Perfect State Distinguishability and Computational Speedups with Postselected Closed Timelike Curves

Todd A. Brun · Mark M. Wilde

Abstract Bennett and Schumacher's postselected quantum teleportation is a model of closed timelike curves (CTCs) that leads to results physically different from Deutsch's model. We show that even a single qubit passing through a postselected CTC (P-CTC) is sufficient to do any postselected quantum measurement with certainty, and we discuss an important difference between "Deutschian" CTCs (D-CTCs) and P-CTCs in which the future existence of a P-CTC might affect the present outcome of an experiment. Then, based on a suggestion of Bennett and Smith, we explicitly show how a party assisted by P-CTCs can distinguish a set of linearly independent quantum states, and we prove that it is not possible for such a party to distinguish a set of linearly dependent states. The power of P-CTCs is thus weaker than that of D-CTCs because the Holevo bound still applies to circuits using them, regardless of their ability to conspire in violating the uncertainty principle. We then discuss how different notions of a quantum mixture that are indistinguishable in linear quantum mechanics lead to dramatically differing conclusions in a nonlinear quantum mechanics involving P-CTCs. Finally, we give explicit circuit constructions that can efficiently factor integers, efficiently solve any decision problem in the intersection of NP and coNP, and probabilistically solve any decision problem in NP. These circuits accomplish these tasks with just one qubit traveling back in time, and they exploit the ability of postselected closed timelike curves to create grandfather paradoxes for invalid answers.

Keywords Postselected closed time-like curves · State distinguishability · Paradoxical computation

T.A. Brun
Communication Sciences Institute, University of Southern California, Los Angeles, CA 90089, USA
e-mail: tbrun@usc.edu

M.M. Wilde (✉)
School of Computer Science, McGill University, Montreal, Quebec H3A 2A7, Canada
e-mail: mwilde@gmail.com

🖄 Springer

1 Introduction

Einstein's field equations for general relativity predict the existence of closed timelike curves (CTCs) in certain exotic spacetime geometries [1–3], but the bizarre consequences lead many physicists to doubt that such "time machines" could exist. Closed timelike curves, if they existed, would allow particles to interact with their former selves, suggesting the possibility of grandfather-like paradoxes in both classical and quantum theories. Physicists have considered the ramifications of closed timelike curves for quantum mechanics by employing path-integral approaches in an effort to avoid contradictions [4, 5].

Deutsch showed that closed timelike curves also have consequences for classical and quantum computation [6], and he suggested imposing a self-consistency condition on the density matrix of a CTC qubit in order to avoid grandfather-like paradoxes. Since Deutsch's seminal work, quantum information theorists have produced a flurry of results under his model. They have shown that "Deutschian" closed timelike curves (D-CTCs) can help solve NP-complete problems [7], that a D-CTC-assisted classical or quantum computer has computational power equivalent to that of PSPACE [8], that a D-CTC-assisted quantum computer can perfectly distinguish an arbitrary set of non-orthogonal states [9], that evolutions of chronology-respecting qubits can be a discontinuous function of the initial state [10], and that it is not possible to purify mixed states of qubits that traverse a D-CTC while still being consistent with interactions with chronology-respecting qubits [11]. The result of Brun *et al.* [9] concerning state distinguishability is perhaps the most striking for any firm believers in unitarity, considering that a D-CTC-assisted quantum computer can violate both the uncertainty principle and the Holevo bound [12].

Since these findings, Bennett *et al.* [13] questioned the above results of Aaronson and Watrous and Brun *et al.* on D-CTC-assisted computation and distinguishability, respectively. They showed that the circuits of Aaronson *et al.* do not operate as advertised when acting on a classically-labeled mixture of states and argued that this implies their circuits "become impotent" [14]. In their work, they exploited *linear* mixtures of states to suggest that the aforementioned authors fell into a "linearity trap". But recent papers cast doubt on the claims of Bennett *et al.* and come to the same conclusion as Aaronson and Watrous and Brun *et al.* [15, 16]—a first paper tracks the information flow of quantum systems in a D-CTC with a Heisenberg-picture approach [15], and another paper shows how a density matrix description is not valid in a nonlinear theory [16]. Further work revisits Deutsch's self-consistency conditions [17], showing that they are concealing paradoxes from an observer rather than eliminating them as they should. These dramatically differing conclusions have to do with the ontological status of quantum states, which, for the most part, is not a major concern in standard linear quantum mechanics, but clearly leads to differing results in a nonlinear quantum mechanics.

Recently, a different model of closed timelike curves has emerged [18–20], based on Bennett and Schumacher's well-known but unpublished work on postselected quantum teleportation [21]. This alternative theory features a postselected closed timelike curve (P-CTC), which is physically inequivalent to a D-CTC [18, 19]. Sending a qubit into the past by a P-CTC is somewhat like teleporting the qubit's state [22].

Normally, states can only be teleported forward in time, because the receiver requires a measurement outcome from the sender in order to recover the state. By somehow postselecting with certainty on only a single measurement outcome, however, this requirement is removed. Postselection of quantum teleportation in this fashion implies that an entangled state effectively creates a noiseless quantum channel into the past. P-CTCs have the benefit of preserving correlations with external systems, while also being consistent with path-integral formulations of CTCs [4, 18, 19]. Lloyd *et al*. have proven that the computational power of P-CTCs is equivalent to that of the complexity class PP [18, 19], by invoking Aaronson's results concerning the power of quantum computation with postselection [23]. In this paper, we show that the same result can be derived from a different direction: by invoking the ideas of Ref. [24] to eliminate invalid answers to a decision problem by making them "paradoxical". One can exploit this particular aspect of P-CTCs to give explicit constructions of P-CTC-assisted circuits with dramatic computational speedups.

Our first result is to show that one can postselect with certainty the outcome of any generalized measurement using just one P-CTC qubit. Lloyd *et al*. state that it is possible to perform any desired postselected quantum computation with certainty with the help of a P-CTC system [18, 19], but they did not explicitly state that it requires just one P-CTC qubit. Next, we discuss a difference between D-CTCs and P-CTCs, in which the existence of a future P-CTC might affect the outcome of a present experiment. This observation might potentially lead to a way that one could test for a future P-CTC, by noticing deviations from expected probabilities in quantum mechanical experiments.

Further results concern state distinguishability with P-CTC-assisted circuits. We begin by showing that the SWAP-and-controlled-Hadamard circuit from Ref. [9] can perfectly distinguish $|1\rangle$ and $|+\rangle$ when assisted by a P-CTC (recall that this circuit can distinguish $|0\rangle$ and $|-\rangle$ when assisted by a D-CTC [9]). We show that the circuit from Ref. [9] for distinguishing the BB84 states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ when assisted by a D-CTC cannot do so when assisted by a P-CTC. The proof of Theorem 1 then constructs a P-CTC-assisted circuit, similar to the general construction from Ref. [9], that can perfectly distinguish an arbitrary set of linearly independent states. The proof offers an alternate construction that accomplishes this task with just one P-CTC qubit, by exploiting the generalized measurement of Ref. [25] and the ability of a P-CTC to postselect with certainty on particular measurement outcomes. The theorem also states that no P-CTC-assisted circuit can perfectly distinguish a set of linearly dependent states. Bennett and Smith both suggested in private communication [26, 27] that such a theorem should hold true. The theorem implies that a P-CTC-assisted circuit cannot beat the Holevo bound, so that their power is much weaker than that of a D-CTC-assisted circuit for this task [9]. We then discuss how different representations of a quantum state in P-CTC-assisted circuits lead to dramatically differing conclusions, even though they give the same results in linear quantum mechanics.

Our final set of results concerns the use of P-CTC-assisted circuits in certain computational tasks. We first show that a P-CTC-assisted circuit can efficiently factor integers without the use of the quantum Fourier transform. We then generalize this result to a P-CTC-assisted circuit that can efficiently solve any decision problem in the intersection of NP and co-NP. Our final construction is a P-CTC-assisted circuit for probabilistically solving any problem in NP. All of our circuits can accomplish

these computational tasks using just one P-CTC qubit. These circuits exploit the idea in Ref. [24] of making invalid answers paradoxical, which yields results that are surprisingly similar to Aaronson's construction in Ref. [23] concerning the power of postselected quantum computation.

We structure this paper as follows. The next section briefly reviews the P-CTC model, and we prove that a single qubit in a P-CTC allows postselecting on any measurement outcome with certainty. We also discuss an important difference between D-CTCs and P-CTCs and provide an example to illustrate this difference. Section 3 presents our results for P-CTCs and state distinguishability, and Sect. 4 presents our results for P-CTCs in certain computational tasks. We end by summarizing our results.

2 The Theory of Postselected Closed Timelike Curves

We first briefly review the theory of P-CTCs [18–21]. A P-CTC-assisted circuit operates by combining a chronology respecting qubit in a state ρ with a chronology-violating qubit and interacting them with a unitary evolution. After the unitary, the chronology-respecting qubit proceeds forward in time while the chronology-violating qubit goes back in time. The assumption of the model is that this evolution is mathematically equivalent to combining the state ρ with a maximally entangled Bell state $|\Phi\rangle$ where

$$|\Phi\rangle \equiv \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle |i\rangle.$$

There is then a unitary interaction U between the CR qubit and half of the entangled state. The final step is to project the two systems of the entangled state onto the state $|\Phi\rangle$, renormalize the state, and trace out the last two systems. The renormalization induces a nonlinearity in the evolution. This approach is the same as the controversial "final state projection" method from the theory of black hole evaporation [28, 29]. Figure 1 depicts the operation of a P-CTC.

As pointed out by Lloyd *et al.* [19], the action of a unitary $U_{\mathrm{SYS},A}$ on a joint system consisting of a chronology-respecting pure state $|\psi\rangle_{\mathrm{SYS}}$ and a CTC system A is as follows (before renormalization):

$$\langle\Phi|_{AB} U_{\mathrm{SYS},A}(|\psi\rangle_{\mathrm{SYS}} \otimes |\Phi\rangle_{AB})$$

$$= \frac{1}{d} \sum_{i,j} \langle i|_A \langle i|_B U_{\mathrm{SYS},A} |\psi\rangle_{\mathrm{SYS}} |j\rangle_A |j\rangle_B$$

$$= \frac{1}{d} \sum_{i,j} \langle i|_A U_{\mathrm{SYS},A} |j\rangle_A |\psi\rangle_{\mathrm{SYS}} \langle i|j\rangle_B$$

$$= \frac{1}{d} \sum_{i} \langle i|_A U_{\mathrm{SYS},A} |i\rangle_A |\psi\rangle_{\mathrm{SYS}}$$

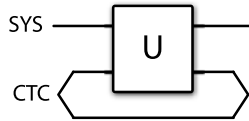$$= \frac{1}{d} \mathrm{Tr}_A\{U_{\mathrm{SYS},A}\} |\psi\rangle_{\mathrm{SYS}},$$

Fig. 1 The interpretation of the above circuit is that a chronology-respecting qubit named SYS and a chronology-violating qubit CTC interact according to a unitary evolution. After the unitary interaction, the chronology-respecting qubit proceeds forward in time, while the chronology-violating qubit goes back in time, forming a closed loop. The assumption of the postselected closed timelike curve (P-CTC) model is that the above sequence of events is mathematically equivalent to a "postselected teleportation protocol". In such a protocol, the circuit begins with a chronology-respecting qubit named SYS and a maximally entangled state $|\Phi\rangle$. We then feed the SYS system and half of the maximally entangled state into a unitary U. The final step is to project the two systems of the maximally entangled state onto the state $|\Phi\rangle$ and renormalize. The assumption of the P-CTC model is that this final projection is certain and not probabilistic and that this procedure is mathematically equivalent to creating a "quantum channel into the past" which the CTC qubit can exploit to go back in time

implying the following evolution for a mixed state ρ_{SYS} (before renormalization):

$$\langle\Phi|_{AB}U_{\text{SYS},A}(\rho_{\text{SYS}}\otimes|\Phi\rangle\langle\Phi|_{AB})U_{\text{SYS},A}^{\dagger}|\Phi\rangle_{AB}$$

$$= \langle\Phi|_{AB}U_{\text{SYS},A}\left(\sum_i\lambda_i|\psi_i\rangle\langle\psi_i|_{\text{SYS}}\otimes|\Phi\rangle\langle\Phi|_{AB}\right)U_{\text{SYS},A}^{\dagger}|\Phi\rangle_{AB}$$

$$= \sum_i\lambda_i\langle\Phi|_{AB}U_{\text{SYS},A}(|\psi_i\rangle\langle\psi_i|_{\text{SYS}}\otimes|\Phi\rangle\langle\Phi|_{AB})U_{\text{SYS},A}^{\dagger}|\Phi\rangle_{AB}$$

$$= \sum_i\lambda_i\langle\Phi|_{AB}U_{\text{SYS},A}(|\psi_i\rangle_{\text{SYS}}|\Phi\rangle_{AB}\otimes\langle\psi_i|_{\text{SYS}}\langle\Phi|_{AB})U_{\text{SYS},A}^{\dagger}|\Phi\rangle_{AB}$$

$$= \frac{1}{d^2}\sum_i\lambda_i\,\text{tr}_A\{U_{\text{SYS},A}\}|\psi_i\rangle_{\text{SYS}}\langle\psi_i|_{\text{SYS}}\,\text{tr}_A\{U_{\text{SYS},A}^{\dagger}\}$$

$$= \frac{1}{d^2}\,\text{tr}_A\{U_{\text{SYS},A}\}\sum_i\lambda_i|\psi_i\rangle_{\text{SYS}}\langle\psi_i|_{\text{SYS}}\,\text{tr}_A\{U_{\text{SYS},A}^{\dagger}\}$$

$$= \frac{1}{d^2}\,\text{tr}_A\{U_{\text{SYS},A}\}\rho_{\text{SYS}}\,\text{tr}_A\{U_{\text{SYS},A}^{\dagger}\},$$

where the fourth equality follows from the above development for pure states. Thus, the induced map on the chronology-respecting state is as follows (after renormalization):

$$\rho \to \frac{1}{\text{tr}\{C\rho C^{\dagger}\}}C\rho C^{\dagger}, \tag{1}$$

where

$$C \equiv \text{Tr}_{\text{CTC}}\{U\}.$$

There is always the possibility that the operator C is equivalent to the null operator, in which case Lloyd *et al.* suggest that "the evolution does not happen" [19]. This result

is perhaps strange, suggesting that somehow the system interacting with the P-CTC is annihilated. An explanation for what could happen resorts to potential imperfections in the unitary interaction. There is only a paradox for the evolution if the overlap of the CTC qubit with the final projected state $|\Phi\rangle_{AB}$ is identically zero. In practice, evolutions do not occur with arbitrary precision, so that the P-CTC-assisted circuit magnifies errors dramatically, and unlikely influences outside the system of interest could intervene before the circuit can create a paradox.[1]

P-CTCs allow us to postselect with certainty the outcomes of a generalized measurement [18, 19]. Suppose the generalized measurement consists of measurement operators $M_0, \ldots, M_{n-1}$. Suppose that we would like to postselect the measurement in such a way so that outcome 0 definitely occurs. We can perform the generalized measurement by appending an ancilla of dimension at least n, in state $|0\rangle$, to the system, which we assume to be in a state $|\psi\rangle$. The initial state is thus $|\psi\rangle \otimes |0\rangle$. We then perform a unitary U_1 that has the following effect:

$$U_1(|\psi\rangle \otimes |0\rangle) = \sum_k M_k |\psi\rangle \otimes |k\rangle.$$

(This is the standard construction for a generalized measurement [30].) Now we do a second unitary U_2, from the ancilla to the P-CTC qubit. This unitary is as follows:

$$U_2 = I \otimes |0\rangle\langle 0| \otimes I + I \otimes (I - |0\rangle\langle 0|) \otimes X,$$

where the third operator in the tensor product acts on the P-CTC qubit. This construction makes every outcome except M_0 paradoxical, and measuring the ancilla in the standard basis postselects so that the resulting state is

$$\frac{M_0 |\psi\rangle}{\|M_0 |\psi\rangle\|_2} \otimes |0\rangle.$$

We can postselect on any subset of the measurement outcomes by varying the projectors in U_2. For example, we can postselect by accepting any measurement outcome except M_0. To do this, we would use the following unitary as the last one:

$$U_2 = I \otimes |0\rangle\langle 0| \otimes X + I \otimes (I - |0\rangle\langle 0|) \otimes I.$$

There is an important difference between D-CTCs and P-CTCs that follows straightforwardly from their definitions. Recall that Deutsch's self-consistency condition requires that the density matrix of the D-CTC system after an interaction be equal to the density matrix before the interaction [6]. In this way, Deutsch designed D-CTCs explicitly to replicate exactly the predictions of standard quantum mechanics in the absence of CTCs. That is, before a CTC comes into existence, or after it ends, quantum mechanics behaves exactly as usual.

---

[1] All of the results in this paper should be understood as taking place in a "hypothetical world", where the projection onto the maximally entangled state $|\Phi\rangle$ occurs with certainty. We adopt the nomenclature "postselection with certainty" in order to make this point clear.

P-CTCs, by contrast, act in a way equivalent to "postselection with certainty", and they specifically rule out evolutions that lead to a paradox. This implies that the probabilities of measurement outcomes can be altered *even in the absence of CTCs*, if CTCs *will* come into existence in the future. In principle this means that the possibility of CTCs could be tested indirectly, by looking for deviations from standard quantum probabilities, a fact that was also pointed out by Hartle in Ref. [4]. Needless to say, it is far from obvious how to do such a test in practice. The bizarre behavior of nonlinear quantum mechanics would seem to cast doubt that CTCs can exist in the real world.

We offer a simple example to illustrate the idea in the previous paragraph. Suppose we have systems A, B, and C, where C is a P-CTC qubit. We prepare A and B in a maximally entangled state $(|00\rangle^{AB} + |11\rangle^{AB})/\sqrt{2}$ and measure A in the Pauli Z basis. Then we perform a CNOT from qubit B to qubit C. This circuit leads to a paradox if the result of measuring A is $|1\rangle$, so it must be $|0\rangle$ (equivalently, one can check that the transformation induced by the P-CTC is $I^A \otimes |0\rangle\langle 0|^B$). But now consider what happens if we move the preparation and measurement of AB before the P-CTC comes into existence. There are two possibilities:

1. The usual rules of quantum mechanics apply, and the probabilities of $|0\rangle$ and $|1\rangle$ are equal. If the result is $|1\rangle$, we avoid a paradox by magnifying tiny deviations from the exact unitaries, or other external effects to prevent the CNOT from happening.
2. The certain postselection forces the measurement result on A to be $|0\rangle$, even though the P-CTC does not exist yet.

Option 2 is perhaps more natural in this ideal noiseless setting, and it also matches the qualitative results found by Hartle using path integrals [4]. It is interesting that the system A does not have to interact directly with the CTC in order for this effect to occur.

3 Distinguishing Linearly-Independent States with P-CTCs

We begin this section by discussing some simple examples, and we then prove a general theorem that states that a P-CTC-assisted circuit can perfectly distinguish an arbitrary set of linearly independent states and cannot do so if the states are linearly dependent. This section ends with a discussion of how these circuits act on different ontological representations of a quantum state.

Our first circuit in Fig. 2 distinguishes $|1\rangle$ from $|+\rangle$ and can thus break the security of the Bennett-92 protocol for quantum key distribution [31]. The circuit consists of a cascade of a SWAP gate followed by a controlled Hadamard, where

$$\mathrm{SWAP} \equiv |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|,$$

Fig. 2 A PCTC-assisted circuit that can distinguish when $|1\rangle$ or $|+\rangle$ is input
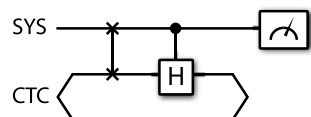
$$\text{C-}H \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes H,$$

so that

$$(\text{C-}H)(\text{SWAP}) = |00\rangle\langle 00| + |01\rangle\langle 10| + |1+\rangle\langle 01| + |1-\rangle\langle 11|.$$

The first qubit upon which the unitary acts is the system qubit, and the second one is the CTC qubit. After tracing over the CTC system (as prescribed in (1)), we get the following transformation

$$C_{\text{B92}} \equiv |0\rangle\langle 0| + |1\rangle\langle -|.$$

This transformation then gives $|0\rangle$ if we input $|+\rangle$ and $|1\rangle$ if we input $|1\rangle$ (after renormalization). Interestingly, this same circuit distinguishes the antipodal states $|0\rangle$ and $|-\rangle$ when assisted by a D-CTC [9].

We can generalize the above example to find a P-CTC-assisted circuit that can distinguish two arbitrary non-orthogonal states. Without loss of generality, suppose that the two states we are trying to distinguish are $|1\rangle$ and $|\phi\rangle$ where $|\langle 1|\phi\rangle| > 0$. We would like to build the following transformation:

$$C_{\phi} \equiv |0\rangle\langle 0| + |1\rangle\langle \phi^{\perp}|,$$

so that $C_{\phi}|1\rangle = |1\rangle$ and $C_{\phi}|\phi\rangle = |0\rangle$ (after renormalization). We follow the same prescription as above and exploit the following unitary U:

$$U \equiv |0\rangle\langle\phi| + |1\rangle\langle\phi^{\perp}|.$$

We use a cascade of a SWAP and a controlled-U where

$$\text{C-}U \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U,$$

so that the cascade $(\text{C-}U)(\text{SWAP})$ is as follows:

$$\begin{aligned}
= & |00\rangle\langle 00| + |01\rangle\langle 10| + \langle\phi|0\rangle|10\rangle\langle 01| + \langle\phi^{\perp}|0\rangle|11\rangle\langle 01| \\
& + \langle\phi|1\rangle|10\rangle\langle 11| + \langle\phi^{\perp}|1\rangle|11\rangle\langle 11|.
\end{aligned}$$

After tracing out the CTC system, we get

$$\begin{aligned}
|0\rangle\langle 0| + \langle\phi^{\perp}|0\rangle|1\rangle\langle 0| + \langle\phi^{\perp}|1\rangle|1\rangle\langle 1| & = |0\rangle\langle 0| + |1\rangle\langle\phi^{\perp}|0\rangle\langle 0| + |1\rangle\langle\phi^{\perp}|1\rangle\langle 1| \\
& = |0\rangle\langle 0| + |1\rangle\langle\phi^{\perp}|,
\end{aligned}$$

which is the desired transformation.

The D-CTC-assisted circuit presented in Ref. [9] for distinguishing BB84 states is not able to distinguish these same states when assisted by a P-CTC. In fact, the orthogonality relations of the BB84 states remain the same after going through the P-CTC-assisted circuit. The transformation induced by the circuit in Ref. [9] is as follows under the P-CTC model:

$$|00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle +0| + |11\rangle\langle -0|.$$

It is perhaps striking that the transformation takes on this form, considering that the transformation in Ref. [9] takes $|00\rangle \rightarrow |00\rangle$, $|10\rangle \rightarrow |01\rangle$, $|+0\rangle \rightarrow |10\rangle$, and $|-0\rangle \rightarrow |11\rangle$. One can check that the output states of the above transformation are as follows (after renormalization):

$$|00\rangle \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |1+\rangle),$$

$$|10\rangle \rightarrow \frac{1}{\sqrt{2}}(|01\rangle + |1-\rangle),$$

$$|+0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0+\rangle + |10\rangle),$$

$$|-0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0-\rangle + |11\rangle).$$

These states have the same orthogonality relations as the original input states, and there is thus no improvement in distinguishability. This result leads us to the main theorem of the next section.

3.1 P-CTC-Assisted Circuits Produce Perfectly Distinguishable Outputs for Linearly Independent Input States

We now state a general theorem regarding state distinguishability and P-CTCs.[2] One of our constructions in the proof has similarities with the general construction in Ref. [9] for distinguishing an arbitrary set of non-orthogonal states with a D-CTC-assisted circuit.

Theorem 1 *There exists a P-CTC-assisted circuit that can perfectly distinguish an arbitrary set $\{|\phi_i\rangle\}_{i=1}^{N}$ of linearly independent states, but a P-CTC-assisted circuit cannot perfectly distinguish a set of linearly dependent states.*

Proof We present two constructions with the first requiring an N-dimensional P-CTC system, while the second requires only one P-CTC qubit.

Our first construction is similar to the construction in Ref. [9] that uses N D-CTC qubits to distinguish N states. Consider a particular vector $|\phi_j\rangle$ in the set $\{|\phi_i\rangle\}_{i=1}^{N}$. Arbitrary superpositions of all the other vectors besides this one outline a hyperplane of dimension $N - 1$ because these states form a linearly independent set on their own, and let j also refer to this hyperplane. We cannot write the vector $|\phi_j\rangle$ as an arbitrary superposition of the other states in the set because all the states in it are linearly independent:

$$|\phi_j\rangle \neq \sum_{i \neq j} \alpha_i |\phi_i\rangle.$$

---

[2]Bennett and Smith both suggested in private communication [26, 27] that it holds true.

For each hyperplane j, there is a normal vector $|\widetilde{\phi}_j\rangle$ such that

$$\forall i \neq j : \langle \widetilde{\phi}_j | \phi_i \rangle = 0.$$

It follows that $|\langle \widetilde{\phi}_j | \phi_j \rangle| > 0$—were it not so, then $|\phi_j\rangle$ would lie in hyperplane j, which contradicts the assumption of linear independence.

We would like to have a circuit that implements the following transformation:

$$C \equiv \sum_j |j\rangle \langle \widetilde{\phi}_j|.$$

Such a transformation acts as follows (after renormalization) on any state $|\phi_j\rangle$ in the linearly independent set:

$$C|\phi_j\rangle = |j\rangle.$$

The output of this transformation is then distinguishable with a von Neumann measurement.

We now explicitly construct a unitary that implements the above transformation after tracing over the CTC system. It is a cascade of a qudit SWAP gate and a particular controlled unitary gate (a generalization of our examples from before). The qudit SWAP gate is as follows:

$$\sum_{j,k} |j\rangle \langle k| \otimes |k\rangle \langle j|,$$

and the controlled unitary gate is

$$\sum_l |l\rangle \langle l| \otimes U_l,$$

where we choose each unitary U_l above so that

$$\langle l| U_l = \langle \widetilde{\phi}_l|,$$

and its action on other basis states besides $|l\rangle$ is not important. Then the cascade of these gates gives

$$\left(\sum_l |l\rangle \langle l| \otimes U_l \right) \left(\sum_{j,k} |j\rangle \langle k| \otimes |k\rangle \langle j| \right) = \sum_{j,k,l} |l\rangle \langle l|j\rangle \langle k| \otimes U_l |k\rangle \langle j|$$

$$= \sum_{j,k} |j\rangle \langle k| \otimes U_j |k\rangle \langle j|.$$

We finally trace out the CTC system to determine the actual transformation on the chronology-respecting system:

$$\sum_{j,k} |j\rangle\langle k|\langle j|U_j|k\rangle = \sum_{j,k} |j\rangle\langle j|U_j|k\rangle\langle k|$$

$$= \sum_j |j\rangle\langle j|U_j \sum_k |k\rangle\langle k|$$

$$= \sum_j |j\rangle\langle j|U_j$$

$$= \sum_j |j\rangle\langle\widetilde{\phi}_j|.$$

This last step proves that the construction gives the desired transformation.

There is another construction which can accomplish the same task with just one P-CTC qubit. By choosing the POVM that distinguishes any set of linearly independent states [25], and ruling out result M_0 (which is "I do not know"), we can construct a P-CTC-assisted circuit of the form in Sect. 2 that can distinguish any set of linearly independent states with just one P-CTC qubit. This circuit performs the transformation $|\phi_i\rangle \to |i\rangle$ so that the states at the output of the circuit are perfectly distinguishable with a von Neumann measurement.

We now prove the other part of Theorem 1—that linearly-dependent states are not perfectly distinguishable with a P-CTC-assisted circuit. Consider an arbitrary unitary U that acts on the chronology-respecting system and the CTC system. We can decompose it as follows:

$$U = \sum_{j,k} A_{j,k} \otimes |j\rangle\langle k|,$$

with respect to some basis $\{|j\rangle\}$ for the CTC system. Tracing out the CTC system gives the transformation that the P-CTC-assisted circuit induces

$$C = \text{tr}_{\text{CTC}}\{U\} = \sum_j A_{j,j}.$$

Now suppose that a P-CTC can distinguish a state $|\phi_0\rangle$ from $|\phi_1\rangle$ in the sense that $C|\phi_0\rangle = |0\rangle$ and $C|\phi_1\rangle = |1\rangle$ after renormalization. Then consider a linearly dependent state $|\psi\rangle$ where we can write $|\psi\rangle = \alpha|\phi_0\rangle + \beta|\phi_1\rangle$ for some $\alpha, \beta \neq 0$. Then, by linearity of the transformation C before renormalization, it follows that

$$C|\psi\rangle = C(\alpha|\phi_0\rangle + \beta|\phi_1\rangle) = \alpha C|\phi_0\rangle + \beta C|\phi_1\rangle = \alpha\mathcal{N}_0|0\rangle + \beta\mathcal{N}_1|1\rangle,$$

where $\mathcal{N}_0$ and $\mathcal{N}_1$ are non-zero normalization constants. After renormalization, this state is not distinguishable from $|0\rangle$ or $|1\rangle$ by any measurement. This proof generalizes easily so that any P-CTC transformation would not be able to distinguish a general set of linearly dependent states. $\qquad\square$

As an afterthought, the above theorem demonstrates that the power of a P-CTC-assisted circuit is rather limited in comparison to a D-CTC-assisted one. A D-CTC-assisted circuit can violate the Holevo bound [9], but a P-CTC-assisted one can never

violate it because one can never have more than N linearly independent states in N dimensions. Of course, if the receiver has access to a P-CTC, that will raise the classical capacity of certain channels, since it increases the ability to distinguish states beyond that of ordinary quantum mechanics. The theorem also implies that a P-CTC-assisted circuit cannot break the security of the BB84 [32] or SARG04 [33] protocols for quantum key distribution, though a P-CTC will increase the power of the eavesdropper to a certain degree. These results might lend further credence to the belief that P-CTCs are a more reasonable model of time travel because their information processing abilities are not as striking as those of D-CTCs (even though they still violate the uncertainty principle).

3.2 The "Linearity Trap" for Labeled Mixtures

The operation of a D-CTC-assisted circuit on a labeled mixture of states is controversial [13, 15, 16] and can lead to dramatically different conclusions depending on how one interprets such a labeled mixture. A similar phenomenon happens with P-CTCs as we discuss below.

Let us consider a general ensemble $\{(p(x), |\phi_x\rangle)\}$ of non-orthogonal, linearly independent states. In linear quantum mechanics, this ensemble has a one-to-one correspondence with the following labeled mixture:

$$\sum_x p(x)|x\rangle\langle x|^X \otimes |\phi_x\rangle\langle\phi_x|^A, \qquad (2)$$

where the states $\{|x\rangle^X\}$ are an orthonormal set. Suppose the preparer holds on to the X label and sends the A system through the transformation from Theorem 1. A first way to renormalize would be to act with the P-CTC transformation on each state $|\phi_x\rangle$ in the ensemble and renormalize each resulting state. This procedure assumes that the classical labeling information is available, in principle. This process leads to the output ensemble $\{(p(x), |x\rangle^A)\}$, which has a one-to-one correspondence with the following labeled mixture:

$$\sum_x p(x)|x\rangle\langle x|^X \otimes |x\rangle\langle x|^A, \qquad (3)$$

so that the systems on X and A are now classically correlated according to the distribution $p(x)$.

Another method for renormalization leads to a drastically different result. Considering the labeled mixture as a "true density matrix" and acting on this state with the transformation from Theorem 1 gives

$$\sum_j |j\rangle\langle\tilde{\phi}_j|^A \left(\sum_x p(x)|x\rangle\langle x|^X \otimes |\phi_x\rangle\langle\phi_x|^A\right) \sum_{j'} |\tilde{\phi}_{j'}\rangle\langle j'|^A$$

$$= \sum_x p(x)|x\rangle\langle x|^X \otimes \sum_{j,j'} |j\rangle\langle\tilde{\phi}_j|\phi_x\rangle\langle\phi_x|\tilde{\phi}_{j'}\rangle\langle j'|^A$$

$$= \sum_x p(x)|x\rangle\langle x|^X \otimes \sum_j |\langle\widetilde{\phi}_j|\phi_x\rangle|^2 \, |j\rangle\langle j|^A$$

$$= \sum_{x,j} p(x)|\langle\widetilde{\phi}_j|\phi_x\rangle|^2 |x\rangle\langle x|^X \otimes |j\rangle\langle j|^A$$

$$= \sum_x p(x)|\langle\tilde{\phi}_x|\phi_x\rangle|^2 |x\rangle\langle x|^X \otimes |x\rangle\langle x|^A.$$

After renormalization, the state is as follows:

$$\sum_x q(x)|x\rangle\langle x|^X \otimes |x\rangle\langle x|^A, \tag{4}$$

where

$$q(x) \equiv \frac{1}{\sum_x p(x)|\langle\tilde{\phi}_x|\phi_x\rangle|^2} p(x)|\langle\tilde{\phi}_x|\phi_x\rangle|^2.$$

The systems on X and A are classically correlated again, but the distribution for the correlation can be drastically different if the overlap $|\langle\tilde{\phi}_x|\phi_x\rangle|^2$ is not uniform over x. The interpretation of the above result is bizarre: the P-CTC-assisted circuit changes the original probabilities of the states in the mixture, in spite of the fact that the preparer generated these probabilities well before the P-CTC even came into existence.

Let us examine a third scenario. Consider the following purification of the state in (2):

$$\sum_x \sqrt{p(x)}|x\rangle^X |x\rangle^{X'} |\phi_x\rangle^A.$$

Suppose that Alice sends the A system through the P-CTC-assisted circuit. Acting on this state with the transformation from Theorem 1 gives

$$\sum_j |j\rangle\langle\tilde{\phi}_j|^A \sum_x \sqrt{p(x)}|x\rangle^X |x\rangle^{X'} |\phi_x\rangle^A = \sum_{x,j} \sqrt{p(x)}|x\rangle^X |x\rangle^{X'} |j\rangle^A \langle\tilde{\phi}_j|\phi_x\rangle^A$$

$$= \sum_x \sqrt{p(x)}\langle\tilde{\phi}_x|\phi_x\rangle^A |x\rangle^X |x\rangle^{X'} |x\rangle^A.$$

Renormalizing the last line above leads to the following state:

$$\frac{1}{\mathcal{N}} \sum_x \sqrt{p(x)}\langle\tilde{\phi}_x|\phi_x\rangle^A |x\rangle^X |x\rangle^{X'} |x\rangle^A, \tag{5}$$

where

$$\mathcal{N} \equiv \sqrt{\sum_x p(x)|\langle\tilde{\phi}_x|\phi_x\rangle|^2}.$$

The coefficients $\langle\tilde{\phi}_x|\phi_x\rangle^A$ can generally be complex, and this state is different from the other outcomes illustrated above because there is quantum interference. Though,

this state is a purification of the state in (4), so that the resulting state is the same as in (4) if we discard the system X'.

What should we make of these differing results? In standard quantum mechanics, there are three concepts that are indistinguishable from each other:

1. An ensemble $\{p(x), |\phi_x\rangle\langle\phi_x|\}$ of pure states (classical ignorance);
2. An entangled state $|\psi\rangle\langle\psi|^{AB}$ where subsystem B is assumed to be inaccessible;
3. A density matrix ρ.

The first is what d'Espagnat called a "proper mixture", and the second is what he called an "improper mixture" [34]. The density matrix is a mathematical object introduced to summarize the observable consequences of either of the other two. One could imagine such a thing as a "true density matrix"—an intrinsically mixed state that does not represent either classical ignorance or entanglement—though it is not clear what such an object would mean, physically. However, some researchers suggest that density matrices, rather than pure states, should be the fundamental objects in quantum theory. For instance, mixed states arise naturally in Deutsch's approach to CTCs [6].

These three different ontological representations of a quantum state are all indistinguishable in standard quantum mechanics because it is a linear theory. But in a nonlinear version of quantum mechanics (as we get using either D-CTCs or P-CTCs) we have no reason to expect them to behave the same, and they do not. This is the major criticism that Ref. [16] levies against Ref. [13]. Bennett *et al.* use "labeled mixtures" to represent classical ensembles, which is not necessarily justifiable in nonlinear quantum mechanics.

So what should be done? If the "labeled mixture" represents classical ignorance about how the system was prepared, that implies that, in principle, information exists which would specify a pure state. One should therefore apply the calculation separately to each state $|\phi_x\rangle$ in the ensemble, and then combine them in a new ensemble. If the output state is random (e.g., the result of a measurement), one gets the probabilities of the new ensemble using the Bayes rule. This is the first approach in (3).

If the mixture is really part of an entangled state, one should apply the calculation to the purification of the state and then trace out the inaccessible subsystem as in (5). This procedure will, in general, give a different answer, as (5) demonstrates.

Finally, if there are such objects as "true density matrices", one can calculate with them directly. This is what we do in (4), and it gives the same answer as tracing out the reference system X' of the purified state in (5). Also, Bennett *et al.* assume that a labeled mixture of states is a "true density matrix," and this assumption is what leads them to conclude that D-CTCs are "impotent" in Refs. [13, 14].

In summary, the first ontological representation of a quantum state as a proper mixture leads to a dramatically different conclusion for P-CTC-assisted circuits than the second and third ontological representations (which both lead to the same conclusion). We also note that it is the same with D-CTC-assisted circuits (the first representation leads to differing conclusions than the second/third), but the states output by a D-CTC-assisted circuit are different from those output by a P-CTC-assisted one.

Fig. 3 A PCTC-assisted circuit
that can factor an integer
efficiently. The circuit exploits
the ability of a P-CTC to
eliminate incorrect solutions by
making them paradoxical
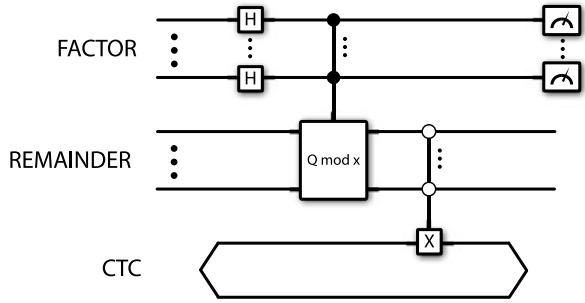
4 P-CTCs Can Help Solve Hard Problems

Lloyd *et al.* prove that the computational power of quantum computers and P-CTCs is equivalent to PP ("Probabilistic Polynomial time") [18], whereas the computational power of Deutsch's CTCs [6] is PSPACE [8]. The proof is simple—since we can simulate any postselected measurement with P-CTCs, and can simulate P-CTCs with postselected measurements, the two paradigms have equivalent computational power. Since Aaronson proved that quantum mechanics with postselection has computational power PP [23], PCTCs indeed have computational power equivalent to that of PP. PP is a rather powerful computational class, including (for example) all problems in NP. It is known to be contained in PSPACE, however, and is generally believed to be less powerful.

It is instructive to outline explicit P-CTC-assisted circuits that illustrate the power of P-CTCs. In the next few sections, we give explicit P-CTC-assisted circuits that can factor efficiently, can solve any problem in the intersection of NP and co-NP, and can probabilistically solve any problem in NP. All of these circuits use just one P-CTC qubit. The structure of these circuits draws on ideas from the algorithms in Ref. [24], and are closely related to the construction of Aaronson [23] in his proof that NP ⊆ PostBQP.

4.1 Factoring

Let Q be the number to factor and suppose that it is N bits long (so that $N \approx \log(Q)$). The P-CTC-assisted circuit consists of a CTC qubit and two N-qubit registers: a REMAINDER register and a FACTOR register. The steps of the circuit are as follows (depicted in Fig. 3):

1. Initialize the FACTOR and REMAINDER registers to $|0\rangle$. Apply Hadamard gates to all the qubits in the FACTOR register. This first set of Hadamards is equivalent to the following unitary:

$$U_1 \equiv (H^{\otimes N})_F,$$

where "F" denotes the FACTOR register.

2. Act with a controlled unitary that calculates the modulo operation on the FACTOR register and places it in the REMAINDER register:

$$U_2 \equiv \sum_{j=0}^{2^N-1} (U_j)_R \otimes |j\rangle\langle j|_F.$$

In the above, "R" indicates the REMAINDER register, and U_j is some unitary chosen so that

$$U_j|0\rangle = \begin{cases} |1\rangle & \text{if } j \in \{0, Q\}, \\ |Q \bmod j\rangle & \text{else.} \end{cases}$$

If j divides Q and j is not equal to 0 or Q, then the REMAINDER register contains 0. Otherwise, it contains a nonzero number, the remainder of Q/j.

3. Apply the following controlled unitary from the REMAINDER register to the CTC register:

$$U_3 \equiv |0\rangle\langle 0|_R \otimes I_F \otimes I_{CTC} + (I - |0\rangle\langle 0|)_R \otimes I_F \otimes X_{CTC}.$$

4. Measure the FACTOR register, and let the CTC qubits continue through the CTC.

We can verify that the P-CTC-assisted circuit is behaving as it should by considering the induced transformation (as in (1)). The cascade of U_1, U_2, and U_3 is the following unitary:

$$\sum_{j=0}^{2^N-1} [|0\rangle\langle 0|U_j]_R \otimes [|j\rangle\langle j|H^{\otimes N}]_F \otimes I_{CTC}$$

$$+ \sum_{j=0}^{2^N-1} [(I - |0\rangle\langle 0|)U_j]_R \otimes [|j\rangle\langle j|H^{\otimes N}]_F \otimes X_{CTC}.$$

Tracing over the CTC qubit gives the induced transformation:

$$\sum_{j=0}^{2^N-1} [|0\rangle\langle 0|U_j]_R \otimes [|j\rangle\langle j|H^{\otimes N}]_F.$$

Applying this transformation to a FACTOR and REMAINDER register both initialized to $|0\rangle$ gives the following state:

$$|0\rangle_R \sum_{j \,:\, Q \bmod j=0 \wedge j\neq Q \wedge j\neq 0} |j\rangle_F,$$

where we see that the effect of the last controlled gate in Fig. 2 is to eliminate all of the invalid answers or the ones for which $j \in \{0, Q\}$ by making these possibilities paradoxical. Measuring the FACTOR register then returns a factor of Q. The algorithm
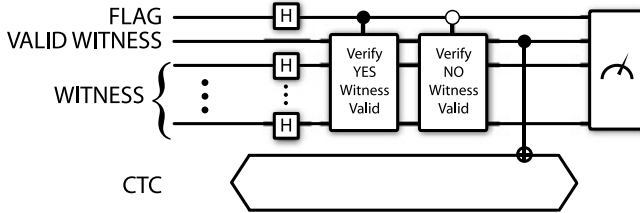
Fig. 4 A PCTC-assisted circuit for determining a valid witness for a decision problem in the intersection of NP and co-NP

fails in the case where Q is prime. But since primality can be checked efficiently, we just assume that we only use the algorithm with a composite (non-prime) Q.

If the CTC qubits produce a number $|j\rangle$ that is not a factor of Q, then a NOT is applied to the CTC qubit. This would produce a paradox, which is forbidden for P-CTCs. Because the initial state coming out of the CTC contains components including all numbers $|j\rangle$, those components that are factors of Q have their probabilities magnified, and all others have their probabilities suppressed. The circuit uses the grandfather paradox such that the only histories that return a factor are self-consistent. This idea is the same as that in Ref. [24] and also exploited by Aaronson to illustrate the power of postselected quantum computation [23].

4.2 Decision Problems in the Intersection of NP and co-NP

A decision problem lying in the intersection of NP and co-NP is one for which there is a short witness for both a YES answer and a NO answer. We can solve any decision problem in this complexity class with a P-CTC-assisted circuit. The idea here is essentially the same as in the P-CTC-assisted factoring algorithm, only there are now two parts. Suppose that for a particular decision problem both witnesses can be represented using no more than N bits. The P-CTC-assisted circuit consists of four quantum registers: a FLAG qubit, a VALID WITNESS qubit, a WITNESS register with N qubits, and a CTC qubit. It operates as follows (depicted in Fig. 4):

1. Initialize the FLAG qubit, the VALID WITNESS qubit, and the WITNESS register to $|0\rangle$. Apply Hadamard gates to the FLAG qubit and to the N qubits in the WITNESS register. The flag qubit being equal to 1 means that the answer is YES. The FLAG qubit being equal to 0 means the answer is NO.
2. Conditioned on the FLAG qubit being equal to 1, the answer is (claimed to be) YES and the remaining N qubits hold a witness $|y\rangle$. The FLAG qubit acts as a control bit. If FLAG $= 1$, then pass the N qubits of the witness, plus the VALID WITNESS qubit in the state $|0\rangle_V$, through a circuit that verifies whether the witness is valid:

$$|0\rangle_V|y\rangle_W \rightarrow |j\rangle_V|y\rangle_W,$$

where "V" denotes the VALID WITNESS qubit, "W" denotes the WITNESS register, $j = 0$ if the witness is valid, and $j = 1$ otherwise.
3. Conditioned on the FLAG qubit being equal to 0, the answer is (claimed to be) NO and the remaining N qubits hold a witness $|n\rangle$. The FLAG qubit again acts as

a control bit. If FLAG $= 0$, then pass the N qubits of the witness, plus the VALID WITNESS qubit in the state $|0\rangle_V$, through a circuit that verifies whether the witness is valid:

$$|0\rangle_V|n\rangle_W \rightarrow |j\rangle_V|n\rangle_W,$$

where $j = 0$ if the witness is valid, and $j = 1$ otherwise.

4. Apply a CNOT from the VALID WITNESS qubit holding $|j\rangle$ to the CTC qubit.
5. Measure the FLAG qubit, the VALID WITNESS qubit, and the WITNESS register. The measurement results give an answer to the decision problem (in the FLAG qubit and in the VALID WITNESS qubit) plus the witness.

The reasoning that this algorithm works is essentially the same as that for factoring. The last CNOT gate makes a paradox out of any scenario in which the VALID WITNESS qubit is equal to one, thus eliminating the possibilities for which the witness is invalid.

4.3 SAT

A satisfiability (SAT) decision problem tries to determine if there exists a satisfying solution for a Boolean formula (one which makes the formula evaluate to TRUE). We now show that we can probabilistically solve a SAT decision problem, which implies that we can probabilistically solve any problem in NP because SAT is NP-complete [35]. Suppose that we want to solve SAT on N bits. There is a Boolean function $f(x_1, \ldots, x_N)$ defined by a formula that can be evaluated efficiently. We want to know if there are values of $x_1, \ldots, x_N$ that make $f(x_1, \ldots, x_N) = 1$, and if so, we would like to have a satisfying assignment. (The latter is not necessary for a decision problem, of course, but we get it for free.)

The P-CTC-assisted circuit acts on four different quantum registers: a FLAG qubit, a VALID WITNESS qubit, an N-qubit WITNESS register, and a CTC qubit. If the FLAG qubit is equal to 1, the function has a satisfying assignment, and if it is 0, it does not. The circuit has the following steps:

1. Initialize the FLAG qubit, the VALID WITNESS qubit, and the WITNESS register to $|0\rangle$. Apply Hadamard gates to the FLAG qubit and the N-qubit WITNESS register.
2. Conditioned on the FLAG qubit being equal to 1, the answer is (claimed to be) YES, and the WITNESS register holds a satisfying assignment $|x_1, \ldots, x_N\rangle_W$. The FLAG qubit acts as a control bit. If FLAG $= 1$, then pass the N-qubit WITNESS register, plus the VALID WITNESS qubit in the state $|0\rangle_V$, through a circuit that calculates

$$|x_1, \ldots, x_N\rangle_W|0\rangle_V \rightarrow |x_1, \ldots, x_N\rangle_W|j\rangle_V,$$

where $j = \neg f(x_1, \ldots, x_N)$. (That is, $j = 0$ if $x_1, \ldots, x_N$ is satisfying, and $j = 1$ if not.)
3. Conditioned on the FLAG qubit being equal to 0, the answer is (claimed to be) NO, and we require that the N-qubit WITNESS register hold all zeros: $|00 \ldots 0\rangle$. Apply the following controlled-unitary:

$$I_F \otimes |0\ldots0\rangle\langle0\ldots0|_W \otimes I_V + |1\rangle\langle1|_F \otimes (I - |0\ldots0\rangle\langle0\ldots0|)_W$$
$$\otimes I_V + |0\rangle\langle0|_F \otimes (I - |0\ldots0\rangle\langle0\ldots0|)_W \otimes X_V.$$

The VALID WITNESS qubit now holds $|1\rangle_V$ if the qubits in the N-qubit WITNESS register are not all zeros, and $|0\rangle_V$ if they are.

4. Apply a CNOT from the VALID WITNESS qubit $|j\rangle_V$ to the CTC qubit.
5. Measure all the ancillas.

There are two cases:

1. If the function has no satisfying assignment, then the only non-paradoxical output is all zeros (including the flag bit): $|0\rangle_F|0\rangle_V|00\ldots0\rangle_W$. This outcome occurs with probability one in this case.
2. If the function has m satisfying assignments, then there are $m+1$ non-paradoxical results: the m satisfying assignments, plus the all zero state $|0\rangle_F|0\rangle_V|00\ldots0\rangle_W$. These $m+1$ results occur with equal probability.

So in case 1, the correct answer (NO) always occurs, and in case 2, a satisfying assignment (YES) occurs with probability

$$\frac{m}{m+1} \geq 1/2,$$

and the false answer (NO) occurs with probability

$$\frac{1}{m+1} \leq 1/2.$$

To improve the probabilities, we can replicate some of these steps while still using just one CTC qubit. Replicate steps 1–3 k times on k copies of all of the above registers (except for the CTC qubit). So we now get k different flag bits and (potentially) satisfying assignments. We then do the following unitary from the k VALID WITNESS qubits to the P-CTC qubit:

$$|00\ldots0\rangle\langle00\ldots0| \otimes I + (I - |00\ldots0\rangle\langle00\ldots0|) \otimes X.$$

In case 1, we get the result $|0\rangle_F|0\rangle_V|00\ldots0\rangle_W$ every time. In case 2, we get the wrong answer $|0\rangle_F|0\rangle_V|00\ldots0\rangle_W$ every time only with probability:

$$\frac{1}{(m+1)^k} \leq \frac{1}{2^k}.$$

We can make this failure probability as small as we like with only logarithmic overhead.

5 Conclusion

Prior research has shown that closed timelike curves operating according to Deutsch's model can have dramatic consequences for computation and information processing

[8, 9] if one operates on "proper" mixtures of quantum states [34]. Lloyd *et al.* then showed that postselected closed timelike curves have computational power equivalent to the complexity class PP [18, 19], by exploiting a result of Aaronson on postselected quantum computation [23].

In this paper, we showed how to implement any postselected operation with certainty with just one P-CTC qubit, and we discussed an important difference between D-CTCs and P-CTCs in which the future existence of a P-CTC could affect the probabilistic results of a present experiment by creating a paradox for particular outcomes. Theorem 1 then proves that P-CTCs can help distinguish an arbitrary set of linearly independent states, but they are of no use for helping to distinguish linearly dependent states. We also discussed how three different ontological descriptions of a state (equivalent in standard linear quantum mechanics) do not necessarily lead to the same consequences in the nonlinear theory of postselected closed timelike curves. Finally, we provided explicit P-CTC-assisted circuits that efficiently factor an integer, solve any decision problem in the intersection of NP and co-NP, and probabilistically solve any decision problem in NP (all using just one P-CTC qubit).

References

1. Gödel, K.: An example of a new type of cosmological solutions of Einstein's field equations of gravitation. Rev. Mod. Phys. **21**(3), 447–450 (1949)
2. Bonnor, W.B.: The rigidly rotating relativistic dust cylinder. J. Phys. A, Math. Gen. **13**(6), 2121 (1980)
3. Gott, J.R.: Closed timelike curves produced by pairs of moving cosmic strings: Exact solutions. Phys. Rev. Lett. **66**(9), 1126–1129 (1991)
4. Hartle, J.B.: Unitarity and causality in generalized quantum mechanics for nonchronal spacetimes. Phys. Rev. D, Part. Fields **49**(12), 6543–6555 (1994)
5. Morris, M.S., Thorne, K.S., Yurtsever, U.: Wormholes, time machines, and the weak energy condition. Phys. Rev. Lett. **61**(13), 1446–1449 (1988)
6. Deutsch, D.: Quantum mechanics near closed timelike lines. Phys. Rev. D, Part. Fields **44**(10), 3197–3217 (1991)
7. Bacon, D.: Quantum computational complexity in the presence of closed timelike curves. Phys. Rev. A **70**(3), 032309 (2004)
8. Aaronson, S., Watrous, J.: Closed timelike curves make quantum and classical computing equivalent. Proc. R. Soc. A **465**(2102), 631–647 (2009)
9. Brun, T.A., Harrington, J., Wilde, M.M.: Localized closed timelike curves can perfectly distinguish quantum states. Phys. Rev. Lett. **102**(21), 210402 (2009)
10. DeJonghe, R., Frey, K., Imbo, T.: Discontinuous quantum evolutions in the presence of closed timelike curves. Phys. Rev. D, Part. Fields **81**, 087501 (2010). arXiv:0908.2655
11. Pati, A.K., Chakrabarty, I., Agrawal, P.: Purification of mixed state with closed timelike curve is not possible. May 2010. arXiv:1003.4221
12. Holevo, A.S.: Bounds for the quantity of information transmitted by a quantum channel. Probl. Inf. Transm. **9**, 177–183 (1973)
13. Bennett, C.H., Leung, D., Smith, G., Smolin, J.A.: Can closed timelike curves or nonlinear quantum mechanics improve quantum state discrimination or help solve hard problems? Phys. Rev. Lett. **103**(17), 170502 (2009)

14. Bennett, C.H., Leung, D., Smith, G., Smolin, J.: The impotence of nonlinearity: Why closed timelike curves and nonlinear quantum mechanics don't improve quantum state discrimination, and haven't been shown to dramatically speed up computation, if computation is defined in a natural, adversarial way. In: Rump Session Presentation at the 13th Workshop on Quantum Information Processing, Zurich, Switzerland, January 2010 (2010)

15. Ralph, T.C., Myers, C.R.: Information flow of quantum states interacting with closed timelike curves. March 2010. arXiv:1003.1987

16. Cavalcanti, E.G., Menicucci, N.C.: Verifiable nonlinear quantum evolution implies failure of density matrices to represent proper mixtures. April 2010. arXiv:1004.1219

17. Wallman, J.J., Bartlett, S.D.: Revisiting consistency conditions for quantum states of systems on closed timelike curves: an epistemic perspective. May 2010. arXiv:1005.2438

18. Lloyd, S., Maccone, L., Garcia-Patron, R., Giovannetti, V., Shikano, Y., Pirandola, S., Rozema, L.A., Darabi, A., Soudagar, Y., Shalm, L.K., Steinberg, A.M.: Closed timelike curves via post-selection: theory and experimental demonstration. May 2010. arXiv:1005.2219

19. Lloyd, S., Maccone, L., Garcia-Patron, R., Giovannetti, V., Shikano, Y.: The quantum mechanics of time travel through post-selected teleportation. July 2010. arXiv:1007.2615

20. Svetlichny, G.: Effective quantum time travel. February 2009. arXiv:0902.4898

21. Bennett, C.H.: Talk at QUPON, Wien. http://www.research.ibm.com/people/b/bennetc/, May 2005

22. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. **70**, 1895–1899 (1993)

23. Aaronson, S.: Quantum computing, postselection, and probabilistic polynomial-time. Proc. R. Soc. A **461**(2063), 3473–3482 (2005)

24. Brun, T.A.: Computers with closed timelike curves can solve hard problems. Found. Phys. Lett. **16**, 245–253 (2003)

25. Chefles, A.: Unambiguous discrimination between linearly independent quantum states. Phys. Lett. A **239**, 339–347 (1998)

26. Bennett, C.H.: Private communication. In: 12th Workshop on Quantum Information Processing, Albuquerque, New Mexico, January 2009 (2009)

27. Smith, G.: Private communication. In: International Symposium on Information Theory, Austin, Texas, June 2010 (2010)

28. Horowitz, G.T., Maldacena, J.: The black hole final state. J. High Energy Phys. **2004**(02), 008 (2004)

29. Lloyd, S.: Almost certain escape from black holes in final state projection models. Phys. Rev. Lett. **96**(6), 061302 (2006)

30. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)

31. Bennett, C.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)

32. Bennett, C., Brassard, G.: Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, December 1984, pp. 175–179 (1984)

33. Scarani, V., Acin, A., Ribordy, G., Gisin, N.: Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys. Rev. Lett. **92**, 057901 (2004)

34. d'Espagnat, B.: On Physics and Philosophy. Princeton University Press, Princeton (2006). ISBN:978-0-691-11964-9

35. Cook, S.A.: The complexity of theorem proving procedures. In: Proceedings of the 3rd Annual ACM Symposium on the Theory of Computing, pp. 151–158 (1971)