# Optimal sequence of POVMs in the sense of Stein's lemma in quantum hypothesis testing

**Masahito Hayashi**
**Laboratory for Mathematical Neuroscience, Brain Science Institute, RIKEN**
**2-1 Hirosawa, Wako, Saitama, 351-0198, Japan**

We propose an asymptotically optimal measurement for simple quantum hypothesis testing. As is mentioned the below, the quantum Stein's lemma is proved from Hiai-Petz result[1] and Ogawa-Nagaoka's result[2]. We give another proof of the quantum Stein's lemma from an information spectrum viewpoint. We consider a relation between the quantum Stein's lemma and the measurement proposed by Hayashi[3].

Let $\mathcal{H}$ be the Hilbert space of interest, and $\mathcal{S}(\mathcal{H})$ be the set of densities on $\mathcal{H}$. When we perform a measurement corresponding to POVM (Positive Operator Valued Measure) $M = \{M_i\}$ to the system in the state $\rho$, the data obeys the probability $\mathrm{P}_\rho^M = \{\mathrm{P}_\rho^M(i) = \operatorname{Tr} M_i \rho\}$. In particular, the POVM $M = \{M_i\}$ is called a PVM (Projection Valued Measure) if any $M_i$ is a projection. In the hypothesis testing, the testing is described by a 2-valued POVM $\{M_a, M_r\}$, where $M_a$ corresponds to accept and $M_r$ corresponds to reject. In the sequel, an operator $A$ satisfying $0 \le A \le \mathrm{I}$ is called a *test* identifying it with the POVM $\{M_a, M_r\} = \{A, \mathrm{I} - A\}$.

We introduce the quantum $n$-i.i.d. condition in order to treat an asymptotic setting. Suppose that $n$ independent physical systems are given in the same state $\rho$, then the quantum state of the composite system is described by $\rho^{\otimes n}$ defined by
$\rho^{\otimes n} := \underbrace{\rho \otimes \cdots \otimes \rho}_{n}$ on $\mathcal{H}^{\otimes n}$,
where the tensored space $\mathcal{H}^{\otimes n}$ is defined by
$\mathcal{H}^{\otimes n} := \underbrace{\mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n}$.
We call this condition the quantum $n$-i.i.d. condition, which is a quantum analogue of the independent-identical distribution condition. Under the quantum $n$-i.i.d. condition, the equation $D(\rho^{\otimes n} \| \sigma^{\otimes n}) = n D(\rho\|\sigma)$ holds, where $D(\rho\|\sigma)$ is the quantum relative entropy $\operatorname{Tr} \rho(\log \rho - \log \sigma)$.

Under the quantum $n$-i.i.d. condition, we study the hypothesis testing problem for the null hypothesis $H_0 : \rho^{\otimes n} \in \mathcal{S}(\mathcal{H}^{\otimes n})$ versus the alternative hypothesis $H_1 : \sigma^{\otimes n} \in \mathcal{S}(\mathcal{H}^{\otimes n})$, where $\rho^{\otimes n}$ and $\sigma^{\otimes n}$ are the $n$th-tensor powers of arbitrarily given density operators $\rho$ and $\sigma$ in $\mathcal{S}(\mathcal{H})$. In the sequel, an operator $A^n$ on $\mathcal{H}^{\otimes n}$ satisfying $0 \le A^n \le \mathrm{I}$ or a sequence $\{A^n\}$ of such operators, is called a *test*. For a test $A^n$ the error probabilities of the first and the second are, respectively, defined by

$$\alpha_n(A^n) = \operatorname{Tr} \rho^{\otimes n}(\mathrm{I} - A^n) \text{ and } \beta_n(A^n) = \operatorname{Tr} \sigma^{\otimes n} A^n.$$

We can understand that $\alpha_n(A^n)$ is the probability of erroneously rejecting $\rho^{\otimes n}$ when $\rho^{\otimes n}$ is true and $\beta_n(A^n)$ is the error probability of erroneously accepting $\rho^{\otimes n}$. when $\rho^{\otimes n}$ is not true. We discuss the trade-off of the two type error probabilities, under the quantum $n$-i.i.d. condition.

The following is well-known as quantum Stein's lemma.

**Theorem 1** *For any $1 > \epsilon > 0$, the equation*

$$\lim_{n\to\infty} \frac{1}{n} \log \beta_n^*(\epsilon) = -D(\rho\|\sigma) \tag{1}$$

*holds, where*

$$\beta_n^*(\epsilon) := \min\{\beta_n(A^n) | 0 \le A^n \le \mathrm{I}, \alpha_n(A^n) \le \epsilon\}. \tag{2}$$

The part of $\ge$ was proved by Hiai-Petz [1]. The infinite-dimensional case was proved by Petz [1]. The part of $\le$ is proved by Ogawa-Nagaoka[1]. The purpose of this paper follows: One is a construction of the testing whose 1st error probability goes to 0 and whose 2nd error probability goes to 0 with the decreasing rate $D(\rho\|\sigma)$. The other is giving another proof of Theorem 1 from an information spectrum method, which is initiated by Han-Verdú [4] and Han [5]. An application of the information spectrum method to quantum hypothesis testing was initiated by Nagaoka [6,7]. An information spectrum approach to exponents in quantum hypothesis testing was discussed by Nagaoka-Hayashi [8], which can be regarded as a quantum analogue of Han [9]. This work was motivated by Nagaoka[6,7].

# References

[1] F. Hiai and D. Petz, Commun. Math. Phys. 143, 99-114 (1991).
[2] T. Ogawa and H. Nagaoka, "Strong Converse and Stein's Lemma in the Quantum Hypothesis Testing," IEEE Trans. IT-46, 2428-2433 (2000). LANL e-print quant-ph/9906090, (1999).
[3] M. Hayashi, "Asymptotics of quantum relative entropy from a representation theoretical viewpoint," J. Phys. A: Math. and Gen. 34, 3413, (2001). LANL e-print quant-ph/9704040 (1997).
[4] T. S. Han and S. Verdú, "Approximation theory of output statistics," IEEE Trans. IT-39, 752-772 (1993).
[5] T. S. Han, Information-Spectrum Methods in Information Theory, Baifukan-Press, Tokyo, 1998 (in Japanese).
[6] H. Nagaoka, "On asymptotic theory of quantum hypothesis testing," Proceeding of Symposium "Statistical inference theory and its information theoretical aspect" 49-52, (1998) (in Japanese).
[7] H. Nagaoka, "Information Spectrum Theory of Quantum Hypothesis Testing," Proc. of the 22nd Symposium on Information Theory and Its Applications (SITA99), pp.245-247 (1999) (in Japanese).
[8] H. Nagaoka and M. Mayashi, "An Information-Spectrum Approach to Classical and Quantum Hypothesis Testing" UEC-IS-2000-5, IS Technical Reports, Univ. of Electro-Comm., (2000).
[9] T. S. Han, "Hypothesis testing with the general source," IEEE Trans. IT-46, 2415-2427 (2000).