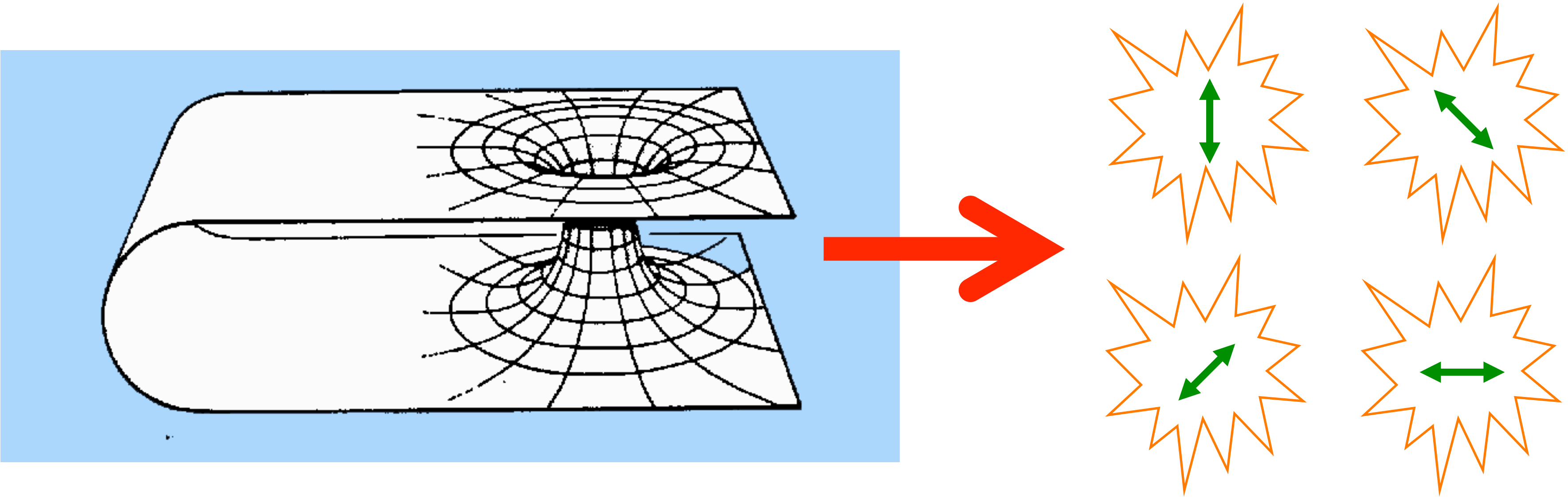


Quantum Information with Closed Timelike Curves

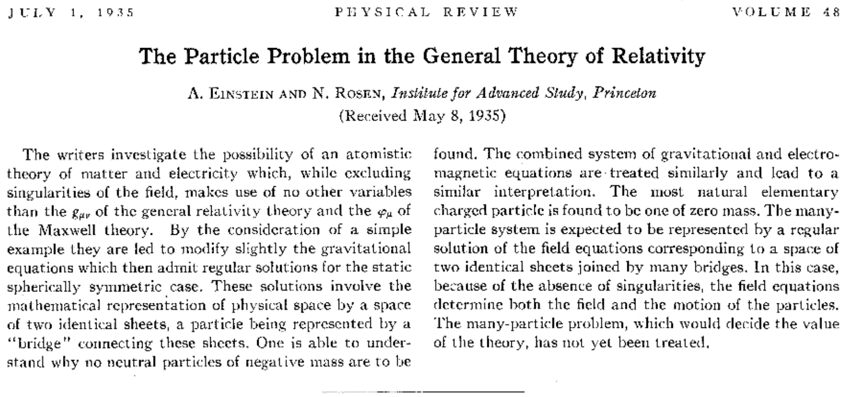
Todd A. Brun (USC)

In collaboration with Jim Harrington and Mark M. Wilde

…or as I prefer to put it:

As I told you tomorrow, time machines can solve hard problems

Closed timelike curves



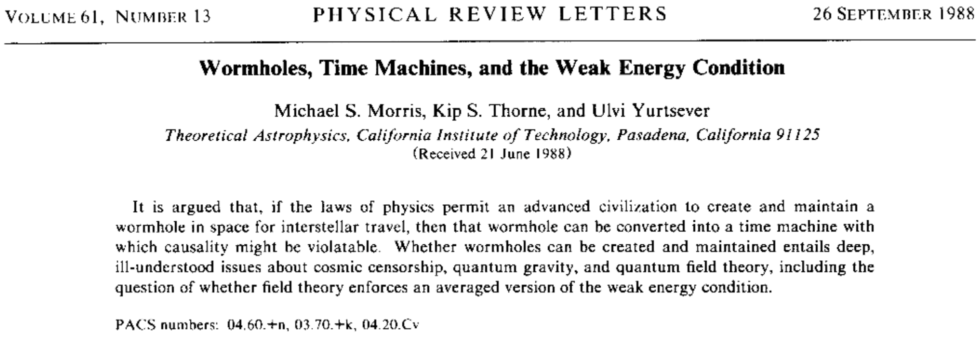
JULY 1, 1935 PHYSICAL REVIEW VOLUME 48

The Particle Problem in the General Theory of Relativity

A. EINSTEIN AND N. ROSEN, *Institute for Advanced Study, Princeton*

(Received May 8, 1935)

The writers investigate the possibility of an atomistic theory of matter and electricity which, while excluding singularities of the field, makes use of no other variables than the $g_{\mu\nu}$ of the general relativity theory and the φ_μ of the Maxwell theory. By the consideration of a simple example they are led to modify slightly the gravitational equations which then admit regular solutions for the static spherically symmetric case. These solutions involve the mathematical representation of physical space by a space of two identical sheets, a particle being represented by a "bridge" connecting these sheets. One is able to understand why no neutral particles of negative mass are to be found. The combined system of gravitational and electromagnetic equations are treated similarly and lead to a similar interpretation. The most natural elementary charged particle is found to be one of zero mass. The many-particle system is expected to be represented by a regular solution of the field equations corresponding to a space of two identical sheets joined by many bridges. In this case, because of the absence of singularities, the field equations determine both the field and the motion of the particles. The many-particle problem, which would decide the value of the theory, has not yet been treated.



VOLUME 61, NUMBER 13 PHYSICAL REVIEW LETTERS 26 SEPTEMBER 1988

Wormholes, Time Machines, and the Weak Energy Condition

Michael S. Morris, Kip S. Thorne, and Ulvi Yurtsever

Theoretical Astrophysics, California Institute of Technology, Pasadena, California 91125

(Received 21 June 1988)

It is argued that, if the laws of physics permit an advanced civilization to create and maintain a wormhole in space for interstellar travel, then that wormhole can be converted into a time machine with which causality might be violatable. Whether wormholes can be created and maintained entails deep, ill-understood issues about cosmic censorship, quantum gravity, and quantum field theory, including the question of whether field theory enforces an averaged version of the weak energy condition.

PACS numbers: 04.60.+n, 03.70.+k, 04.20.Cv

- Closed timelike curves (CTCs) are spacetime objects allowed by the theory of general relativity (although perhaps not by a complete theory of quantum gravity).
- Recent work has shown how CTC resources would greatly boost classical and quantum computational power.
- Question: how are information processing tasks affected when a party has access to (localized) CTCs?

Time-travel paradoxes

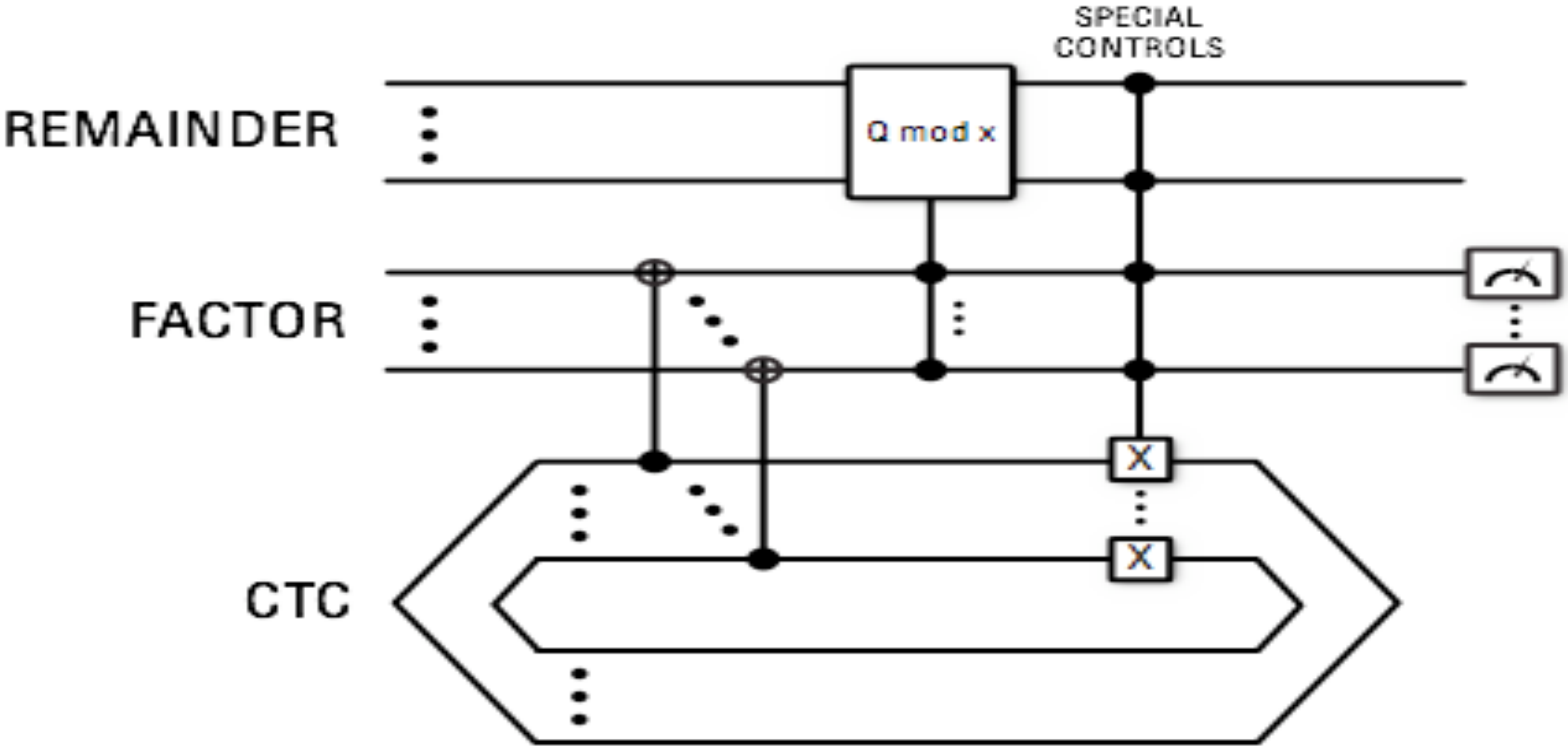
- The possibility of time travel has always raised difficult questions about causality. These are often phrased in terms of paradoxes, that fall into two main types:
- *Grandfather paradoxes*. A time traveler goes back before his father was born and kills his grandfather. Therefore, he was never born, and never went back.
- *Uncaused effects*. A time traveler receives a piece of information from her future self; in the future, she passes in back to her earlier self. Where did the information come from?

Solving hard problems with CTCs

- Grandfather paradoxes seem difficult to accommodate within a reasonable theory (though Deutsch makes a good try, as we shall see). But the kind of self-consistent evolution described in the second paradox might actually be exploited.
- Suppose we set up a situation in which an inconsistency will occur *unless* some specified information appears. We could then find the answers to hard problems without going to the trouble of actually solving them.

Brun, Found. Phys. Lett. 16, 245 (2003).

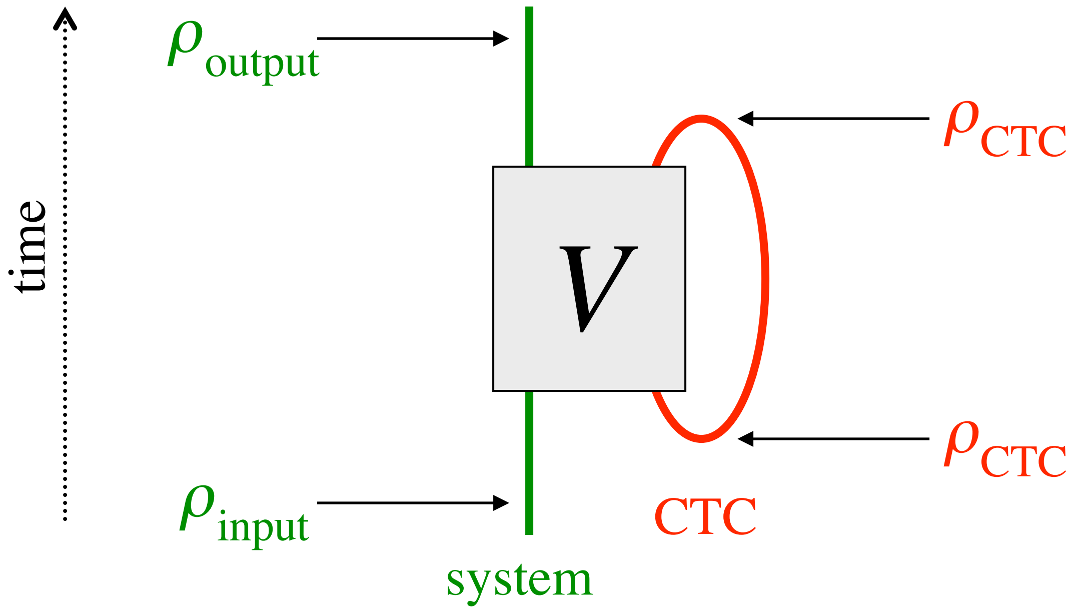
Factoring numbers



I also gave a (flawed) argument that CTCs enabled efficient solution of even harder problems—NP-complete and PSPACE-complete problems. To show this, though, one needs a more precise model of how CTCs work.

D. Deutsch, Phys. Rev. D 44, 3197 (1991)

Deutsch’s self-consistency criteria



$$\boxed{\rho_{\text{CTC}} = \text{Tr}_{\text{system}}\left\{V(\rho_{\text{input}} \otimes \rho_{\text{CTC}})V^{\dagger}\right\}}$$

$$\rho_{\text{output}} = \text{Tr}_{\text{CTC}}\left\{V(\rho_{\text{input}} \otimes \rho_{\text{CTC}})V^{\dagger}\right\}$$

Bacon, PRA 70, 032309 (2004); Aaronson and Watrous, Proc. R. Soc. A 465, 631 (2009)

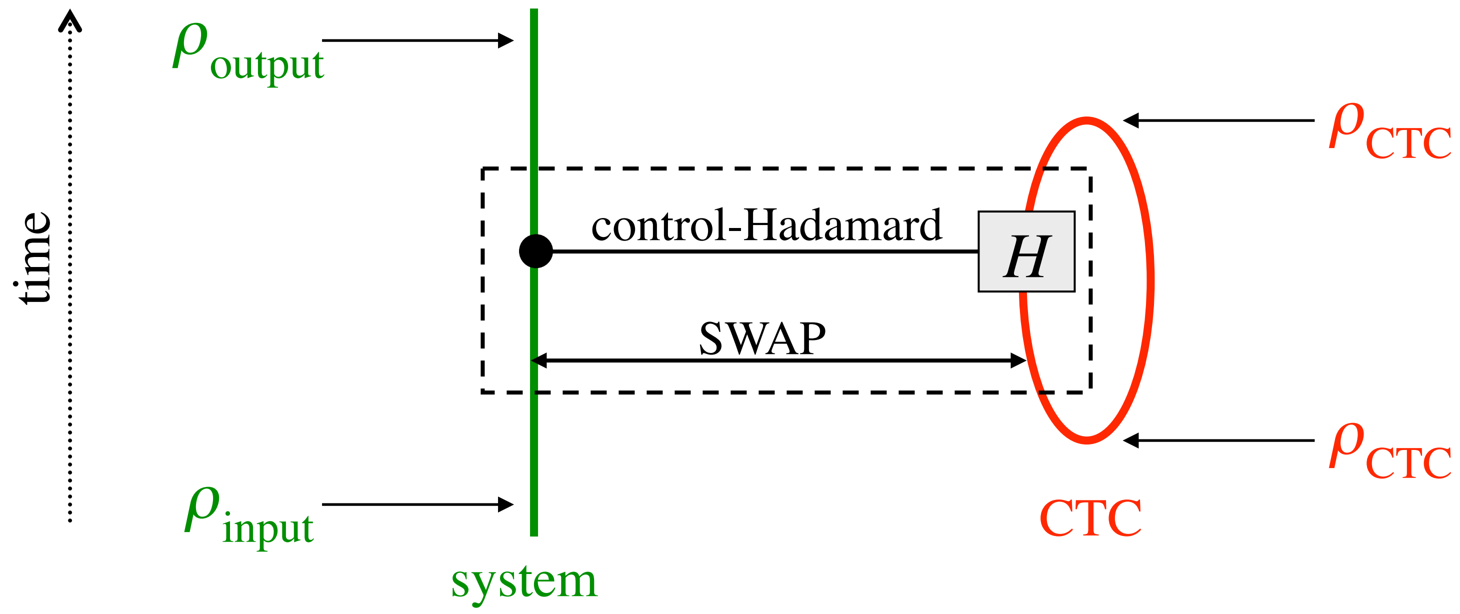
Solving problems with DCTCs

- Since DCTCs produce an effective nonlinear evolution, they can (for example) magnify the probability of distinguishing one quantum state from another, nonorthogonal, state.
- Bacon showed that this could be used to solve NP-complete problems—in particular, the problem SAT. A nonlinear evolution allows him to distinguish between the cases of zero and nonzero satisfying assignments for a Boolean function.

- Aaronson and Watrous carried this a step further, showing that both classical and quantum computers with CTCs could efficiently solve any problem in PSPACE.
- They used the property of the Deutsch approach that it finds a self-consistent solution for ρ_{CTC}. They set up the program so that the only self-consistent evolution is a loop over all configurations of a Turing machine, with a control bit *b* set to the final answer to the problem.
- DCTCs can also enhance other tasks besides computation.

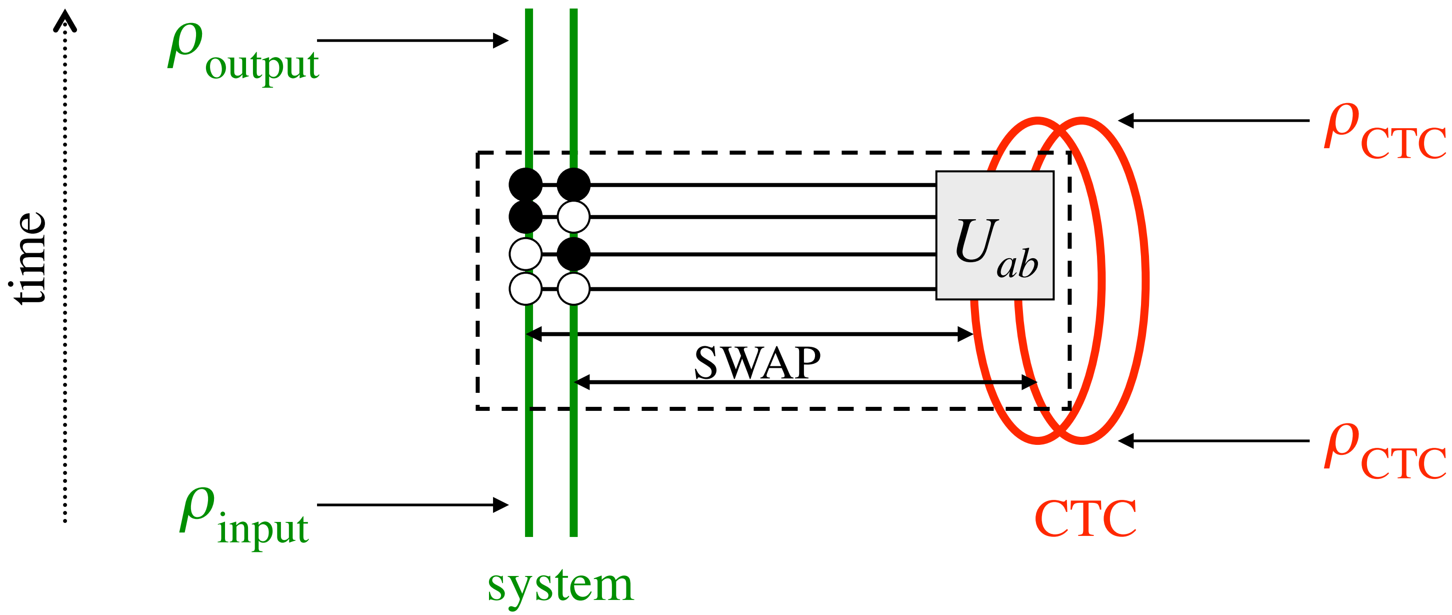
Brun, Harrington and Wilde, Phys. Rev. Lett. 102, 210402 (2009).

Breaking B92 QKD



- This circuit maps $|0\rangle\langle 0| \rightarrow |0\rangle\langle 0|$ and $|-\rangle\langle -| \rightarrow |1\rangle\langle 1|$.
- A straightforward modification of the unitaries enables perfect distinguishability of any two quantum states.

Breaking BB84 QKD

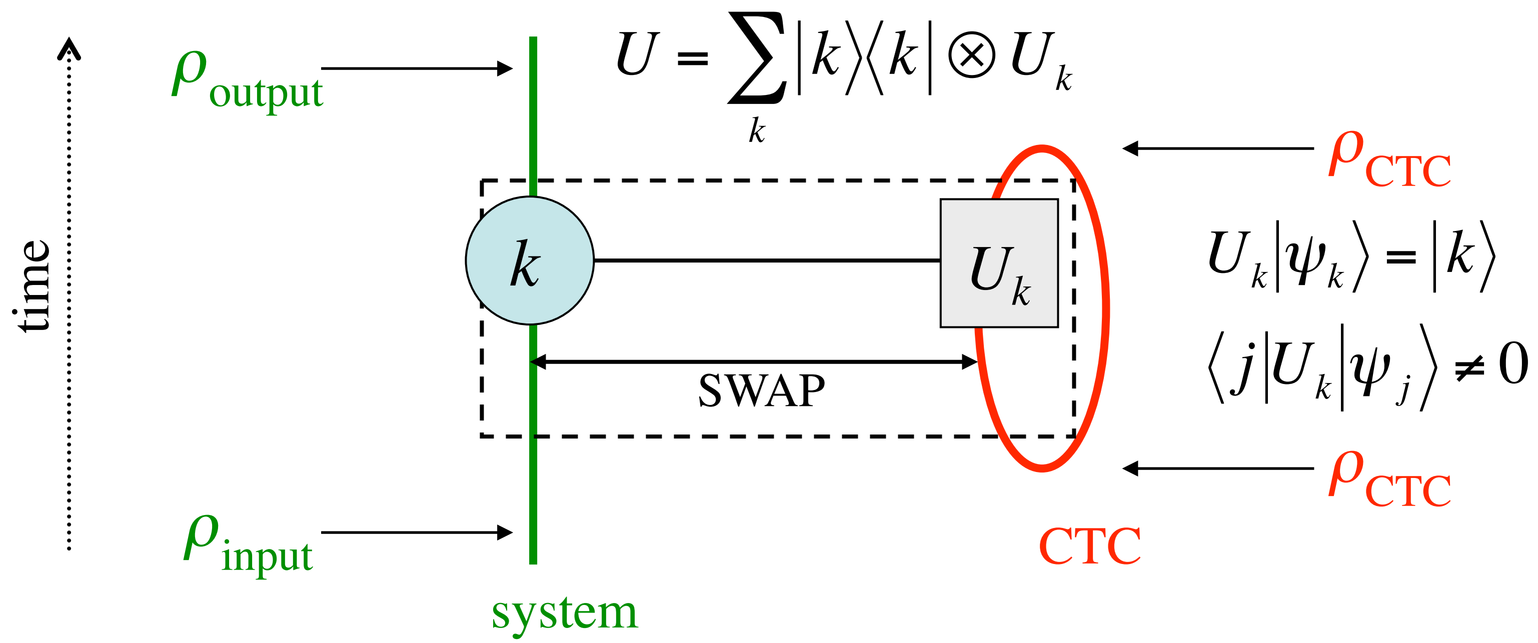


- This circuit maps $|\psi\rangle\langle\psi|\otimes|0\rangle\langle 0| \rightarrow |\mathrm{a}\rangle\langle \mathrm{a}|\otimes|\mathrm{b}\rangle\langle \mathrm{b}|$, where *a* denotes the basis and *b* denotes the bit value.
- The controlled unitaries are:

$$U_{00} = \mathrm{SWAP} \qquad U_{10} = (X\otimes I)\circ(H\otimes I)$$

$$U_{01} = X\otimes X \qquad U_{11} = (X\otimes H)\circ\mathrm{SWAP}$$

Distinguishing Arbitrary States



$$U = \sum_k |k\rangle\langle k| \otimes U_k$$

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

$$\langle j|U_k|\psi_j\rangle \neq 0$$

- We can do the same thing with an arbitrary set of (in general nonorthogonal) states $\{|\psi_k\rangle\}$.
- This will break any QKD protocol that relies on nonorthogonality; it also allows a single q-bit to carry an arbitrary amount of information.

Infinite channel capacity

- To make a single quantum bit carry *n* bits of information, choose 2^n nonorthogonal states:

$$|\varphi_0\rangle, |\varphi_1\rangle, \ldots, |\varphi_{2^n-1}\rangle.$$

- Alice encodes her *n*-bit message by selecting one of these states and sending it to Bob. Using a DCTC, he can determine which state was sent and extract *n* bits of information, where in principle *n* is arbitrarily large.

Bennett et al., PRL 103, 170502 (2009).

A linearity trap?

- In a more recent paper, Bennett et al. suggested that this protocol cannot really succeed. Since the receiver (Bob) does not know the state, he should describe it by a mixed state:

$$\rho = \frac{1}{2}\sum_{x=0,-} |\phi_x\rangle_A \langle\phi_x| \otimes |x\rangle_B \langle x|.$$

- The protocol, which succeeds on both 0 and -, fails on this mixed state. They termed this a “linearity trap.”

Ralph and Myers, PRA 82, 062330 (2010).

- This argument, however, has some flaws of its own. The authors assume that a probabilistic mixture can be represented by a density matrix, just as in standard QM. In a nonlinear theory, however, this is *not* true.
- Moreover, that choice of state is subjective from Bob's point of view. Alice will certainly not use that mixture to describe the state, since she knows the value of x.
- However, there is a related argument that does raise serious questions about the Deutsch criterion.

Pati, Chakrabarty and Agrawal, PRA 84, 062325 (2011).

DCTCs and Many-Worlds

- Suppose that Alice and Bob are in the following *superposition* state:

$$\left|\psi_{AB}\right\rangle = \left(1/\sqrt{2}\right)\sum_{x=0,-}\left|\phi_x\right\rangle_A \otimes \left|x\right\rangle_B .$$

- Since Deutsch justifies his criterion within the Many-Worlds interpretation of QM, this is a natural state to arise. But note, here again the protocol fails!
- It seems that to use the Deutsch criterion, one must know the state of the full wavefunction, not just your own "branch."

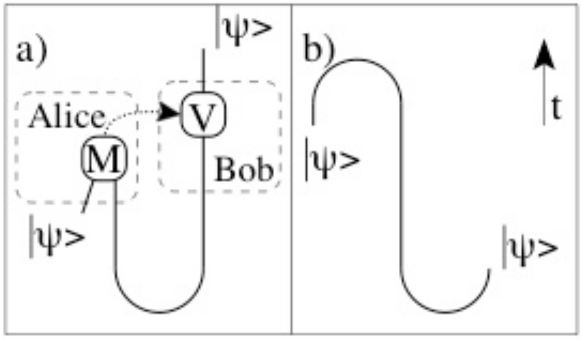
Discussion

- The CTC in this construction need only exist a very short time (just long enough for the unitaries); for state discrimination, they are needed only on Bob's side.
- In the absence of noise, an arbitrary number of classical bits can then be stored and retrieved with a single qubit, thus violating Holevo's bound of one bit per qubit.
- This system also raises uncomfortable questions about superluminal signaling.
- It is also not entirely clear how it works within the Many-Worlds theory used to justify it.

Lloyd et al., PRL 106, 040403 (2011); Lloyd et al., arXiv:1007.2615v1; Svetlichny, arXiv:0902.4898.

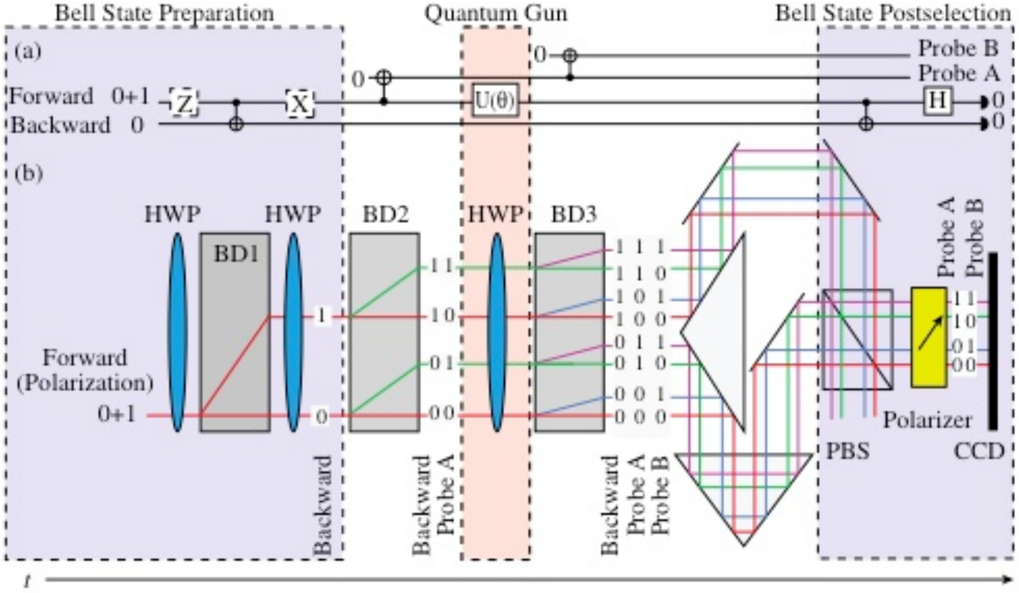
Postselected CTCs

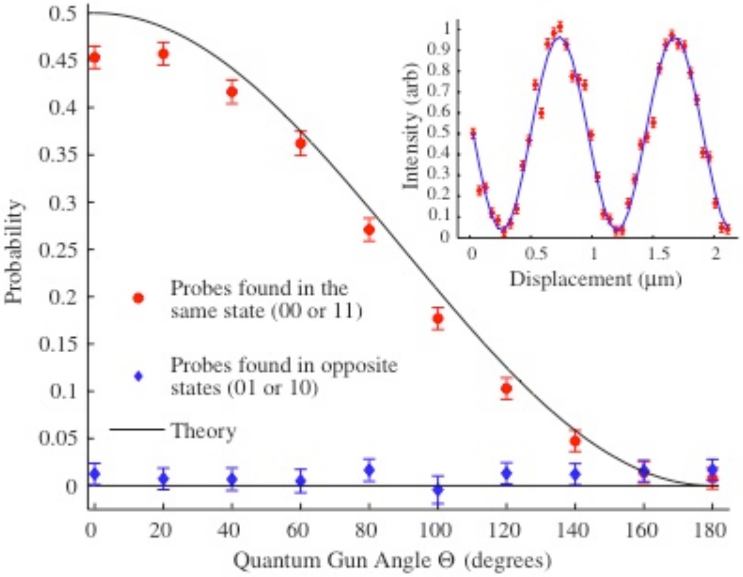
- A different approach to describing QM with CTCs was invented (but never published) by Bennett and Schumacher.



- This approach is based on *teleportation*. If one were guaranteed to always get a particular desired measurement outcome, one could teleport a copy of a state *into the past*. This type of CTC can therefore be simulated by QM with *postselection*.

A time-travel experiment!



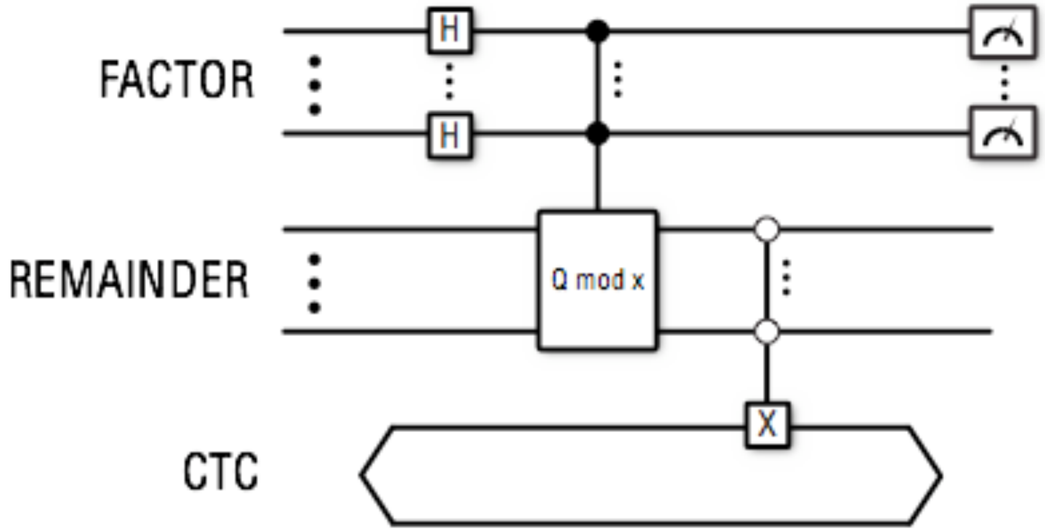


- A PCTC protocol was simulated (by post-selection) in the lab of Aephraim Steinberg.
- The experiment showed that in this approach, Grandfather paradoxes are forbidden.

Brun and Wilde, Found. Phys. 42, 341 (2011).

Computational Power of PCTCs

- PCTCs also enable efficient algorithms for hard problems. Here is a circuit for factoring:



- Note that this requires only a *single* qubit to be sent back in the CTC.

Complexity Alphabet Soup

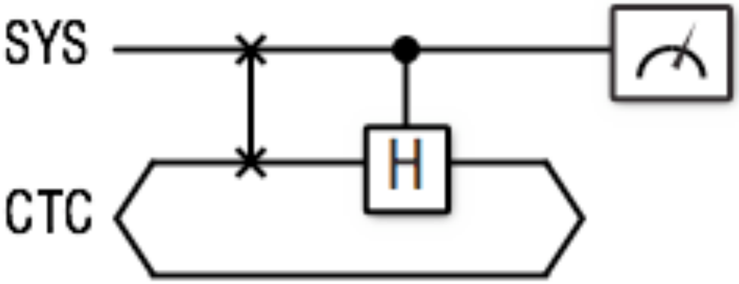
- In fact, it is not difficult to show that quantum computers with PCTCs are as powerful as quantum computers with postselection: they can solve any problem in the complexity class PP.
- The most widely believed inclusions for computational complexity classes are:

  $$\mathrm{P} = \mathrm{BPP} \subset \mathrm{NP} \subset \mathrm{PH} \subset \mathrm{PP} \subset \mathrm{PSPACE}.$$

- If this is true, the PCTCs are more powerful than standard QCs, but less than DCTCs.

Distinguishing Nonorthogonal States

- PCTCs also allow us to distinguish nonorthogonal states. (In fact, the same circuit works as with DCTCs.)

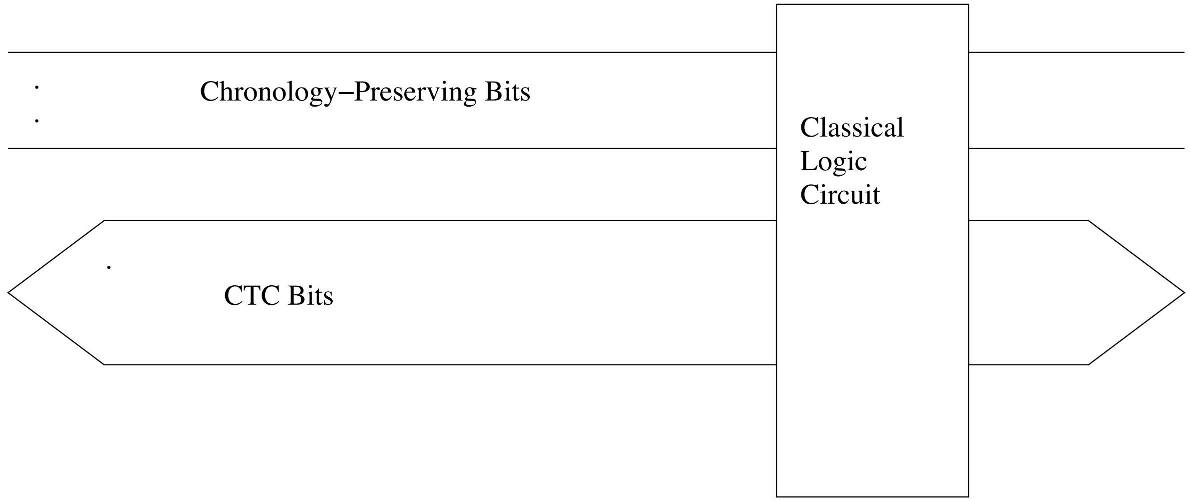


- However, PCTCs can only distinguish sets of states that are *linearly independent*. So they don’t violate the Holevo bound.

Are PCTCs paradox-free?

- Unlike DCTCs, PCTCs do not have solutions for every situation. Inconsistent evolutions—grandfather paradoxes—do not admit solutions.
- This gives another way of understanding the information-processing power of PCTCs. By setting up two alternatives—one paradoxical, the other one not—the probability of the second alternative can be dramatically enhanced.
- However, paradoxes of the second type—in which information seemingly appears out of nowhere—are still allowed by PCTCs.

A Classical Analogy



There are two natural ideas of self-consistency: we could require the CTC bits to have the same value before and after the circuit, or require them to have the same probability distribution. These two approaches are analogous to the PCTC and DCTC criteria.

Politzer, Phys. Rev. D 49, 3981 (1994); Hartle, Phys. Rev. D 49, 6543 (1994).

Other Approaches to CTCs

- A number of other approaches have been suggested for QM with CTCs.
- In the 1990s, both H. David Politzer and James Hartle did calculations for quantum evolutions on spacetimes with CTCs. While the results are not exactly comparable, the are somewhat similar in flavor to PCTCs.
- More recently, Tim Ralph has suggested a Heisenberg-like approach to CTCs, and shown that he can derive Deutsch's criterion from it.

Ralph, Phys. Rev. A 76, 012336 (2007); Ralph and Myers, PRA 82, 062330 (2010).

Conclusions

- DCTCs have advantages, in terms of guaranteed solutions and straightforward interpretation. But it is not clear that they can really be fit into a Many-Worlds picture, as claimed, and they are disturbingly powerful.
- PCTCs may make connection to other approaches (e.g., that of Hartle), and avoid some of the paradoxes of DCTCs without having to invoke Many Worlds. But they still lead to strange evolutions, and in some ways have broader effects than DCTCs.

- Of course, we have no evidence that CTCs exist at all! And if they do, this becomes at least partially an experimental question.
- But playing around with these systems is a lot of fun, and raises interesting logical questions about causality and information that may have applications elsewhere. And it certainly beats working for a living.