proceedings

MDPI

Proceedings

Privacy in Quantum Estimation †

Milajiguli Rexiti [1,2,*,‡] and Stefano Mancini [3,‡]

1 Department of Mathematics and Physics, Xinjiang Agricultural University, 830053 Urumqi, China
2 School of Advanced Studies, University of Camerino, 62032 Camerino, Italy
3 School of Science and Technology, University of Camerino, 62032 Camerino, Italy; stefano.mancini@unicam.it
* Correspondence: milajiguli.milajiguli@unicam.it
† Presented at the 11th Italian Quantum Information Science conference (IQIS2018), Catania, Italy, 17–20 September 2018.
‡ These authors contributed equally to this work.

Published: 25 June 2019

Abstract: We introduce the notion of privacy in quantum estimation by considering an one-parameter family of isometries taking one input into two output systems. It stems on the separate and adversarial control of the two output systems as well as on the local minimization of the mean square error. Applications to two-qubit unitaries (with one qubit in a fixed input state) are presented.

Keywords: quantum information; quantum measurement theory; decoherence

1. Introduction

Parameter estimation is becoming important in quantum information processing which takes place by quantum channel maps (see e.g., [1]). It is well known that any quantum channel admits an isometry as a dilation [2]. Hence we can conceive the estimation of a family of isometries *through* quantum channels. This models a realistic situation where not all information concerning the measured systems is accessible. More precisely, given a one parameter family of isometries $\{V_\alpha^{A\to BF}\}$, we consider the parameter α's estimation by accessing only the system B. This amounts to use the quantum channel between A and B of which $V_\alpha^{A\to BF}$ represents the Stinespring dilation [2].

In communication theory channels are also characterized by their privacy [3]. This notion captures the ability to convey more information through the channel than the one that is lost into environment. To link this notion with estimation we assume system F is under control of a malicious being. Then the problem we are facing with becomes of what are the conditions under which a legitimate user controlling the B system (besides A ones) can perform a better estimation. We address this issue by minimizing mean square error.

2. Private Quantum Estimation

Consider a family of isometries $V_\alpha : \mathscr{H}_A \to \mathscr{H}_B \otimes \mathscr{H}_F$, which is parametrized by $\alpha \in \mathscr{I} \subset \mathbb{R}$. Assume parameter α has an a priori probability distribution function $p(\alpha)$ over $\mathscr{I}$, the probe system A is prepared in the state ρ_A. Then the output on B reads

$$\rho_B(\alpha) = \mathrm{Tr}_F\left(V_\alpha \rho_A V_\alpha^\dagger\right) =: \mathcal{N}(\rho_A). \tag{1}$$

We perform measurement on this state, and estimate of the unknown parameter α using the measurement outcome. As goodness of this process, we consider average quadratic cost function:

$$\bar{C}^B := \int_{\mathscr{I}} p(\alpha)\mathrm{Tr}\left[\rho_B(\alpha)\left(\hat{S}_B - \alpha I\right)^2\right] d\alpha, \tag{2}$$

where $\hat{S}_B$ is the measurement operator used to estimate α. The best of such operator is obtained by minimizing $\bar{C}^B$. Personik's theorem [4] provided the solution to this optimization problem through the following operator equation

$$W_B^{(0)}\hat{S}_B + \hat{S}_B W_B^{(0)} = 2W_B^{(1)}, \tag{3}$$

where $W_B^{(0)} := \int_{\mathscr{J}} p(\alpha)\rho_B(\alpha)d\alpha$ and $W_B^{(1)} := \int_{\mathscr{J}} \alpha\, p(\alpha)\rho_B(\alpha)d\alpha$. On the other hand we can consider the state emerging from the channel complementary to $\mathcal{N}$ in Equation (1), namely

$$\rho_F(\alpha) = \mathrm{Tr}_B\left(V_\alpha \rho_A V_\alpha^\dagger\right) =: \widetilde{\mathcal{N}}(\rho). \tag{4}$$

If this is controlled by an adversary, a strategy similar to the above can be employed to estimate α and leading to $\bar{C}^F_{min}$ with a suitable optimal measurement $\hat{S}_F$.

By considering the system B (as well as A) hold by a legitimate user, we define the *privacy of estimation* through the difference between the minimum of the average quadratic cost functions

$$\mathcal{P}_e := \max\left\{\bar{C}^F_{min} - \bar{C}^B_{min}, 0\right\}. \tag{5}$$

Whenever it results positive, it means that $\bar{C}^B_{min} < \bar{C}^F_{min}$ and hence B can better estimate α than F. This definition of the privacy assumes that the adversary can control the system F and at the same time has information about the input state. A weaker notion of privacy can be introduced by assuming the adversary with no information about the input state. This amounts to consider $\bar{C}^F_{min}$ in (5) averaged overall possible input states.

3. Application to Two-Qubit Unitaries

For a two-qubit system we consider $V_\alpha = U_\alpha|0\rangle_E$, where $U_\alpha : \mathscr{H}_A \otimes \mathscr{H}_E \to \mathscr{H}_B \otimes \mathscr{H}_F$ ($\mathscr{H}_A = \mathscr{H}_E = \mathscr{H}_B = \mathscr{H}_F \simeq \mathbb{C}^2$) are entangling unitaries that can be parameterized as [5]:

$$U(\alpha_x, \alpha_y, \alpha_z) = \exp\left[-\frac{i}{2}\left(\alpha_x \sigma_x \otimes \sigma_x + \alpha_y \sigma_y \otimes \sigma_y + \alpha_z \sigma_z \otimes \sigma_z\right)\right], \tag{6}$$

with the parameter space

$$\mathscr{S} = \left\{(\alpha_x, \alpha_y, \alpha_z) : \frac{\pi}{2} \geq \alpha_x \geq \alpha_y \geq \alpha_z \geq 0\right\}. \tag{7}$$

The state in the system A (probe's state) will be generically considered as

$$\rho_A = \left(\sqrt{x}\,|0\rangle + e^{i\varphi}\sqrt{1-x}\,|1\rangle\right)\left(\sqrt{x}\,\langle 0| + e^{-i\varphi}\sqrt{1-x}\,\langle 1|\right), \tag{8}$$

with $x \in [0,1]$ and $\varphi \in [0, 2\pi]$. Below we will consider the estimation of a single parameter be either α_x or α_y or α_z, by assuming the values of the other two to be known. To this end the states ρ_B of Equation (1) and ρ_F of Equation (4) can be readily calculated. There, the parameter φ appears as added to α_z. Thus it has no effect in the estimation of the latter. But it can affect the estimation of α_x and α_y.

(i) **Estimation of** α_z. We took 325 points in the region $0 \leq \alpha_y \leq \alpha_x \leq \frac{\pi}{2}$ and for each point we estimated α_z through ρ_B and independently through ρ_F. This is done by also optimizing the privacy (5) over the probe's state, i.e., by considering

$$\mathcal{P}_e(\alpha_x, \alpha_y) = \max\left\{\max_x\left[\bar{C}^F_{min}(\alpha_x, \alpha_y, x) - \bar{C}^B_{min}(\alpha_x, \alpha_y, x)\right], 0\right\}, \tag{9}$$

whose contour plot is reported in Figure 1.

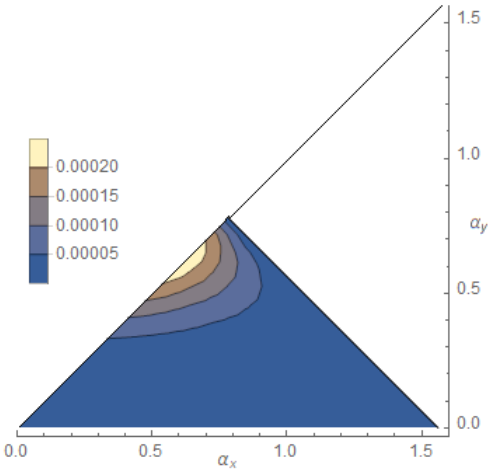

Figure 1. Contour plot of the privacy $\mathcal{P}_e$ for estimating α_z.

On the line $\alpha_x + \alpha_y = \frac{\pi}{2}$ we have $\bar{C}^B_{min} = \bar{C}^F_{min}$ and this divides the region $0 \leq \alpha_y \leq \alpha_x \leq \frac{\pi}{2}$ into two triangles. Only in the lower one the estimation is private (in the upper one $\bar{C}^F_{min}$ results smaller than $\bar{C}^B_{min}$). Furthermore there is a specific and small region where the privacy increases with respect to the background.

(ii) **Estimation of** α_y. In this case we took 325 points in the region $0 \leq \alpha_z \leq \alpha_x \leq \frac{\pi}{2}$, and for each point we estimated α_y through ρ_B and independently through ρ_F likewise the previous case. Then we evaluated the privacy

$$\mathcal{P}_e(\alpha_x, \alpha_z) = \max\left\{\max_{x,\varphi}\left[\bar{C}^F_{min}(\alpha_x, \alpha_z, x, \varphi) - \bar{C}^B_{min}(\alpha_x, \alpha_z, x, \varphi)\right], 0\right\}, \tag{10}$$

whose contour plot is reported in Figure 2. Notice that although $\bar{C}^B_{min}$ can be made zero by choosing $\alpha_z = \alpha_x$[1], this does not give the maximum privacy since in such a case also $\bar{C}^F_{min}$ turns out to be zero. The maximum privacy is obtained when α_z decrease to 0 and α_x increase to $\pi/2$.

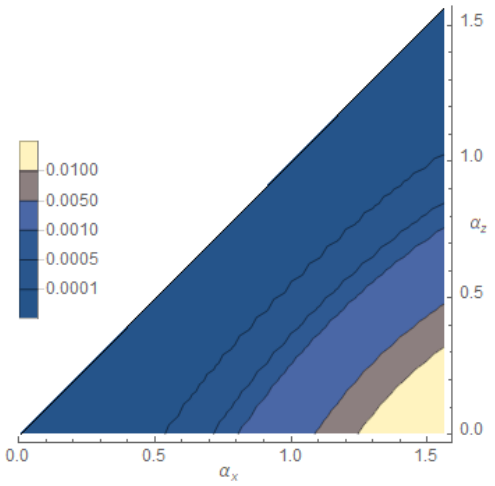

Figure 2. Contour plot of the privacy $\mathcal{P}_e$ for estimating α_y.

[1] This choice by virtue of (7) forces α_y to be exactly determined.

(iii) **Estimation of** α_x. In this last case we took 325 points in the region $0 \leq \alpha_z \leq \alpha_y \leq \frac{\pi}{2}$ and for each point we estimated α_x through ρ_B and independently through ρ_F. We actually computed

$$\mathcal{P}_e(\alpha_y, \alpha_z) = \max\left\{\max_{x,\varphi}\left[\bar{C}^F_{min}(\alpha_y, \alpha_z, x, \varphi) - \bar{C}^B_{min}(\alpha_y, \alpha_z, x, \varphi)\right], 0\right\}, \tag{11}$$

whose contour plot is shown in Figure 3.

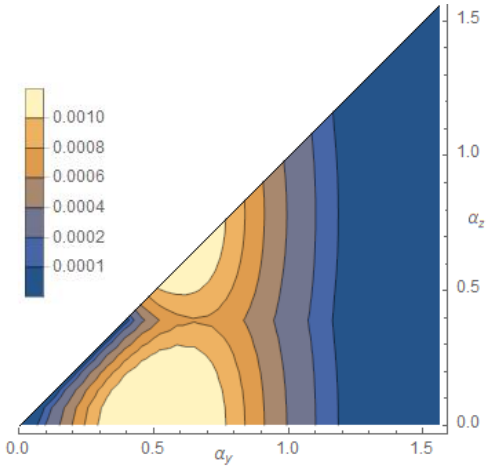

Figure 3. Contour plot of the privacy $\mathcal{P}_e$ for estimating α_x.

Comparing the three cases we can see that the highest privacy is achievable for the estimation of α_y, while it decreases by one order of magnitude for α_x and by a further order of magnitude for α_z. In this latter case the privacy is also not guaranteed in half of the parameter space. It is worth saying that $\mathcal{P}_e(\alpha_x, \alpha_y)$ is not affected by the maximization over φ, while the quantities $\mathcal{P}_e(\alpha_x, \alpha_z)$ and $\mathcal{P}_e(\alpha_y, \alpha_z)$ are, but in a different way. In particular the former is almost insensible to φ, instead the latter strongly depends on it.

4. Conclusion

In conclusion we have considered the single parameter estimation of isometries representing Stinespring dilations of quantum channels, in which the environment is under control of an adversary and the goal is to allow the legitimate user of the channels to outperform the estimation. The optimal strategy has been found by minimizing the average quadratic cost. Applications to two-qubit unitaries show that the largest privacy is obtainable when estimating α_y, i.e., the parameter in front of the generator $\sigma_y \otimes \sigma_y$. The developed approach can be extended to conceive the possibility of separate but *cooperative control* (instead of adversarial) of the two output systems [6].

Author Contributions: The authors equally contributed to this paper.

Funding: The work of M.R. is supported by China Scholarship Council.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wilde, M.M. *Quantum Information Theory*; Cambridge University Press: Cambridge, UK, 2017.
2. Stinespring, W.F. Positive functions on C^*-algebras. *Proc. Am. Math. Soc.* **1955**, *6*, 211.
3. Cai, N.; Winter, A.; Yeung, R.W. Quantum privacy and quantum wiretap channels. *P*roblems of Information Transmission. **2004**, *40*, 318; Devetak, I. The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans. Inf. Theory* **2005**, *51*, 44.
4. Personick, S.D. Application of quantum estimation theory to analog communication over quantum channels. *IEEE Trans. Inf. Theory* **1971**, *17*, 240.

5. Rexiti, M; Mancini, S. Estimation of two-qubit interactions through channels with environment assistance. *Int. J. Quantum Inf.* **2017**, *15*, 1750053.
6. Rexiti, M.; Mancini, S. Adversarial versus cooperative quantum estimation. *Quantum Inf. Processing* **2019**, *18*, 102 .