Unambiguous elimination of pairs of quantum states for quantum communication

Ittoop V. Puthoor[1], Jonathan Crickmore[1], Joseph Ho[1], Berke Ricketti[1],
Sarah Croke[2], Mark Hillery[3], Alessandro Fedrizzi[1], Erika Andersson[1]

[1] Institute of Photonics & Quantum Sciences, Heriot-Watt University, UK.
[2] School of Physics and Astronomy, University of Glasgow, UK.
[3] Department of Physics and Astronomy, Hunter College of the City University of New York, USA.

Introduction

◆A single quantum measurement cannot perfectly determine the state of a quantum system; however it is possible to perfectly rule out certain states.

◆Quantum state elimination is of foundational interest, related to the reality of the wave function [1].

◆Quantum state elimination also has applications in quantum cryptography and communication. Examples of this are the communication complexity problems in [2], and a protocol for quantum oblivious transfer (OT) proposed in [3].

Background

◆We consider states of two qubits, where each qubit has one of the states

$$|\pm\theta\rangle = \cos\theta|0\rangle \pm \sin\theta|1\rangle \qquad 0 \leq \theta \leq 45^\circ$$

◆ Then for two qubits, the four possible states are

$$\begin{aligned}
|+\theta,+\theta\rangle &= \cos^2\theta|00\rangle + \sin^2\theta|11\rangle + \cos\theta\sin\theta(|01\rangle + |10\rangle)\\
|+\theta,-\theta\rangle &= \cos^2\theta|00\rangle - \sin^2\theta|11\rangle - \cos\theta\sin\theta(|01\rangle - |10\rangle)\\
|-\theta,+\theta\rangle &= \cos^2\theta|00\rangle - \sin^2\theta|11\rangle + \cos\theta\sin\theta(|01\rangle - |10\rangle)\\
|-\theta,-\theta\rangle &= \cos^2\theta|00\rangle + \sin^2\theta|11\rangle - \cos\theta\sin\theta(|01\rangle + |10\rangle).
\end{aligned}$$

◆ 6 ways to choose two states out of four to be excluded. Using the notation

$$\boxed{|\theta,\theta\rangle \rightarrow \{++\} \qquad |\theta,-\theta\rangle \rightarrow \{+-\}}$$

$$\boxed{\begin{aligned}\{++,+-\} &\rightarrow A\\ \{++,-+\} &\rightarrow B\\ \{+-,--\} &\rightarrow C\\ \{-+,--\} &\rightarrow D\end{aligned}}$$

The state of either the first or the second qubit is the same in both excluded states.

$$\boxed{\begin{aligned}\{+-,-+\} &\rightarrow E\\ \{++,--\} &\rightarrow F\end{aligned}}$$

Eliminating two qubits that have the same state, or that they have different states.

◆ Perfectly eliminating two states is possible when,

$$\cos(2\theta) \leq \sqrt{2} - 1 \qquad 2\theta \gtrsim 65.5^\circ$$

More details are provided in [4].

Motivation and Future work:

◆ Eliminating two states out of four could be used for an XOR Oblivious Transfer (OT) protocol, where a receiver obtains either the first, second, or XOR of two bits a sender sends.

◆One could also envisage novel quantum key distribution schemes employing quantum state elimination (QSE). The novel feature of such a scheme is that the final bit value cannot be thought of as created at the sender and transmitted to the receiver, but is only realised once the receiver's measurement is complete.

◆Establishing the security proofs for XOR OT protocol using QSE. An experimental realisation of the discussed QSE protocol is the subject of ongoing work.

Construction of QSE realisation

◆ A generalised quantum measurement can be realised as a projective von Neumann measurement in an extended higher-dimensional space [5].

✧ Construct six measurement operators where the subscript denotes the pair of states that are eliminated by the measurement operator.

$$\Pi_A, \Pi_B, \Pi_C, \Pi_D, \Pi_E, \Pi_F$$

✧ Extend the four-dimensional space to six dimensions by adding two auxiliary basis states $\{|aux_1\rangle, |aux_2\rangle\}$. Construct a unitary transform,

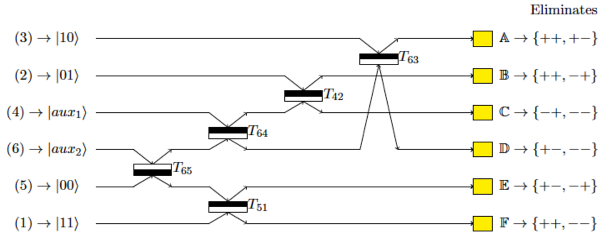
$$U = \begin{pmatrix}
\sqrt{\frac{1}{\sqrt{2}} - \frac{1}{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 & \frac{1}{2} & \frac{1}{2} - \frac{1}{\sqrt{2}}\\
\sqrt{\frac{1}{\sqrt{2}} - \frac{1}{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{2} & \frac{1}{2} - \frac{1}{\sqrt{2}}\\
\sqrt{\frac{1}{\sqrt{2}} - \frac{1}{2}} & 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{2} & \frac{1}{2} - \frac{1}{\sqrt{2}}\\
\sqrt{\frac{1}{\sqrt{2}} - \frac{1}{2}} & \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{2} & \frac{1}{2} - \frac{1}{\sqrt{2}}\\
1 - \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & \sqrt{\sqrt{2} - 1}\\
1 - \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & \sqrt{\sqrt{2} - 1}
\end{pmatrix}.$$

so that the measurement can be realised by applying the unitary transform and projecting in the 6 D basis.

✧Decompose the unitary matrix to a sequence of beam splitters and phase shifts, denoted by matrices T_{ij}. A decomposition with the smallest number of matrices is,

$$\boxed{D = U_{opt} \times T_{65} \times T_{64} \times T_{63} \times T_{51} \times T_{42}}$$

Schematic layout of quantum state elimination


Eliminates
$(3) \rightarrow |10\rangle$
$(2) \rightarrow |01\rangle$
$(4) \rightarrow |aux_1\rangle$
$(6) \rightarrow |aux_2\rangle$
$(5) \rightarrow |00\rangle$
$(1) \rightarrow |11\rangle$
T_{63}
T_{42}
T_{64}
T_{65}
T_{51}
$\mathbb{A} \rightarrow \{++,+-\}$
$\mathbb{B} \rightarrow \{++,-+\}$
$\mathbb{C} \rightarrow \{-+,--\}$
$\mathbb{D} \rightarrow \{+-,--\}$
$\mathbb{E} \rightarrow \{+-,-+\}$
$\mathbb{F} \rightarrow \{++,--\}$

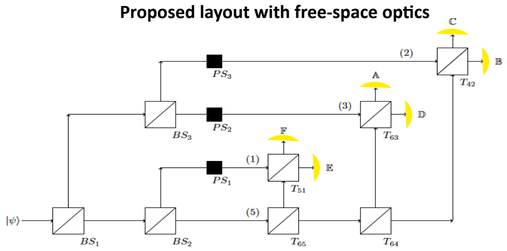
◆ There are 6 spatial modes where each mode is a basis state.

◆ Modes 1, 2, 5, 3 are the basis states used for state preparation.

◆ Modes 4 and 6 are auxiliary states with vacuum states as input.

◆ Beam splitters are represented by white and black boxes, with the black region indicating the negative phase shift upon reflection. The yellow boxes represent detectors. A click in any detector excludes two of the four possible prepared states.

Proposed layout with free-space optics



References

1. M. Pusey, J. Barrett and T. Rudolph, On the reality of the quantum state, Nat. Phys. 8, 475 (2012).
2. C. Perry, R. Jain, and J. Oppenheim, Communication tasks with infinite quantum-classical separation, Phys. Rev. Lett. 115, 030504 (2015).
3. R. Amiri *et.al.*, Imperfect 1-out-of-2 quantum oblivious transfer: bounds, a protocol, and its experimental implementation, arxiv preprint:2007.04712, (2020).
4. **J. Crickmore, I. V. Puthoor, B. Ricketti, S. Croke, M. Hillery and E. Andersson, Unambiguous quantum state elimination for qubit sequences, Phys. Rev. Res. 2, 013256 (2020).**
5. M. Reck and A. Zeilinger, Experimental realization of any discrete unitary operator, Phys. Rev. Lett., 73 (1994).