LA-UR- 08-6563

Approved for public release;
distribution is unlimited.

Title:	Closed timelike curves enable perfect state distinguishability
Author(s):	James Harrington Mark Wilde Todd Brun
Intended for:	Quantum Information Processing 2009 Physical Review Letters arXiv.org

Los Alamos
NATIONAL LABORATORY
EST.1943

Form 836 (7/06)

Closed timelike curves enable perfect state distinguishability

Jim Harrington
Applied Modern Physics, MS D454, Los Alamos National Laboratory, Los Alamos, NM 87545, USA

Mark M. Wilde and Todd A. Brun
Center for Quantum Information Science and Technology,
Communication Sciences Institute, Department of Electrical Engineering,
University of Southern California, Los Angeles, CA 90089, USA

The causal self-consistency condition for closed timelike curves can give rise to nonlinear interactions on chronology-respecting qubits. We demonstrate that particular unitary interactions between closed timelike curve qubits and chronology-respecting qubits implement perfect state distinguishability of nonorthogonal states. As a result, an adversary with access to closed timelike curves can break the B92, BB84, and SARG04 quantum key distribution protocols. We offer a constructive proof for generalizing these examples to an arbitrary number of non-orthogonal states. This generalization can thus break any prepare-and-measure quantum key distribution scheme. Our result also implies that a party with access to closed timelike curves can violate the Holevo bound by accessing more than $\log(N)$ bits of information from an N-dimensional quantum state.

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

Introduction—The theories of general relativity and quantum gravity point to the possible existence of closed timelike curves (CTCs) [1]. Recently, several quantum information researchers have assumed that CTCs exist and have examined the consequences of this assumption for information and computation [2–5]. Brun showed that a classical treatment (assuming a lack of contradictions) allows NP-hard problems to be computed with a polynomial number of gates [3]. 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 [4]. 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 [5].

In this brief article, we continue along these lines and show how a party with access to CTCs, or a "CTC-assisted" party, can distinguish any set of non-orthogonal states. We first show how to distinguish between the non-orthogonal states $|0\rangle$ and $|-\rangle$ where $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$. We then show how to distinguish between the "BB84" states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ where $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$. It follows that a CTC-assisted adversary can break the security of both the B92 [6] and BB84 [7] quantum key distribution protocols. Our main theorem states that a CTC-assisted party can distinguish an arbitrary set of states (the proof is in the Appendix for the interested reader). We end by discussing how a CTC-assisted party can break the Holevo bound [8].

Qubits traveling around closed timelike curves (CTC qubits) may appear to give rise to paradoxes, but Deutsch showed how to maintain causality by imposing a self-consistency condition on them [2]. The self-consistency condition is that the final state of the CTC quantum system should match its initial state even after it interacts with a chronology-respecting qubit $|\psi\rangle^A$ on a system A:

$$\rho_{\text{CTC}} = \text{Tr}_A \left(V \left(|\psi\rangle_A \langle\psi| \otimes \rho_{\text{CTC}} \right) V^\dagger \right),$$

where ρ_{CTC} is the initial density matrix of the CTC quantum system, V is the interaction unitary, and the expression on the right hand side is the density matrix of the CTC system after the interaction.

Deutsch showed that there always exists at least one self-consistent solution to the above equation [2]. In the examples and the main theorem that we discuss in this article, we enable perfect distinguishability of any set of non-orthogonal, distinct states by engineering the density matrix of the CTC system to be unique.

Distinguishing two non-orthogonal states—We first show how to distinguish between the non-orthogonal states $|0\rangle$ and $|-\rangle$ without uncertainty or error. Let $|\psi\rangle^A$ denote the unknown 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. Let B denote the system of the CTC qubit. First perform a SWAP gate between systems A and B. Then perform a controlled-Hadamard with system A as the control and system B as the target. System B is destroyed after some time because it travels along a closed timelike curve. We then measure system A in the computational basis. A measurement result of zero reveals that $|\psi\rangle = |0\rangle$ and a measurement result of one reveals that $|\psi\rangle = |-\rangle$. Figure 1 depicts the quantum circuit that implements these interactions.

Let us trace backward through the circuit in Figure 1 to describe its operation. 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 final state of the chronology-respecting qubit implies that the Hadamard does not act on the CTC qubit. Therefore,

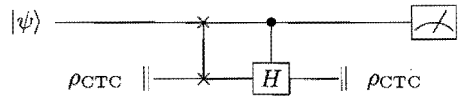

FIG. 1: The double vertical bars on the bottom left indicate the past mouth of the wormhole for the CTC and the vertical bars on the bottom right indicate the future mouth of the wormhole. The circuit can perfectly distinguish the non-orthogonal states $|0\rangle$ and $|-\rangle$.

self-consistency of the initial and final state of the CTC qubit implies that $\rho_{CTC} = |\psi\rangle\langle\psi| = |0\rangle\langle 0|$ 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 $\rho_{CTC} = |1\rangle\langle 1|$ (again, because the SWAP). This action can occur whenever $|\psi\rangle\langle\psi| = |-\rangle\langle -|$.

It only remains to show that these self-consistent solutions for ρ_{CTC} are unique. Let $\rho_{CTC} = \alpha|0\rangle\langle 0| + \beta|0\rangle\langle 1| + \gamma|1\rangle\langle 0| + \delta|1\rangle\langle 1|$, with non-negative reals α, δ such that $\alpha + \delta = 1$. When $|\psi\rangle\langle\psi| = |0\rangle\langle 0|$, we find that the self-consistency condition requires that $\alpha = \alpha + \delta/2$, and hence $\delta = 0$ and $\alpha = 1$. That is, $\rho_{CTC} = |0\rangle\langle 0|$ is the only solution. When $|\psi\rangle\langle\psi| = |-\rangle\langle -|$, we similarly find that $\delta = \delta + \alpha/2$, so $\alpha = 0$ and $\delta = 1$.

This scheme completely breaks the security of the B92 quantum key distribution protocol [6]. Even in the case of 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 on to Bob. There need not be any disturbance for an adversary to gain full information.

Distinguishing the BB84 states—Next, we consider how to distinguish perfectly the four BB84 states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Our scheme first appends the unknown state $|\psi\rangle$ (one of the four BB84 states) with an ancillary state $|0\rangle$ and then utilizes two CTC qubits to effect the following mapping: $|00\rangle \rightarrow |00\rangle$, $|10\rangle \rightarrow |01\rangle$, $|+0\rangle \rightarrow |10\rangle$, and $|-0\rangle \rightarrow |11\rangle$. That is, by measuring the output of the chronology-preserving 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 Figure 2 implements such a mapping where we define the unitaries U_{00}, U_{01}, U_{10}, and U_{11} as follows:

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

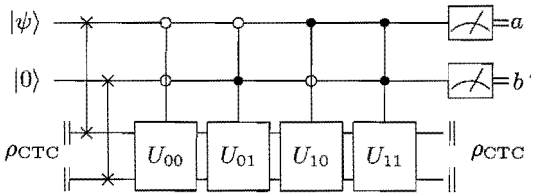

FIG. 2: The circuit can perfectly distinguish the BB84 states. The circuit uses the standard quantum circuit notation in Ref. [9] and we define the unitaries U_{00}, U_{01}, U_{10}, and U_{11} in the text.

The circuit in Figure 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 is a self-consistent solution for the CTC qubits. The argument that the solution is unique proceeds as before. We consider a general density matrix and can show that all but one of the diagonal terms in the computational basis is zero. This result implies that ρ_{CTC} is pure and equals a computational basis state.

As in the previous section, The circuit in Figure 2 renders any quantum key distribution protocols using these states (including BB84 [7], SARG04 [10], and the three-state protocol [11]) completely insecure. 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.

Main Theorem—We now present our main theorem that constructively proves it is possible to use a CTC system to distinguish an arbitrary number of non-orthogonal states. The proof of this theorem is in the Appendix for the interested reader.

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.*

Implications for the Holevo bound—As a final note, we point out that a CTC-assisted party can violate the Holevo bound [8]. 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. Bob can then access two classical bits of information and violates the Holevo bound of one classical bit per qubit.

If CTC qubits are treated as a free resource, then the achievable rate of classical information conveyed by a sin-

gle noiseless quantum transmission is unbounded, based on the generalization described in the Appendix [12].

It will be interesting to study the effect of noise on these results; how stable are the maps effected by the CTC qubits to perturbations in the input states?

Appendix—We now prove the main theorem in the text.

Proof. We want to demonstrate a mapping of $|\psi_j\rangle \to |j\rangle$ for $0 \leq j \leq N-1$, where $\{|j\rangle\}$ forms a standard orthonormal basis for the input space. We will utilize a closed timelike curve (CTC) containing an N-dimensional system in a closed loop.

- THE SET-UP

  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.

  Before the interaction, the CTC system is in the state $\rho_{\rm CTC}$. This must satisfy the self-consistency condition

  $$\rho_{\rm CTC} = {\rm Tr}_{sys}\{V\left(|\psi_j\rangle\langle\psi_j| \otimes \rho_{\rm CTC}\right)V^\dagger\}.$$

  The output state of the system is

  $$\rho_{out} = {\rm Tr}_{\rm CTC}\{V\left(|\psi_j\rangle\langle\psi_j| \otimes \rho_{\rm CTC}\right)V^\dagger\}.$$

- SELF-CONSISTENCY

  If we choose each of the U_k such that

  $$U_k|\psi_k) = |k\rangle$$

  then we can see that the solution $\rho_{\rm CTC} = |k\rangle\langle k|$ satisfies the self-consistency condition, and gives us the desired output state.

  However, this is not enough by itself for the construction to work. We also need the $\rho_{\rm CTC}$ to be unique. (More exactly, the ρ_{out} needs to be unique. But uniqueness of $\rho_{\rm CTC}$ is a sufficient condition for that.)

- UNIQUENESS

  Suppose that the $\{U_k\}$ satisfy the condition above. Consider a general state for $\rho_{\rm CTC}$:

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

  If we plug this into the self-consistency equation for $\rho_{\rm CTC}$ using a unitary of the above from, we get

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

  We want to choose the unitaries $\{U_k\}$ such that the unique solution to the above equation is $\rho_{jj} = 1$, and all other elements of $\rho_{\rm CTC}$ are zero.

  Let's focus on the jth diagonal element. Since $U_j|\psi_j\rangle = |j\rangle$, we get

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

  For any k such that $\langle j|U_k|\psi_j\rangle \neq 0$, the above equation implies $\rho_{kk} = 0$. If the $\rho_{kk} = 0$ for all $k \neq j$, that implies that all off-diagonal terms are also zero, and therefore $\rho_{jj} = 1$, which is what we want. Therefore, sufficient conditions for a unique, self-consistent solution are:

  1. $U_j|\psi_j\rangle = |j\rangle$ for all j.
  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.

- CONSTRUCTION OF THE U_k

  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 $|c_1\rangle = |k\rangle$.

  2. Pick another vector from the set S. Label this vector $|\psi_{j_{21}}\rangle$. Using this vector, do Gram-Schmidt to construct a new orthonormal basis vector $|b_2\rangle$:

  $$|b_2\rangle = \frac{1}{\mathcal{N}}\Big(|\psi_{j_{21}}\rangle - |b_1\rangle\langle b_1|\psi_{j_{21}}\rangle\Big).$$

  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 the vector $|\psi_{j_{21}}\rangle$). Suppose there are m_2 such

vectors. Label these vectors $|\psi_{j_{21}}\rangle, \ldots, |\psi_{j_{2m_2}}\rangle$. Construct the basis vector

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

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

4. We are now going to 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 the $t+1$ vectors as follows. Pick a state from S that has not yet been used. Label this state $|\psi_{j_{(t+1)1}}\rangle$. Do Gram-Schmidt using this state and the already constructed vectors $|b_1\rangle, \ldots, |b_t\rangle$ to make the new orthonormal basis vector

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

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 $|\psi_{j_{t+1)1}}\rangle, \ldots, |\psi_{j_{(t+1)m_{t+1}}}\rangle$. Now construct the new basis vector

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

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.

□

Note that this construction is certainly not the only way to build a unitary V that will work. The conditions it satisfies are sufficient, but not necessary. But it does show that such a construction exists.

---

[1] M. S. Morris, K. S. Thorne, and U. Yurtsever, Phys. Rev. Lett. **61**, 1446 (1988).

[2] D. Deutsch, Phys. Rev. D **44**, 3197 (1991).

[3] T. A. Brun, Found. Phys. Lett. **16**, 245 (2003).

[4] D. Bacon, Phys. Rev. A **70**, 032309 (2004).

[5] S. Aaronson and J. Watrous, arXiv:0808.2669v1 (2008).

[6] C. Bennett, Physical Review Letters **68**, 3121 (1992).

[7] C. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing pp. 175–179 (1984).

[8] A. S. Holevo, Problems of Information Transmission **9**, 177 (1973).

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[10] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Physical Review Letters **92**, 057901 (2004), arXiv:quant-ph/0211131v4.

[11] C.-H. F. Fung and H.-K. Lo, Physical Review A **74**, 042342 (2006), arXiv:quant-ph/0607056v3.

[12] Perhaps this is yet another implication of closed timelike curves that casts doubt on their existence.