数理解析研究所講究録
第 1834 巻 2013 年 68-76

Optimal Min-Max Tests for Quantum Hypothesis Testing Problems on Gaussian States

Wataru Kumagai

Graduate School of Information Sciences, Tohoku University, Graduate School of Mathematics, Nagoya University

Abstract

This paper is a summary of [1]. We formulate some problem on quantum hypothesis testing for special Gaussian states, which naturally appear in photonic systems. Moreover, we introduce an optimal test for each quantum hypothesis testing problem. Optimal tests are constructed by using group symmetry of Gaussian states and some results in classical hypothesis testing.

1 Gaussian state

We introduce Gaussian states on $\mathcal{H}=L^{2}(\mathbb{R})$, which represents a single-mode bosonic system and is spanned by sets $\{|k\rangle\}_{k\in \mathbb{Z}_{\geq 0}}$ of the k-th Hermitian functions $|k\rangle$. A most typical example of a single-mode bosonic system is the one-mode photonic system, in which the vector $|k\rangle$ is called the k-photon number state because it is regarded as the state corresponding to k photons. Then, the set $M_{N}=\{|k\rangle\langle k|\}_{k\in \mathbb{Z}_{\geq 0}}$, the *number measurement*, forms a positive-operator-valued measure (POVM). When the vector $|\xi)\in L^{2}(\mathbb{R})$ $(\xi\in \mathbb{C})$ is defined by

$$|\xi):=e^{-\frac{|\xi|^{2}}{2}}\sum_{k=0}^{\infty}\frac{\xi^{k}}{\sqrt{k!}}|k\rangle,$$

the state $|\xi)(\xi|$ is called a coherent state because it corresponds to coherent light in an optical system. Then, the *(special quasiclassical) Gaussian state* is defined as a Gaussian mixture of coherent states in the following way:

$$\rho_{\zeta,N}=\frac{1}{\pi N}\int_{\mathbb{C}}|\xi)(\xi|e^{-\frac{|\zeta-\xi|^{2}}{N}}d\xi,$$

where $\zeta\in \mathbb{C}$ and $N\in \mathbb{R}_{\geq 0}$. This is a special case of the general Gaussian state ([28]), but throughout this paper, we will use the term *Gaussian state* to refer to the quantum state having the above form. The mean parameter ζ and the number parameter N correspond, respectively, to the mean and variance of the Gaussian distribution. When the number measurement M_{N} is performed for the system with the Gaussian state $\rho_{\zeta,N}$, the measured value k is obtained with the probability

$$P_{\zeta,N}(k):=\langle k|\rho_{\zeta,N}|k\rangle=\frac{1}{N+1}\left(\frac{N}{N+1}\right)^{k}e^{-\frac{|\zeta|^{2}}{N+1}}L_{k}\left(-\frac{|\zeta|^{2}}{N(N+1)}\right), \tag{1}$$

where $L_{k}(x)=\displaystyle\sum_{j=0}^{k}\binom{k}{j}\frac{(-x)^{j}}{j!}$ is the k-th Laguerre polynomial.

It is known that there exist unitary operators W_ζ ($\zeta \in \mathbb{C}$) on $L^2(\mathbb{R})$ and U_n on $L^2(\mathbb{R})^{\otimes n}$ which satisfy the following.

$$W_{\zeta'}\rho_{\zeta,N}W_{\zeta'}^* = \rho_{\zeta+\zeta',N}, \tag{2}$$

$$U_n\rho_{\zeta,N}^{\otimes n}U_n^* = \rho_{\sqrt{n}\zeta,N} \otimes \rho_{0,N}^{\otimes(n-1)}. \tag{3}$$

We call the above unitary operators the displacement operator and concentrating operator, respectively.

2 Quantum hypothesis testing

In this section, we describe the formulation for quantum hypothesis testing.

2.1 Basic formulation for quantum hypothesis testing

In quantum hypothesis testing, in order to describe the null hypothesis H_0 and the alternative hypothesis H_1, we introduce two disjoint sets $\mathcal{S}_0$ and $\mathcal{S}_1$ of quantum states so that the unknown state ρ belongs to the union set $\mathcal{S} := \mathcal{S}_0 \cup \mathcal{S}_1$. Then, our problem is described in the following way:

$$H_0 : \rho \in \mathcal{S}_0 \quad vs. \quad H_1 : \rho \in \mathcal{S}_1.$$

We now apply a two-valued POVM $\{T_0, T_1\}$ to the quantum system with the unknown state to determine whether ρ belongs to $\mathcal{S}_0$ or $\mathcal{S}_1$. . In this method, we support the hypothesis H_i when the outcome is $i \in \{0, 1\}$. There are two types of decision error. The first is that we accept H_1 although H_0 is true, which is called a type I error. The second is to accept H_0 although H_1 is true, which is called a type II error.

Since an arbitrary two-valued POVM $\{T_0, T_1\}$ is represented by an operator $0 \leq T \leq I$ as $T_0 = I - T, T_1 = T$ where I is the identity operator, an operator $0 \leq T \leq I$ is called a *test (operator)* in hypothesis testing. Then, the probabilities of a type I or type II error are expressed as

$$\alpha_T(\rho) := \mathrm{Tr}\,\rho T \quad (\rho \in \mathcal{S}_0), \qquad \beta_T(\rho) := 1 - \mathrm{Tr}\,\rho T \quad (\rho \in \mathcal{S}_1). \tag{4}$$

A test with lower error probabilities is better, but the probabilities of type I and type II errors cannot be minimized simultaneously. Since there often exists a trade-off between the probabilities of type I and type II errors, we choose a permissible error constant $\alpha \in (0, 1)$ for the probability of a type I error; this is called the *(significance) level.* Hence, we consider tests T with level α, i.e., $\mathrm{Tr}\,T\rho \leq \alpha$ for all states $\rho \in \mathcal{S}_0$, and denote the set of tests T with level α as follows;

$$\mathcal{T}_\alpha := \{T | 0 \leq T \leq 1, \ \mathrm{Tr}\,T\rho \leq \alpha, \forall\rho \in \mathcal{S}_0\}. \tag{5}$$

A test T with level α is called a uniformly most powerful (UMP) test when the probability of type II error is the minimum among tests with level α, i.e., $\beta_T(\rho) \leq \beta_{T'}(\rho)$ for all states $\rho \in \mathcal{S}_1$ and for all tests $T' \in \mathcal{T}_\alpha$. UMP tests are often desirable in quantum hypothesis testing, but a UMP test may not exist when the null hypothesis H_1 is composite. Thus we need to modify this formulation.

The family of quantum states in a hypothesis testing problem often has parameters that are unrelated to the hypotheses. We call these unrelated parameters the nuisance parameters. For example, let us consider the following hypothesis testing problem of the number parameter N for a family of Gaussian states $\{\rho_{\zeta,N}\}_{\zeta\in\mathbb{C},N\in\mathbb{R}_{>0}}$:

$$H_0 : N \leq N_0 \ vs. \ H_1 : N > N_0,$$

where N_0 is a positive constant. In this case, the nuisance parameter is the mean parameter $\zeta \in \mathbb{C}$, which is unrelated to the number parameter N.

This situation can be formulated in the following way. It is assumed that our parameterized family is given as $\{\rho_{\theta,\xi}\}_{\theta\in\Theta,\xi\in\Xi}$, in which the parameter $\xi \in \Xi$ is the nuisance parameter and the parameter $\theta \in \Theta$ is related to our hypotheses. In order to formulate our problem, we assume that the parameter space Θ is given as the union of two disjoint subsets Θ_0 and Θ_1. When $\mathcal{S}_i = \{\rho_{\theta,\xi}\}_{\theta\in\Theta_i,\xi\in\Xi}$ for $i = 0, 1$, our problem is described in the following way:

$$H_0 : \theta \in \Theta_0 \ vs. \ H_1 : \theta \in \Theta_1 \ with \ \{\rho_{\theta,\xi}\}_{\theta\in\Theta,\xi\in\Xi}.$$

The min-max criterion for the nuisance parameter $\xi \in \Xi$ is based on the idea that it is better for a test to have a smaller maximum value of the probability of type II error among all nuisance parameters $\xi \in \Xi$. Then, the optimal test with level α is given as the test T_0 with level α satisfying the following equation:

$$\sup_{\xi\in\Xi} \beta_{T_0}(\rho_{\theta,\xi}) = \inf_{T\in\mathcal{T}_\alpha} \sup_{\xi\in\Xi} \beta_T(\rho_{\theta,\xi}) \quad (\forall\theta \in \Theta_1).$$

We call the above optimal test a *UMP min-max test* with level α. Note that a UMP min-max test coincides a UMP test when there are no nuisance parameters. Therefore the min-max criterion is a generalization of the optimality for a UMP test. Our main task, which we will do in the following sections, is to derive a UMP min-max test for various hypothesis testing problems for Gaussian states.

2.2 Invariance of the UMP min-max test

For a simple derivation of the optimal test, we sometimes focus on a unitary representation V of a group G on a Hilbert space $\mathcal{H}$. The unitary representation V is called *covariant* concerning the nuisance parameter space Ξ, when there is an action of group G to the nuisance parameter space Ξ such that

$$V_g \rho_{\theta,\xi} V_g^* = \rho_{\theta,g\cdot\xi}, \quad \forall\theta \in \Theta, \ \forall\xi \in \Xi, \ \forall g \in G. \tag{6}$$

Now, we impose the invariance for tests under the above covariance. A test T is called a *G invariant test* concerning a representation V if $V_g T V_g^* = T$ holds for any $g \in G$. A *UMP invariant test* is defined by an invariant test with the minimum type II error in the class of tests with level α. That is, an invariant test T with level α is called a UMP invariant test with level α when $\beta_T(\rho) \le \beta_{T'}(\rho)$ holds for all states $\rho \in \mathcal{S}_1$ and for all invariant tests $T' \in \mathcal{T}_\alpha$.

It is often easy to optimize the invariant test by virtue of the invariance, and accordingly, to derive the UMP invariant test. The quantum Hunt-Stein theorem guarantees that a UMP min-max test of level α is a UMP invariant test. The quantum Hunt-Stein theorem for a compact group was given by Holevo [27, 28] and for a noncompact case was shown by Bogomolov [7] and Ozawa [38], although it was not stated in the context of quantum hypothesis testing. In the following, we restate the quantum Hunt-Stein theorem as a theorem concerning the following testing problem with the min-max criterion:

$$H_0 : \theta \in \Theta_0 \ vs. \ H_1 : \theta \in \Theta_1 \ with \ \{\rho_{\theta,\xi}\}_{\theta\in\Theta,\xi\in\Xi} \tag{7}$$

for a family of quantum states $\{\rho_{\theta,\xi}\}_{\theta\in\mathbb{C},\xi\in\Xi}$ on $\mathcal{H}$ with a nuisance parameter ξ.

We state the quantum Hunt-Stein theorem for the noncompact case, which requires amenability for a group G. The definition and several properties of an amenable group are presented in [13, 8]. In particular, for a locally compact Hausdorff group G, it is known that there exists an asymptotic invariant probability measure on G if and only if G is amenable. Here, an asymptotic invariant probability measure $\{\nu_n\}$ on G is defined by a sequence of probability measures on G satisfying

$$\lim_{n\to\infty} |\nu_n(g \cdot B) - \nu_n(B)| = 0$$

for any $g \in G$ and any Borel set $B \subset G$. For example, all compact Lie groups are amenable groups. A finite-dimensional Euclid space $\mathbb{R}^n$ and the whole $\mathbb{Z}$ of integers are also amenable groups.

In addition, we need completeness of a family of quantum states. A family of quantum states is called complete if for any bounded linear operator X the following equivalence holds:

$$\mathrm{Tr}(\rho X) = 0 \ (\forall \rho \in \mathcal{S}) \quad \Longleftrightarrow \quad X = 0.$$

For example, the entirety of pure states on a finite-dimensional quantum system and the Gaussian states $\{\rho_{\zeta,N}\}_{\zeta\in\mathbb{C}}$ are complete for any $N > 0$.

Theorem 1 (*Quantum Hunt-Stein theorem [7], [38]*) *Let $\mathcal{S}$ be a complete family of quantum states on a Hilbert space $\mathcal{H}$ of at most countable dimension. When a unitary representation of an amenable group G satisfies the covariant condition* (6) *concerning the nuisance parameter space Ξ, the following equations hold.*

$$\inf_{\tilde{T}\in\mathcal{T}_{\alpha,V}} \sup_{\xi\in\Xi} \beta_{\tilde{T}}(\rho_{\theta,\xi}) = \inf_{T\in\mathcal{T}_{\alpha}} \sup_{\xi\in\Xi} \beta_{T}(\rho_{\theta,\xi}) \quad (\forall\theta\in\Theta_1),$$
$$\inf_{\tilde{T}\in\mathcal{T}_{\alpha,u,V}} \sup_{\xi\in\Xi} \beta_{\tilde{T}}(\rho_{\theta,\xi}) = \inf_{T\in\mathcal{T}_{\alpha,u}} \sup_{\xi\in\Xi} \beta_{T}(\rho_{\theta,\xi}) \quad (\forall\theta\in\Theta_1).$$

Theorem 1 yields that a UMP (unbiased) invariant test T_0 with level α for (7) is a UMP (unbiased) min-max test with level α under the assumption in Theorem 1.

2.3 Reduction methods on quantum hypothesis testing problems

A realistic quantum hypothesis testing problem often has a complicated structure, and it is necessary to simplify it. The following theorem is very useful to obtain optimal tests for several hypothesis testing problems.

Theorem 2 *Let $\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_3$ be Hilbert spaces with at most countable dimension, and*

$$\mathcal{S}_1 := \{\rho_{\theta,\xi_1}\}_{\theta\in\Theta,\xi_1\in\Xi_1}, \mathcal{S}_2 := \{\rho_{\xi_2}\}_{\xi_2\in\Xi_2}, \mathcal{S}_3 := \{\rho_{\theta,\xi_1,\xi_3}\}_{\theta\in\Theta,\xi_1\in\Xi_1,\xi_3\in\Xi_3}$$

be families of quantum states on $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$, respectively. We assume that V is an irreducible representation of an amenable group G on $\mathcal{H}_3$ and is covariant concerning the nuisance parameter space $\Xi_1 \times \Xi_3$ of the family of quantum states $\{\rho_{\theta,\xi_1,\xi_3}\}_{\theta\in\Theta,\xi_1\in\Xi_1,\xi_3\in\Xi_3}$. In addition, if G is noncompact, we assume that the family of quantum states $\{\rho_{\theta,\xi_1} \otimes \rho_{\theta,\xi_1,\xi_3}\}_{\theta\in\Theta,\xi_1\in\Xi_1,\xi_3\in\Xi_3}$ is complete. Then, the following equivalent relation holds.

A test T is a UMP (unbiased) min-max test with level α for

$$H_0 : \theta \in \Theta_0 \ vs. \ H_1 : \theta \in \Theta_1 \ with \ \{\rho_{\theta,\xi_1}\}_{\theta\in\Theta,\xi_1\in\Xi_1} \tag{8}$$

if and only if a test $U^*(T \otimes I_{\mathcal{H}_2} \otimes I_{\mathcal{H}_3})U$ is a UMP (unbiased) min-max test with level α for

$$H_0 : \theta \in \Theta_0 \ vs. \ H_1 : \theta \in \Theta_1 \ with \ \{U^*(\rho_{\theta,\xi_1} \otimes \rho_{\xi_2} \otimes \rho_{\theta,\xi_1,\xi_3})U\}_{\theta\in\Theta,\xi_1\in\Xi_1,\xi_2\in\Xi_2,\xi_3\in\Xi_3}, \tag{9}$$

where U is a unitary operator on $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$.

In addition, when $\mathcal{H}_3$ is the empty set ϕ, a test T is a UMP (unbiased, min-max) test with level α for (8) *if and only if a test $U'^*(T \otimes I_{\mathcal{H}_2})U'$ is a UMP (unbiased, min-max) test with level α for*

$$H_0 : \theta \in \Theta_0 \ vs. \ H_1 : \theta \in \Theta_1 \ with \ \{U'^*(\rho_{\theta,\xi_1} \otimes \rho_{\xi_2})U'\}_{\theta\in\Theta,\xi_1\in\Xi_1,\xi_2\in\Xi_2}, \tag{10}$$

where U' is a unitary operator on $\mathcal{H}_1 \otimes \mathcal{H}_2$.

The above reduction theorem and the Hunt-Stein theorem play essential roles to derive optimal tests in section 3 and 4.

3 Hypothesis testing of the mean parameter

We now consider the hypothesis testing problem for the mean parameter of the Gaussian states.

We consider the hypothesis testing problem

$$H_0 : |\zeta| \in [0, R_0] \ vs. \ H_1 : |\zeta| \in (R_0, \infty) \ with \ \{\rho_{\zeta,N}^{\otimes n}\}_{\zeta\in\mathbb{C}} \tag{H-1}$$

for $1 \leq n \in \mathbb{N}$ and $R_0 \in \mathbb{R}_{\geq 0}$ when the number parameter N is fixed. That is, we suppose that the number parameter N is known. Then, the nuisance parameter space is $S^1 = \{a \in \mathbb{C} | |a| = 1\}$, which represents the phase of the mean parameter ζ. The UMP test for (H-1) does not exist. Thus, our purpose is to derive a UMP min-max test. Here, we define a test $T_{R,N}^{[A],\alpha}$ for $R \in \mathbb{R}_{\geq 0}$ by

$$T_{R,N}^{[A],\alpha} := \gamma_R |k_R\rangle\langle k_R| + \sum_{k=k_R+1}^{\infty} |k\rangle\langle k|,$$

where $k_R \in \mathbb{Z}_{\geq 0}$, and $0 < \gamma_R \leq 1$ is determined by level α as

$$1 - \sum_{k=0}^{k_R} P_{R,N}(k) < \alpha \leq 1 - \sum_{k=0}^{k_R-1} P_{R,N}(k), \tag{11}$$

$$\gamma_R := \frac{\alpha - \left(1 - \sum_{k=0}^{k_R} P_{R,N}(k)\right)}{P_{R,N}(k_R)}, \tag{12}$$

where $P_{R,N}$ is the probability distribution in (1).

Theorem 3 *For the hypothesis* (H-1), *the test*

$$T_{\alpha,R_0,N}^{[1],n} := U_n^*(T_{\sqrt{n}R_0,N}^{[A],\alpha} \otimes I^{\otimes(n-1)})U_n \tag{13}$$

is a UMP min-max test with level α.

Next, we consider the hypothesis testing problem

$$H_0 : |\zeta| \in [0, R_0] \ vs. \ H_1 : |\zeta| \in (R_0, \infty) \ with \ \{\rho_{\zeta,N}^{\otimes n}\}_{\zeta\in\mathbb{C}, N\in\mathbb{R}_{>0}} \tag{H-2}$$

for $2 \leq n \in \mathbb{N}$ and $R_0 \in \mathbb{R}_{\geq 0}$. But it is difficult to derive an optimal test for the above hypothesis testing problem for an arbitrary $R_0 \in \mathbb{R}_{\geq 0}$ since the number parameter N is unknown. Hence, we consider the hypothesis testing problem (H-2) at $R_0 = 0$:

$$H_0 : |\zeta| \in \{0\} \ vs. \ H_1 : |\zeta| \in (0, \infty) \ with \ \{\rho_{\zeta,N}^{\otimes n}\}_{\zeta\in\mathbb{C}, N\in\mathbb{R}_{>0}}.$$

We define a test $T_\alpha^{[t],n}$ by

$$T_\alpha^{[t],n} = \sum_{k=(k_0,\cdots,k_n)\in\mathbb{Z}_{\geq 0}^{n+1}} \varphi'^{(n)}(k)|k\rangle\langle k|$$

where the test function

$$\varphi'^{(n)}(k) := \begin{cases} 0 & (k_0 < c(s(k))) \\ \gamma(s(k)) & (k_0 = c(s(k))) \\ 1 & (k_0 > c(s(k))) \end{cases}$$

depends on the total count $s(k) := \sum_{j=0}^{n} k_j$ of $k = (k_0, \cdots, k_n)$, and functions

$$c : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}, \ \gamma : \mathbb{Z}_{\geq 0} \to (0, 1] \tag{14}$$

are determined as

$$\sum_{l=c(s)+1}^{s} \binom{s-l+n-1}{n-1} < \alpha \binom{s+n}{n} \leq \sum_{l=c(s)}^{s} \binom{s-l+n-1}{n-1} , \tag{15}$$

$$\gamma(s) := \frac{\alpha\binom{s+n}{n} - \sum_{l=c(s)+1}^{s} \binom{s-l+n-1}{n-1}}{\binom{s-c(s)+n-1}{n-1}} \tag{16}$$

for each total count $s \in \mathbb{Z}_{\geq 0}$.

Theorem 4 *For the hypothesis* (H-2) *at* $R_0 = 0$, *the test*

$$T_\alpha^{[2],n} := U_n^* T_\alpha^{[t],n-1} U_n \tag{17}$$

is a UMP unbiased min-max test with level α.

It is not known if there exists an optimal test for the hypothesis testing problem (H-2) when $R_0 \neq 0$. This quantum hypothesis testing problem is analogous to the classical hypothesis testing problem for the size of the mean parameter of the Gaussian distribution with unknown variance. The problem is called the bioequivalence problem [9], and it is not known if there is an optimal test for it. But the problem appears in several situations, including medicine and pharmacy, and a solution is hoped for due to the demand of not only the theoretical aspect but also the practical aspect. The problem (H-2) is expected to be important for quantum hypothesis testing because of the importance of the bioequivalence problem.

4 Hypothesis testing of the number parameter

We now consider the hypothesis testing problem for the number parameter of Gaussian states.

We treat the hypothesis testing problem

$$H_0 : N \in [0, N_0] \ vs. \ H_1 : N \in (N_0, \infty) \ with \ \{\rho_{\zeta,N}^{\otimes n}\}_{N \in \mathbb{R}_{>0}} \tag{H-5}$$

for $1 \leq n \in \mathbb{N}$ and $N \in \mathbb{R}_{>0}$ when the mean parameter ζ is fixed. That is, we suppose that the mean parameter ζ is known.

The test function $\varphi : \mathbb{Z}_{\geq 0}^n \to [0, 1]$ is defined by

$$\varphi(k) := \begin{cases} 0 & (X_1(k) < K_0) \\ \gamma & (X_1(k) = K_0) \\ 1 & (X_1(k) > K_0), \end{cases} \tag{18}$$

where $X_1(k) := \sum_{j=1}^n k_j$ for $k = (k_1, \cdots, k_n) \in \mathbb{Z}_{\geq 0}^n$, and the constants $K_0 \in \mathbb{Z}_{\geq 0}$ and $\gamma \in (0, 1]$ are uniquely determined by

$$\begin{aligned} 1 - \sum_{K=0}^{K_0} \binom{K+n-1}{n-1} \left(\frac{1}{N_0+1}\right)^n \left(\frac{N_0}{N_0+1}\right)^K &< \alpha \\ \leq 1 - \sum_{K=0}^{K_0-1} \binom{K+n-1}{n-1} \left(\frac{1}{N_0+1}\right)^n \left(\frac{N_0}{N_0+1}\right)^K &, \end{aligned} \tag{19}$$

$$\gamma := \frac{\alpha - \left(1 - \sum_{K=0}^{K_0} \binom{K+n-1}{n-1} \left(\frac{1}{N_0+1}\right)^n \left(\frac{N_0}{N_0+1}\right)^K\right)}{\binom{K_0+n-1}{n-1} \left(\frac{1}{N_0+1}\right)^n \left(\frac{N_0}{N_0+1}\right)^{K_0}}. \tag{20}$$

Then we define a test as follows.
$$T^{[x^2],n}_{\alpha,N_0} := \sum_{k\in\mathbb{Z}^n_{\geq 0}} \varphi(k)|k\rangle\langle k|$$

Theorem 5 *For the hypothesis testing problem* (H-5)*, the test*
$$T^{[5],n}_{\alpha,\zeta,N_0} := (W^{\otimes n}_{-\zeta})^* T^{[x^2],n}_{\alpha}(W^{\otimes n}_{-\zeta}) \tag{21}$$
is a UMP test with level α.

Next, we consider the hypothesis testing problem
$$H_0 : N \in (0, N_0] \ vs. \ H_1 : N \in (N_0, \infty) \ with \ \{\rho^{\otimes n}_{\zeta,N}\}_{\zeta\in\mathbb{C},N\in\mathbb{R}_{>0}} \tag{H-6}$$
for $2 \leq n \in \mathbb{N}$ and $N \in \mathbb{R}_{>0}$. The nuisance parameter space is $\mathbb{C}$.

Theorem 6 *For the hypothesis testing problem* (H-6)*, the test*
$$T^{[6],n}_{\alpha,N_0} := U^*_n(I \otimes T^{[x^2],n-1}_{\alpha})U_n \tag{22}$$
is a UMP test with level α.

5 Conclusion

We have treated several composite quantum hypothesis testing problem with nuisance parameters in the quantum Gaussian system. Moreover, we have established a general theorem for reducing complicated problems to fundamental problems (Theorem 2). In both deriving optimal tests and reducing complicated problems, group symmetry played important roles, in which the quantum Hunt-Stein Theorem was applied. Since the Gaussian state in quantum system corresponds to the Gaussian distribution in a classical system, our testing problems for Gaussian states plays the same role as do the testing problems for Gaussian distributions in the classical hypothesis setting.

Acknowledgment

This is joint work with Prof. Masahito Hayashi. The author would like to thank Prof. Fumio Hiai for providing us with a proof of the weak compactness theorem, and Dr. Masaki Owari for the realization of the displacement operation in an optical system. The author acknowledges support from Grant-in-Aid for JSPS Fellows No. 233283.

References

[1] Kumagai, W., Hayashi, M.: *Quantum hypothesis testing for Gaussian states: Quantum analogues of chi-square, t-, and F-tests.* arXiv:1110.6255 (2012)

[2] Aspachs, M., Calsamiglia, J., Munoz-Tapia, R., Bagan, E.: Phase estimation for thermal Gaussian states. Phys. Rev. A **79**, 033834 (2009)

[3] Audenaert, K.M.R., Calsamiglia, J., Masanes, Ll., Munoz-Tapia, R., Acin, A., Bagan, E., Verstraete, F.: Discriminating states: the quantum Chernoff bound. Phys. Rev. Lett. **98**, 160501 (2007)

[4] Audenaert, K.M.R., Nussbaum, M., Szkola, A., Verstraete, F.: Asymptotic Error Rates in Quantum Hypothesis Testing. Comm. Math. Phys. **279**, 251-283 (2008)

[5] Amari, S., Nagaoka, H.: *Methods of Information Geometry.* Transl. Math. Monographs **191**: Amer. Math. Soc. (2000)

[6] Bagan, E., Ballester, M.A., Gill, R.D., Monras, A., Munoz-Tapia, R.: Optimal full estimation of qubit mixed states,. Phys. Rev. A **73**, 032301 (2006)

[7] Bogomolov, N.A.: Minimax measurements in a general statistical decision theory. Theor. Prob. Appl. Vol. **26**, no. 4, 787-795. (1982)

[8] Bondar, J.V., Mitnes, P.: Amenability: A Survey for Statistical Applications of Hunt-Stein and Related Conditions on Groups. Z. Wahrscheinlichkeitstheorie verw. Gebiete **57**, 103-128 (1981)

[9] Brown, L.D., Hwang, J.T.G., Munk, A.: An unbiased test for the bioequivalence problem. Ann. Statist. **25** 2345-2367 (1997)

[10] Guta, M., Butucea, C.: Quantum U-statistics. J. Math. Phys. **51**, 102202 (2010)

[11] Gurland, J., Chen, E. E., Hernandez, F.M.: A new discreate distribution involving Laguerre polynomials. Comm Statist A **12** (1983)

[12] Gradshteyn, I.S., Ryzhik, I.M., Jeffrey, A.: *Table of Integrals, Series, and Products.* Seventh Edition, (1994)

[13] Greenleaf, F.P.: *Invariant means on topological groups and their applications.* Van Nostrand Reinhold (1969)

[14] Guta, M., Jencova, A.: Local asymptotic normality in quantum statistics. Commun. Math. Phys., **276**, 341-379 (2007)

[15] Kahn, J., Guta, M.: Local asymptotic normality for finite dimensional quantum systems. Commun. Math. Phys. **289**, 597-652 (2009)

[16] Guta, M., Kahn, J.: Local asymptotic normality for qubit states. Phys. Rev. A, **73**, 052108 (2006)

[17] Hayashi, M.: Group theoretical study of LOCC-detection of maximally entangled states using hypothesis testing. New J. of Phys. vol.**11**, 043028 (2009)

[18] Hayashi, M.: *Quantum estimation and the quantum central limit theorem.* American Mathematical Society Translations Series 2, Vol. **277**, 95 - 123 (2009).

[19] Hayashi, M.: Error exponent in asymmetric quantum hypothesis testing and its application to classical-quantum channel coding. Phys. Rev. A **76**, 062301 (2007)

[20] Hayashi, M.: *Quantum Information: An Introduction.* Springer-Verlag, (2006)

[21] Hayashi, M.: Optimal sequences of quantum measurements in the sense of Stein's lemma in quantum hypothesis testing. J. Phys. A: Math. Gen., vol. **35**, pp. 10759-0773, (2002)

[22] Hayashi, M., Matsumoto, K.: Asymptotic performance of optimal state estimation in qubit system. Journal of Mathematical Physics, Vol.**49**, 102101 (2008); quant-ph/0411073.

[23] Hayashi, M., Matsumoto, K., Tsuda, Y.: A study of LOCC-detection of a maximally entangled state using hypothesis testing J. Phys. A: Math. Gen. **39** 14427-14446 (2006)

[24] Hayashi, M.: Asymptotic estimation theory for a finite dimensional pure state model. Journal of Physics A: Mathematical and General, **31**, No.20, pp.4633-4655 (1998).

[25] Hiai, F., Mosonyi, M., Hayashi, M.: Quantum hypothesis testing with group symmetry. J. Math. Phys. **50**, 103304 (2009)

[26] Helstrom, C.W.: *Quantum Detection and Estimation Theory.* Academic Press, New York, (1976)

[27] Holevo, A.S.: Covariant measurements and uncertainty relations. Rep. Math. Phys., **16**, 385-400, (1979)

[28] Holevo, A.S.: *Probabilistic and Statistical Aspects of Quantum Theory.* North-Holland, Amsterdam, (1982)

[29] Holevo, A.S.: *An analog of the theory of statistical decisions in noncommutative theory of probability.* Trudy Moskov. Mat. Obšč., vol. **26**, 133-149 (1972) (English translation is Trans. Moscow Math. Soc., vol. 26, 133-149 (1972))

[30] Massar, S., Popescu, S.: Optimal Extraction of Information from Finite Quantum Ensembles. Phys. Rev. Lett. **74**, 1259 (1995)

[31] Walls, D.F., Milburn, G.J.: *Quantum Optics* Springer-Verlag; 2nd edition (2008)

[32] Mosonyi, M.: Hypothesis testing for Gaussian states on bosonic lattices. J. Math. Phys. **50**, 032105 (2009)

[33] Nagaoka, H.: *The converse part of the theorem for quantum Hoeffding bound.* e-print arXiv:quant-ph/0611289.

[34] Ogawa, T., Nagaoka, H.: Strong converse and Stein's lemma in quantum hypothesis testing. IEEE Trans. Inf. Theory **46**, 2428-2433 (2000)

[35] Yuen, H.P., Lax, M.: Multiple-parameter quantum estimation and measurement of nonselfadjoint observables. IEEE Trans. Inform. Theory, IT-**19**, 740-750 (1973)

[36] Lehmann, E.L.: *Testing statistical hypotheses.* Springer; 2nd edition, (1997)

[37] Nussbaum, M., Szkola, A.: The Chernoff lower bound for symmetric quantum hypothesis testing. Ann. Stat. **37**, 1040 (2009)

[38] Ozawa, M.: *On the noncommutative theory of statistical decision.* Research Reports on Information Sciences (1980)

[39] Petz, D.: *An invitation to the algebra of canonical commutation relations.* Leuven notes in mathematical and theoretical physics, vol. **2**, series A (1990)