mathcal{X}(T_\rho P, \mathcal{H}, g) & \to & \mathbf{R} \\ & \bigcup & & \bigcup \\ & M & \mapsto & \int_{T_\rho P} \langle e_i, x \rangle \, \mathrm{tr}_{\mathcal{H}} \, M(\, dx) e^j \\ g \star \rho : & \mathcal{X}(T_\rho P, \mathcal{H}, g) & \to & \mathbf{R} \\ & \bigcup & & \bigcup \\ & M & \mapsto & \int_{T_\rho P} g(x) \, \mathrm{tr}_{\mathcal{H}} \, M(\, dx) \rho. \end{array}$$

As $e^1, \ldots, e^n$ are linearly dependent, let D_i^+, D_i^- be nonnegative bounded selfadjoint operators such that $\langle e_i, e^j \rangle = \mathrm{tr}_{\mathcal{H}}(D_i^+ - D_i^-) e^j$ for $(1 \leq j \leq n)$. Therefore, we define that $D := \sum_{i=1}^n (D_i^+ + D_i^-) \in \mathcal{B}_{sa}^+(\mathcal{H}), d := \|D\|_{\mathcal{B}_{sa}(\mathcal{H})} = \sup_{\{\phi \in \mathcal{H} | \|\phi\| = 1\}} \|D\phi\|$.

It suffices to prove that for any Cauchy sequence $\{a_k\} \subset \mathcal{F} \cap \mathcal{G}$ such that $\lim_{k \to \infty} a_k \in \mathcal{E}$, there exists a Cauchy sequence $\{b_k\} \subset \mathcal{F} \cap \mathcal{E}$ such that $\lim_{k \to \infty} a_k = \lim_{k \to \infty} b_k \in \mathcal{E}$. The components of a_k are denoted by $a_k = d_k \times a_{k,j}^i \times \mathrm{Id}_{\mathcal{H}} \in \mathbf{R} \times \mathrm{End}(T_\rho P) \times \mathcal{B}_{sa}(\mathcal{H})$. Notice that $E(M)_j^i = \langle e_j \star e^i, M \rangle$ for $M \in \mathcal{M}(T_\rho P, \mathcal{H}, g)$. c_k denotes the maximum $\max_{0 \leq i \leq n} \sum_{j=1}^n |a_{k,j}^i - \delta_j^i|^2$. Since there exists the limit of a sequence a_k, then we have $\lim_{k \to \infty} c_k = 0$ i.e.

$$\forall m \in \mathbf{N} \ , \ \exists k(m) \in \mathbf{N} \ s.t. \ c_{k(m)} < (md)^{-1}.$$

For $M_k \in (\mathcal{C} \times \mathcal{A})^{-1}(a_k) \subset \mathcal{M}(T_\rho P, \mathcal{H}, g)$ elements $\{M_{m,1} \ , \ M_{m,2}\}_{m=1}^\infty \in \mathcal{L}(T_\rho P, \mathcal{H}, g)$ are defined in the following:

$$\begin{aligned} M_{m,1}(B) &:= \frac{m-1}{m} \cdot M_{k(m)}(\frac{m-1}{m} \cdot B) \ , \quad \text{for } \forall B \in \mathcal{B}(\mathbf{R}^{n \times n}) \\ M_{m,2} &:= \sum_{i=1}^n (\delta_{m \cdot d \cdot \sum_{j=1}^n (\delta_j^i - a_{k(m),j}^i) e^j} \cdot \frac{1}{m \cdot d} \cdot D_i^+ + \delta_{m \cdot d \cdot \sum_{j=1}^n (-\delta_j^i + a_{k(m),j}^i) e^j} \cdot \frac{1}{m \cdot d} \cdot D_i^-), \end{aligned}$$

where $\delta_{\sum_{j=1}^n a_j e^j}$ is the delta measure which takes value only $e_j(x) = a_j$ and for $c \in \mathbf{R}^+$, $B \in \mathcal{B}(T_\rho P)$ the set $c \cdot B \in \mathcal{B}(T_\rho P)$ is defined as follows:

$$c \cdot B := \{x \in T_\rho P | c \cdot x \in B\}.$$

Thus,

$$M_{m,1}(T_\rho P) = \frac{m-1}{m} \mathrm{Id}_{\mathcal{H}} \ , \ M_{m,2}(T_\rho P) \leq \frac{1}{m \cdot d} D \leq \frac{1}{m} \mathrm{Id}_{\mathcal{H}} .$$

A measurement $M_{b,m}$ is defined in the following way:

$$M_{b,m} := M_{m,1} + M_{m,2} + \delta_0(\frac{1}{m} \mathrm{Id}_{\mathcal{H}} - M_{m,2}(T_\rho P)) \in \mathcal{M}(T_\rho P, \mathcal{H}, g).$$

Thus,

$$E(M_{m,1})_j^i = \langle e_j \star e^i, M_{m,1} \rangle = \langle e_j \star e^i, M_{k(m)} \rangle = a_{k(m),j}^i.$$

Therefore, we obtain

$$\langle \mathcal{C} - E^*(a) - \mathrm{Int}^*(S), M_{P,x} \rangle = \langle g(x,x)\rho - a(x) - S, P \rangle. \tag{106}$$

Thus, the following are equivalent.

$$\circ \quad \forall P \in \mathcal{B}^+_{sa}(\mathcal{H}) \ , \ \langle \mathcal{C} - E^*(a) - \mathrm{Int}^*(S), M_{P,x} \rangle \geq 0 \tag{107}$$
$$\circ \quad \forall x \in T_\rho P \ , \ g(x,x)\rho - a(x) - S \in \mathcal{B}^{*,+}_{sa}(\mathcal{H}). \tag{108}$$

Therefore, the following are equivalent.

$$\circ \quad \mathcal{C} - E^*(a) - \mathrm{Int}^*(S) \in \mathcal{L}^* \tag{109}$$
$$\circ \quad \forall x \in T_\rho P \ , \ g(x,x)\rho - a(x) - S \in \mathcal{B}^{*,+}_{sa}(\mathcal{H}). \tag{110}$$

Thus, the proof is complete. □

B.4 Normality

In this section, we prove that $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ is normal.

Definition 19 The subsets $\mathcal{F}$, $\mathcal{G}$, $\mathcal{E}$ of $\mathcal{Y}$ are defined in the following:

$$\begin{aligned} \mathcal{F} &:= \mathcal{F}_{\mathcal{A},\mathcal{C}} = \{\mathcal{C}(M) \times \mathcal{A}(M) | M \in \mathcal{L}(T_\rho P, \mathcal{H}, W)\} \\ \mathcal{G} &:= \mathbf{R} \times \mathrm{End}(T_\rho P) \times \{\mathrm{Id}_{\mathcal{H}}\} \\ \mathcal{E} &:= \mathcal{E}_{\mathcal{B}} = \mathbf{R} \times \{(\mathrm{Id}_{T_\rho P}, \mathrm{Id}_{\mathcal{H}})\}. \end{aligned}$$

Notice that $\mathcal{G}$ and $\mathcal{E}$ are closed sets.

Lemma 21 *If*

$$\overline{\mathcal{F} \cap \mathcal{G}} = \overline{\mathcal{F} \cap \mathcal{G}} \ , \ \overline{\mathcal{F} \cap \mathcal{G}} \cap \mathcal{E} = \overline{\mathcal{F} \cap \mathcal{E}}, \tag{111}$$

then

$$\overline{\mathcal{F} \cap \mathcal{E}} = \overline{\mathcal{F} \cap \mathcal{E}}. \tag{112}$$

Proof

$$\text{The left-hand in (112)} = \overline{\mathcal{F}} \cap \mathcal{G} \cap \mathcal{E} = \overline{\mathcal{F} \cap \mathcal{G}} \cap \mathcal{E} = \overline{\mathcal{F} \cap \mathcal{E}}.$$

□

Lemma 22 *We obtain*

$$\overline{\mathcal{F} \cap \mathcal{G}} \cap \mathcal{E} = \overline{\mathcal{F} \cap \mathcal{E}}.$$

Therefore, to prove Theorem 6, we have to prove the following equation:

$$\sup_{(a,S)\in\mathcal{U}^*(g)} \mathrm{Spur}(a,S) = \sup_{\{f\in\mathcal{Y}^*|\mathcal{C}-\mathcal{A}^*f\in\mathcal{L}^*\}} \langle f,\mathcal{B}\rangle. \tag{95}$$

Notice that $\mathcal{Y}^* = \mathrm{End}(T_\rho P)\times\mathcal{B}^*_{sa}(\mathcal{H})$. $\mathrm{End}(T_\rho P)$ is regarded as the dual space of itself by

$$\begin{array}{rccc} \langle\ ,\ \rangle: & \mathrm{End}(T_\rho P)\times\mathrm{End}(T_\rho P) & \to & \mathbf{R} \\ & \Downarrow & & \Downarrow \\ & (A,B) & \mapsto & \langle A,B\rangle = \mathrm{tr}_{T_\rho P}\, AB. \end{array} \tag{96}$$

Lemma 20 *For $(a,S)\in\mathrm{End}(T_\rho P)\times\mathcal{B}^*_{sa}(\mathcal{H})$, the following are equivalent.*

$$\circ \quad (a,S)\in\mathcal{U}(g) \tag{97}$$

$$\circ \quad \mathcal{C}-\mathcal{A}^*(a,S)\in\mathcal{L}^*. \tag{98}$$

From this Lemma, we obtain

$$\sup_{(a,S)\in\mathcal{U}^*(g)} \mathrm{Spur}(a,S) = \sup_{\{f\in\mathcal{Y}^*|\mathcal{C}-\mathcal{A}^*f\in\mathcal{L}^*\}} \langle f,\mathcal{B}\rangle. \tag{99}$$

Thus, if it is proved that $(\mathcal{A},\mathcal{B},\mathcal{C})$ is normal, the proof of Theorem 6 is complete.

Proof

$$\mathcal{C}-\mathcal{A}^*(a,S) = \mathcal{C}-E^*(a)-\mathrm{Int}^*(S). \tag{100}$$

For $x\in T_\rho P$, $P\in\mathcal{B}^+_{sa}(\mathcal{H})$ $M_{P,x}\in\mathcal{L}(T_\rho P,\mathcal{H},g)$ is defined in the following:

$$M_{P,x}(B) := \begin{cases} 0 & (x\notin B) \\ P & (x\in B) \end{cases}.$$

Thus, the following are equivalent.

$$\circ \quad \mathcal{C}-E^*(a)-\mathrm{Int}^*(S)\in\mathcal{L}^* \tag{101}$$

$$\circ \quad \forall x\in T_\rho P\ ,\ \forall P\in\mathcal{B}_{sa}(\mathcal{H})\ ,\ \langle\mathcal{C}-E^*(A)-\mathrm{Int}^*(S),M_{P,x}\rangle\geq 0. \tag{102}$$

Therefore,

$$\begin{aligned} \langle\mathcal{C},M_{P,x}\rangle &= \int_{T_\rho P} g(y,y)\,\mathrm{tr}_{\mathcal{H}}\, M_{P,x}(\,dy)\rho \\ &= g(x,x)\langle\rho,P\rangle. \end{aligned} \tag{103}$$

Let the map $U: T_\rho P\to\mathcal{T}_{sa}(\mathcal{H})$ be a trivial embedding. As $\mathcal{T}^*_{sa}(\mathcal{H})=\mathcal{B}_{sa}(\mathcal{H})$ with respect to the norm topology, we define $U^*:\mathcal{B}_{sa}(\mathcal{H})\to T^*_\rho P$ in the natural sense.

$$\begin{aligned} \langle E^*(a),M_{P,x}\rangle &= \langle a,E(M_{P,x})\rangle \\ &= \langle a,x\otimes U^*(P)\rangle \quad (\text{From } \mathrm{End}(T_\rho P)\cong T_\rho P\otimes T^*_\rho P) \\ &= \mathrm{tr}_{T_\rho P}\, a(x\otimes U^*(P)) \\ &= \mathrm{tr}_{T_\rho P}\, a(x)\otimes U^*(P) \\ &= \langle U^*P,a(x)\rangle \\ &= \langle P,a(x)\rangle \end{aligned} \tag{104}$$

$$\begin{aligned} \langle\mathrm{Int}^*(S),M_{P,x}\rangle &= \langle S,\mathrm{Int}(M_{P,x})\rangle \\ &= \langle S,P\rangle. \end{aligned} \tag{105}$$

Definition 17 The map Int from $\mathcal{X}(T_\rho P, \mathcal{H}, g)$ to $\mathcal{B}_{sa}(\mathcal{H})$ is defined in the following:

$$\mathrm{Int}(M) := M(T_\rho P),\ \forall M \in \mathcal{X}(T_\rho P, \mathcal{H}, g). \tag{90}$$

Lemma 18 *The map* Int *is a continuous linear map.*

Proof The linearity is trivial. We prove that the map is bounded.

$$\|\mathrm{Int}(M)\| = \|M(T_\rho P)\| \leq \|M\|_1 \leq \|M\|.$$

Thus, it is bounded. □

Definition 18 The map $C : \mathcal{X}(T_\rho P, \mathcal{H}, g) \to \mathbf{R}$ is defined as follows:

$$C(M) := \int_{T_\rho P} g(x,x)\,\mathrm{tr}_{\mathcal{H}}\, M(\,dx)\rho,\ \forall M \in \mathcal{X}(T_\rho P, \mathcal{H}, g). \tag{91}$$

Lemma 19 *C is a bounded linear functional.*

Proof The linearity is trivial.

$$\|C(M)\| = \|M\|_3 \leq \|M\|.$$

Thus, it is bounded. □
An element M of $\mathcal{L}(T_\rho P, \mathcal{H}, g)$ is an element of $\mathcal{U}(T_\rho P)$, iff

$$E(M) = \mathrm{Id}_{T_\rho P}\ ,\ \ \mathrm{Int}(M) = \mathrm{Id}_{\mathcal{H}}\,. \tag{92}$$

For $M \in \mathcal{U}(T_\rho P)$,

$$\mathcal{D}_g^\rho(M) = C(M). \tag{93}$$

B.3 Applying the infinite linear programming duality theorem

We put in the following:

$$\begin{aligned}
\mathcal{X} &:= \mathcal{X}(T_\rho P, \mathcal{H}, g)\\
\mathcal{Y} &:= \mathrm{End}(T_\rho P) \times \mathcal{B}_h(\mathcal{H})\\
\mathcal{L} &:= \mathcal{L}(T_\rho P, \mathcal{H}, g)\\
\mathcal{A} &:= E \times \mathrm{Int}\\
\mathcal{B} &:= (\mathrm{Id}_{T_\rho P}, \mathrm{Id}_{\mathcal{H}})\\
\mathcal{C} &:= C.
\end{aligned}$$

From the preceding discussion $\mathcal{X}, \mathcal{Y}, \mathcal{L}, \mathcal{A}, \mathcal{B}, \mathcal{C}$ satisfy the condition of Theorem 10. Thus,

$$\inf_{M \in \mathcal{U}(T_\rho P)} \mathcal{D}_g^\rho(M) = \inf_{\{x \in \mathcal{L} \mid \mathcal{A}x = \mathcal{B}\}} \langle \mathcal{C}, x \rangle. \tag{94}$$

As $\mathcal{B}_{sa}(\mathcal{H})$ is a vector space, $\mathcal{X}(T_\rho P, \mathcal{H}, g)$ is a vector space, too.

The norm $\|\cdot\|$ of $\mathrm{End}(T_\rho P)$ is defined in the following:

$$\|A\| := \sqrt{\mathrm{tr}_{T_\rho P} AA^*}, \ \forall A \in \mathrm{End}(T_\rho P). \tag{86}$$

The topology of $\mathrm{End}(T_\rho P)$ is defined by this norm. The map $E : \mathcal{X}(T_\rho P, \mathcal{H}, g) \to \mathrm{End}(T_\rho P)$ is defined in the following:

$$\begin{array}{rccc} E(M): & T_\rho P & \to & T_\rho P \\ & \Downarrow & & \Downarrow \\ & y & \mapsto & \int_{T_\rho P} x \, \mathrm{tr}_{\mathcal{H}} M(\,dx) y \end{array}, \ \forall M \in \mathcal{X}(T_\rho P, \mathcal{H}, g). \tag{87}$$

This definition of E is well defined by condition (84).

We will define the topology of $\mathcal{X}(T_\rho P, \mathcal{H}, g)$. For this definition, a norm $\|\cdot\|_1$ and two semi-norms $\|\cdot\|_2, \|\cdot\|_3$ in $\mathcal{X}(T_\rho P, \mathcal{H}, g)$ are defined as follows: for $M \in \mathcal{X}(T_\rho P, \mathcal{H}, W)$,

$$\begin{aligned} \|M\|_1 &:= \sup_{B \in \mathcal{B}(T_\rho P)} \|M(B)\| && \textit{by} \ (83) \\ \|M\|_2 &:= \|E(M)\| && \textit{by} \ (84) \\ \|M\|_3 &:= \left| \int_{T_\rho P} g(x,x) \, \mathrm{tr}_{\mathcal{H}} M(\,dx) \rho \right| && \textit{by} \ (85) \ . \end{aligned}$$

A norm $\|\cdot\|$ in $\mathcal{X}(T_\rho P, \mathcal{H}, g)$ is defined in the following:

$$\|M\| := \|M\|_1 + \|M\|_2 + \|M\|_3, \ \forall M \in \mathcal{X}(T_\rho P, \mathcal{H}, W). \tag{88}$$

We define the topology of $\mathcal{X}(T_\rho P, \mathcal{H}, g)$ by this norm. A closed convex cone $\mathcal{L}(T_\rho P, \mathcal{H}, g)$ in $\mathcal{X}(T_\rho P, \mathcal{H}, g)$ is defined as follows:

$$\mathcal{L}(T_\rho P, \mathcal{H}, g) := \{M \in \mathcal{X}(T_\rho P, \mathcal{H}, g) | \forall B \in \mathcal{B}(T_\rho P) \ , \ M(B) \in \mathcal{B}^+_{sa}(\mathcal{H})\}. \tag{89}$$

Lemma 16 *$\mathcal{L}(T_\rho P, \mathcal{H}, g)$ is a closed convex cone.*

Proof It is trivial that it is a convex cone. We have to prove that it is a closed set. Let $\{M_k\}$ be a converging sequence of $\mathcal{L}(T_\rho P, \mathcal{H}, g)$. Its convergence point is denoted by $M \in \mathcal{X}(T_\rho P, \mathcal{H}, g)$. It suffices to prove that M is included in $\mathcal{L}(T_\rho P, \mathcal{H}, W)$. Since $\|M_k - M\| \to 0$, then $\|M_k - M\|_1 \to 0$. Because $\|M_k(B) - M(B)\| \to 0$, $M_K(B) \in \mathcal{B}^+_{sa}(\mathcal{H})$, and $\mathcal{B}^+_{sa}(\mathcal{H})$ is a closed convex cone, we obtain $M(B) \in \mathcal{B}^+_{sa}(\mathcal{H})$. Therefore, $M \in \mathcal{L}(T_\rho P, \mathcal{H}, g)$. □

Lemma 17 *The map $E : \mathcal{X}(T_\rho P, \mathcal{H}, g) \to \mathrm{End}(T_\rho P)$ is a continuous linear map.*

Proof The linearity is trivial. We will prove the map is bounded.

$$\|E(M)\| = \|M\|_2 \leq \|M\|.$$

□

where

$$\begin{aligned}
\tilde{\mathcal{U}}^*(g) &:= \{(a,S) \subset \mathrm{End}(T_\rho P) \times \mathcal{B}^*_{sa}(\mathcal{H}) | \forall x \in T_\rho P \ , \ R^\rho_g(a,S;x) \in \mathcal{B}^{*,+}_{sa}(\mathcal{H})\} \\
\mathrm{Spur}(a,S) &:= \mathrm{tr}_{T_\rho P}\, a + \langle S, \mathrm{Id}_{\mathcal{H}} \rangle \\
R^\rho_g(a,S;x) &:= g(x,x) \cdot \rho - S - a(x).
\end{aligned}$$

The purpose of this section is to prove the preceding theorem by applying the following duality theorem.

B.1 Infinite dimensional duality theorem (linear programming)

Let $\mathcal{X}, \mathcal{Y}$ be a locally convex Hausdorff real topological linear space, $\mathcal{A}$ a continuous linear operator form $\mathcal{X}$ to $\mathcal{Y}$ and $\mathcal{L}$ a closed convex cone in $\mathcal{X}$. Let $\mathcal{X}^*, \mathcal{Y}^*$ be the topological dual space of $\mathcal{X}, \mathcal{Y}$ and $\mathcal{A}^*$ the continuous adjoint map of $\mathcal{A}$. Let $\mathcal{L}^*$ be the conjugate cone of $\mathcal{L}$ in $\mathcal{X}^*$ i.e. $\mathcal{L}^* := \{f \in \mathcal{X}^* | \forall x \in \mathcal{L} \ , \ f(x) \geq 0\}$.

Definition 14 Let $\mathcal{C}$ be an element of $\mathcal{X}^*, \mathcal{B}$ an element of $\mathcal{Y}$. We define $\mathcal{F}_{\mathcal{A},\mathcal{C}} \ , \ \mathcal{E}_{\mathcal{B}} \subset \mathbf{R} \times \mathcal{Y}$ below:

$$\begin{aligned}
\mathcal{F}_{\mathcal{A},\mathcal{C}} &:= \{(r,y) \in \mathbf{R} \times \mathcal{Y} | r = (\mathcal{C},x), y = \mathcal{A}x \ for \ some \ x \in \mathcal{L}\} \\
\mathcal{E}_{\mathcal{B}} &:= \mathbf{R} \times \{\mathcal{B}\}.
\end{aligned}$$

Definition 15 Let $\mathcal{C}$ be an element of $\mathcal{X}^*$ and $\mathcal{B}$ an element of $\mathcal{Y}$. $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ is called *normal*, if $\overline{\mathcal{F}_{\mathcal{A},\mathcal{C}} \cap \mathcal{E}_{\mathcal{B}}} = \overline{\mathcal{F}_{\mathcal{A},\mathcal{C}}} \cap \mathcal{E}_{\mathcal{B}}$.

Theorem 10 *[General duality theorem]*

We obtain the following inequality for $\mathcal{C} \in \mathcal{X}^*, \mathcal{B} \in \mathcal{Y}$. We have the equality in (82), iff $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ is normal. We assume that $\inf(\mathcal{C}, x) = +\infty$, $\sup(f, \mathcal{B}) = -\infty$ in the case of $\{x \in \mathcal{L} | \mathcal{A}x = \mathcal{B}\} = \emptyset$, $\{f \in \mathcal{Y}^* | \mathcal{C} - \mathcal{A}^* f \in \mathcal{L}^*\} = \emptyset$ with respectively.

$$\inf_{\{x \in \mathcal{L} | \mathcal{A}x = \mathcal{B}\}} \langle \mathcal{C}, x \rangle \geq \sup_{\{f \in \mathcal{Y}^* | \mathcal{C} - \mathcal{A}^* f \in \mathcal{L}^*\}} \langle f, \mathcal{B} \rangle. \tag{82}$$

To know this theorem, see Ref. 9. To apply this theorem to the proof of Theorem 6, we have to define $\mathcal{X}, \mathcal{Y}, \mathcal{L}, \mathcal{A}, \mathcal{B}, \mathcal{C}$ such that $\{x \in \mathcal{L} | \mathcal{A}x = \mathcal{B}\} = \mathcal{U}(T_\rho P) \ , \ \mathcal{D}^\rho_W(M) = \langle \mathcal{C}, M \rangle$.

B.2 Topology

To apply Theorem 10 to the proof of Theorem 6 we will construct $\mathcal{X}, \mathcal{L}$.

Definition 16 $\mathcal{X}(T_\rho P, \mathcal{H}, g)$ is defined the set of the map $M : \mathcal{B}(T_\rho P) \to \mathcal{B}_{sa}(\mathcal{H})$ which satisfies the following conditions:

- $M\left(\bigcup_{\lambda \in \Lambda} B_\lambda\right) = \sum_{\lambda \in \Lambda} M(B_\lambda) \quad (B_\lambda \in \mathcal{B}(T_\rho P) \ , \ \lambda_1 \neq \lambda_2 \in \Lambda \ \Rightarrow \ B_{\lambda_1} \cap B_{\lambda_2} = \emptyset \ , \ |\Lambda| = \aleph_0)$
- $$\sup_{B \in \mathcal{B}(T_\rho P)} \|M(B)\| < \infty \tag{83}$$
- $$\forall f \in T^*_\rho P \ , \ \forall y \in T_\rho P \ , \ \left| \int_{T_\rho P} f(x)\, \mathrm{tr}_{\mathcal{H}}\, M(dx) y \right| < \infty \tag{84}$$
- $$\left| \int_{T_\rho P} g(x,x)\, \mathrm{tr}_{\mathcal{H}}\, M(dx) \rho \right| < \infty. \tag{85}$$

By the definition of Q, we obtain

$$\begin{aligned} \langle f(\lambda), x(\lambda)\rangle &\leq \langle f(\lambda), y\rangle & (76)\\ \langle f, x(\lambda)\rangle &\geq \langle f, y\rangle = 0 & (77)\end{aligned}$$

From (76) and (77),

$$\begin{aligned} \langle f, x(\lambda)\rangle - \lambda\langle g(y), x(\lambda)\rangle &= \langle f(\lambda), x(\lambda)\rangle && \text{by (75)}\\ &\leq \langle f(\lambda), y\rangle && \text{by (76)}\\ &= \langle f, y\rangle - \lambda\langle g(y), y\rangle && \text{by (75)}\\ &= -\lambda\langle g(y), y\rangle && \text{by (77) .}\end{aligned}$$

Thus,

$$\lambda\langle g(y), x(\lambda) - y\rangle \geq \langle f, x(\lambda)\rangle > 0. \quad (78)$$

Hence, $\langle g(y), x(\lambda) - y\rangle > 0$. Thus, $\|y - x(\lambda)/2\|^2 < \|x(\lambda)\|^2/4$ i.e. $\|y - x(\lambda)/2\| < \|x(\lambda)\|/2$. Therefore,

$$\begin{aligned} \|x(\lambda)\| - \|y\| &\geq \|x(\lambda)\| - (\|y - \frac{x(\lambda)}{2}\| + \|\frac{x(\lambda)}{2}\|)\\ &= \|\frac{x(\lambda)}{2}\| - \|y - \frac{x(\lambda)}{2}\|\\ &> 0. \quad (79)\end{aligned}$$

But by the continuity of Q, $\lim_{\lambda\to 0} Q(f(\lambda)) = Q(f)$. Thus $\lim_{\lambda\to 0}\|x(\lambda)\| = 0$. From (79), $y = 0$. We obtain a contradiction. Therefore, we have (2). □

Lemma 15 *We obtain the following relations:*

$$B(C, (L^*)^i) \subset E(C, L) \subset \overline{B(C, (L^*)^i)}, \quad (80)$$

where

$$B(C, (L^*)^i) := \{x \in C | \exists f \in (L^*)^i \ , \ \forall x \in C \ , \ f(x) \leq f(y)\}. \quad (81)$$

To know a proof of this lemma, see Ref 9.

Proof of Theorem 2 From Lemma 9 and Lemma 14, If Q is C-conic, then $\mathrm{Im}\, Q = B(C, (L^*)^i)$. By Lemma 15, we obtain (61). □

B Proof of Theorem 6

It is the purpose of this section to prove the Theorem 6. Theorem 6 is described as follows.
Theorem 6 *We obtain*

$$\inf_{M\in\mathcal{U}(T_\rho P)} \mathcal{D}_g^\rho(M) = \sup_{(a,S)\in\tilde{\mathcal{U}}^*(g)} \mathrm{Spur}(a, S),$$

By (67) and (64),

$$\langle \alpha, Q(t\alpha + f) - Q(\alpha + f) \rangle \geq 0. \tag{68}$$

By (67) and (63),

$$\langle \alpha, Q(t\alpha + f) - Q(\alpha + f) \rangle \leq 0. \tag{69}$$

Because of (68) and (69),

$$\langle \alpha, Q(t\alpha + f) - Q(\alpha + f) \rangle = 0. \tag{70}$$

From (70) and (62),

$$\langle \alpha + f, Q(t\alpha + f) - Q(\alpha + f) \rangle = 0. \tag{71}$$

By the continuity of Q, we obtain

$$\langle k, Q(f) - Q(k) \rangle = 0. \tag{72}$$

Step 2: Let $h \in (L^*)^i$ such that $h \neq f, k$. We will prove $\langle h, Q(f) - Q(k) \rangle = 0$. By Step 1, we may assume that $\langle h, Q(f) - Q(k) \rangle \geq 0$. Let $\beta := h - f$, $1 > t > 0$. From the definition of Q,

$$\langle t\beta + f, Q(t\beta + f) - Q(k) \rangle \leq 0 \tag{73}$$
$$\langle f, Q(t\beta + f) - Q(f) \rangle \geq 0. \tag{74}$$

By (62) and (74), $\langle f, Q(t\beta + f) - Q(k) \rangle \geq 0$. From (73) and the preceding inequality, $\langle \beta, Q(t\beta + f) - Q(k) \rangle \leq 0$. By the continuity of Q, $\langle \beta, Q(f) - Q(k) \rangle \leq 0$. Therefore, we obtain $\langle h, Q(f) - Q(k) \rangle \leq 0$. By the hypothesis, $\langle h, Q(f) - Q(k) \rangle \geq 0$. Therefore $\langle h, Q(f) - Q(k) \rangle = 0$. We obtain $Q(f) - Q(k) = 0$. Therefore, the proof is complete. □

Definition 13 A continuous map $Q : (L^*)^i \to L$ is *quasi conic* if it satisfies the condition of lemma 13.

Lemma 14 *Let Q a quasi conic map. When C is L stable and convex and* $\mathrm{Im}\, Q \subset C$*,the following are equivalent:*

$$(1) \quad f \in (L^*)^i,\ x \in C \ \Rightarrow\ \langle f, x \rangle \geq \langle f, Q(f) \rangle$$
$$(2) \quad f \in (L^*)^i,\ x \in C,\ x \neq Q(f) \ \Rightarrow\ \langle f, x \rangle > \langle f, Q(f) \rangle.$$

Proof (2) ⇒ (1) is trivial. We will prove that (1) ⇒ (2) by reductive absurdity. There exist $f \in (L^*)^i$ and $x \in C$ such that $x \neq Q(f)$, $\langle f, Q(f) \rangle \geq \langle f, x \rangle$. By the hypothesis, $\langle f, Q(f) \rangle = \langle f, x \rangle$. y, $f(\lambda)$ and $x(\lambda)$ are defined as follows: for $\lambda > 0$,

$$y := x - Q(f),\ f(\lambda) := f - \lambda g(y),\ x(\lambda) := Q(f(\lambda)) - Q(f). \tag{75}$$

Appendices

A L-stable set

The purpose of this section is proving the following theorem about a finite dimensional real vector space W and its normal convex cone L.

Definition 12 We assume that $C \subset L$ is L-stable and convex. A continuous map $Q : (L^*)^i \to C$ is called *C-conic* if $\langle f, x\rangle \geq \langle f, Q(f)\rangle$ for arbitrary $x \in C$, $f \in (L^*)^i$, where we denote X^i the inner of a topological space X.

Theorem 9 *Let C be a subset of L. We assume that C is L-stable and convex. If there exists a C-conic map Q, then*

$$\mathrm{Im}\, Q \subset K(C) \subset \overline{\mathrm{Im}\, Q} \tag{61}$$

Lemma 13 *When $Q : (L^*)^i \to L$ is continuous, then the following are equivalent.*

(1) $\forall f \in (L^*)^i$, $x \in \mathrm{Im}\, Q$, $\langle f, x\rangle \geq \langle f, Q(f)\rangle$
(2) $\forall f \in (L^*)^i$, $x \in \mathrm{Im}\, Q \setminus \{Q(f)\}$, $\langle f, x\rangle > \langle f, Q(f)\rangle$

Proof (2) $\Rightarrow$ (1) is trivial. We prove that (1) $\Rightarrow$ (2). Let $f, k \in (L^*)^i$. It is sufficient to verify that if

$$\langle f, Q(k)\rangle = \langle f, Q(f)\rangle, \tag{62}$$

then $Q(f) = Q(k)$.
Step 1: We will prove $\langle k, Q(k) - Q(f)\rangle = 0$.
Let $\alpha := k - f$. By the assumption of (1), for $1 > t > 0$,

$$\begin{aligned} \langle t\alpha + f, Q(t\alpha + f) - Q(\alpha + f)\rangle &\leq 0 && (63)\\ \langle \alpha + f, Q(t\alpha + f) - Q(\alpha + f)\rangle &\geq 0 && (64)\\ \langle f, Q(t\alpha + f) - Q(f)\rangle &\geq 0. && (65) \end{aligned}$$

From (63) and (64),

$$\langle f, Q(t\alpha + f) - Q(\alpha + f)\rangle \leq 0.$$

Because of (65) and (62),

$$\langle f, Q(t\alpha + f) - Q(\alpha + f)\rangle \geq 0. \tag{66}$$

By (65) and (66),

$$\langle f, Q(t\alpha + f) - Q(\alpha + f)\rangle = 0. \tag{67}$$

Lemma 12 *If $e \in T_\rho P$, $\|e\| = 1$, then*

$$J^{-1}(e) \cdot \rho \cdot J^{-1}(e) = \mathrm{Id}_{\mathcal{H}} - \rho. \tag{59}$$

Proof We have

$$J^{-1}(e) = y^3 \frac{1}{1-\alpha^2}(-\alpha\,\mathrm{Id}_{\mathcal{H}} + \sigma_3) + \sum_{i=2}^{3} e^i \sigma_i. \tag{60}$$

Since there exists $t \in \mathbf{R}$ such that $\exp(\sqrt{-1}t\sigma_3)(e^1\sigma_1 + e^2\sigma_2)\exp(-\sqrt{-1}t\sigma_3) = \sqrt{(y^1)^2 + (y^2)^2}\sigma_1$, we may assume that $e^2 = 0$. Then we have

$$\begin{aligned} J^{-1}(e) \cdot \rho \cdot J^{-1}(e) &= \begin{pmatrix} \frac{-\alpha+1}{\sqrt{1-\alpha^2}}e^3 & e^1 \\ e^1 & \frac{-\alpha-1}{\sqrt{1-\alpha^2}}e^3 \end{pmatrix} \begin{pmatrix} \frac{1+\alpha}{2} & 0 \\ 0 & \frac{1-\alpha}{2} \end{pmatrix} \begin{pmatrix} \frac{-\alpha+1}{\sqrt{1-\alpha^2}}e^3 & e^1 \\ e^1 & \frac{-\alpha-1}{\sqrt{1-\alpha^2}}e^3 \end{pmatrix} \\ &= \begin{pmatrix} \frac{1-\alpha}{2} & 0 \\ 0 & \frac{1+\alpha}{2} \end{pmatrix} = \mathrm{Id}_{\mathcal{H}} - \rho. \end{aligned}$$

□

We obtain the following theorem.

Theorem 8 *When $\mathcal{H} = \mathbf{C}^2$, $T_\rho P$ is a random model.*

8 Conclusions

We have found a necessary and sufficient condition that a Cramér-Rao type bound is attained by a random measurement. But, we don't know the condition (1) or (2) in Theorem 7 very well.We know no random model whose dimension is greater than 3. Thus, it is conjectured that when $T_\rho P$ is a random model, the dimension of $T_\rho P$ is limited.

Acknowledgments

I wish to thank Dr. A. Fujiwara for introducing me into this subject, and Prof. K. Ueno for useful comments about this paper. I also benefited from e-mail discussions with Dr. K. Matsumoto.

where P_m denotes the projection of V_m.

$$\begin{aligned}
(X-X_m)^2 &= (X-P_mXP_m)^2 \\
&= 2X^2+2(P_mXP_m)^2-(X+P_mXP_m)^2 \\
&\leq 2X^2+2(P_mXP_m)^2 \\
&= 2X^2+2P_mX^2P_m \\
&\leq 4X^2 \\
\mathrm{tr}_{\mathcal{H}}(X-X_m)\rho(X-X_m) &= \mathrm{tr}_{\mathcal{H}}(X-X_m)^2\rho \\
&= \mathrm{tr}_{\mathcal{H}}(X-X_m)^2\rho_m+\mathrm{tr}_{\mathcal{H}}(X-X_m)^2(\rho-\rho_m) \\
&\leq 0+\mathrm{tr}_{\mathcal{H}}\,4X^2(\rho-\rho_m)\to 0.
\end{aligned}$$

□

Lemma 11 *Let $X(S)$ be an element of $L^2_{sa}(\rho)(\mathcal{B}^*_{sa}(\mathcal{H}))$ respectively. If*

$$(x-X)\rho(x-X)+S\in\mathcal{B}^{*,+}_{sa}(\mathcal{H}),\ \forall x\in\mathbf{R}, \tag{58}$$

then we obtain $S\in\mathcal{B}^{*,+}_{sa}(\mathcal{H})$.

Proof Let $\{X_m\}$ be a sequence of finite rank selfadjoint operators on $\mathcal{H}$ such that $\mathrm{tr}_{\mathcal{H}}(X-X_m)\rho(X-X_m)\to 0$ as $m\to\infty$. $X_m:=\sum_{i=1}^{k_m}x_i^m|\phi_i^m\rangle\langle\phi_i^m|$ denotes the spectral decomposition of X_m. For $\forall\psi\in\mathcal{H}$,

$$\begin{aligned}
&\sum_{i=1}^{k_m}\langle(x_i^m-X)\rho(x_i^m-X)+S,|\phi_i^m\rangle\langle\phi_i^m|\psi\rangle\langle\psi|\phi_i^m\rangle\langle\phi_i^m|\rangle \\
=\ &\langle(X_m-X)\rho(X_m-X)+S,|\psi\rangle\langle\psi|\rangle \\
=\ &\langle\psi|(X_m-X)\rho(X_m-X)|\psi\rangle+\langle S,|\psi\rangle\langle\psi|\rangle \\
\geq\ &0.
\end{aligned}$$

Since $\langle\psi|(X_m-X)\rho(X_m-X)|\psi\rangle\to 0$, we get $\langle S,|\psi\rangle\langle\psi|\rangle\geq 0$. □

7 3-parameter Spin 1/2 model

In this section, we will prove that if $\mathcal{H}=\mathbf{C}^2$, then $T_\rho P$ is random model. Let us define the Pauli matrices $\sigma_1,\sigma_2,\sigma_3$ in the usual way:

$$\sigma_1=\begin{pmatrix}0&1\\1&0\end{pmatrix},\ \sigma_2=\begin{pmatrix}0&-i\\i&0\end{pmatrix},\ \sigma_3=\begin{pmatrix}1&0\\0&-1\end{pmatrix}.$$

Assume that $T_\rho P=\mathcal{T}^0_{sa}(\mathbf{C}^2)$, $\rho=\frac{1}{2}(Id+\alpha\sigma_3)$,$-1<\alpha<1$ and that g is a quadratic form on $T_\rho P$. $f_3=\frac{\sqrt{1-\alpha^2}}{2}\sigma_3$, $f_i=\frac{\sigma_i}{2}$,$(i=1,2)$ are orthonormal bases on $T_\rho P$. The dual bases of f^i are $f^3=\frac{-\alpha}{\sqrt{1-\alpha^2}}\,\mathrm{Id}+\frac{1}{\sqrt{1-\alpha^2}}\sigma_3$, $f^i=\sigma_i$ $(i=1,2)$. We need the following lemma.

Next, let's prove (4) $\Rightarrow$ (1). Without loss of generality, we can assume that $g = W^*JW$, $W \in \mathrm{End}_{sa}(T_\rho P)$, $\mathrm{tr}_{T_\rho P} W = 1$. From the assumption of (4) and Theorem 6, There exists a sequence $\{(2a_m, S_m)\}$ of $\tilde{\mathcal{U}}^*(g)$ such that $\mathrm{Spur}(2a_m, S_m) \to 1$ as $m \to \infty$. From §4 and Theorem 6, we have $\mathcal{D}_g^\rho(M_W^T) = 1$.

Thus,

$$\mathcal{R}_g^\rho(2a_m, S_m; M_W^T) \to 0 \text{ as } m \to \infty. \tag{52}$$

Then,

$$\mathcal{R}_g^\rho(2a_m, S_m; M^T(W^{-1}e_i, J^{-1}e_i)) \to 0 \text{ as } m \to \infty. \tag{53}$$

For $e \in T_\rho P$, $\|e\| = 1$,

$$\begin{aligned} & R_g^\rho(2a_m, S_m; xW^{-1}e) \\ = \; & y^2\rho - 2xa_m(W^{-1}e) - S_m \\ = \; & (x - J^{-1}a_mW^{-1}e)\rho(x - J^{-1}a_mW^{-1}e) - S(a_mW^{-1}e) - S_m \in \mathcal{B}_{sa}^{*,+}(\mathcal{H}). \end{aligned} \tag{54}$$

By Lemma 11, we obtain

$$-S(a_mW^{-1}e) - S_m \in \mathcal{B}_{sa}^{*,+}(\mathcal{H}). \tag{55}$$

From (53),(55) and (54)

$$\lim_{m\to\infty} \mathrm{tr}_{\mathcal{H}}\Big(\int_{\mathbf{R}} \Big(y - J^{-1}a_m(W^{-1}e_i)\Big)\rho\Big(y - J^{-1}a_m(W^{-1}e_i)\Big) M^T_{J^{-1}e_i}(\,dy)\Big) = 0. \tag{56}$$

From (54), (53) and (56)

$$\lim_{m\to\infty} \langle -S(a_mW^{-1}e_i) - S_m, \mathrm{Id}_{\mathcal{H}}\rangle = 0. \tag{57}$$

By (56) $\lim_{m\to\infty} J^{-1}a_mW^{-1}e_i = J^{-1}e_i$. Thus, $\lim_{m\to\infty} a_m = W$.

Then $S(a_mW^{-1}e) \to S(e)$ in the trace norm. From (57) and (55), $-S(a_mW^{-1}e) - S_m \to 0$ in the trace norm. Thus, $-S(e) - S_m \to 0$ in the trace norm. Therefore, $S(e) = S(e')$ for $e, e' \in T_\rho P$, $e \neq e'$, $\|e\| = \|e'\| = 1$. □

Lemma 10 *For $X \in L^2(\rho)$, there exists a sequence $\{X_m\}$ of finite rank selfadjoint operators on $\mathcal{H}$ such that $\mathrm{tr}_{\mathcal{H}}(X - X_m)\rho(X - X_m) \to 0$ as $m \to \infty$.*

Proof Let $\rho = \sum_{i=1}^\infty s_i|\phi_i\rangle\langle\phi_i|$ be the spectral decomposition of ρ. We define as follows:

$$\begin{aligned} \rho_m &:= \sum_{i=1}^m s_i|\phi_i\rangle\langle\phi_i| \\ V_m' &:= \mathrm{Im}\,\rho_m \\ V_m'' &:= X(V_m') \\ V_m &:= V_m' + V_m'' \\ X_m &:= P_mXP_m, \end{aligned}$$

6 Randomness condition

Theorem 7 *The following four conditions are equivalent.*

(1) $\forall X, Y \in T_\rho^* P,\ \|X\| = \|Y\| = 1 \Rightarrow X\rho X = Y\rho Y.$

(2) *There exists a complete orthonarmal base* $\{X_1, \dots X_n\}$ *of* $T_\rho^* P$ *such that* $X_i\rho X_j + X_j\rho X_i = 0,\ X_i\rho X_i = X_j\rho X_j$ *for* $(i \neq j)$.

(3) $\mathcal{V}_\rho = \mathcal{V}_{\rho,R}$.

(4) *There exists* $g > 0$ *such that* $\inf_{M \in \mathcal{U}(T_\rho P)} \mathcal{D}_g^\rho = (\mathrm{tr}_{T_\rho P} \sqrt{Jg})^2$.

Definition 11 If $T_\rho P$ satisfies the preceding condition, $T_\rho P$ is called a *random model*.

Proof (3) $\Rightarrow$ (4), (2) $\Leftrightarrow$ (1) is easy. In this proof, W_i denotes an eigenvalue of W, and e_i denotes an eigenvector of W, where $\|e_i\| = 1$.

For simplicity, $S(x)$ denotes $J^{-1}x\rho J^{-1}x$ for $x \in T_\rho P$. First, let's prove (1) $\Rightarrow$ (3). $W \in \mathrm{End}_{sa}(T_\rho P),\ \mathrm{tr}_{T_\rho P} W = 1$, For $g := W^* J W$, we calculate $\inf_{M \in \mathcal{U}(T_\rho P)} \mathcal{D}_g^\rho$. Take the Lagrange multipliers in the following way:

$$\begin{aligned} a &:= 2W \\ S &:= -X\rho X, \end{aligned}$$

where we put $X \in T_\rho^* P,\ \|X\| = 1$. Then, we have

$$\begin{aligned} & R_g^\rho(2W, S; yW^{-1}z) \\ = \ & g(yW^{-1}z, yW^{-1}z) \cdot \rho - 2W(yW^{-1}z) + J^{-1}(z)\rho J^{-1}(z) \\ = \ & y^2 \cdot \rho - 2yz + J^{-1}(z)\rho J^{-1}(z) \\ = \ & y^2 \cdot \rho - 2yJ^{-1}(z) \circ \rho + J^{-1}(z)\rho J^{-1}(z) \\ = \ & \Big(y - J^{-1}(z)\Big)\rho\Big(y - J^{-1}(z)\Big), \end{aligned}$$

where $z \in T_\rho P,\ \|z\| = 1,\ y \in \mathbf{R}$. Therefore, $(2W, S) \in \mathcal{U}^*(g)$. Thus, $\mathrm{Spur}(2W, S) = 1$ is a Cramér-Rao type bound. Substitute $M = M_W^T$, then

$$\mathcal{R}_g^\rho(a, S; M_W^T) = \sum_{i=1}^n W_i \mathcal{R}_g^\rho(a, S; M^T(W_i^{-1}e_i, J^{-1}e_i)) = 0$$

because

$$\begin{aligned} & \mathcal{R}_g^\rho(a, S; M^T(W_i^{-1}e_i, J^{-1}e_i)) \\ = \ & \mathrm{tr}_{\mathcal{H}}\Big(\int_{\mathbf{R}} R_g^\rho(a, S; yW_i^{-1}e_i) M^T_{J^{-1}(e_i)}(\,dy)\Big) \\ = \ & \mathrm{tr}_{\mathcal{H}}\Big(\int_{\mathbf{R}} \Big(y - J^{-1}(e_i)\Big)\rho\Big(y - J^{-1}(e_i)\Big) M^T_{J^{-1}(e_i)}(\,dy)\Big) = 0. \end{aligned}$$

As $(2W, S)$ and M_W^T satisfy the conditions of Corollary 2, the random measurement M_W^T attains a Cramér-Rao type bound 1. Therefore (1) $\Rightarrow$ (3) is proved.

Thus, we get

$$\mathrm{tr}_{\mathcal{H}}\, S \leq -\frac{1}{4g(z,z)}\langle a(z)|a(z)\rangle_S^{\rho} = -\frac{\|a\|_o^2}{4g(z,z)},$$

$$\mathrm{tr}_{\mathcal{H}}\, S \leq -\frac{\|a\|_o^2}{4\|g\|_o}.$$

Therefore, we obtain

$$0 \leq \mathrm{Spur}(a,S) \leq n\|a\|_o - \frac{\|a\|_o^2}{4\|g\|_o}.$$

Hence, $0 \leq \|a\|_o(n - \frac{\|a\|_o}{4\|g\|_o})$. Thus, $0 \leq \|a\|_o \leq 4n\|g\|_o$. As $-S \geq 0$, we have $\|S\| = -\mathrm{tr}_{\mathcal{H}}\, S$. Therefore, we obtain the following inequalities:

$$0 \leq \|S\| \leq \mathrm{tr}\, a \leq n\|a\|_o \leq 4\|g\|_o n^2.$$

Thus, $\mathcal{U}^*(g) \cap \mathrm{Spur}^{-1}([0,\infty))$ is bounded, hence compact. □
We have the following corollary.

Corollary 3 *There exists the maximum of the right hand side of (42).*

Assume that $\rho \in P_1 \subset P_2$ and $T_\rho P_1 \subset T_\rho P_2$, $T_\rho P_1 \neq T_\rho P_2$. From the embedding map $i : P_1 \hookrightarrow P_2$, we have $di_\rho : T_\rho P_1 \hookrightarrow T_\rho P_2$ and $di_\rho^* : T_\rho^* P_2 \to T_\rho^* P_1$. By identifying the dual $T_\rho^* P_i$ with $T_\rho P_i$ $(i = 1, 2)$, di_ρ^* can be regarded as $di_\rho^* : T_\rho P_2 \to T_\rho P_1$. Let g be a nonnegative inner product on $T_\rho P_1$, then $di_\rho g\, di_\rho^*$ is a nonnegative inner product on $T_\rho P_2$.

Lemma 9 *We have the inequality:*

$$\max_{(a,S)\in\mathcal{U}^*(g)} \mathrm{Spur}(a,S) \leq \max_{(a',S)\in\mathcal{U}^*(\,di_\rho g\, di_\rho^*)} \mathrm{Spur}(a',S). \tag{49}$$

Moreover the equality in (49) holds, if and only if there exists $(a', S) \in \mathcal{U}^*(\,di_\rho g\, di_\rho^*)$ such that $a'(T_\rho P_1) \subset T_\rho P_1$, and the maximum of the right hand side is attained by (a', S).

Proof We have $(\,di_\rho a\, di_\rho^*, S) \in \mathcal{U}^*(\,di_\rho g\, di_\rho^*)$ for $(a, S) \in \mathcal{U}^*(g)$.

$$\begin{array}{rccc} F: & \mathcal{U}^*(g) & \to & \mathcal{U}^*(\,di_\rho g\, di_\rho^*) \\ & \Downarrow & & \Downarrow \\ & (a,S) & \mapsto & (\,di_\rho a\, di_\rho^*, S). \end{array} \tag{50}$$

Then, $\mathrm{Spur}(a,S) = \mathrm{Spur}(F(a,S))$. Therefore we obtain Inequality (49) The equality holds in (49), if and only if

$$\max_{(a',S)\in\mathrm{Im}\,F} \mathrm{Spur}(a',S). = \max_{(a',S)\in\mathcal{U}^*(\,di_\rho g\, di_\rho^*)} \mathrm{Spur}(a',S) \tag{51}$$

By the definition of $\mathcal{U}^*(\,di_\rho g\, di_\rho^*)$, as $di_\rho g\, di_\rho^*(\mathrm{Ker}\; di_\rho^*) = 0$, we have $a'(\mathrm{Ker}\; di_\rho^*) = 0$ for $(a', S) \in \mathcal{U}^*(\,di_\rho g\, di_\rho^*)$. Thus, $(a', S) \in \mathrm{Im}\, F$ for $(a', S) \in \mathcal{U}^*(\,di_\rho g\, di_\rho^*)$, if and only if $a'(T_\rho P_1) \subset T_\rho P_1$. Thus, the proof is complete. □

5.1 Maximum

In this section, we consider the dual problem. $T_\rho P$ is regarded as a real Hilbert space with respect to $J_S^{\rho,-1}$.

Lemma 8 *If the dimension of $\mathcal{H}$ is finite, then the set $\mathcal{U}^*(g) \cap \mathrm{Spur}^{-1}([0,\infty))$ is compact.*

We assume that the norm of $\mathrm{End}(T_\rho P)$ is the operator norm $\| \ \|_o$, and the norm of $\mathcal{T}_{sa}(\mathcal{H})$ is the trace norm $\| \ \|_t$. The norm $\| \ \|_{o,t}$ of $\mathrm{End}(T_\rho P) \times \mathcal{T}_{sa}(\mathcal{H})$ is defined as follows:

$$\|(a,S)\|_{o,t} := \|a\|_o + \|S\|_t, \ \forall (a,S) \in \mathrm{End}(T_\rho P) \times \mathcal{T}_{sa}(\mathcal{H}).$$

Proof We have

$$\mathcal{U}^*(g) = \cap_{x \in T_\rho P} \{(a,S) | g(x,x) \cdot \rho - S - a(x) \in \mathcal{T}_{sa}^+(\mathcal{H})\}.$$

Moreover, $\{(a,S) | g(x,x) \cdot \rho - S - a(x) \in \mathcal{T}_{sa}^+(\mathcal{H})\}$ is closed. Thus, $\mathcal{U}^*(g)$ is closed. Because $\mathrm{Spur}^{-1}([0,\infty))$ is closed. $\mathcal{U}^*(g) \cap \mathrm{Spur}^{-1}([0,\infty))$ is closed. Therefore, it is sufficient to show that it is bounded with respect to the norm $\| \ \|_{o,t}$. Denote $n := \dim T_\rho P$. For $(a,S) \in \mathcal{U}^*(g) \cap \mathrm{Spur}^{-1}([0,\infty))$, we have $\mathrm{tr}_{T_\rho P}\, a \leq n\|a\|_o$. Choose $z \in T_\rho P$ such that $\|z\|_S = 1$, $\|a(z)\|_S = \|a\|_o$. For $r > 0$, we have

$$g(r \cdot z, r \cdot z)\rho - a(r \cdot z) - S \geq 0. \tag{47}$$

Substitute $r = 0$, then $-S \geq 0$. Let us calculate the left hand side of (47).

$$\begin{aligned} & g(r \cdot z, r \cdot z)\rho - a(r \cdot z) - S = r^2 \cdot g(z,z)\rho - r \cdot J_S^{\rho,-1}(a(z)) \circ \rho - S \\ = \ & \Big(\sqrt{g(z,z)} r - \frac{1}{2\sqrt{g(z,z)}} J_S^{\rho,-1}(a(z))\Big) \cdot \rho \cdot \Big(\sqrt{g(z,z)} r - \frac{1}{2\sqrt{g(z,z)}} J_S^{\rho,-1}(a(z))\Big) \\ & - \frac{1}{4g(z,z)} J_S^{\rho,-1}(a(z)) \cdot \rho \cdot J_S^{\rho,-1}(a(z)) - S. \end{aligned} \tag{48}$$

Let $\{e_i\}$ be a complete orthonormal system of $\mathcal{H}$ which consists of eigenvectors of $J_S^{\rho,-1}(a(z))$. Substitute r for the eigenvalue α_i of $\frac{1}{2g(z,z)} J_S^{\rho,-1}(a(z))$ corresponding to the eigenvector e_i, then we have

$$\Big\langle e_i \Big| \Big(\sqrt{g(z,z)}\alpha_i - \frac{1}{2\sqrt{g(z,z)}} J_S^{\rho,-1}(a(z))\Big) \cdot \rho \cdot \Big(\sqrt{g(z,z)}\alpha_i - \frac{1}{2\sqrt{g(z,z)}} J_S^{\rho,-1}(a(z))\Big) \Big| e_i \Big\rangle = 0.$$

By (47), we have

$$\Big\langle e_i \Big| - \frac{1}{4g(z,z)} J_S^{\rho,-1}(a(z)) \cdot \rho \cdot J_S^{\rho,-1}(a(z)) - S \Big| e_i \Big\rangle \geq 0.$$

Sum up for i from 1 to n.

$$\mathrm{tr}_{\mathcal{H}} \Big(- \frac{1}{4g(z,z)} J_S^{\rho,-1}(a(z)) \cdot \rho \cdot J_S^{\rho,-1}(a(z)) - S \Big) \geq 0.$$

The calculation of $\sup_{(a,S)\in\mathcal{U}^*(g)} \mathrm{Spur}(a,S)$ is called the dual problem.

Corollary 2 *If there exist a sequence of locally unbiased measurements* $\{M_k\}$ *and an element* (a',S') *of* $\mathcal{U}^*(g)$ *satisfying the condition:*

$$\mathcal{R}_g^\rho(a',S';M_k) \to 0 \ (as\ k\to 0), \tag{43}$$

then

$$\lim_{k\to\infty} \mathcal{D}_g^\rho(M_k) = \mathrm{Spur}(a',S') = \inf_{M\in\mathcal{U}(T_\rho P)} \mathcal{D}_g^\rho(M) = \sup_{(a,S)\in\mathcal{U}^*(g)} \mathrm{Spur}(a,S), \tag{44}$$

where $\mathcal{R}_g^\rho$ *is defined as:*

$$\mathcal{R}_g^\rho(a,S;M) := \mathrm{tr}_{\mathcal{H}} \int_{T_\rho P} R_g^\rho(a,S;x) M(\,dx). \tag{45}$$

$(a,S)\in\mathcal{U}^*(g)$ is called the Lagrange multiplier.

Proof of Theorem 5 and Corollary 2 For $M\in\mathcal{U}(T_\rho P)$ and $(a,S)\in\mathcal{U}^*(g)$, we have

$$\begin{aligned} & \mathcal{R}_g^\rho(a,S;M) \\ = \ & \mathrm{tr}_{\mathcal{H}} \int_{T_\rho P} g(x,x)\cdot\rho M(\,dx) - \mathrm{tr}_{\mathcal{H}} \int_{T_\rho P} SM(\,dx) - \mathrm{tr}_{\mathcal{H}} \int_{T_\rho P} a(x) M(\,dx) \\ = \ & \mathcal{D}_g^\rho(M) - \mathrm{tr}_{T_\rho P}\, a - \mathrm{tr}_{\mathcal{H}}\, S. \end{aligned} \tag{46}$$

Since $R_g^\rho(a,S;x)\geq 0$ for any $x\in T_\rho P$, we obtain $\mathcal{R}_g^\rho(a,S;M)\geq 0$. By (46), the proof of Theorem 5 is complete. Substitute $(a,S)=(a',S')$, then the proof of Corollary 2 is complete. □

Indeed we obtain the following theorem. A proof of Theorem 6 is too long. See Appendix B.

Theorem 6 *We obtain*

$$\inf_{M\in\mathcal{U}(T_\rho P)} \mathcal{D}_g^\rho(M) = \sup_{(a,S)\in\tilde{\mathcal{U}}^*(g)} \mathrm{Spur}(a,S),$$

where

$$\begin{aligned} \tilde{\mathcal{U}}^*(g) &:= \{(a,S)\subset \mathrm{End}(T_\rho P)\times\mathcal{B}_{sa}^*(\mathcal{H}) | \forall x\in T_\rho P \ , \ R_g^\rho(a,S;x)\in\mathcal{B}_{sa}^{*,+}(\mathcal{H})\} \\ \mathrm{Spur}(a,S) &:= \mathrm{tr}_{T_\rho P}\, a + \langle S, \mathrm{Id}_{\mathcal{H}}\rangle \\ R_g^\rho(a,S;x) &:= g(x,x)\cdot\rho - S - a(x). \end{aligned}$$

$\mathcal{B}_{sa}^*(\mathcal{H})$ *is the topological dual space of* $\mathcal{B}_{sa}(\mathcal{H})$ *with respect to the norm topology. By the preceding equation we have the equality in (42) in the case of* $\dim\mathcal{H}<\infty$. *But we don't know whether we have the equality in the case of* $\dim\mathcal{H}=\infty$. *The calculation of* $\sup_{(a,S)\in\mathcal{U}^*(g)} \mathrm{Spur}(a,S)$ *is called the dual problem.*

From the preceding proof, the map Q_R is derived in the following:

$$\begin{array}{rccc} Q_R: & S(T_\rho^* P \otimes T_\rho^* P) & \to & S(T_\rho P \otimes T_\rho P) \\ & \Downarrow & & \Downarrow \\ & W^* J W & \mapsto & \frac{W^{-1} J}{\mathrm{tr}_{T_\rho P} W}. \end{array} \tag{38}$$

$\mathrm{Im}\, Q_R = \{W^{-1} J | \, \mathrm{tr}_{T_\rho P} W = 1\}$ is closed. Since this map is $S^+(T_\rho P \otimes T_\rho P)$-conic, we have the following Theorem.

Theorem 4 *The limit set of $\mathcal{V}_{\rho,R}$ is described as follows:*

$$K(\mathcal{V}_{\rho,R}) = \{W^{-1} J | \, \mathrm{tr}_{T_\rho P} W = 1\}. \tag{39}$$

This limit set is called the random limit.

Lemma 7 *In two parameter case, the random limit is described below:*

$$K(\mathcal{V}_{\rho,R}) = \{J + X J | \, \det X = 1\}. \tag{40}$$

5 Linear programming approach

We introduce a new approach to the attainable Cramér-Rao type bound. In this approach, applying the duality theorem of the infinite dimensional linear programming, the bound is characterized. But, we don't have to know the duality theorem for this section. If the reader is interested in the duality theorem, see Ref 5. In the noncommutative case, there is no infimum of covariance matrices under the locally unbiasedness conditions. Therefore, we minimize the following value $\mathcal{D}_g^\rho$ under the locally unbiasedness conditions. Let g be a nonnegative inner product on $T_\rho P$.

Definition 10 *The deviation $\mathcal{D}_g^\rho$ for a measurement $M \in \mathcal{M}(T_\rho P, \mathcal{H})$ is defined as follows:*

$$\mathcal{D}_g^\rho(M) := \mathrm{tr}_{T_\rho^* P}\, g V_\rho(M) = \int_{T_\rho P} g(x,x)\, \mathrm{tr}_{\mathcal{H}}\, M(\, dx)\rho. \tag{41}$$

Let us define a linear functional on $\mathrm{End}(T_\rho P) \times \mathcal{T}_{sa}(\mathcal{H})$, denoted by Spur in the following way. We introduce a useful theorem to minimize the deviation $\mathcal{D}_g^\rho(M)$ under the locally unbiasedness conditions.

Theorem 5 *We have the inequality:*

$$\inf_{M \in \mathcal{U}(T_\rho P)} \mathcal{D}_g^\rho(M) \geq \sup_{(a,S) \in \mathcal{U}^*(g)} \mathrm{Spur}(a,S), \tag{42}$$

where

$$\begin{array}{rcl} \mathrm{Spur}(a,S) & := & \mathrm{tr}_{T_\rho P}\, a + \mathrm{tr}_{\mathcal{H}}\, S \\ \mathcal{U}^*(g) & := & \{(a,S) \in \mathrm{End}(T_\rho P) \times \mathcal{T}_{sa}(\mathcal{H}) | R_g^\rho(a,S;x) \geq 0, \ \forall x \in T_\rho P\} \\ R_g^\rho(a,S;x) & := & g(x,x) \cdot \rho - S - a(x). \end{array}$$

Notice that $T_\rho P$ is a subset of $\mathcal{T}_{sa}(\mathcal{H})$.

then we obtain

$$\mathcal{D}^{\rho}_{g,R}(p') = \mathrm{tr}_{T_\rho P}\, a' + S' = \inf_{p\in\mathcal{U}_R(T_\rho P)} \mathcal{D}^{\rho}_{g,R}(p) = \sup_{(a,S)\in\mathcal{U}^*_R(g)} \mathrm{tr}_{T_\rho P}\, a + S, \tag{30}$$

where $\mathcal{R}^{\rho}_{g,R}$ *is defined as:*

$$\mathcal{R}^{\rho}_{g}(a,S;p) := \int_{T_\rho P}\int_{T^*_\rho P} R^{\rho}_{g,R}(a,S;x,X)p(\,dX\,dx). \tag{31}$$

$(a,S)\in\mathcal{U}^*(g)$ is called the Lagrange multiplier.

Proof of Theorem 2 and Corollary 1 For $p\in\mathcal{U}_R(T_\rho P)$ and $(a,S)\in\mathcal{U}^*_R(g)$, we have

$$\begin{aligned} & \mathcal{R}^{\rho}_{g,R}(a,S;p) \\ = & \int_{T_\rho P}\int_{T^*_\rho P} g(x,x)\|X\|^2 p(\,dX\,dx) - \int_{T_\rho P}\int_{T^*_\rho P}\langle X, a(x)\rangle p(\,dX\,dx) - \int_{T_\rho P}\int_{T^*_\rho P} Sp(\,dX\,dx) \\ = & \mathcal{D}^{\rho}_{g,R}(p) - \mathrm{tr}_{T_\rho P}\, a - S. \end{aligned} \tag{32}$$

Since we have $R^{\rho}_{g,R}(a,S;x,X)\geq 0$ for $\forall(x,X)\in T_\rho P\times T^*_\rho P$, we obtain $\mathcal{R}^{\rho}_{g,R}(a,S;p)\geq 0$. By (32), the proof of Theorem 2 is complete. Substitute $(a,S)=(a',S'), p=p'$, then the proof of Corollary 1 is complete. □

Theorem 3 *If* $g=W^*JW$, $\mathrm{tr}_{T_\rho P}\, W=1$, *then*

$$\inf_{p\in\mathcal{U}_R(T_\rho P)} \mathcal{D}^{\rho}_{g,R}(p) = 1. \tag{33}$$

The Optimal measurement is given by (35).

Proof Let Lagrange multiplier (a,S) be $(2W,-1)$, then

$$\mathcal{R}^{\rho}_{g,R}(2W,-1;x,X) = \|W(x)\|^2\|X\|^2 - 2\langle X, W(x)\rangle + 1 \geq 0. \tag{34}$$

Let W_i be an eigen value of W and, e_i be an eigenvector of W, where $\|e_i\|=1$. M^T_W is defined as follows:

$$M^T_W := \sum_{i=1}^{n} W_i M^T(W_i^{-1}e_i, J^{-1}e_i). \tag{35}$$

Then $M^T_W\in\mathcal{U}_R(T_\rho P)$ and,

$$\mathcal{R}^{\rho}_{g,R}(2W,-1;M^T_W) = \sum_{i=1}^{n} W_i(\|e_i\|^2\|J^{-1}e_i\|^2 - 2\langle J^{-1}e_i, e_i\rangle + 1) = 0. \tag{36}$$

M^T_W and $(2W,-1)$ satisfy the condition of Corollary 1. Since $\mathrm{tr}_{T_\rho P}\, 2W-1=1$, we obtain (33). □

When a state ρ is measured by the measurement M^T_W, the following covariance matrix by (18).

$$V_\rho(M^T_W) = \sum_{i=1}^{n} W_i(W_i^{-1}e_i)\otimes(W_i^{-1}e_i)\|e_i\|^2 = \sum_{i=1}^{n} W_i^{-1}e_i\otimes e_i = W^{-1}J. \tag{37}$$

Definition 8 For a subset C of L, the *limit set* $K(C)$ of C is defined as follows:

$$K(C) := \{x \in C | (x - L) \cap C = \{x\}\}. \tag{25}$$

Lemma 6 *When a subset C of L is L-stable and closed, then $C = K(C) + L$.*

Proof It suffices to verify that there exists an element $y \in (C)$ such that $x \in y + L$ for arbitrary $x \in C \setminus K(C)$. $(x - L) \cap C \subset L$ is a compact set. Therefore, there exists $y \in (x - L) \cap C$ so that $g(z, z) \geq f(y, y)$ for arbitrary $z \in (x - L) \cap C$. Now we prove that $(y - L) \cap C = \{y\}$ by reductive absurdity. Let $z \in (y - L) \cap C$, $z \neq y$, then there exists $l \in L$, $l \neq 0$ so that $y = z + l$. Because $z, l \in L$, $l \neq 0$, from (20)

$$g(y, y) > g(z, z). \tag{26}$$

(26) contradicts the definition of y. Hence $(y - L) \cap C = \{y\}$, thus $y \in K(C)$. Because $y \in (x - L) \cap C$, we conclude $x \in y + L$. □

In Appendix A, we prove a useful theorem to calculate $K(\mathcal{V}_{\rho,R})$ and $K(\mathcal{V}_\rho)$.

4 Random Limit

Next, we minimize the following value $\mathcal{D}^\rho_{g,R}$ in locally unbiased and random measurements $\mathcal{U}_R(T_\rho P)$.

Definition 9 The *deviation* $\mathcal{D}^\rho_{g,R}$ for a measurement $p \in P(T_\rho P \times T^*_\rho P)$ is defined as follows:

$$\mathcal{D}^\rho_{g,R}(p) := \mathrm{tr}_{T^*_\rho P}\, g V_{\rho,R}(p) = \int_{T_\rho P} \int_{T^*_\rho P} g(x, x) \| X \|^2 p(\, dX\, dx). \tag{27}$$

We introduce the useful theorem to minimize the deviation $\mathcal{D}^\rho_{g,R}(M)$ under the locally unbiasedness conditions.

Theorem 2 *We have the inequality:*

$$\inf_{M \in \mathcal{U}_R(T_\rho P)} \mathcal{D}^\rho_{g,R}(M) \geq \sup_{(a,S) \in \mathcal{U}^*_R(g)} (\mathrm{tr}_{T_\rho P}\, a + S), \tag{28}$$

where

$$\begin{aligned} \mathcal{U}^*_R(g) &:= \{(a, S) \in \mathrm{End}(T_\rho P) \times \mathbf{R} | R^\rho_{g,R}(a, S; x, X) \geq 0,\ \forall (x, X) \in T_\rho P \times T^*_\rho P\} \\ R^\rho_{g,R}(a, S; x, X) &:= g(x, x)\| X \|^2 - \langle X, a(x) \rangle - S. \end{aligned}$$

Corollary 1 *If there exist a locally unbiased and random measurement $p' \in P(T_\rho P \times T^*_\rho P)$ and an element (a', S') of $\mathcal{U}^*_R(g)$ satisfying the condition:*

$$\mathcal{R}^\rho_{g,R}(a', S'; p') = 0, \tag{29}$$

3 Covariance matrix

In this section we characterize $\mathcal{V}_\rho$ and $\mathcal{V}_{\rho,R}$ For this purpose we need some definitions. Let W be a finite dimensional vector space. We call a closed convex cone L of W a normal convex cone, if it satisfies the following conditions:

$$\begin{aligned} &\circ \quad x \neq 0 \in L \ , \ \lambda < 0 \ \Rightarrow \ \lambda x \notin L \\ &\circ \quad W = L + (-L). \end{aligned} \tag{19}$$

Now we let L a normal convex cone. Let g be an inner product such that satisfies the following condition:

$$l_1, l_2 \in L \ , \ g(l_1, l_1) \geq g(l_1 + l_2, l_1 + l_2) \Longrightarrow l_2 = 0. \tag{20}$$

When W is $S(T_\rho P \otimes T_\rho P)$, $S^+(T_\rho P \otimes T_\rho P)$ is a normal positive cone.

Definition 7 A subset C of L is called *L-stable* set if

$$C = C + L. \tag{21}$$

Proposition 1 *$\mathcal{V}_\rho$ and $\mathcal{V}_{\rho,R}$ are $S^+(T_\rho P \otimes T_\rho P)$-stable and convex.*

Proof From Lemma 5, they are convex. First we prove that $\mathcal{V}_\rho$ is $S^+(T_\rho P \otimes T_\rho P)$-stable. It is sufficient to show that $V_\rho(M) + x \otimes x \in \mathcal{V}_\rho$ for any $M \in \mathcal{U}(T_\rho P)$,and $x \in \mathrm{tr}_{T_\rho P}$. We define an affine map S_x in the following way:

$$\begin{array}{rccc} S_x : & T_\rho P & \to & T_\rho P \\ & \Downarrow & & \Downarrow \\ & y & \mapsto & y + x \end{array} \tag{22}$$

Let the map $M_x := 1/2(M \circ S_x + M \circ S_{-x})$. As $E_{M_x} = 1/2((S_x)^{-1} + (S_{-x})^{-1})$, $M_x \in \mathcal{U}(T_\rho P)$.

$$\begin{aligned} V_\rho(M_x) &= \frac{1}{2} V_\rho(M \circ S_x) + \frac{1}{2}(M \circ S_{-x}) \\ &= \frac{1}{2} \int_{T_\rho P} (y - x) \otimes (y - x) + (y + x) \otimes (y + x) \, \mathrm{tr}_{\mathcal{H}}(M(\, dy)\rho) \\ &= \int_{T_\rho P} y \otimes y + x \otimes x \, \mathrm{tr}_{\mathcal{H}}(M(\, dy)\rho) \\ &= V_\rho(M) + x \otimes x. \end{aligned} \tag{23}$$

We obtain $V_\rho(M) + x \otimes x \in \mathcal{V}_\rho$. Similarly it is proved that $\mathcal{V}_{\rho,R}$ is $S^+(T_\rho P \otimes T_\rho P)$-stable. □

From the quantum Cramér-Rao inequality, we get the following relation:

$$\mathcal{V}_{\rho,R} \subset \mathcal{V}_\rho \subset \{J_\rho^S\}. \tag{24}$$

To characterize a L-stable set C, we define the following set $K(C)$.

By taking basis, it is easy to verify this.

Let g be a nonnegative inner product on $T_\rho P$, then $\inf_{M \in \mathcal{U}(T_\rho P)} \mathrm{tr}_{T_\rho P} V_\rho(M) g$ is called the attainable Cramér-Rao type bound, where $V_\rho(M) := \int_{T_\rho P} x \otimes x \, \mathrm{tr}_{\mathcal{H}}(M(\, dx)\rho)$ is the covariance matrix.

Next, we consider locally unbiased and random measurements (i.e. convex combinations of simple measurements). $P(T_\rho P \times T_\rho^* P)$ denotes the set of probability measures on $T_\rho P \times T_\rho^* P$. The element p of $P(T_\rho P \times T_\rho^* P)$ is regarded a random measurement as:

$$\begin{array}{rccc} M_m^T : & P(T_\rho P \times T_\rho^* P) & \to & \mathcal{M}(T_\rho P, \mathcal{H}) \\ & \bigcup & & \bigcup \\ & p & \mapsto & \int_{T_\rho P} \int_{T_\rho^* P} M^T(x, X) p(\, dx, \, dX) \end{array} \tag{16}$$

where,

$$\begin{array}{rccc} M^T : & T_\rho P \times T_\rho^* P & \to & \mathcal{M}(T_\rho P, \mathcal{H}) \\ & \bigcup & & \bigcup \\ & (x, X) & \mapsto & (M_X^T) \circ (x)^{-1} \end{array}$$

$$\begin{array}{rccc} (x) : & \mathbf{R} & \to & T_\rho P \\ & \bigcup & & \bigcup \\ & c & \mapsto & cx. \end{array}$$

Therefore, the set $\mathcal{U}_R(T_\rho P) := P(T_\rho P \times T_\rho^* P) \cap M_m^{T\,-1}(\mathcal{U}(T_\rho P))$ is regarded the set of locally unbiased and random measurements. The set $\mathcal{U}_R(T_\rho P)$ is independent of T.

Lemma 3 *For $p \in P(T_\rho P \times T_\rho^* P)$, p is a locally unbiased measurement iff*

$$\int_{T_\rho P} \int_{T_\rho^* P} \langle X, a(x) \rangle p(\, dx, \, dX) = \mathrm{tr}_{T_\rho P} \, a, \forall a \in \mathrm{End}(T_\rho P). \tag{17}$$

It is trivial from Lemma 2.

Lemma 4 *For $p \in P(T_\rho P \times T_\rho^* P)$, the covariance matrix of p is described as follows:*

$$V_\rho \circ M_m^T(p) = \int_{T_\rho P} \int_{T_\rho^* P} \| X \|^2 x \otimes x \; p(\, dx, \, dX). \tag{18}$$

Since $V_\rho \circ M_m^T$ is independent of T, $V_{\rho,R}$ denotes $V_\rho \circ M_m^T$.

Definition 6 *We define the sets of covariance matrices in the following:*

$$\begin{aligned} \mathcal{V}_\rho &:= \left\{ V_\rho(M) \in S^+(T_\rho P \otimes T_\rho P) \middle| M \in \mathcal{U}(T_\rho P) \right\} \\ \mathcal{V}_{\rho,R} &:= \left\{ V_{\rho,R}(p) \in S^+(T_\rho P \otimes T_\rho P) \middle| p \in \mathcal{U}_R(T_\rho P) \right\}, \end{aligned}$$

where $S(T_\rho P \otimes T_\rho P)$ denotes the symmetric tensor space of $T_\rho P \otimes T_\rho P$. $S^+(T_\rho P \otimes T_\rho P)$ denotes the set of nonnegative elements of $S(T_\rho P \otimes T_\rho P)$.

Lemma 5 *$\mathcal{V}_\rho$ and $\mathcal{V}_{\rho,R}$ are convex sets.*

Proof $\mathcal{U}(T_\rho P)$ and $\mathcal{U}_R(T_\rho P)$ are convex sets. V_ρ and M_m^T are affine maps. Then $\mathcal{V}_\rho$ and $\mathcal{V}_{\rho,R}$ are convex sets. □

For a proof see Ref. 6.

We define $\rho \circ X := \frac{1}{2}(\rho \cdot X + X \cdot \rho) \in \mathcal{T}_{sa}(\mathcal{H})$ for $X \in \mathcal{L}^2_{sa}(\rho)$. J^S_ρ denotes the inner product of the real Hilbert space $\mathcal{L}^2_{sa}(\rho)$. $\mathcal{L}^{2,*}_{sa}(\rho) := \{\rho \circ X | X \in \mathcal{L}^2_{sa}(\rho)\}$ is regarded as the dual of $\mathcal{L}^2_{sa}(\rho)$ in the following:

$$\begin{array}{ccc} \mathcal{L}^{2,*}_{sa}(\rho) \times \mathcal{L}^2_{sa}(\rho) & \to & \mathbf{R} \\ \bigcup & & \bigcup \\ (x, X) & \mapsto & \mathrm{tr}_{\mathcal{H}}\, xX. \end{array}$$

J^S_ρ can be regarded as an element of $\mathrm{Hom}_{sa}(\mathcal{L}^2_{sa}(\rho), \mathcal{L}^{2,*}_{sa}(\rho))$ by

$$\begin{array}{rccc} J^S_\rho : & \mathcal{L}^2_{sa}(\rho) & \to & \mathcal{L}^{2,*}_{sa}(\rho) \\ & \bigcup & & \bigcup \\ & X & \mapsto & \rho \circ X. \end{array} \tag{11}$$

Definition 2 *For a subset $\Theta \subset \mathbf{R}^n$ the map $f : \Theta \to \mathcal{T}_{sa}(\mathcal{H})$ is called a C^k-map, if the k-th derivative of f is well defined on the interior of Θ, where $\mathcal{T}_{sa}(\mathcal{H})$ is the set of selfadjoint trace class operators on $\mathcal{H}$.*

$\mathcal{T}^{+,1}_{sa}(\mathcal{H})$ denotes the set of $\{\rho \in \mathcal{T}_{sa}(\mathcal{H}) | \rho \geq 0,\ \mathrm{tr}_{\mathcal{H}}\, \rho = 1\}$.

Definition 3 *We call $P \subset \mathcal{T}^{+,1}_{sa}(\mathcal{H})$ an n-dimensional model, if there exist $\Theta \subset \mathbf{R}^n$ and $\phi : \Theta \to P$ such that ϕ is homeomorphism on the norm topology and C^1-map.*

In this paper, $\frac{\partial}{\partial \theta^i} \in T_\rho P$ is identified with $\frac{\partial \phi}{\partial \theta^i} \in \mathcal{T}_{sa}(\mathcal{H})$. In this identification, we assume that $T_\rho P$ is a subset of $\mathcal{L}^{2,*}_{sa}(\rho)$. For simplicity, we denote $J^\rho_S|_{T^*_\rho P}$ by J^ρ_S, too. $T^*_\rho P$ is identified with $J^{\rho,-1}_S(T_\rho P)$. The inner product $J^{\rho,-1}_S$ on $T_\rho P$ is called the *SLD inner product and $\| \ \|_S$ denotes this norm. In this paper, n denotes the dimension of $T_\rho P$. $\mathcal{M}(\Omega, \mathcal{H})$ denotes the set of generalized measurements on $\mathcal{H}$ whose measurable space is Ω. For $X \in \mathcal{L}^2_{sa}(\rho)$, M^T_X denotes the spectral decomposition of $T(X)$.

Definition 4 *An affine map E from $\mathcal{M}(T_\rho P, \mathcal{H})$ to $\mathrm{Hom}(\mathcal{T}_{sa}(\mathcal{H}), T_\rho P)$ is defined by*

$$E(M)(\tau) := \int_{T_\rho P} x\, \mathrm{tr}_{\mathcal{H}}\Big(M(\,dx)\tau\Big),\ \forall \tau \in \mathcal{T}_{sa}(\mathcal{H}). \tag{12}$$

Let us define the locally unbiasedness conditions.

Definition 5 *A measurement $M \in \mathcal{M}(T_\rho P, \mathcal{H})$ is called a locally unbiased measurement at $\rho \in P$, if the map $E(M) : \mathcal{T}_{sa}(\mathcal{H}) \to T_\rho P$ satisfies the following conditions:*

$$E(M)(\rho) = 0 \tag{13}$$

$$E(M)|_{T_\rho P} = \mathrm{Id}_{T_\rho P}\,. \tag{14}$$

$\mathcal{U}(T_\rho P)$ denotes the set of locally unbiased measurements on $\rho \in P$.

Lemma 2 *For $M \in \mathcal{M}(T_\rho P, \mathcal{H})$, the condition (14) is equivalent to the following equation:*

$$\int_{T_\rho P} \mathrm{tr}_{\mathcal{H}}\, a(x) M(\,dx) = \mathrm{tr}_{T_\rho P}\, a,\ \forall a \in \mathrm{End}(T_\rho P). \tag{15}$$

In §7, it is proved that when the dimension of quantum system is 2, any model satisfies the condition.

In general, $\langle\ ,\ \rangle$ denotes the linear pairing between a linear space and the dual. $\langle\ |\ \rangle$ means a inner product on a linear space.

2 SLD inner product and locally unbiased conditions

For $\rho \in \mathcal{T}_{sa}^{+}(\mathcal{H})$, the space $L_{sa}^{2}(\rho)$ is defined as follows, where $\mathcal{T}_{sa}^{+}(\mathcal{H})$ denotes the set of $\{\rho \in \mathcal{T}_{sa}(\mathcal{H}) | \rho \geq 0\}$.

Definition 1 *For $\rho \in \mathcal{T}_{sa}(\mathcal{H})$, $L_{sa}^{2}(\rho)$ consists of selfadjoint operators X on $\mathcal{H}$ satisfying the following conditions:*

$$\circ \quad \phi_j \in \mathcal{D}(X) \text{ with respect to } j \text{ such that } s_j \neq 0 \tag{1}$$

$$\circ \quad \langle X|X\rangle_{\rho}^{sa} := \sum_j s_j \langle X\phi_j | X\phi_j\rangle < \infty, \tag{2}$$

where $\rho = \sum_j s_j |\phi_j\rangle\langle\phi_j|$ is the spectral decomposition of ρ.

For $X, Y \in L_{sa}^{2}(\rho)$, define:

$$\langle X|Y\rangle_{\rho}^{sa} := \frac{1}{4}\Big(\langle X+Y|X+Y\rangle_{\rho}^{sa} - \langle X-Y|X-Y\rangle_{\rho}^{sa}\Big). \tag{3}$$

The inner product is called the SLD inner product, and $\|\ \ \|_{\rho}^{S}$ denotes the norm with respect to this inner product.

Lemma 1 *For $X \in L_{sa}^{2}(\rho)$, the following conditions are equivalent:*

$$\circ \quad \langle X|X\rangle_{\rho}^{sa} = 0 \tag{4}$$

$$\circ \quad X\rho + \rho X = 0 \tag{5}$$

$$\circ \quad X\rho X = 0 \tag{6}$$

$$\circ \quad \langle X|Y\rangle_{\rho}^{sa} = 0, \ \textit{for } \forall Y \in L_{sa}^{2}(\rho) \tag{7}$$

$$\circ \quad X\rho Y + Y\rho X = 0, \ \textit{for } \forall Y \in L_{sa}^{2}(\rho) \tag{8}$$

$\mathcal{L}_{sa}^{2}(\rho)$ denotes the quotient space $L_{sa}^{2}(\rho)/K_{sa}^{2}(\rho)$. From Lemma 1, for $X, Y \in \mathcal{L}_{sa}^{2}(\rho)$ the following are independent of a lifting T of the projection $L_{sa}^{2}(\rho) \to \mathcal{L}_{sa}^{2}(\rho)$:

$$\langle X|Y\rangle_{\rho}^{sa} := \langle T(X)|T(Y)\rangle_{\rho}^{sa} \tag{9}$$

$$\frac{1}{2}(X\rho Y + Y\rho X) := \frac{1}{2}(T(X)\rho T(Y) + T(Y)\rho T(X)). \tag{10}$$

Theorem 1 *If $\mathcal{H}$ is separable, $\mathcal{L}_{sa}^{2}(\rho)$ is a real Hilbert space with respect to the SLD inner product.*

A Linear Programming Approach to Attainable Cramér-Rao type Bounds and Randomness Condition

Masahito Hayashi
Department of Mathematics, Kyoto University, Kyoto 606-01, Japan
e-mail address: masahito@kusm.kyoto-u.ac.jp

Abstract

The author studies the Cramér-Rao type bound by a linear programming approach. By this approach, he found a necessary and sufficient condition that the Cramér-Rao type bound is attained by a random measurement. In a spin 1/2 system, this condition is satisfied.

1 Introduction

It is well-known that the lower bound of quantum Cramér-Rao inequality $V_\rho(M) \geq J_\rho^S$ cannot be attained unless all the SLDs commute, where we denote by $V_\rho(M)$ a covariance matrix for a state ρ by a measurement M, the SLD Fisher information matrix for a state ρ by J_ρ^S. We therefore often treat an optimization problem for $\mathrm{tr}\, gV_\rho(M)$ to be minimized, where g is an arbitrary real positive symmetric matrix. If there is a function C_ρ (possibly depending on g) such that $\mathrm{tr}\, gV_\rho \geq C_\rho$ holds for all M, C_ρ is called a Cramér-Rao type bound, or simply a CR bound. Our purpose is to find the most informative (i.e. attainable) CR bound under locally unbiasedness conditions.

There is a few model, in which the attainable Cramer-Rao type bound is calculated. To author's knowledge, there has been known only two mixed state models for which this optimization problem was explicitly solved. One is the estimation of complex amplitudes of coherent signals in Gaussian noise solved by Yuen and Lax, and Holevo. See Ref. 1. 2. Another one is the estimation of a 2-parameter spin 1/2 model solved by Nagaoka. See Ref. 3. Otherwise, recently pure state models have been studied on advanced level by Matsumoto, Fujiwara and Nagaoka. See Ref. 10. 4.

In two parameter case, Fujiwara and Nagaoka study the minimization problem for $\mathrm{tr}\, gV_\rho(M)$ in random measurements. See Ref. 10. In this paper, in multi-parameter case, this minimization problem is explicitly solved in §4.

Otherwise, in §3 and Appendix A, a technique to calculate the set $\{V_\rho(M)|M$ is locally unbiased measurement at $\rho\}$ is introduced.

In §5, a completely different approach to the optimization problem is given based on an infinite dimensional linear programming technique. See Ref 5. By this approach, the minimization problem is translated into the other maximization problem. In finite dimensional case, this maximization problem has the maximumvalue.

In §6, we drive a necessary and sufficient condition that the optimal measurement in §4 is the optimal under the locally unbiasedness conditions. This condition is called the randomness condition.