Direct Estimations of Linear and Nonlinear Functionals of a Quantum State

Artur K. Ekert, Carolina Moura Alves,* and Daniel K. L. Oi

Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, United Kingdom

Michał Horodecki

Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland

Paweł Horodecki

Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80-952 Gdańsk, Poland

L. C. Kwek

*Department of Natural Sciences, National Institute of Education, Nanyang Technological University,
1 Nanyang Walk, Singapore 637616, Republic of Singapore*

We present a simple quantum network, based on the controlled-SWAP gate, that can extract certain properties of quantum states without recourse to quantum tomography. It can be used as a basic building block for direct quantum estimations of both linear and nonlinear functionals of any density operator. The network has many potential applications ranging from purity tests and eigenvalue estimations to direct characterization of some properties of quantum channels. Experimental realizations of the proposed network are within the reach of quantum technology that is currently being developed.

Certain properties of a quantum state ϱ, such as its purity, degree of entanglement, or its spectrum, are of significant importance in quantum information science. They can be quantified in terms of linear or nonlinear functionals of ϱ. Linear functionals, such as average values of observables $\{A\}$, given by $\mathrm{Tr}A\varrho$, are quite common as they correspond to directly measurable quantities. Nonlinear functionals of state, such as the von Neumann entropy $-\mathrm{Tr}\varrho \ln\varrho$, eigenvalues, or a measure of purity $\mathrm{Tr}\varrho^2$, are usually extracted from ϱ by classical means; i.e., ϱ is first estimated and once a sufficiently precise classical description of ϱ is available, classical evaluations of the required functionals can be made. However, if only a limited supply of physical objects in state ϱ is available, then a direct estimation of a specific quantity may be both more efficient and more desirable [1]. For example, the estimation of purity of ϱ does not require knowledge of all matrix elements of ϱ; thus any prior state estimation procedure followed by classical calculations is, in this case, inefficient. However, in order to bypass tomography and to estimate nonlinear functionals of ϱ more directly, we need quantum networks [2,3] performing quantum computations that supersede classical evaluations.

In this Letter, we present a simple quantum network which can be used as a basic building block for direct quantum estimations of both linear and nonlinear functionals of any ϱ. The network can be realized as multiparticle interferometry. While conventional quantum measurements, represented as quantum networks or otherwise, allow the estimation of $\mathrm{Tr}A\varrho$ for some Hermitian A, our network can also provide a direct estimation of the overlap of any two unknown quantum states ϱ_a and ϱ_b, i.e., $\mathrm{Tr}\varrho_a\varrho_b$. Here, and in the following, we use terminology developed in quantum information science. For a comprehensive overview of this terminology, including quantum logic gates and quantum networks see, for example, [4].

In order to explain how the network works, let us start with a general observation related to modifications of visibility in interferometry. Consider a typical interferometric setup for a single qubit: Hadamard gate, phase shift φ, Hadamard gate, followed by a measurement in the computational basis. We modify the interferometer by inserting a controlled-U operation between the Hadamard gates, with its control on the qubit and with U acting on a quantum system described by some unknown density operator ρ, as shown in Fig. 1 (cf. Ref. [5] for another application of controlled unitary operations in the context of NMR quantum computing). The action of the controlled-U on ρ modifies the interference pattern by the factor [6],

$$\mathrm{Tr}\rho U = v e^{i\alpha}, \qquad (1)$$
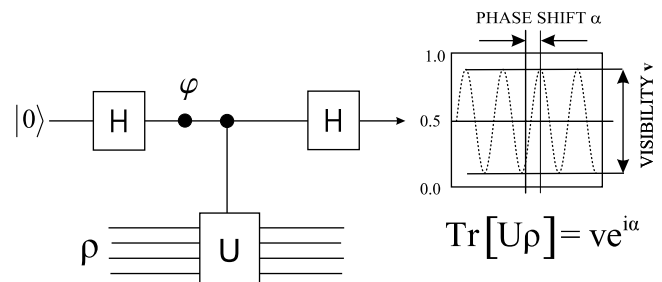

$$\mathrm{Tr}[U\rho] = v e^{i\alpha}$$

FIG. 1. Both the visibility and the shift of the interference patterns of a single qubit (top line) are affected by the controlled-U operation on a general state, ρ.

where v is the new visibility and α is the shift of the interference fringes, also known as the Pancharatnam phase [7]. The observed modification of the visibility gives an estimate of $\mathrm{Tr}U\rho$, i.e., the average value of the unitary operator U in state ρ. Let us mention in passing that this property, among other things, allows us to estimate an unknown quantum state ρ as long as we can estimate $\mathrm{Tr}U_k\rho$ for a set of unitary operators U_k which form a basis in the vector space of density operators.

Let us now consider a quantum state ρ of two separable subsystems, such that $\rho = \varrho_a \otimes \varrho_b$. We choose our controlled-U to be the controlled-V, where V is the swap operator, defined as, $V|\alpha\rangle_A|\beta\rangle_B = |\beta\rangle_A|\alpha\rangle_B$, for any pure states $|\alpha\rangle_A$ and $|\beta\rangle_B$. In this case, the modification of the interference pattern given by Eq. (1) can be written as

$$\mathrm{v} = \mathrm{Tr}V(\varrho_a \otimes \varrho_b) = \mathrm{Tr}\varrho_a\varrho_b, \qquad (2)$$

which is easily proved using the spectral decomposition of ϱ_a and ϱ_b. Since $\mathrm{Tr}\varrho_a\varrho_b$ is real, we can fix $\varphi = 0$ and the probability of finding the qubit in state $|0\rangle$ at the output, P_0, is related to the visibility by $\mathrm{v} = 2P_0 - 1$. This construction, shown in Fig. 2, provides a direct way to measure $\mathrm{Tr}\varrho_a\varrho_b$ (cf. [8] for a related idea).

There are many possible ways of utilizing this result. For pure states $\varrho_a = |\alpha\rangle\langle\alpha|$ and $\varrho_b = |\beta\rangle\langle\beta|$ the formula above gives $\mathrm{Tr}\varrho_a\varrho_b = |\langle\alpha|\beta\rangle|^2$, i.e., a direct measure of orthogonality of $|\alpha\rangle$ and $|\beta\rangle$. If we put $\varrho_a = \varrho_b = \varrho$ then we obtain an estimation of $\mathrm{Tr}\varrho^2$. In the single qubit case, this measurement allows us to estimate the length of the Bloch vector, leaving its direction completely undetermined. For qubits $\mathrm{Tr}\varrho^2$ gives the sum of squares of the two eigenvalues which allows us to estimate the spectrum of ϱ.

In general, in order to evaluate the spectrum of any $d \times d$ density matrix ϱ we need to estimate $d - 1$ parameters $\mathrm{Tr}\varrho^2, \mathrm{Tr}\varrho^3, \ldots, \mathrm{Tr}\varrho^d$. For this we need the controlled-shift operation, which is a generalization of the controlled-SWAP gate. Given k systems of dimension d we define the shift $V^{(k)}$ as

$$V^{(k)}|\phi_1\rangle|\phi_2\rangle\ldots|\phi_k\rangle = |\phi_k\rangle|\phi_1\rangle\ldots|\phi_{k-1}\rangle, \quad (3)$$

for any pure states $|\phi\rangle$. Such an operation can be easily constructed by cascading $k - 1$ swaps V. If we extend the network and prepare $\rho = \varrho^{\otimes k}$ at the input, then the interference will be modified by the visibility factor,

$$\mathrm{v} = \mathrm{Tr}V^{(k)}\varrho^{\otimes k} = \mathrm{Tr}\varrho^k = \sum_{i=1}^{m} \lambda_i{}^k. \qquad (4)$$

Thus measuring the average values of $V^{(k)}$ for $k = 2, 3, \ldots, d$ allows us to evaluate the spectrum of ϱ [1]. Although we have not eliminated classical evaluations, we have reduced them by a significant amount. The average values of $V^{(k)}$ for $k = 2, 3, \ldots, d$ provide just enough information to evaluate the spectrum of ϱ but certainly not enough to estimate the whole density matrix.

So far we have treated the two inputs, ϱ_a and ϱ_b, in a symmetric way. However, there are several interesting applications in which one of the inputs, say ϱ_a, is predetermined and the other is unknown. For example, projections on a prescribed vector $|\psi\rangle$, or on the subspace perpendicular to it, can be implemented by choosing $\varrho_a = |\psi\rangle\langle\psi|$. By changing the input state $|\psi\rangle$ we effectively "reprogram" the action of the network which then performs different projections. This property can be used in quantum communication, in a scenario where one carrier of information, in state $|\psi\rangle$, determines the type of detection measurement performed on the second carrier. N.B. as the state $|\psi\rangle$ of a single carrier cannot be determined; the information about the type of the measurement to be performed by the detector remains secret until the moment of detection.

Another interesting application is the estimation of the extremal eigenvalues and eigenvectors of ϱ_b without reconstructing the entire spectrum. In this case, the input states are of the form $|\psi\rangle\langle\psi| \otimes \varrho_b$ and we vary $|\psi\rangle$ searching for the minimum and the maximum of $\mathrm{v} = \langle\psi|\varrho_b|\psi\rangle$. This, at first sight, seems to be a complicated task as it involves scanning $2(d - 1)$ parameters of ψ. The visibility is related to the overlap of the reference state $|\psi\rangle$ and ϱ_b by

$$\mathrm{v}_\psi = \mathrm{Tr}\left(|\psi\rangle\langle\psi| \sum_i \lambda_i|\eta_i\rangle\langle\eta_i| \right)$$

$$= \sum_i \lambda_i|\langle\psi|\eta_i\rangle|^2 = \sum_i \lambda_i p_i, \qquad (5)$$

where $\sum_i p_i = 1$. This is a convex sum of the eigenvalues of ϱ_b and is minimized (maximized) when $|\psi\rangle = |\eta_{\min}\rangle$ ($|\eta_{\max}\rangle$). For any $|\psi\rangle \neq |\eta_{\min}\rangle$ ($|\eta_{\max}\rangle$), there exists a state, $|\psi'\rangle$, in the neighborhood of $|\psi\rangle$ such that $\mathrm{v}_{\psi'} < \mathrm{v}_\psi$ ($\mathrm{v}_{\psi'} > \mathrm{v}_\psi$); thus this global optimization problem can easily be solved using standard iterative methods, such as steepest descent [9].

Estimation of extremal eigenvalues plays a significant role in the direct detection [1] and distillation [10] of quantum entanglement. For example, in a special case, if two qubits described by the density operator ϱ_b such that the reduced density operator of one of the qubits is maximally mixed, we can test for the separability of ϱ_b by checking
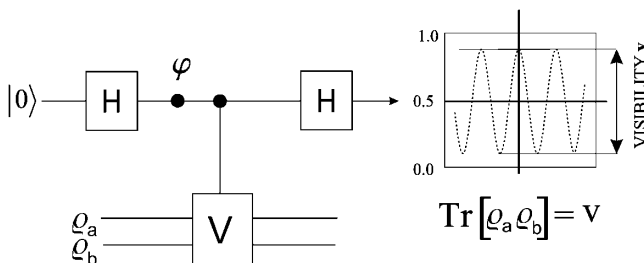

FIG. 2. A quantum network for direct estimations of both linear and nonlinear functions of state. The probability of finding the control (top line) qubit in state $|0\rangle$ at the output depends on the overlap of the two target states (two bottom lines). Thus estimation of this probability leads directly to an estimation of $\mathrm{Tr}\varrho_a\varrho_b = \mathrm{v} = 2P_0 - 1$.

whether the maximal eigenvalue of ϱ_b does not exceed $\frac{1}{2}$ [11].

Finally, we may want to estimate an unknown state, say a $d \times d$ density operator, ϱ_b. Such an operator is determined by $d^2 - 1$ real parameters. In order to estimate matrix elements $\langle \psi | \varrho_b | \psi \rangle$, we run the network as many times as possible (limited by the number of copies of ϱ_b at our disposal) on the input $|\psi\rangle\langle\psi| \otimes \varrho_b$, where $|\psi\rangle$ is a pure state of our choice. For a fixed $|\psi\rangle$, after several runs, we obtain an estimation of

$$\mathrm{v} = \langle \psi | \varrho_b | \psi \rangle. \qquad (6)$$

In some chosen basis $\{|n\rangle\}$ the diagonal elements $\langle n | \varrho_b | n \rangle$ can be determined using the input states $|n\rangle\langle n| \otimes \varrho_b$. The real part of the off-diagonal element $\langle n | \varrho_b | k \rangle$ can be estimated by choosing $|\psi\rangle = (|n\rangle + |k\rangle)/\sqrt{2}$, and the imaginary part by choosing $|\psi\rangle = (|n\rangle + i|k\rangle)/\sqrt{2}$. In particular, if we want to estimate the density operator of a qubit, we can choose the pure states, $|0\rangle$ (spin $+ z$), $(|0\rangle + |1\rangle)/\sqrt{2}$ (spin $+ x$), and $(|0\rangle + i|1\rangle)/\sqrt{2}$ (spin $+ y$), i.e., the three components of the Bloch vector.

Needless to say, quantum tomography can be performed in many other ways, the practicalities of which depend on technologies involved. However, it is worth stressing that our scheme is based on a network of a fixed architecture which is controlled only by input data, a feature that can be useful in some quantum communication scenarios.

We can extend the procedure above to cover estimations of expectation values of arbitrary observables. This can be done with the network shown in Fig. 2 because estimations of mean values of *any* observable can always be reduced to estimations of a binary two-output positive operator valued measure [12]. We shall apply the technique developed in Refs. [1,13]. As $A' = \gamma \mathbb{I} + A$ is positive if $-\gamma$ is the minimum negative eigenvalue of A, we can construct the state $\varrho_a = \varrho_{A'} = \frac{A'}{\mathrm{Tr}(A')}$ and apply our interference scheme to the pair $\varrho_{A'} \otimes \varrho_b$. The visibility gives us the mean value of V,

$$\mathrm{v} = \langle V \rangle_{\varrho_{A'} \otimes \varrho_b} = \mathrm{Tr}\left(\frac{A'}{\mathrm{Tr}(A')} \varrho_b \right), \qquad (7)$$

which leads us to the desired value,

$$\langle A \rangle_{\varrho_b} \equiv \mathrm{Tr}(\varrho_b A) = \mathrm{v}\,\mathrm{Tr}A + \gamma(\mathrm{v}d - 1), \qquad (8)$$

where $\mathrm{Tr}\mathbb{I} = d$.

Any technique that allows direct estimations of properties of quantum states can be also used to estimate certain properties of quantum channels. Recall that, from a mathematical point of view, a quantum channel is a trace preserving linear map, $\varrho \to \Lambda(\varrho)$, which maps density operators into density operators, and whose trivial extensions, $\mathcal{I}_k \otimes \Lambda$, do the same; i.e., Λ is a completely positive map. In a chosen basis the action of the channel on a density operator $\varrho = \sum_{kl} \varrho_{kl} |k\rangle\langle l|$ can be written as

$$\Lambda(\varrho) = \Lambda\left(\sum_{kl} \varrho_{kl} |k\rangle\langle l| \right) = \sum_{kl} \varrho_{kl} \Lambda(|k\rangle\langle l|). \qquad (9)$$

Thus the channel is completely characterized by operators $\Lambda(|k\rangle\langle l|)$. In fact, with every channel Λ we can associate a quantum state ϱ_Λ which provides a complete characterization of the channel. For if we prepare a maximally entangled state of two particles described by the density operator $P_+ = \frac{1}{d} \sum_{kl} |k\rangle\langle l| \otimes |k\rangle\langle l|$, and if we send only one particle through the channel, as shown in Fig. 3, then we obtain

$$P_+ \to [\mathcal{I} \otimes \Lambda] P_+ = \varrho_\Lambda, \qquad (10)$$

where

$$\varrho_\Lambda = \frac{1}{d} \sum_{kl} |k\rangle\langle l| \otimes \Lambda(|k\rangle\langle l|). \qquad (11)$$

We may interpret this as mapping the $|k\rangle\langle l|$th element of an input density matrix to the output matrix, $\Lambda(|k\rangle\langle l|)$. Thus, knowledge of ϱ_Λ allows us to determine the action of Λ on an arbitrary state, $\varrho \to \Lambda(\varrho)$. If we perform a state tomography on ϱ_Λ we effectively perform a quantum channel tomography. If we choose to estimate directly some functions of ϱ_Λ, then we gain some knowledge about specific properties of the channel without performing the full tomography of the channel.

For example, consider a single qubit channel. Suppose we are interested in the maximal rate of a reliable transmission of qubits per use of the channel, which can be quantified as the channel capacity. However, unlike in the classical case, quantum channels admit several capacities [14,15], because users of quantum channels can also exchange classical information. We have then the capacities Q_C, where $C = \emptyset, \leftarrow, \rightarrow, \leftrightarrow$ stands for zero-way, one-way, and two-way classical communication. In general, it is very difficult to calculate the capacity of a given channel. However, our extremal eigenvalue estimation scheme provides a simple necessary and sufficient condition for a one qubit channel to have nonzero two-way capacity. Namely,
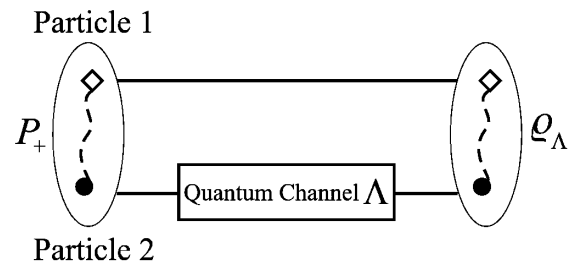
Particle 1

Particle 2

FIG. 3. A quantum channel Λ acting on one of the subsystems of a bipartite maximally entangled state of the form $|\psi_+\rangle = \sum_k |k\rangle |k\rangle/\sqrt{d}$. P_+ is the corresponding density operator, i.e., $P_+ = |\psi_+\rangle\langle\psi_+|$. The output is the state described by the density operator $\varrho_\Lambda = \frac{1}{d} \sum_{kl} |k\rangle\langle l| \otimes \Lambda(|k\rangle\langle l|)$, which contains complete information about the channel. This isomorphism between Λ and ϱ_Λ allows us to infer all properties of the channel from the corresponding properties of the state. Any subsequent estimations of ϱ_Λ, or any of its functions, provide information about the completely positive map Λ.

$Q_{\hookrightarrow} > 0$ if and only if (iff) ϱ_Λ has a maximal eigenvalue greater than $\frac{1}{2}$. (Clearly, this a necessary condition for the other three capacities to be nonzero.)

This result becomes apparent by noticing that if we trace ϱ_Λ over the qubit that went through the channel Λ (particle 2 in Fig. 3), we obtain the maximally mixed state. Furthermore, the two qubit state, ϱ_Λ, is two-way distillable iff the operator $\frac{\mathbb{1}}{2} \otimes \mathbb{1} - \varrho_\Lambda$ has a negative eigenvalue (see [11] for details), or equivalently, when ϱ_Λ has the maximal eigenvalue greater than $\frac{1}{2}$. This implies $Q_{\hookrightarrow}(\Lambda) > 0$ because two-way distillable entanglement, which is nonzero iff the given state is two-way distillable, is the lower bound for $Q_{\hookrightarrow}(\Lambda)$ [15].

In summary, we have described a simple quantum network which can be used as a basic building block for direct quantum estimations of both linear and nonlinear functionals of any density operator ϱ. It provides a direct estimation of the overlap of any two unknown quantum states ϱ_a and ϱ_b, i.e., $\mathrm{Tr}\varrho_a\varrho_b$. Its straightforward extension can be employed to estimate functionals of any powers of density operators. The network has many potential applications ranging from purity tests and eigenvalue estimations to direct characterization of some properties of quantum channels.

Finally let us also mention that the controlled-SWAP operation is a direct generalization of a Fredkin gate [16] and can be constructed out of simple quantum logic gates [3]. This means that experimental realizations of the proposed network are within the reach of quantum technology that is currently being developed (for an overview see, for example, [17]).

*Electronic address: carolina.mouraalves@qubit.org

[1] P. Horodecki and A. Ekert, quant-ph/0111064.
[2] D. Deutsch, Proc. R. Soc. London A **425**, 73 (1989).
[3] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. W. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[4] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[5] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
[6] E. Sjoqvist, A. K. Pati, A. K. Ekert, J. S. Anandan, M. Ericsson, D. K. L. Oi, and V. Vedral, Phys. Rev. Lett. **85**, 2845 (2000).
[7] S. Pancharatnam, Proc. Indian. Acad. Sci. A **44**, 247 (1956).
[8] R. Filip, quant-ph/0108119.
[9] P. E. Gill, W. Murray, and M. H. Wright, *Practical Optimization* (Academic Press, Inc., London, 1981).
[10] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997); P. Horodecki, quant-ph/0111082.
[11] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).
[12] P. Horodecki (unpublished).
[13] P. Horodecki, quant-ph/0111036.
[14] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **85**, 433 (2000).
[15] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wooters, Phys. Rev. A **54**, 3824 (1996).
[16] E. Fredkin and T. Toffoli, Int. J. Theor. Phys. **21**, 219 (1982).
[17] *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation,* edited by Dirk Bouwmeester, Artur K. Ekert, and Anton Zeilinger (Springer, New York, 2000).