5-26-2009

Localized closed timelike curves can perfectly distinguish quantum states

Todd A. Brun
University of Southern California

Jim Harrington
Los Alamos National Laboratory

Mark M. Wilde
University of Southern California

Recommended Citation

Brun, T., Harrington, J., & Wilde, M. (2009). Localized closed timelike curves can perfectly distinguish quantum states. *Physical Review Letters, 102* (21) https://doi.org/10.1103/PhysRevLett.102.210402

Localized closed timelike curves can perfectly distinguish quantum states

Todd A. Brun,[1] Jim Harrington,[2] and Mark M. Wilde[1,3]

[1]*Communication Sciences Institute, Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089, USA*
[2]*Applied Modern Physics (P-21), MS D454, Los Alamos National Laboratory, Los Alamos, NM 87545, USA*
[3]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*

(Dated: October 22, 2018)

We show that qubits traveling along closed timelike curves are a resource that a party can exploit to distinguish perfectly any set of quantum states. As a result, an adversary with access to closed timelike curves can break any prepare-and-measure quantum key distribution protocol. Our result also implies that a party with access to closed timelike curves can violate the Holevo bound.

PACS numbers: 03.65.Wj, 03.67.Dd, 03.67.Hk, 04.20.Gz

Introduction—The theory of general relativity points to the possible existence of closed timelike curves (CTCs) [1, 2]. The *grandfather paradox* is one criticism raised to their existence, but Deutsch resolved this paradox by presenting a method for finding self-consistent solutions of CTC interactions [3].

Recently, several quantum information researchers have assumed that CTCs exist and have examined the consequences of this assumption for *computation* [4, 5, 6]. Brun showed that a classical treatment (assuming a lack of contradictions) allows NP-hard problems to be computed with a polynomial number of gates [4]. Bacon followed with a purely quantum treatment that demonstrates the same reduction of NP-hard problems to P, along with a sketch of how to perform this reduction in a fault-tolerant manner [5]. Aaronson and Watrous have recently established that either classical or quantum computers interacting with closed timelike curves can compute any function in PSPACE in polynomial time [6].

In this Letter, we show how a party with access to CTCs, or a "CTC-assisted" party, can perfectly distinguish among a set of non-orthogonal quantum states. The result has implications for fundamental protocols in quantum *communication* because a simple corollary is that a CTC-assisted party can break any prepare-and-measure quantum key distribution protocol [7, 8, 9]. (The security of such a scheme relies on the information-disturbance tradeoff for identifying quantum states.) Furthermore, the capacity for quantum systems to carry classical information becomes unbounded.

Our work here raises fundamental questions concerning the nature of a physical world in which closed timelike curves exist because it challenges the postulate of quantum mechanics that non-orthogonal states cannot be perfectly distinguished. A full theory of quantum gravity would have to resolve this apparent contradiction between the implication of CTCs and the laws of quantum mechanics. Note that any alternative source of nonlinearity would raise similar questions.

We structure this Letter as follows. First, we give some background on Deutsch's formalism regarding CTCs in quantum information theory [3]. We then show how to distinguish the non-orthogonal states $|0\rangle$ and $|-\rangle$ where $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$ and follow by showing how to distinguish the "BB84" states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ where $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$. Our main theorem then shows that a CTC-assisted party can perfectly distinguish among an arbitrary set of states. We end by discussing how a CTC-assisted party can break Holevo's bound [10].

Background—Qubits traveling around closed timelike curves (CTC qubits) may give rise to highly nonintuitive behavior, but Deutsch showed how to avoid certain paradoxes by imposing a self-consistency condition [3]. This self-consistency condition requires that the input density matrix of a CTC quantum system match its output density matrix following its interaction with another system:

$$\rho_{\text{CTC}} = \text{Tr}_{\text{sys}}\{V\left(|\psi\rangle\langle\psi| \otimes \rho_{\text{CTC}}\right)V^{\dagger}\}, \tag{1}$$

where $|\psi\rangle$ is the input state of the chronology-respecting system, the matrix ρ_{CTC} is the initial density matrix of the CTC quantum system before the two systems interact, and V is the interaction unitary. The expression on the right hand side of (1) is the partial density matrix of the CTC system after the interaction. The output state of the chronology-respecting system is then

$$\rho_{\text{out}} = \text{Tr}_{\text{CTC}}\{V\left(|\psi\rangle\langle\psi| \otimes \rho_{\text{CTC}}\right)V^{\dagger}\}. \tag{2}$$

The output state is in general a nonlinear function of the input state $|\psi\rangle$, because ρ_{out} depends on both $|\psi\rangle$ and ρ_{CTC}, and ρ_{CTC} also depends on $|\psi\rangle$. It is this nonlinearity that enables us to transcend the usual limitations of quantum mechanics.

Deutsch showed in Ref. [3] that there always exists a self-consistent solution to Eq. (1), but it does not necessarily have to be unique. In the examples and main theorem of this Letter, we construct an interaction and measurement scheme to distinguish perfectly any set of non-orthogonal states. To achieve this result, we engineer the density matrix of the CTC system to be unique as well as self-consistent.

Distinguishing two non-orthogonal states—We first show how to distinguish the non-orthogonal states $|0\rangle$

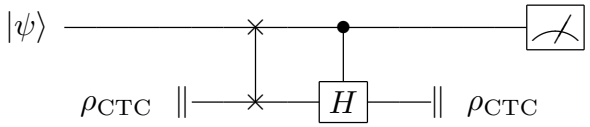

FIG. 1: The above circuit can perfectly distinguish the non-orthogonal states $|0\rangle$ and $|-\rangle$. The first qubit in state $|\psi\rangle$ is the unknown qubit ($|0\rangle$ or $|-\rangle$) and the second qubit with density matrix ρ_{CTC} travels along a closed timelike curve. The double vertical bars on the bottom left and right indicate the past and future mouths of the wormhole for the CTC.

and $|-\rangle$ without uncertainty or error. Let $|\psi\rangle^A$ denote the unknown initial state ($|0\rangle$ or $|-\rangle$) that lives on a system A. Suppose that we have access to one CTC qubit for a length of time and let B denote its corresponding system. The desired interaction is as follows:

1. Swap systems A and B.
2. Perform a controlled-Hadamard with system A as the control and system B as the target.
3. Measure system A in the computational basis.

System B "disappears" after some time because it travels along a closed timelike curve and enters the future mouth of its wormhole. The measurement of system A occurs after this point. A measurement result of zero reveals that $|\psi\rangle = |0\rangle$, and a measurement result of one reveals that $|\psi\rangle = |-\rangle$. Fig. 1 depicts the quantum circuit for this procedure.

Let us describe the operation of the circuit in Fig. 1 by tracing backward through it. First suppose that the final state of the chronology-respecting qubit is $|0\rangle\langle 0|$. The circuit is then simply a SWAP gate because the Hadamard does not act on the CTC qubit. Therefore, self-consistency of the initial and final state of the CTC qubit implies that $\rho_{\mathrm{CTC}} = |\psi\rangle\langle\psi| = |0\rangle\langle 0|$ because the two qubits are invariant under the SWAP operation.

Alternatively, suppose the final state of the chronology-respecting qubit is $|1\rangle\langle 1|$. Then the controlled-Hadamard reduces to application of the Hadamard gate on the CTC qubit. The input state to the Hadamard gate is $|\psi\rangle\langle\psi|$ (because of the SWAP), and the output state is $\rho_{\mathrm{CTC}} = |1\rangle\langle 1|$ (again, because of the SWAP). This action occurs when $|\psi\rangle\langle\psi| = |-\rangle\langle -|$.

It only remains to show that these self-consistent solutions for ρ_{CTC} are unique. Let

$$\rho_{\mathrm{CTC}} = \alpha\,|0\rangle\langle 0| + \beta\,|0\rangle\langle 1| + \gamma\,|1\rangle\langle 0| + \delta\,|1\rangle\langle 1|\,.$$

For ρ_{CTC} to be a density matrix, it must be Hermitian, positive semi-definite, and have trace 1; these conditions imply that α, δ must be non-negative reals such that $\alpha + \delta = 1$, that $\gamma = \beta^*$, and that $|\beta|^2 \leq \alpha\delta$. Suppose $|\psi\rangle\langle\psi| = |0\rangle\langle 0|$. Then $\delta = 0$ and $\alpha = 1$ because self-consistency requires that $\alpha = \alpha + \delta/2$. Thus $\rho_{\mathrm{CTC}} = |0\rangle\langle 0|$ is the only solution. Now suppose $|\psi\rangle\langle\psi| = |-\rangle\langle -|$. Then $\alpha = 0$ and $\delta = 1$ because self-consistency requires that $\delta = \delta + \alpha/2$. Thus $\rho_{\mathrm{CTC}} = |1\rangle\langle 1|$ is the only solution.

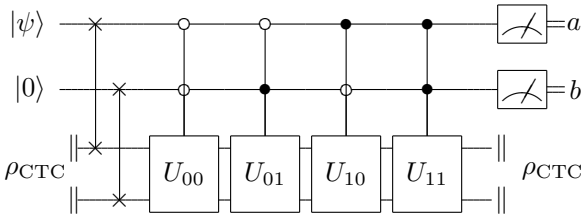

FIG. 2: The above circuit can perfectly distinguish the BB84 states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$. The circuit uses the standard quantum circuit notation from Ref. [11] and we define the unitaries U_{00}, U_{01}, U_{10}, and U_{11} in (3).

Straightforward modifications to the unitaries in Fig. 1 can be introduced to distinguish between any two non-orthogonal states. This scheme then breaks the security of the B92 quantum key distribution protocol [8]. Even with no loss on the quantum channel, a CTC-assisted adversary can learn the identity of every signal that Alice transmits and then prepare and transmit the same state to Bob. The adversary gains full information without producing any disturbance.

Distinguishing the BB84 states—We next consider how to distinguish the four BB84 states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Our scheme first appends an ancillary state $|0\rangle$ to the unknown state $|\psi\rangle$ (one of the four BB84 states) and then uses two CTC qubits to effect the following map:

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle\,, & |+0\rangle &\rightarrow |10\rangle\,,\\ |10\rangle &\rightarrow |01\rangle\,, & |-0\rangle &\rightarrow |11\rangle\,. \end{aligned}$$

That is, by measuring the output of the chronology-respecting qubits in the computational basis, the result $a = 0$ reveals that the unknown state $|\psi\rangle$ is a Z-eigenstate with eigenvalue $(-1)^b$, and $a = 1$ reveals that $|\psi\rangle$ is an X-eigenstate with eigenvalue $(-1)^b$. We claim that the circuit in Fig. 2 implements such a mapping, where we define the unitaries U_{00}, U_{01}, U_{10}, and U_{11} as follows:

$$\begin{aligned} U_{00} &\equiv \mathrm{SWAP},\\ U_{01} &\equiv X \otimes X,\\ U_{10} &\equiv (X \otimes I) \circ (H \otimes I),\\ U_{11} &\equiv (X \otimes H) \circ (\mathrm{SWAP}). \end{aligned} \tag{3}$$

The circuit in Fig. 2 consists of two SWAPs between the chronology-respecting qubits and the CTC qubits, followed by four controlled unitaries, such that a distinct unitary acts on the CTC qubits for each output state $|ab\rangle$. For each input state, the desired output of the chronology-respecting qubits corresponds to a self-consistent solution for the CTC qubits. The argument that the solution is unique proceeds as before: we consider a general density matrix for ρ_{CTC}, and we then show

that all but one of the diagonal elements in the computational basis must be zero. This result implies that $\rho_{\rm CTC}$ is pure and equal to a computational basis state.

As in the previous section, the circuit in Fig. 2 renders insecure any quantum key distribution protocol using these states [7, 9]. An adversary can learn the basis and bit values of each signal state (and then prepare an identical state) without introducing any loss or disturbance in the quantum transmission.

General state distinguishability—We now present our main theorem and proof, that constructively demonstrates how to use a CTC system to distinguish perfectly an arbitrary number of distinct quantum states.

Theorem. *Suppose there is a set $\{|\psi_j\rangle\}_{j=0}^{N-1}$ of N distinct states in a space of dimension N. Suppose we have access to an N-dimensional CTC system in a closed loop. Then we can implement the following map:*

$$\forall j \qquad |\psi_j\rangle \rightarrow |j\rangle$$

where the states $|j\rangle$ are a standard orthonormal basis for the N-dimensional space.

Proof. We want to demonstrate a mapping of $|\psi_j\rangle \rightarrow |j\rangle$ for $0 \leq j \leq N-1$, where $\{|j\rangle\}$ forms a standard orthonormal basis for the input space. We utilize a closed timelike curve (CTC) containing an N-dimensional system in a closed loop. We prepare the input system in one of the states $|\psi_j\rangle$. We then let it interact with the CTC system via a unitary transformation V. The output state will be $|j\rangle$. We choose V as follows:

1. First, swap the input system with the CTC system.

2. Next, apply the following controlled unitary from the system to the CTC:

$$\sum_{k=0}^{N-1} |k\rangle\langle k| \otimes U_k,$$

where the $\{U_k\}$ are a set of N unitary transformations acting just on the CTC system.

Let the input state of the chronology-respecting system by $|\psi_j\rangle$. Before the interaction, the CTC system is in the state $\rho_{\rm CTC}$, which must satisfy the self-consistency condition Eq. (1) for $|\psi\rangle = |\psi_j\rangle$. The state of the output system will be given by Eq. (2). We first show how to satisfy self-consistency. If we choose each U_k such that

$$U_k |\psi_k\rangle = |k\rangle\,, \tag{4}$$

then the solution $\rho_{\rm CTC} = |k\rangle\langle k|$ satisfies the self-consistency condition and gives the desired output state. However, this is not enough by itself for the construction to work. We also need $\rho_{\rm CTC}$ to be unique. (More precisely, $\rho_{\rm out}$ needs to be unique. But uniqueness of $\rho_{\rm CTC}$ is a sufficient condition for that.) We now show how to engineer the state of the CTC system and the output system to be unique. Suppose that the $\{U_k\}$ satisfy the condition above. Consider a general state for $\rho_{\rm CTC}$:

$$\rho_{\rm CTC} = \sum_{m,n} \rho_{mn} |m\rangle\langle n|\,.$$

Plugging this expression into the self-consistency equation (1) for $\rho_{\rm CTC}$ with input state $|\psi_j\rangle$ and a unitary V of the above form, the matrix elements ρ_{mn} must satisfy

$$\rho_{mn} = \sum_k \rho_{kk} \langle m| U_k |\psi_j\rangle \langle\psi_j| U_k^\dagger |n\rangle\,. \tag{5}$$

We want to choose the unitaries $\{U_k\}$ such that the unique solution to Eq. (5) is $\rho_{jj} = 1$, and all other elements of $\rho_{\rm CTC}$ are zero. Let us focus on the jth diagonal element. Since $U_j |\psi_j\rangle = |j\rangle$, we get

$$\rho_{jj} = \rho_{jj} + \sum_{k\neq j} \rho_{kk} |\langle j| U_k |\psi_j\rangle|^2\,. \tag{6}$$

For any k such that $\langle j| U_k |\psi_j\rangle \neq 0$, the above equation implies $\rho_{kk} = 0$. If $\rho_{kk} = 0$ for all $k \neq j$, this implies that all off-diagonal terms are also zero, and therefore $\rho_{jj} = 1$, which is what we want. Therefore, a set of sufficient (but by no means necessary) conditions for a unique, self-consistent solution are as follows:

1. $U_k |\psi_k\rangle = |k\rangle$ for all k, and

2. $\langle j| U_k |\psi_j\rangle \neq 0$ for all j and k.

Next we construct a set of unitaries $\{U_k\}$ satisfying these two conditions. Let $S = \{|\psi_j\rangle\}$ be the set of initial states. Choose a particular k. We will construct two orthonormal bases $|b_m\rangle$ and $|c_m\rangle$ for $m = 1, \ldots, N$ such that

$$U_k = \sum_m |c_m\rangle\langle b_m|\,.$$

This will automatically make U_k unitary. We construct these bases in a series of steps.

1. We need $U_k |\psi_k\rangle = |k\rangle$. So choose $|b_1\rangle = |\psi_k\rangle$ and $|c_1\rangle = |k\rangle$. Let us label the vector $|\psi_k\rangle$ as $|\psi_{1,1}\rangle$.

2. Pick another vector from the set S. Label this vector $|\psi_{2,1}\rangle$. Perform a Gram-Schmidt orthogonalization with this vector to construct orthonormal basis vector $|b_2\rangle$:

$$|b_2\rangle = \frac{1}{\mathcal{N}} \left(|\psi_{2,1}\rangle - |b_1\rangle\langle b_1|\psi_{2,1}\rangle\right).$$

3. Now find all the vectors in the set S that are in the space spanned by $|b_1\rangle$ and $|b_2\rangle$, including at least $|\psi_{2,1}\rangle$, but excluding $|\psi_{1,1}\rangle$. Suppose there are m_2 such vectors. Label these vectors $|\psi_{2,1}\rangle, |\psi_{2,2}\rangle, \ldots, |\psi_{2,m_2}\rangle$. Construct the basis vector $|c_2\rangle$:

$$|c_2\rangle = \frac{1}{\sqrt{m_2}} \left(\sum_{n=1}^{m_2} |j_{2,n}\rangle\right),$$

where the labels $j_{2,n}$ stand for the indices of the vectors $|\psi_{2,n}\rangle$ in the set. Note that $|c_2\rangle$ is also orthogonal to $|c_1\rangle$.

4. We now iterate this procedure. Suppose we have constructed t basis vectors $|b_1\rangle, \ldots, |b_t\rangle$ and $|c_1\rangle, \ldots, |c_t\rangle$. We construct $|b_{t+1}\rangle$ and $|c_{t+1}\rangle$ as follows. Pick a state from S that has not yet been used. Label this state $|\psi_{t+1,1}\rangle$. Perform a Gram-Schmidt orthogonalization using this state and the already constructed vectors $|b_1\rangle, \ldots, |b_t\rangle$ to make the orthonormal basis vector $|b_{t+1}\rangle$:

$$|b_{t+1}\rangle = \frac{1}{\mathcal{N}} \left(|\psi_{t+1,1}\rangle - \sum_{n=1}^{t} |b_n\rangle \langle b_n|\psi_{t+1,1}\rangle \right).$$

5. Take all the vectors from S that have not yet been used and that are contained in the subspace spanned by $|b_1\rangle, \ldots, |b_{t+1}\rangle$. Suppose there are m_{t+1} of them. Label these vectors $|\psi_{t+1,1}\rangle, \ldots, |\psi_{t+1,m_{t+1}}\rangle$. Now construct the new basis vector $|c_{t+1}\rangle$:

$$|c_{t+1}\rangle = \frac{1}{\sqrt{m_{t+1}}} \left(\sum_{n=1}^{m_{t+1}} |j_{t+1,n}\rangle \right).$$

6. Repeat steps 4 and 5 until all the vectors in the set S have been used. If this has not yet produced a complete basis, choose any sets of orthonormal vectors to complete $\{|b_m\rangle\}$ and $\{|c_m\rangle\}$.

7. Now repeat this entire construction for every U_k. From step 1 we get condition 1: $U_k |\psi_k\rangle = |k\rangle$. From the way we construct the $|c_m\rangle$ (in steps 3 and 5), we see that $\langle j| U_k |\psi_j\rangle \neq 0$ for all j and k, so both self-consistency and uniqueness are assured. □

Implications for the Holevo bound—As a final note, we point out that a CTC-assisted party can violate the Holevo bound [10]. Suppose that Alice chooses to send one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to Bob over a noiseless quantum channel. A CTC-assisted Bob can employ the method in the previous section to distinguish Alice's state perfectly and can then access two classical bits of information. This ability to access two classical bits violates the Holevo bound of one classical bit per qubit. Indeed, using a set of 2^n non-orthogonal states would allow Alice to send n classical bits via a single noiseless qubit, if Bob uses the above measurement procedure.

Conclusion—We have shown how to exploit closed timelike curves to distinguish non-orthogonal states. Two direct implications are that one could break any prepare-and-measure quantum key distribution protocol as well as violate the Holevo bound. If CTC qubits are treated as a free resource, then the achievable classical communication rate with a single noiseless quantum transmission is unbounded. We conjecture that the addition of any nonlinearity to quantum mechanics, such as that considered in Ref. [12], could be exploited similarly.

There are at least three ways to consider the implications of the results in this Letter. First, note that even if our universe contains no stable wormholes, the existence of microscopic, short-lived closed timelike curves can still revolutionize information processing tasks if they persist long enough to engineer specific unitary interactions with qubits traveling their worldlines. Second, while issues such as the grandfather paradox are resolved by Deutsch's formalism for stochastic and quantum bits traveling along closed timelike curves [3], the eroding of a finite capacity for classical communication with a qubit is a strong information theoretic argument casting doubt on the allowed existence of CTCs (similar in vein to the quantum communication complexity argument in Ref. [13]). A third tack is to consider whether Deutsch's fixed point solution for resolving CTC paradoxes is itself somehow flawed. If the formalism is invalidated, then computational complexity results such as $\mathrm{P}_{\mathrm{CTC}} = \mathrm{PSPACE}$ [6] should be reexamined. Any theory of quantum gravity will need to reconcile this intersection of quantum information theory and general relativity.

Finally, it should be interesting to study the effect of noise on the physical processes outlined in this Letter. For instance, how stable are these maps to perturbations in the input states? Recent work utilizing the Heisenberg picture may be a useful approach [14]. We conjecture that a CTC-assisted party can construct a universal cloner with fidelity approaching one, at the cost of increasing the available dimensions in ancillary and CTC resources. One area of future work could be to optimize this fidelity given CTC resources of fixed dimension.

We thank Dave Bacon, Steve Flammia, Charlie Bennett, Tim Ralph and Jonathan Oppenheim for helpful discussions. MMW acknowledges support from NSF Grant 0545845, from the National Research Foundation & Ministry of Education, Singapore, and thanks Martin Rötteler and NEC Laboratories America for hosting him as a visitor. TAB received support from NSF Grant No. CCF-0448658.

[1] M. S. Morris, K. S. Thorne, and U. Yurtsever, Phys. Rev. Lett. **61**, 1446 (1988).
[2] J. R. Gott, Phys. Rev. Lett. **66**, 1126 (1991).
[3] D. Deutsch, Phys. Rev. D **44**, 3197 (1991).
[4] T. A. Brun, Found. Phys. Lett. **16**, 245 (2003), arXiv:gr-qc/0209061v1.
[5] D. Bacon, Phys. Rev. A **70**, 032309 (2004), arXiv:quant-ph/0309189v3.
[6] S. Aaronson and J. Watrous (2008), arXiv:0808.2669v1.
[7] C. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing pp. 175–179 (1984).
[8] C. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[9] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004), arXiv:quant-ph/0211131v4.

[10] A. S. Holevo, Problems of Information Transmission **9**, 177 (1973).
[11] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
[12] D. S. Abrams and S. Lloyd, Phys. Rev. Lett. **81**, 3992 (1998), arXiv:quant-ph/9801041v1.
[13] G. Brassard, H. Buhrman, N. Linden, A. A. Mthot, A. Tapp, and F. Unger, Phys. Rev. Lett. **96**, 250401 (2006), arXiv:quant-ph/0508042v1.
[14] T. C. Ralph, Phys. Rev. A **76**, 012336 (2007), arXiv:0708.0449v1.