Adversarial versus cooperative quantum estimation

Milajiguli Rexiti¹,² · Stefano Mancini³,⁴

Received: 11 August 2018 / Accepted: 15 February 2019 / Published online: 21 February 2019
© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract
We address the estimation of a one-parameter family of isometries taking one input into two output systems. This primarily allows us to consider imperfect estimation by accessing only one output system, i.e., through a quantum channel. Then, on the one hand, we consider separate and adversarial control of the two output systems to introduce the concept of privacy of estimation. On the other hand we conceive the possibility of separate but cooperative control of the two output systems. Optimal estimation strategies are found according to the minimum mean square error. This also implies the generalization of Personik’s theorem to the case of local measurements. Finally, applications to two-qubit unitaries (with one qubit in a fixed input state) are discussed.

Keywords Quantum information · Decoherence · Quantum measurement theory

1 Introduction

Parameter estimation, which plays a central role in mathematical statistics, becomes of tantamount importance in quantum information processing too (see, e.g., [1]). A paradigmatic example is represented by the estimation of a parameter characterizing quantum states transformations [2–4]. These are ideally unitary transformations; however, in practice, one has to deal with noisy quantum maps, and hence, parameter estimation has been extended to quantum channels [5–7].

Several aspects of quantum channels have been investigated in recent years. One of this is the privacy, i.e., the amount of information that traverses a channel without
being intelligible to a third party besides the legitimate sender and receiver [8]. Its
determination amounts to consider a competition between the receiver, as accessing the
output channel information, and a third malicious party, as accessing the information
lost into the environment. However, recently also cooperation between actors of a
quantum communication set-up is receiving an increasing attention (see, e.g., [9,10]).
Our aim here is to analyze these two opposite strategies in the quantum estimation
theory framework.

It is well known that any quantum channel, being a completely positive and trace
preserving map, admits an isometry as dilation [11]. Hence, we can conceive the esti-
mation of a family of isometries through quantum channels. More precisely, given
a one-parameter family of isometries \( \{V_s^{A\rightarrow BF}\} \), we consider the parameter s’s esti-
mation by accessing only the system \( B \). This amounts to use the quantum channel
between \( A \) and \( B \) of which \( V_s^{A\rightarrow BF} \) represents the Stinespring dilation [11]. Estima-
tion through such a channel basically models a realistic situation where not all output
information can be gathered.

In this context, we shall first consider the system \( F \) under control of a malicious
being. Then, the question arises of what are the conditions under which a legitimate user
controlling the \( B \) system (besides \( A \) ones) can perform a better estimation. Second, we
shall consider the system \( F \) under control of a benevolent helper. Then, the question
arises of what would be the advantage in estimating locally, but cooperatively the
isometries (i.e., with local measurements and classical communication).

We shall address these issues by considering the mean square error as figure of
merit and pursuing its minimization. In one case, we introduce the concept of private estimation,
which is defined as the difference of the mean square error of the \( F \)

system and the \( B \) system (Sect. 2). In the other case, the possible measurements are
constrained to be local in systems \( B \) and \( F \), and thus, we generalize the Personik’s theorem [12],
which represents the standard way to minimize the mean square error (Sect. 3). Finally, the effectiveness of these approaches in estimation is shown with
applications to two-qubit unitaries, regarded as isometries by fixing one-qubit input
state (Sect. 4).

2 Adversarial quantum estimation

We start with studying the situation that two parties compete in estimating the same
parameter and we want to figure out when one party, considered legitimate, can out-
perform the other. To formalize this, let us take a family of isometries

\[
V_s : \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_F,
\]

parameterized by \( s \in \mathcal{I} \subset \mathbb{R} \). The parameter \( s \) is assumed to have an a priori probability distribution function \( p(s) \) over \( \mathcal{I} \). Furthermore, we consider \( A \) as the

probe system prepared in the state \( \rho_A \). Then, the output on \( B \) reads

\[
\rho_B(s) = \text{Tr}_F \left( V_s \rho_A V_s^\dagger \right) =: \mathcal{N}(\rho_A).
\]
On this state, we perform a measurement whose outcome provides an estimate of the unknown parameter $s$.

The goodness of this process can be measured by the average quadratic cost function corresponding to the mean square error

$$\tilde{C}^B := \int_{\mathcal{S}} p(s) \text{Tr} \left[ \rho_B(s) \left( \hat{S}_B - sI \right)^2 \right] ds,$$

where $\hat{S}_B$ is the measurement operator that we use to estimate $s$. The best of such operator is obtained by minimizing $\tilde{C}^B$. Personik’s theorem \[12\] states that the minimum mean square error estimator must satisfy the following (linear) equation

$$W_{B}^{(0)} \hat{S}_B + \hat{S}_B W_{B}^{(0)} = 2W_{B}^{(1)},$$

where

$$W_{B}^{(0)} := \int_{\mathcal{S}} p(s) \rho_B(s) ds,$$

$$W_{B}^{(1)} := \int_{\mathcal{S}} s p(s) \rho_B(s) ds.$$

Whether the solution of (3) will result in a biased or unbiased estimator will depend on the explicit form of the $W$s in (5); however, this is not relevant for the following. Instead, it is worth noticing that by using the spectral decomposition $\hat{S}_B = \int \hat{S}_B d\Pi(\hat{S}_B)$, with the probability operator valued measure (POVM) $d\Pi(\hat{S}_B) := |\hat{S}_B\rangle\langle\hat{S}_B| d\hat{S}_B$ defined by the eigenvectors of $\hat{S}_B$, Eq. (3) can be recast in the form

$$\tilde{C}^B = \int_{\mathcal{S}} \int_{\mathcal{S}} p(s) \left( \hat{S}_B - sI \right)^2 \text{Tr} \left[ \rho_B(s) \Pi(\hat{S}_B) \right] ds d\hat{S}_B,$$

where $\text{Tr} \left[ \rho_B(s) \Pi(\hat{S}_B) \right]$ represents the conditional probability of getting the estimate value $\hat{S}_B$ given the parameter value $s$.

Although the above approach seems limited to projective measurements, it can be shown that when a single parameter $s$ has to be estimated with minimum mean square error, the POVM defined by the eigenvectors of the operator $\hat{S}_B$ satisfying (4) represents the optimum estimation strategy overall possible POVMs [13].

On the other hand, we can consider the state emerging from the channel complementary to $\mathcal{N}$ in Eq. (2), namely

$$\rho_F(s) = \text{Tr}_B \left( V_s \rho_A V_s^\dagger \right) =: \tilde{\mathcal{N}}(\rho).$$

If this is controlled by an adversary, a strategy similar to the above can be employed to estimate $s$ and leads to $\tilde{C}_F^B$ 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

$$\tilde{C}^B - \tilde{C}_F^B.$$
\[ P_e := \max \left\{ \tilde{C}^F_{\min} - \tilde{C}^B_{\min}, 0 \right\}. \] (8)

Whenever it results positive, it means that \( \tilde{C}^B_{\min} < \tilde{C}^F_{\min} \), and hence, \( B \) can estimate \( s \) better than \( F \). This definition of 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 (8) averaged overall possible input states.

3 Cooperative quantum estimation

Here, in contrast to Sect. 2, we analyze the possibility that two parties cooperate while trying to estimate the same parameter and we ask when this is advantageous. More specifically, suppose now that \( B \) and \( F \) are not adversary, but they want to cooperate in order to estimate \( s \), though acting locally. Starting from \( \rho_A \), we find the joint output on \( B, F \) as

\[ \rho(s) = V_s \rho_A V_s^\dagger. \] (9)

Then, local measurements are performed on this state and the outcomes (after classical communication) provide an estimate of the unknown parameter \( s \).

We want to find the optimal local measurement operator \( \hat{S} = \hat{S}_B \otimes \hat{S}_F \) (with \( \hat{S}_B, \hat{S}_F \) Hermitian operators in \( \mathcal{H}_B, \mathcal{H}_F \) respectively), such that the average quadratic cost function, corresponding to the mean square error

\[ \tilde{C} := \int p(s) \text{Tr} \left[ \rho(s) \left( \hat{S} - sI \right)^2 \right] ds, \] (10)

is minimum.

For the sake of convenience, we define:

\[ W^{(0)} := \int p(s) \rho(s) ds, \] (11a)

\[ W^{(1)} := \int s p(s) \rho(s) ds. \] (11b)

Then, the optimal local measurement can be found according to the following Theorem.

**Theorem 3.1** The optimal local measurement \( \hat{S} = \hat{S}_B \otimes \hat{S}_F \), with \( \hat{S}_B, \hat{S}_F \) Hermitian operators in \( \mathcal{H}_B, \mathcal{H}_F \) respectively, satisfies the following set of coupled equations:

\[ \tilde{W}^{(0)}_B \hat{S}_B + \hat{S}_B \tilde{W}^{(0)}_B = 2W^{(1)}_B, \] (12a)

\[ \tilde{W}^{(0)}_F \hat{S}_F + \hat{S}_F \tilde{W}^{(0)}_F = 2W^{(1)}_F, \] (12b)
where
\[
\tilde{W}^{(0)}_B := \text{Tr}_F \left\{ W^{(0)} \left( I_B \otimes \hat{S}_F \right) \right\},
\]
(13a)
\[
\tilde{W}^{(0)}_F := \text{Tr}_B \left\{ W^{(0)} \left( \hat{S}_B \otimes I_F \right) \right\},
\]
(13b)

while, likewise Sect. 2, \( W^{(1)}_B = \int_{\mathcal{G}} s \, p(s) \rho_B(s) ds = \text{Tr}_F W^{(1)} \) and \( W^{(1)}_F = \int_{\mathcal{G}} s \, p(s) \rho_F(s) ds = \text{Tr}_B W^{(1)} \).

The proof of this Theorem is reported in Appendix A.

Remark 3.2 Equation (12) is a set on nonlinear equations. In fact, if we first consider (12a) as a linear equation with respect to \( \hat{S}_B \) and solve it, given that \( \tilde{W}^{(0)}_B, \tilde{W}^{(0)}_F \) depend on \( \hat{S}_F \), we will have a solution \( \hat{S}_B \left( \hat{S}_F \right) \) depending on \( \hat{S}_F \). In turn, this determines \( \tilde{W}^{(0)}_F, \tilde{W}^{(0)}_B \) depending on \( \hat{S}_F \) in (12b). Thus, the latter becomes a nonlinear equation whose solution is generally hard to find. Equation (12) reduces to linear and uncoupled equations in case \( \tilde{W}^{(0)} \) and \( \tilde{W}^{(1)} \) are local.

Often isometries in Stinespring dilation are considered to be written as
\[
V_s = U_s |0\rangle_E,
\]
(14)
where \( U_s : \mathcal{H}_A \otimes \mathcal{H}_E \to \mathcal{H}_B \otimes \mathcal{H}_F \) are unitaries (\( \mathcal{H}_A \sim \mathcal{H}_B \) and \( \mathcal{H}_E \sim \mathcal{H}_F \)).

Remark 3.3 \( \tilde{W}^{(0)} \) and \( \tilde{W}^{(1)} \) in (13) result local in the case of non entangling \( U_s \), and in particular, when \( U_s \) is simply the product \( u_s \otimes u_s \), with \( u_s : \mathcal{H}_A \to \mathcal{H}_B \) and \( \mathcal{H}_A \sim \mathcal{H}_E \), we recover the original Personik’s Theorem [12].

4 Applications to two-qubit unitaries

In this section, following (14), we will apply the developed adversarial and cooperative estimation strategies to two-qubit unitaries \( U_s : \mathbb{C}^2 \otimes \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2 \). Of course, it is meaningful to consider entangling unitaries.

The state in the system \( A \) (probe’s state) will be generically taken as
\[
\rho_A = \left( \sqrt{\gamma} |0\rangle + e^{i\varphi} \sqrt{1-\gamma} |1\rangle \right) \left( \sqrt{\gamma} \langle 0| + e^{-i\varphi} \sqrt{1-\gamma} \langle 1| \right),
\]
(15)
with \( \gamma \in [0, 1] \) and \( \varphi \in [0, 2\pi] \).

4.1 Phase damping channel dilation

An interesting example to start with is provided by
\[
U_s = |0\rangle \langle 0| \otimes I + |1\rangle \langle 1| \otimes \left( (\cos s) I + i (\sin s) \sigma_y \right),
\]
(16)
that describes a controlled rotation by an angle \( s \). Following the standard convention, we use \( \sigma_x, \sigma_y, \sigma_z \) to denote the Pauli operators. The parameter space is

\[
\mathcal{S} = \left\{ s : \frac{\pi}{2} \geq s \geq 0 \right\}.
\]

(17)

Equation (16) represents the Stinespring dilation of the phase damping channel whose action between system \( A \) and \( B \), by referring to (14), is:

\[
\rho_B = \mathcal{N}(\rho_A) = \text{Tr}_F \left( U_s \rho_A \otimes |0\rangle_E \langle 0| U_s^\dagger \right) = K_0 \rho_A K_0^\dagger + K_1 \rho_A K_1^\dagger,
\]

(18)

with

\[
K_0 = |0\rangle \langle 0| + (\cos s) |1\rangle \langle 1|,
\]

(19a)

\[
K_1 = -(\sin s) |1\rangle \langle 1|.
\]

(19b)

The effect of \( \mathcal{N} \) is to attenuate the off diagonal matrix elements (with respect to the canonical basis \( \{|0\rangle, |1\rangle\} \)) of \( \rho_A \) by a factor \( (\cos s) \).

In turn, the output of the complementary channel is given by

\[
\rho_F = \tilde{\mathcal{N}}(\rho_A) = \text{Tr}_B \left( U_s \rho_A \otimes |0\rangle_E \langle 0| U_s^\dagger \right) = \tilde{K}_0 \rho_A \tilde{K}_0^\dagger + \tilde{K}_1 \rho_A \tilde{K}_1^\dagger,
\]

(20)

with

\[
\tilde{K}_0 = |0\rangle \langle 0|,
\]

(21a)

\[
\tilde{K}_1 = (\cos s) I + i (\sin s) \sigma_y |0\rangle \langle 1|.
\]

(21b)

Following the arguments of Sect. 2 and using (15), we can readily compute the minimum cost function for (18)

\[
\bar{C}^B_{\text{min}} = \frac{\pi^2 (\pi + 2) - 48\gamma (1 - \gamma) (\pi - 2)}{48(\pi + 2)},
\]

(22)

as well as for (20)

\[
\bar{C}^F_{\text{min}} = \frac{48\pi^2 + 4\pi^4 - 192(1 - \gamma)^2 (1 - \gamma) - \pi^6 (1 + \gamma)}{48\pi^2 (4 - \pi^2 - 4\gamma - \pi^2\gamma)}.
\]

(23)

We may notice that they are independent on \( \varphi \), while their dependence on \( \gamma \) is shown in Fig. 1.

The minimum of \( \bar{C}^B_{\text{min}} \) is achieved for \( \gamma = \frac{1}{2} \) as one would expect due to the fact that an equally weighted superposition of canonical basis state vectors gives rise to largest
off diagonal density matrix elements and hence is mostly affected by the channel (18).

The optimal measurement operator results

$$\hat{S}_B = \frac{1}{4(\pi^2 - 4)} \left( 16 - 8\pi + \pi^3 \quad (\pi - 4)\pi \quad 16 - 8\pi + \pi^3 \right).$$

(24)

In contrast, $\bar{C}_F^{\text{min}}$ is monotonically increasing because according to (21) the input (15) is increasingly affected when changing from $|0\rangle\langle0|$ to $|1\rangle\langle1|$.

The privacy (8) can be easily evaluated by means of (22) and (23) as

$$P_e = \max \left\{ \frac{(1 - \gamma)}{\pi^2(\pi^2 - 4) \left( \pi^2\gamma + 4\gamma + \pi^2 - 4 \right)} \left[ \left( \pi^6 - 8\pi^5 + 20\pi^4 - 32\pi^3 + 68\pi^2 - 16 \right) \gamma^2 + \left( \pi^6 - 8\pi^5 + 12\pi^4 + 32\pi^3 - 72\pi^2 + 32 \right) \gamma - (\pi^4 - 8\pi^2 + 16) \right], 0 \right\}. $$

(25)

The privacy of estimation results guaranteed only for $\gamma \in (\gamma_0, 1)$, where $\gamma_0 \approx 0.54$ (the exact expression is given in Appendix B). Furthermore the maximum is achieved for $\gamma = \gamma_* \approx 0.77$ (the exact expression is given in Appendix B), with the measurement operator

$$\hat{S}_B = \frac{1}{4(\pi^2 - 4)} \left( \begin{array}{cc} 32 + \pi^3 - 12\pi - (32 - 8\pi)\gamma_* & 4\pi(\pi - 4)\sqrt{(1 - \gamma_*)\gamma_*} \\ 4\pi(\pi - 4)\sqrt{(1 - \gamma_*)\gamma_*} & \pi^3 - 4\pi + (32 - 8\pi)\gamma_* \end{array} \right).$$

(26)

As for what concern the cooperative strategy, the cost function $\bar{C}_F^{BF,\text{min}}$ obtained from Theorem 3.1 is shown in Fig. 1.

Likewise $\bar{C}_F^{\text{min}}$, it reaches the minimum value $\frac{\pi^4 - 48}{48\pi^4}$ when $\gamma = 0$. The corresponding local measurement operators read

$$\hat{S}_B = \begin{pmatrix} \kappa_1 & 0 \\ 0 & \kappa_2 \end{pmatrix}, \quad \hat{S}_F = \begin{pmatrix} \frac{\pi^2 - 4}{4\pi\kappa_2} & 0 \\ 0 & \frac{\pi^2 - 4}{4\pi\kappa_2} \end{pmatrix},$$

(27)

where $\kappa_1, \kappa_2$ are arbitrary real constant (with $\kappa_2 \neq 0$). This example shows that from Theorem 3.1, we can also have infinitely many solutions.

To evaluate the advantage of the cooperative strategy we consider the difference between the minimum average cost function of single $B$ local estimation and the minimum average cost function of joint $BF$ local estimation defining

$$\Delta := \bar{C}_F^{B,\text{min}} - \bar{C}_F^{BF,\text{min}}.$$  

(28)
From Fig. 1, we may notice that the privacy cannot be guaranteed when $\Delta$ is maximum ($\gamma = 0$). In fact, in such a case, the role of $F$ is dominant over $B$. It is thus reasonable to have maximum privacy away from this region, but not necessarily when $\Delta$ nullifies ($\gamma = 1$). In fact such a condition, although showing that the role of $F$ is irrelevant with respect to $B$, might correspond to $\bar{C}^B_{\text{min}} = \bar{C}^F_{\text{min}}$, which implies $P_e = 0$.

4.2 The core set of entangling unitaries

We now consider a set of unitaries given by

$$U(\vec{s}) = \exp \left[ -\frac{i}{2} \left( s_x \sigma_x \otimes \sigma_x + s_y \sigma_y \otimes \sigma_y + s_z \sigma_z \otimes \sigma_z \right) \right], \quad (29)$$

whose matrix representation is given in Appendix C. The parameter space

$$S = \{ \vec{s} \equiv (s_x, s_y, s_z): \frac{\pi}{2} \geq s_x \geq s_y \geq s_z \geq 0 \}, \quad (30)$$

describes a tetrahedron in $\mathbb{R}^3$ as illustrated in Fig. 2.

We refer to the set of unitaries of (29) as the ‘core set of entangling unitaries’ because it is known that any other two-qubit entangling unitary can be traced back to this form by means of prior and posterior local unitaries [14]. However, latter is not always applicable in a communication scenario, where the environment is not controllable (at beginning and/or at the end). Thus, there are other unitaries that can be considered (an example is provided in the previous subsection).

Below we will consider the estimation of a single parameter be either $s_x$ or $s_y$ or $s_z$ by assuming the values of the other two to be known. While distinguishing between the two strategies described in Sects. 2 and 3, we shall also seek for optimization over probe’s state, i.e., parameters $\gamma$ and $\varphi$. 
Remark 4.1 It can be easily checked that in the states $\rho_B$, $\rho_F$ and $\rho(\vec{s}) = V_s^\dagger \rho_A V_s^\dagger$ (see following subsections), the parameter $\varphi$ appears as added to $s_z$. Thus, it has no effect in the estimation of the latter. Instead, it can affect the estimation of $s_x$ and $s_y$.

4.2.1 Adversarial quantum estimation

The states $\rho_B$ and $\rho_F$ of Eqs. (2) and (7), according to the positions (14) and (29), read in this case

$$\rho_B = \text{Tr}_F \left[ U(\vec{s}) (\rho_A \otimes |0\rangle E \langle 0|) U(\vec{s})^\dagger \right], \quad (31a)$$
$$\rho_F = \text{Tr}_B \left[ U(\vec{s}) (\rho_A \otimes |0\rangle E \langle 0|) U(\vec{s})^\dagger \right], \quad (31b)$$

where $\rho_A$ is as (15). Their matrix representation is given in Appendix C.

Then, we distinguish the following cases:

- **Estimation of $s_x$**
  We took 325 points in the region $0 \leq s_z \leq s_y \leq \frac{\pi}{2}$, and for each point, we estimated $s_x$ through $\rho_B$ and independently through $\rho_F$. We actually computed

$$\mathcal{P}_\epsilon'(s_y, s_z) = \max_{\gamma, \varphi} \left[ \tilde{C}_{\min}^F(s_y, s_z, \gamma, \varphi) - \tilde{C}_{\min}^B(s_y, s_z, \gamma, \varphi) \right], \quad (32)$$

whose contour plot is shown in Fig. 3.

- **Estimation of $s_y$**
  In this case, we took 325 points in the region $0 \leq s_z \leq s_x \leq \frac{\pi}{2}$, and for each point, we estimated $s_y$ through $\rho_B$ and independently through $\rho_F$ likewise the previous
case. Then, we evaluated the privacy

$$P'_{e}(s_x, s_z) = \max \left\{ \max_{\gamma, \varphi} \left[ \bar{C}^F_{\min}(s_x, s_z, \gamma, \varphi) - \bar{C}^B_{\min}(s_x, s_z, \gamma, \varphi) \right], 0 \right\}, \quad (33)$$

whose contour plot is reported in Fig. 3.

Notice that although $\bar{C}^B_{\min}$ can be made zero by choosing $s_z = s_x^1$, this does not give the maximum privacy since in such a case also $\bar{C}^F_{\min}$ turns out to be zero. Actually, the maximum of privacy is obtained for $s_z = 0$ and by increasing $s_x$ toward $\pi/2$.

- **Estimation of $s_z$**

In this last case, we took 325 points in the region $0 \leq s_y \leq s_x \leq \pi/2$ and for each point we estimated $s_z$ through $\rho_B$ and independently through $\rho_F$. This is done by also optimizing the privacy (8) over the probe’s state, i.e., by considering

$$P'_{e}(s_x, s_y) = \max \left\{ \max_{\gamma} \left[ \bar{C}^F_{\min}(s_x, s_y, \gamma) - \bar{C}^B_{\min}(s_x, s_y, \gamma) \right], 0 \right\}, \quad (34)$$

whose contour plot is reported in Fig. 3.

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

Comparing the three cases, we can see that the highest privacy is achievable for the estimation of $s_y$, while it decreases by one order of magnitude for $s_z$ and by a further order of magnitude for $s_x$. In this latter case, the privacy is also not guaranteed in half of the parameters space. In any case, the legitimate user, for a safer estimation, should set the values of other parameters in a suitable way. It is worth saying that $P'_{e}(s_x, s_y)$ is not affected (according to Remark 4.1) by the maximization over $\varphi$, while the quantities $P'_{e}(s_x, s_z)$ and $P'_{e}(s_y, s_z)$ are, but in a different way. In particular, the former is almost insensible to $\varphi$, instead the latter strongly depends on it.

### 4.2.2 Cooperative quantum estimation

We start from the state of the composite system $BF$ which, according to the positions (14) and (29), reads

$$\rho(\vec{s}) = \left[ U(\vec{s}) \left( \rho_A \otimes |0\rangle_E \langle 0| \right) U(\vec{s})^\dagger \right], \quad (35)$$

where $\rho_A$ is as (15). Its matrix representation is reported in Appendix C.

We computed (11) and (13) in order to solve the system of nonlinear equation (12). This has been done numerically (employing MATHEMATICA packages for solving

---

1 This choice by virtue of (30) forces $s_y$ to be exactly determined.
Fig. 3 Contour plot of the privacy $P'_e$ for estimating $s_x$ (top), $s_y$ (middle) and $s_z$ (bottom). The triangle above the dashed line represents the region of not admissible parameters values.
generic equations with high working precision) for values of $\gamma \in [0, 1]$ with step 0.1 and of $\varphi \in [0, 2\pi]$ with step $\pi/8$, finding optimal local measurement operators.

Then we distinguish the following cases.

- **Estimation of $s_x$**
  We took 325 points from the region $0 \leq s_y \leq \pi/2$, $0 \leq s_z \leq s_y$ and for each point evaluated (28) for the estimation of $s_x$. This is done by also optimizing the cost functions over the probe’s state, i.e., considering

$$\Delta'(s_y, s_z) := \min_{\gamma, \varphi} \left[ C_{\text{min}}^B(s_y, s_z, \gamma, \varphi) \right] - \min_{\gamma, \varphi} \left[ C_{\text{min}}^{BF}(s_y, s_z, \gamma, \varphi) \right], \quad (36)$$

whose contour plot is shown in Fig. 4.

We can see that it does not depend on $s_z$. Furthermore, it increases with $s_y$ and this might appear contradictory with the fact that at the value $s_y = \pi/2$ both strategies are equivalent, given that the range of estimated parameter nullifies and it can be exactly determined. Actually, this behavior is due to $C_{\text{min}}^B$ which increases as $s_y \to \pi/2$ and then has a discontinuity in this edge ($s_y = \pi/2$), where its value becomes zero. In contrast $C_{\text{min}}^{BF}$ smoothly decreases to zero for $s_y \to \pi/2$.

- **Estimation of $s_y$**
  In this case, we took 325 points from the region $0 \leq s_x \leq \pi/2$, $0 \leq s_z \leq s_x$, and for each point evaluated (28) for the estimation of $s_y$. This is done by also optimizing the cost functions over the probe’s state, i.e., considering

$$\Delta'(s_x, s_z) := \min_{\gamma, \varphi} \left[ C_{\text{min}}^B(s_x, s_z, \gamma, \varphi) \right] - \min_{\gamma, \varphi} \left[ C_{\text{min}}^{BF}(s_x, s_z, \gamma, \varphi) \right], \quad (37)$$

whose contour plot is shown in Fig. 4.

We may notice that along the line $s_z = s_x$ the quantity $\Delta$ tends to zero because $s_y$ becomes exactly determined. The major improvement due to the cooperative strategy occurs for $s_x = \pi/2$ (around $s_z = \pi/8$).

- **Estimation of $s_z$**
  In this last case, we took 325 points from the region $0 \leq s_x \leq \pi/2$, $0 \leq s_y \leq s_x$, and for each point evaluated (28) for the estimation of $s_z$. This is done by also optimizing the cost functions over the probe’s state, i.e., simply over $x$ according to the Remark 4.1. Hence, we considered

$$\Delta'(s_x, s_y) := \min_{\gamma} \left[ C_{\text{min}}^B(s_x, s_y, \gamma) \right] - \min_{\gamma} \left[ C_{\text{min}}^{BF}(s_x, s_y, \gamma) \right], \quad (38)$$

whose contour plot is shown in Fig. 4.

We can see no dependence on $s_z$ and, above all, that the biggest enhancement in the estimation capability with cooperative strategy takes place on the corner $s_x = s_y = \pi/2$, where the parameter $s_z$ has the largest range. The advantage decreases toward $s_y = 0$, where the range of $s_z$ reduces to zero making the estimation meaningless.
Fig. 4 Contour plot of the difference $\Delta'$ for estimating $s_x$ (top), $s_y$ (middle) and $s_z$ (bottom). The upper white triangle represents the region of not admissible parameters values.
Comparing the three cases, we can see that the highest improvement due to cooperative strategy is achievable for the estimation of $s_x$ and $s_y$, while it is sensibly lower for $s_z$. Anyway, the advantage is always guaranteed in the entire parameters space.

It is worth saying that $\Delta'(s_x, s_y)$ is not affected (according to Remark 4.1) by the maximization over $\varphi$, while the quantities $\Delta'(s_x, s_z)$ and $\Delta'(s_y, s_z)$ are only slightly affected by it (since it is the smaller quantity $C_{BF}^{\min}$ in the difference to be more sensible to it).

5 Concluding remarks

In summary, we have considered the single parameter estimation of isometries representing Stinespring dilations of quantum channels in two different contexts. One 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. Another in which the environment is under control of an helper and the goal is to improve the estimation of the legitimate user of the channels. This shares analogies with feedback assistance models [15,16], where information gathered from environment is fed back to the main system with the aim of improving the channel performance.

In both cases, the optimal strategies have been found by minimizing the mean square error. As such, they are universal, i.e., not depending on the value of the estimated parameter, in contrast to the approach that looks for the POVM maximizing the Fisher information, therefore minimizing the variance of the estimator, at a fixed value of the parameter [17]. This in the second case required a generalization of the Personik’s theorem [12] to local measurements. Such achievement has potential applications in many different contexts whenever locality constraint is imposed on quantum estimation.

The developed approaches have been applied to two-qubit unitaries. The best strategies (input and measurement) are explicitly presented for the physically relevant case of dilation of phase damping channel in Sect. 4.1. Then, the set of unitaries of Sect. 4.2 shows that the largest privacy is obtainable when estimating $s_y$. The cooperative strategy gives maximum advantage for the estimation of $s_x$. The results of Sect. 4.2, although through $P_e'$ and $\Delta'$ support the conclusion drawn in Sect. 4.1 for $P_e$ and $\Delta$, namely the fact that the privacy cannot be guaranteed when cooperation benefit is maximum. Actually, it attains its maximum away from this region, but not necessarily when the cooperative strategy nullifies its benefit.

Clearly, the private region of estimation as well as the effectiveness of local helper can depend on the structure of the unitaries, which becomes more complicate by going beyond $U(2 \times 2)$. Investigations along this direction are left for future work. In such a case, it could be convenient instead of solving the nonlinear Eq. (12), to randomly generate Hermitian matrices $S_F$ (by using, e.g., Gaussian unitary ensemble [18]) and then solve only (12a) by standard methods for Lyapunov equations. The minimum of $\tilde{C}_B$ overall matrices $S_F$ will provide the optimal solution for cooperative strategy (notice that the case with $S_F = I$ corresponds to unassisted estimation by Bob).
Finally, it is worth saying that the devised scenarios could be extended to also contemplate the action of the adversary, or the helper, on the initial state of the environment, rather than just on the final one. This would realize an effective channel between $A$ and $B$ [19,20].

**Acknowledgements** The work of M.R. is supported by China Scholarship Council.

**Appendix A: Proof of Theorem 3.1**

Being $\tilde{C}(\hat{S})$ a minimum, for $\forall H_B \in \mathcal{L}(\mathcal{H}_B), H_F \in \mathcal{L}(\mathcal{H}_F)$ Hermitian, and $\forall \epsilon_1, \epsilon_2 \in \mathbb{R}$, it must be

$$\tilde{C}(\hat{S}) \leq \tilde{C}(\hat{S}_B \otimes \hat{S}_F + \epsilon_1 H_B \otimes I + \epsilon_2 I \otimes H_F)$$

(A1a)

$$= \int_{\mathcal{J}} p(s) \text{Tr}\left[\rho(s)(\hat{S}_B \otimes \hat{S}_F + \epsilon_1 H_B \otimes I + \epsilon_2 I \otimes H_F - s I)^2\right] ds$$

(A1b)

$$= \int_{\mathcal{J}} p(s) \text{Tr}\left[\rho(s)(\hat{S}_B \otimes \hat{S}_F - s I)^2\right] ds$$

$$+ \int_{\mathcal{J}} p(s) \text{Tr}\left[\rho(s)(\hat{S}_B \otimes \hat{S}_F - s I)(\epsilon_1 H_B \otimes I + \epsilon_2 I \otimes H_F)\right] ds$$

$$+ \int_{\mathcal{J}} p(s) \text{Tr}\left[\rho(s)(\epsilon_1 H_B \otimes I + \epsilon_2 I \otimes H_F)(\hat{S}_B \otimes \hat{S}_F - s I)\right] ds$$

$$+ \int_{\mathcal{J}} p(s) \text{Tr}\left[\rho(s)(\epsilon_1 H_B \otimes I + \epsilon_2 I \otimes H_F)^2\right] ds.$$  

(A1c)

In turn, the derivatives of $\tilde{C}(\hat{S}_B \otimes \hat{S}_F + \epsilon_1 H_B \otimes I + \epsilon_2 I \otimes H_F)$ with respect to $\epsilon_1$ and $\epsilon_2$ must be zero at $\epsilon_1 = \epsilon_2 = 0$. Thus, using Eq. (A1c), we get:

$$\frac{\partial \tilde{C}}{\partial \epsilon_1} \bigg|_{\epsilon_1=\epsilon_2=0} = \int_{\mathcal{J}} p(s) \text{Tr}\left\{\rho(s)\left[(\hat{S}_B \otimes \hat{S}_F - s I) H_B \otimes I + H_B \otimes I (\hat{S}_B \otimes \hat{S}_F - s I)\right]\right\} ds = 0,$$

(A2a)

$$\frac{\partial \tilde{C}}{\partial \epsilon_2} \bigg|_{\epsilon_1=\epsilon_2=0} = \int_{\mathcal{J}} p(s) \text{Tr}\left\{\rho(s)\left[(\hat{S}_B \otimes \hat{S}_F - s I) I \otimes H_F + I \otimes H_F (\hat{S}_B \otimes \hat{S}_F - s I)\right]\right\} ds = 0.$$  

(A2b)

Given the definitions (11), the relations (A2) imply

$$\text{Tr}\left(H_B \otimes I \left(W^{(0)}(\hat{S}_B \otimes \hat{S}_F) + (\hat{S}_B \otimes \hat{S}_F) W^{(0)} - 2W^{(1)})\right)\right) = 0,$$

(A3a)

$$\text{Tr}\left(I \otimes H_F \left(W^{(0)}(\hat{S}_B \otimes \hat{S}_F) + (\hat{S}_B \otimes \hat{S}_F) W^{(0)} - 2W^{(1)})\right)\right) = 0.$$  

(A3b)
Now, Eq. (A3a) can be rewritten as
\[
\text{Tr}_B \left\{ \text{Tr}_F \left( H_B \otimes I \left( W(0) \left( \hat{S}_B \otimes \hat{S}_F \right) + \left( \hat{S}_B \otimes \hat{S}_F \right) W(0) - 2W(1) \right) \right) \right\} \\
= \text{Tr}_B \left\{ H_B \text{Tr}_F \left( W(0) \left( \hat{S}_B \otimes \hat{S}_F \right) + \left( \hat{S}_B \otimes \hat{S}_F \right) W(0) - 2W(1) \right) \right\} \\
= \text{Tr}_B \left\{ H_B \left( \hat{W}_B(0) \hat{S}_B + \hat{S}_B \hat{W}_B(0) - 2W_B(1) \right) \right\} = 0. \tag{A4}
\]
The last line can be seen as the Hilbert–Schmidt scalar product in $\mathcal{L}(\mathcal{H}_B)$ between $H_B$ and $\left( \hat{W}_B(0) \hat{S}_B + \hat{S}_B \hat{W}_B(0) - 2W_B(1) \right)$. Given the arbitrariness of $H_B$ we may conclude that it must be
\[
\hat{W}_B(0) \hat{S}_B + \hat{S}_B \hat{W}_B(0) = 2W_B(1). \tag{A5}
\]
With same reasoning from Eq. (A3b), we can get
\[
\hat{W}_F(0) \hat{S}_F + \hat{S}_F \hat{W}_F(0) = 2W_F(1). \tag{A6}
\]

Appendix B: Coefficients $\gamma_0$ and $\gamma_*$

Equating $P_e$ of (25) to zero, we get:
\[
\gamma_0 = \left( \pi^2 - 4 \right) \frac{\pi \sqrt{\pi^2 (\pi^2 - 8\pi + 20)(\pi - 4)^2 + 16 - (\pi - 4)^2 \pi^2 + 8}}{2\pi^2 (\pi^4 - 8\pi^3 + 20\pi^2 - 32\pi + 68) - 32}. \tag{B1}
\]
Still referring to (25), solving $dP_e/d\gamma = 0$ with respect to $\gamma$ yields:
\[
\gamma_* = \frac{\Theta^2 - 2^{1/3} b\Theta + 2^{2/3} (b^2 - 3ac)}{2^{1/3} 3a \Theta}, \tag{B2}
\]
where
\[
a := 2 \left( \pi^2 + 4 \right) \left( -16 + 68\pi^2 - 32\pi^3 + 20\pi^4 - 8\pi^5 + \pi^6 \right), \\
b := 384 - 1376\pi^2 + 640\pi^3 - 208\pi^4 + 64\pi^5 + 40\pi^6 - 24\pi^7 + 3\pi^8, \\
c := 8(\pi^2 - 4) \left( 12 - 35\pi^2 + 16\pi^3 - 2\pi^4 \right), \\
d := (\pi^2 - 4)^2 \left( 8 - 18\pi^2 + 8\pi^3 - \pi^4 \right), \\
\Theta := \sqrt[3]{\sqrt{27a^2 d - 9abc + 2b^3}^2 - 4 (b^2 - 3ac)^3 - 27a^2 d + 9abc - 2b^3}. \tag{B3}
\]
Appendix C: Operators matrix representation

Matrix representation of Eq. (29) (non null elements) in the canonical basis \{\ket{0}\ket{0}, \ket{0}\ket{1}, \ket{1}\ket{0}, \ket{1}\ket{1}\}:

\[
\begin{align*}
[U(\vec{s})]_{11} &= e^{-\frac{1}{2}is_z} \cos\left(\frac{s_x - s_y}{2}\right), \\
[U(\vec{s})]_{14} &= -ie^{-\frac{1}{2}is_z} \sin\left(\frac{s_x - s_y}{2}\right), \\
[U(\vec{s})]_{22} &= e^{is_z} \cos\left(\frac{s_x + s_y}{2}\right), \\
[U(\vec{s})]_{23} &= -ie^{is_z} \sin\left(\frac{s_x + s_y}{2}\right), \\
[U(\vec{s})]_{32} &= -ie^{is_z} \sin\left(\frac{s_x + s_y}{2}\right), \\
[U(\vec{s})]_{33} &= e^{is_z} \cos\left(\frac{s_x + s_y}{2}\right), \\
[U(\vec{s})]_{41} &= -ie^{-\frac{1}{2}is_z} \sin\left(\frac{s_x - s_y}{2}\right), \\
[U(\vec{s})]_{44} &= e^{-\frac{1}{2}is_z} \cos\left(\frac{s_x - s_y}{2}\right).
\end{align*}
\]

(C1)

Matrix representation of Eq. (31a) in the canonical basis \{\ket{0}, \ket{1}\}:

\[
\begin{align*}
[\rho_B]_{11} &= \frac{1}{2} + \left(x - \frac{1}{2}\right) \cos s_x \cos s_y + \frac{1}{2} \sin s_x \sin s_y, \\
[\rho_B]_{12} &= \sqrt{(1-x)x} \left(\cos s_y \cos(s_z + \phi) - i \cos s_x \sin(s_z + \phi)\right), \\
[\rho_B]_{22} &= \frac{1}{2} - \left(x - \frac{1}{2}\right) \cos s_x \cos s_y - \frac{1}{2} \sin s_x \sin s_y.
\end{align*}
\]

(C2)

Matrix representation of Eq. (31b) in the canonical basis \{\ket{0}, \ket{1}\}:

\[
\begin{align*}
[\rho_F]_{11} &= \frac{1}{2} + \left(x - \frac{1}{2}\right) \sin s_x \sin s_y + \frac{1}{2} \cos s_x \cos s_y, \\
[\rho_F]_{12} &= \sqrt{(1-x)x} \left(\sin s_y \sin(s_z + \phi) + i \sin s_x \cos(s_z + \phi)\right), \\
[\rho_F]_{22} &= \frac{1}{2} - \left(x - \frac{1}{2}\right) \sin s_x \sin s_y - \frac{1}{2} \cos s_x \cos s_y.
\end{align*}
\]

(C3)

Matrix representation of Eq. (35) in the canonical basis \{\ket{0}\ket{0}, \ket{0}\ket{1}, \ket{1}\ket{0}, \ket{1}\ket{1}\}:
\[
[\rho(\vec{s})]_{11} = \frac{1}{2} x \left( 1 + \cos s_x \cos s_y + \sin s_x \sin s_y \right), \\
[\rho(\vec{s})]_{12} = \frac{i}{2} \sqrt{x(1-x)} \left( \sin s_x + \sin s_y \right) e^{-i(s_z+\varphi)}, \\
[\rho(\vec{s})]_{13} = \frac{1}{2} \sqrt{x(1-x)} \left( \cos s_x + \cos s_y \right) e^{-i(s_z+\varphi)}, \\
[\rho(\vec{s})]_{14} = \frac{-i}{2} \left( \sin s_x \cos s_y - \cos s_x \sin s_y \right), \\
[\rho(\vec{s})]_{22} = \frac{1}{2} (1-x) \left( 1 - \cos s_x \cos s_y + \sin s_x \sin s_y \right), \\
[\rho(\vec{s})]_{23} = \frac{-i}{2} (1-x) \left( \cos s_x \sin s_y + \sin s_x \cos s_y \right), \\
[\rho(\vec{s})]_{24} = -\frac{1}{2} \sqrt{x(1-x)} \left( \cos s_x - \cos s_y \right) e^{i(s_z+\varphi)}, \\
[\rho(\vec{s})]_{33} = \frac{1}{2} (1-x) \left( 1 + \cos s_x \cos s_y - \sin s_x \sin s_y \right), \\
[\rho(\vec{s})]_{34} = \frac{i}{2} \sqrt{x(1-x)} \left( \sin s_x - \sin s_y \right) e^{i(s_z+\varphi)}, \\
[\rho(\vec{s})]_{44} = \frac{1}{2} x \left( 1 - \cos s_x \cos s_y - \sin s_x \sin s_y \right). \\
\] (C4)

References

1. Paris, M.G.A.: Quantum estimation for quantum technology. Int. J. Quantum Inf. 7, 125 (2009)
2. Ballester, M.A.: Estimation of SU(d) using entanglement. arXiv:quant-ph/0507073 (2005)
3. Hayashi, M.: Parallel treatment of estimation of SU(2) and phase estimation. Phys. Lett. A 354, 183 (2006)
4. Kahn, J.: Fast rate estimation of a unitary operation in SU(d). Phys. Rev. A 75, 022326 (2007)
5. Sasaki, M., Ban, M., Barnett, S.M.: Optimal parameter estimation of a depolarizing channel. Phys. Rev. A 66, 022308 (2002)
6. Fujiwara, A., Imai, H.: Quantum parameter estimation of a generalized Pauli channel. J. Phys. A Math. Gen. 36, 8093 (2003)
7. Ji, Z., Wang, G., Duan, R., Feng, Y., Ying, M.: Parameter estimation of quantum channels. arXiv:quant-ph/0610060 (2006)
8. Cai, N., Winter, A., Yeung, R.W.: Quantum privacy and quantum wiretap channels. Probl. Inf. Transm. 40, 318 (2004)
9. Boche, H., Notzel, J.: The classical-quantum multiple access channel with conferencing encoders and with common messages. Quantum Inf. Process. 13, 2595 (2014)
10. Karumanchi, S., Mancini, S., Winter, A., Yang, D.: Classical capacities of quantum channels with environment assistance. Probl. Inf. Transm. 52, 214 (2016)
11. Stinespring, W.F.: Positive functions on C*-algebras. Proc. Am. Math. Soc. 6, 211 (1955)
12. Personick, S.D.: Application of quantum estimation theory to analog communication over quantum channels. IEEE Trans. Inf. Theory 17, 240 (1971)
13. Helstrom, C.W.: Quantum Detection and Estimation Theory. Academic Press, New York (1976)
14. Kraus, B., Cirac, J.I.: Optimal creation of entanglement using a two-qubit gate. Phys. Rev. A 63, 062309 (2001)
15. Gregoratti, M., Werner, R.F.: Quantum lost and found. J. Mod. Opt. 50, 915 (2003)
16. Memarzadeh, L., Cafaro, C., Mancini, S.: Quantum information reclaiming after amplitude damping. J. Phys. A Math. Theor. 44, 045304 (2011)
17. Cramer, H.: Mathematical Methods of Statistics. Princeton University Press, Princeton (1946)
18. Metha, M.: Random Matrices. Elsevier, Amsterdam (2004)
19. Karumanchi, S., Mancini, S., Winter, A., Yang, D.: Quantum channel capacities with passive environment assistance. IEEE Trans. Inf. Theory \textbf{62}, 1733 (2016)
20. Rexiti, M., Mancini, S.: Estimation of two-qubit interactions through channels with environment assistance. Int. J. Quantum Inf. \textbf{15}, 1750053 (2017)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.