From monopoles to fault-tolerant quantum computation
Conference in honor of John Preskill's 60th birthday

Computational and cryptanalytic consequences of closed timelike curves

March 14, 2013

Charles Bennett
Debbie Leung
Graeme Smith
John Smolin

IBM & IQC U. Waterloo. $CRC, CFI, ORF, CIFAR, NSERC$

Time travel in fiction

Universal desire to remedy past mistakes, to peer into the future, or even to improve it

Examples:

- The Iliad (prophesy by Cassandra) (¼700BC)
- The time machine (Wells 1895)
- Back to Future (1985-90)
- Groundhog day (1993)
- Futurama (2001)
- Interstellar (by Nolan / Kip Thorne!) (Nov 2014)

Deviation from causality, inconsistencies (like the grandfather paradox) and their resolutions are often the full features ...

Time travel in physics

Not ruled out by GR, chronology protection?

A source of deep fundamental questions ...

Caltech *GRP*-340

Closed Timelike Curves

Kip S. Thorne

Theoretical Astrophysics, California Institute of Technology
Pasadena, CA 91125

ABSTRACT

This lecture reviews recent research on closed timelike curves (CTCs), including these questions: Do the laws of physics prevent CTCs from ever forming in classical spacetime? If so, by what physical mechanism are CTCs prevented? Can the laws of physics be adapted in any reasonable way to a spacetime that contains CTCs, or do they necessarily give nonsense? What insights into quantum gravity can one gain by asking questions such as these?

Feb 1993

Time travel in information science

Given CTCs:
- can one solve hard problems faster?
- can one solve impossible problems?

Can one prove results concerning computation without CTCs ?

Not so interesting:
Hide the complexity of the problem inside the CTC

e.g., compute slowly and send the answer back in time

since complexity theory seeks to understand how difficult each problem is and how useful each primitive operation is ...

The computation models using CTCs have been carefully defined so that hardness can be quantified properly.

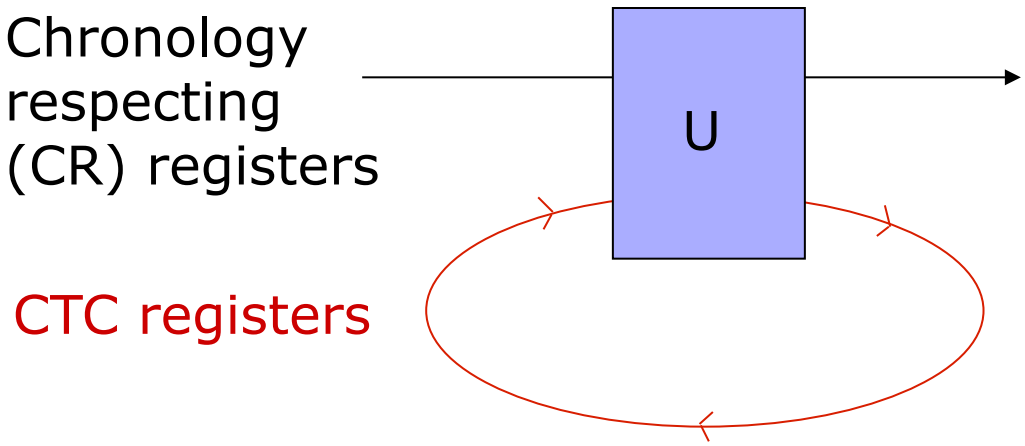
Outline

1. Deutsch CTCs
   - Method to discriminate non-orthogonal states ?
   - Algorithms for solving NP or PSPACE problems ?
   - Nonlinearity trap

2. Postselected CTCs
   - Method to discriminate non-orthogonal states
   - Algorithms for solving PP problems
   - Environmental concerns
   - Fault-tolerance ?

Focus on 2 tasks: first is an info theoretic problem on state discriminate ... second on efficient computation of hard problems. Second problem often built on the first ...

Deutsch CTCs

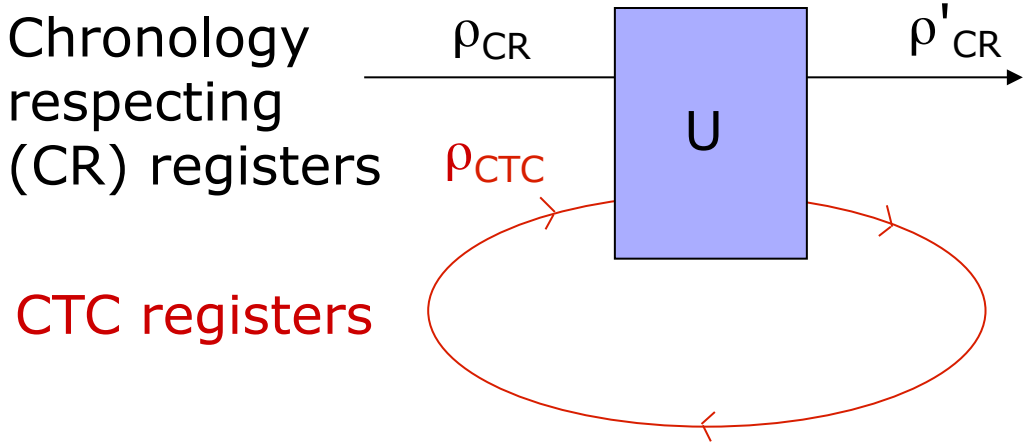


(a) The CTC occupies a compact region of spacetime (evolved from initial conditions).
(b) Two types of qubits – those traversing CTCs and those that do not.
(c) The CR registers and the CTC registers can interact unitarily.
(d) Measurements and preparation of the CTC registers are not allowed.
(e) CTC qubits are not reusable.

The grandfather paradox can be avoided if the state of CTC registers is a fixed point of the mapping induced by interaction with the CR registers. Mixed state fixed point always exists.

Deutsch CTCs

Reduces to QM far away
No Grandfather paradox
Count complexity of U
Unitary freedom in CTC



State emerging from the interaction: $U\ \rho_{CR} - \rho_{CTC}\ U^y$

Consistency requirement:

Output in CTC registers = $Tr_{CR}\ U\ \rho_{CR} - \rho_{CTC}\ U^y = \rho_{CTC}$

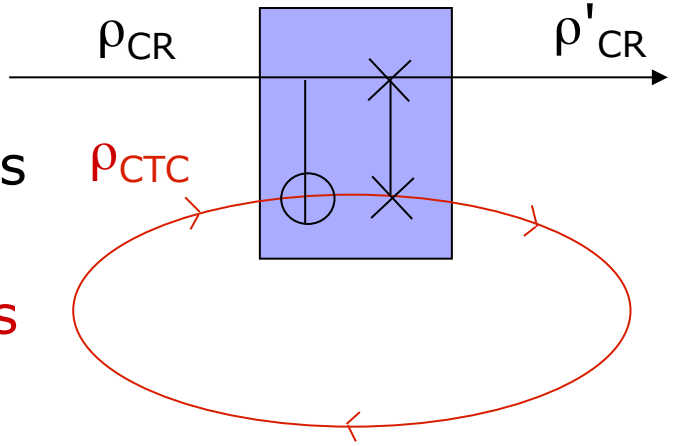
Evolution of CR registers: $\rho'_{CR} = Tr_{CTC}\ U\ \rho_{CR} - \rho_{CTC}\ U^y$

NB The fixed point ρ_{CTC} depends on ρ_{CR} $\therefore$ the CR registers evolve nonlinearly.

Example (Bacon03)

Chronology respecting (CR) registers

CTC registers



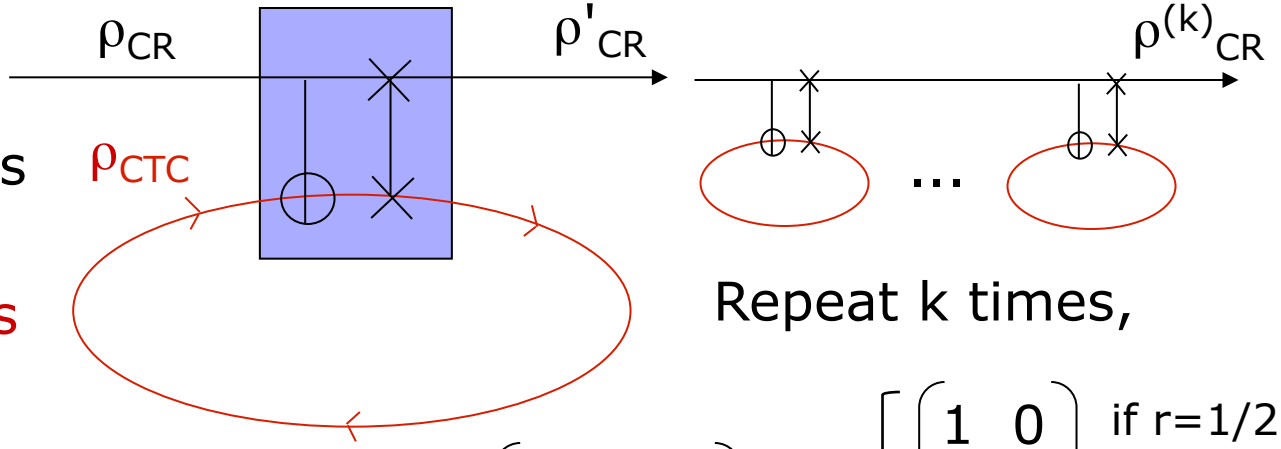
For $\rho_{CR} = \begin{pmatrix} ½+r & w \\ w^* & ½-r \end{pmatrix}$

solving for: $Tr_{CR}\ U\ \rho_{CR} - \rho_{CTC}\ U^y = \rho_{CTC}$

gives $\rho'_{CR} = Tr_{CTC}\ U\ \rho_{CR} - \rho_{CTC}\ U^y = \begin{pmatrix} ½+r^2 & 0 \\ 0 & ½-r^2 \end{pmatrix}$ nonlinear!

Example (Bacon03)

Chronology respecting (CR) registers



For $\rho_{CR} = \begin{pmatrix} ½+r & w \\ w^* & ½-r \end{pmatrix}$

$$\begin{pmatrix} ½+r & 0 \\ 0 & ½-r \end{pmatrix} \longrightarrow \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & \text{if } r=1/2 \\ ¼\begin{pmatrix} ½ & 0 \\ 0 & ½ \end{pmatrix} & \text{if } r<1/2 \end{cases}$$

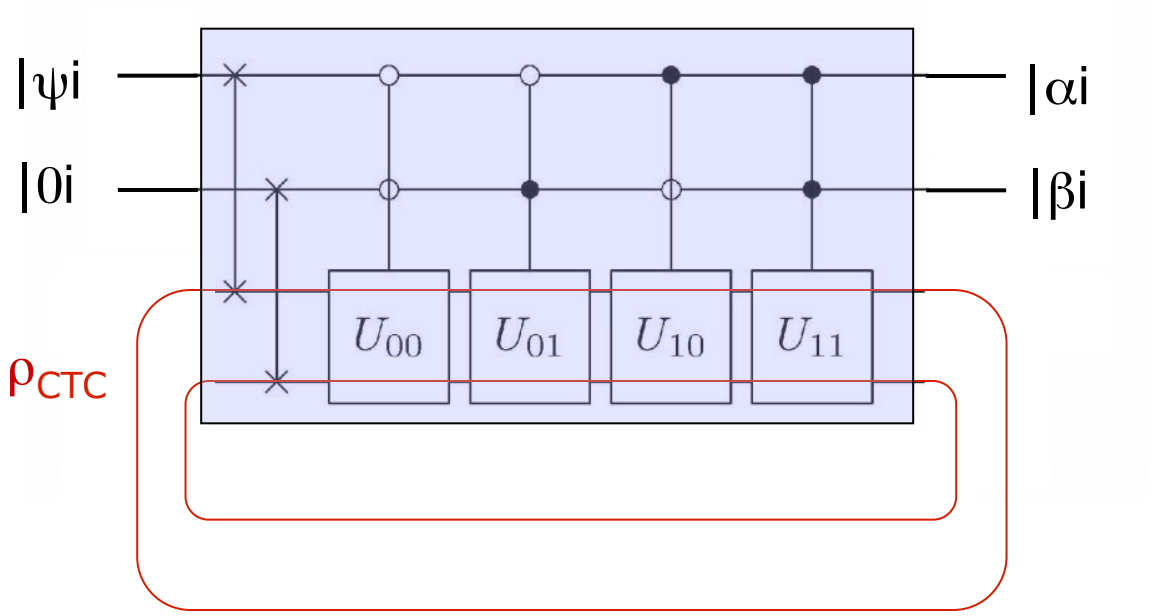
solving for: $Tr_{CR}\ U\ \rho_{CR} - \rho_{CTC}\ U^y = \rho_{CTC}$

gives $\rho'_{CR} = Tr_{CTC}\ U\ \rho_{CR} - \rho_{CTC}\ U^y = \begin{pmatrix} ½+r^2 & 0 \\ 0 & ½-r^2 \end{pmatrix}$

Example (Brun, Harrington, Wilde 2008):

note cannot distinguish nonortho states in QM

explain the +/- states



where U_{00} = SWAP, U_{01} = X - X, U_{10} = XH - I, U_{11} = (X-X) SWAP.

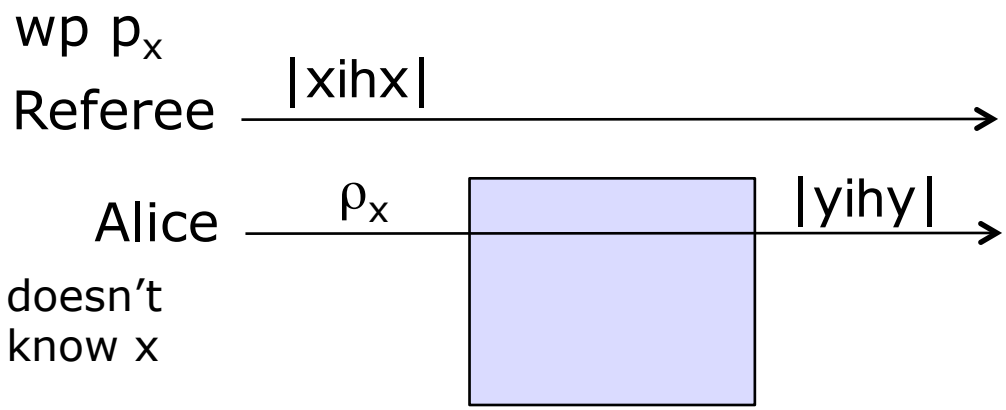
For |ψi = |0i, |1i, |+i, |-i, |αi|βi = |00i, |01i, |10i, |11i resp.

Can this circuit break BB84 ??

What is |Ãi for this problem?

State discrimination

R: someone who knows $\frac{1}{2}_x$ or where $\frac{1}{2}_x$ originates

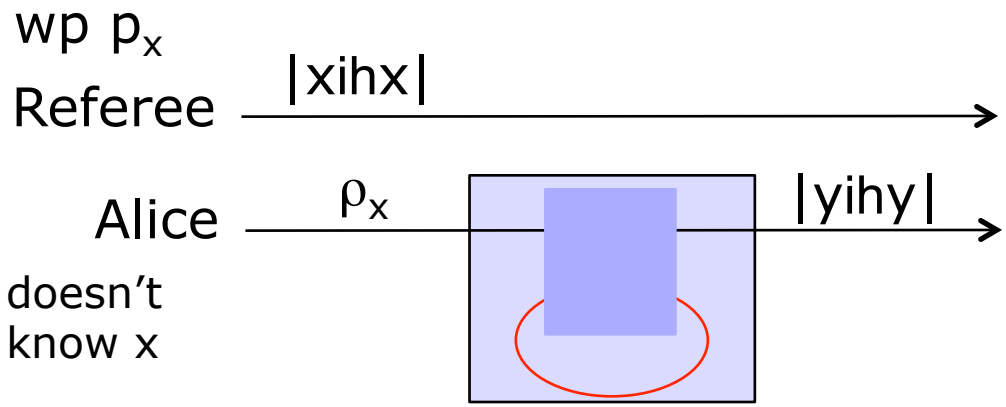


Initial state: $\sum_x p_x$ |xihx| - $\frac{1}{2}_x$

Final state: $\sum_x p_x$ |xihx| - q(y|x) |yihy|

succeeds if $\frac{1}{4} \sum_x p_x$ |xihx| - |xihx|

State discrimination with Deutsch CTCs



The fixed point ¹ is independent of x, and can be calculated and prepared by Alice without a CTC ...

Initial state: $\sum_x p_x$ |xihx| - $½_x$

Thus, $½_{CR} = \sum_x p_x ½_x = ¹$ (or equivalently $\sum_x p_x$ |xihx| - $½_x$)

Solving for: $Tr_{CR}\ U\ \mu_{CR} - \rho_{CTC}\ U^y = \rho_{CTC}$ independent of x

gives $\rho'_{CR} = Tr_{CTC}\ U\ \mu_{CR} - \rho_{CTC}\ U^y = °$ independent of x

Output state: $\sum_x p_x$ |xihx| - °
and the answer is independent of the question

The nonlinearity trap:

If the mapping $\rho \to T(\rho)$ is nonlinear,

then "$\forall x,\ \rho_x \to T(\rho_x)$" $\not\Rightarrow$ "$\sum_x p_x \rho_x \to \sum_x p_x T(\rho_x)$"

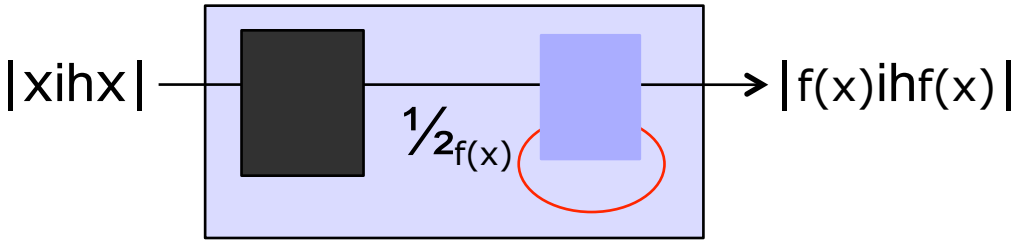
or "$\sum_x p_x |x\rangle\langle x| \to \rho_x$
$\to \sum_x p_x |x\rangle\langle x| \to T(\rho_x)$"

Punchline – the Deutsch CTC does not improve one's ability to perform state discrimination

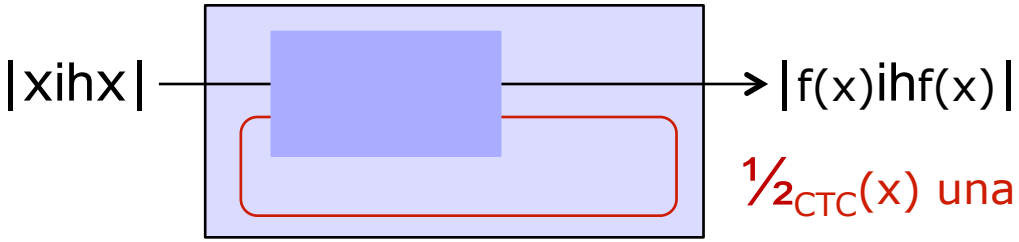
(unless the state to be discriminated is predetermined ...)

Computational consequences:

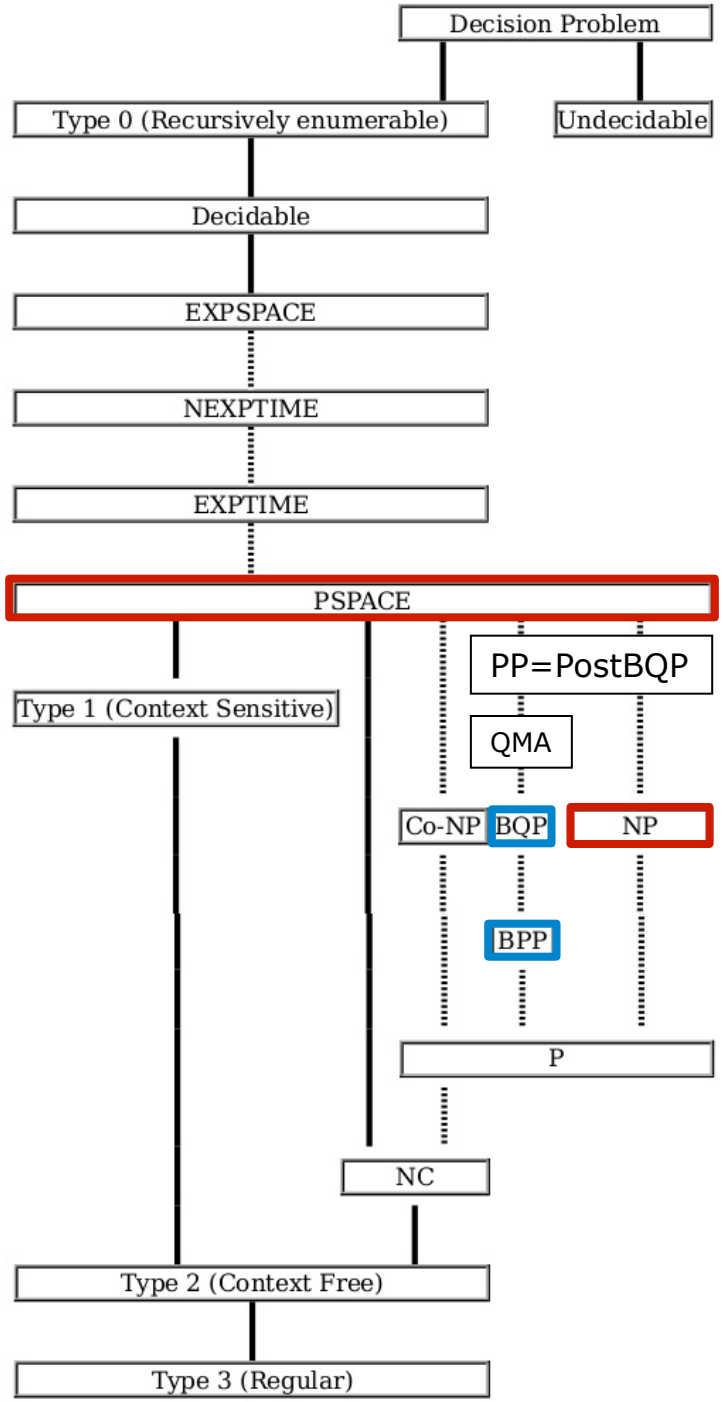
Bacon 03 (for solving NP problems):



Aaronson-Watrous-Fortnow 08 (for solving PSPACE problems):



$\frac{1}{2}_{CTC}(x)$ unambiguously encodes f(x)!



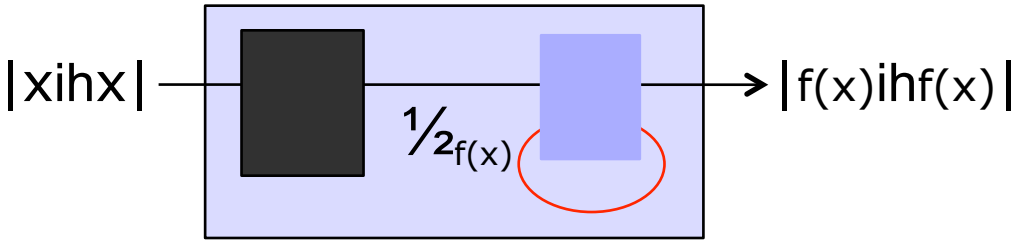
check if PP \subset PSPACE
NP \subset QMA

PSPACE: problems solvable by deterministic Turing machine in poly space

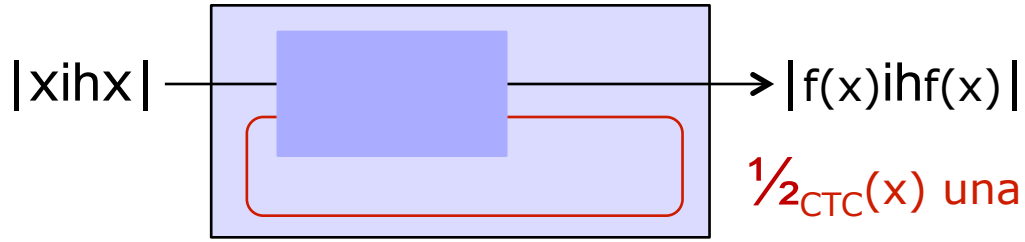
NP: problems solvable by non-deterministic Turing machine in poly time

Computational consequences:

Bacon 03 (for solving NP problems):



Aaronson-Watrous-Fortnow 08 (for solving PSPACE problems):



$\frac{1}{2}_{CTC}(x)$ unambiguously encodes f(x)!

The nonlinearity trap implies that

$$\sum_x p_x \, |xihx| \, - \, |xihx| \; ! \; \sum_x p_x \, |xihx| \, - \, |f(x)ihf(x)|$$

Depending on whether the machine has to succeed on one specific input, or any arbitrary distribution of inputs, the Deutsch CTCs offer spectacular or no advantage.

Outline

1. Deutsch CTCs (closed timelike curves)
   - Method to discriminate non-orthogonal states ?
   - Algorithms for solving NP or PSPACE problems ?
   - Nonlinearity trap

2. Postselected CTCs
   - Method to discriminate non-orthogonal states
   - Algorithms for solving PP problems
   - Environmental concerns
   - Fault-tolerance ?

If : Deustch CTCs are so ineffectual, can post-selecting ones do better?

An optimist is a person who orders a meal in an expensive restaurant, planning to pay for it with the pearl they might find in their oyster.

Postselection:

A regular measurement in quantum mechanics:

$$\rho \to \sum_k A_k \rho A_k^\dagger \quad \text{where } \Pr(k|\rho) = \mathrm{tr}(\rho A_k^\dagger A_k) \text{ and } \sum_k A_k^\dagger A_k = I$$

i.e, one of the outcomes must happen

A postselected measurement allows some terms to be omitted in the above:

$$\rho \to \left[\sum_{k \in S} A_k \rho A_k^\dagger \right] / \left[\sum_{k \in S} \mathrm{tr}(\rho A_k^\dagger A_k) \right]$$

where $\sum_{k \in S} A_k^\dagger A_k \leq I$.

The only nonlinearity is an input-dependent rescaling.
Also, postselection can be delayed until the last step [Aaronson 04, Brun-Wilde 11]).

Nonlinearity trap free !!

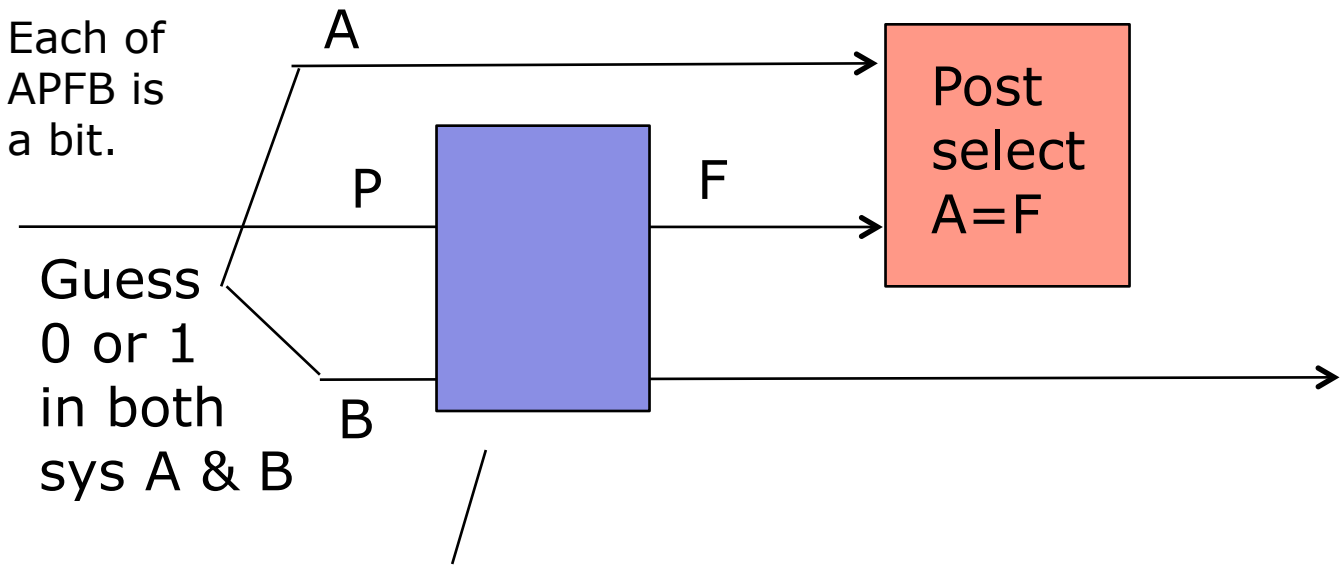
A remark on complexity:

We only consider very simple measurements, and postselection of their outcomes. Else we can cheat, say, by postselecting the correct answers from a uniform distribution of all possibilities ...

Simple postselected measurements:
e.g., postselection of "0" outconme in the von Neumann measurement of {|0i, |1i}
e.g., postselection of the outcome corresponding to $|©_0i=|00i+|11i$ in the measurement along the Bell basis.

Consequences of postselection:

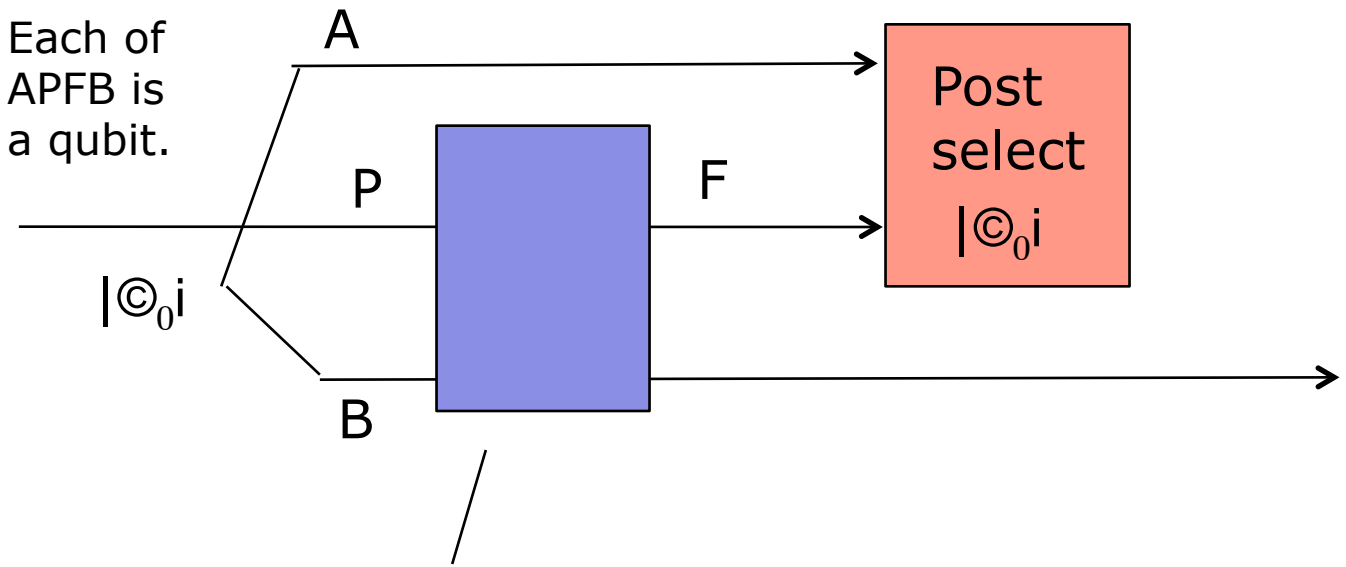
1. Classical simulation of time travel (Bennett & Schumacher 02)



The future F, which is same as A, same as B, has interacted with its past P !

Consequences of postselection:

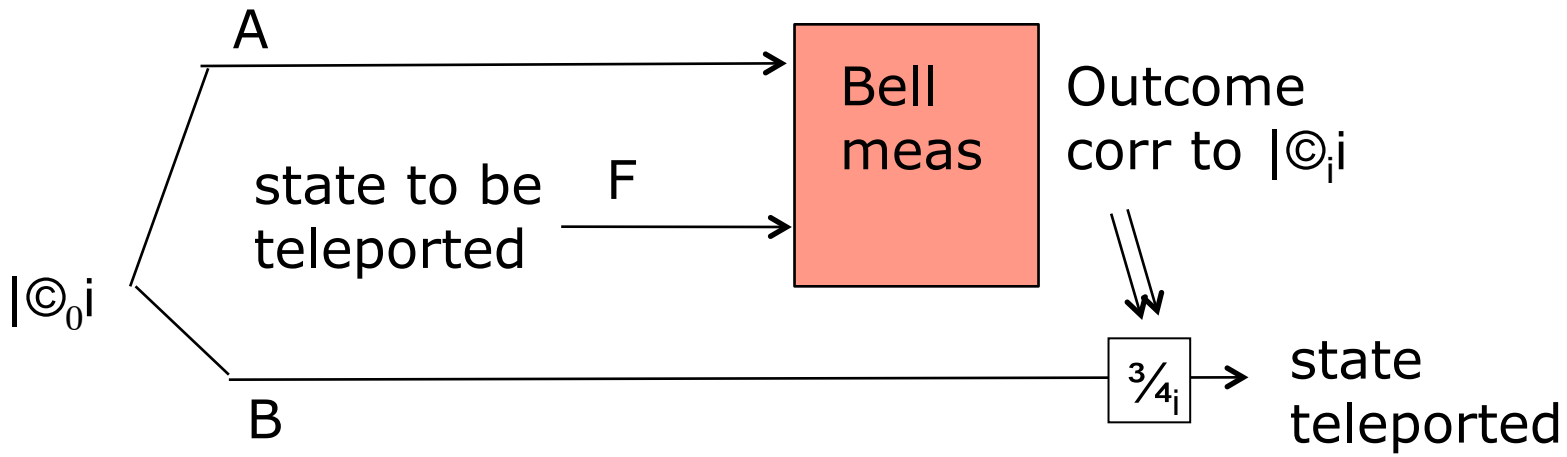
1. Quantum simulation of time travel (Bennett & Schumacher 02)



After postselection, system F is teleported to system B !

Consequences of postselection:

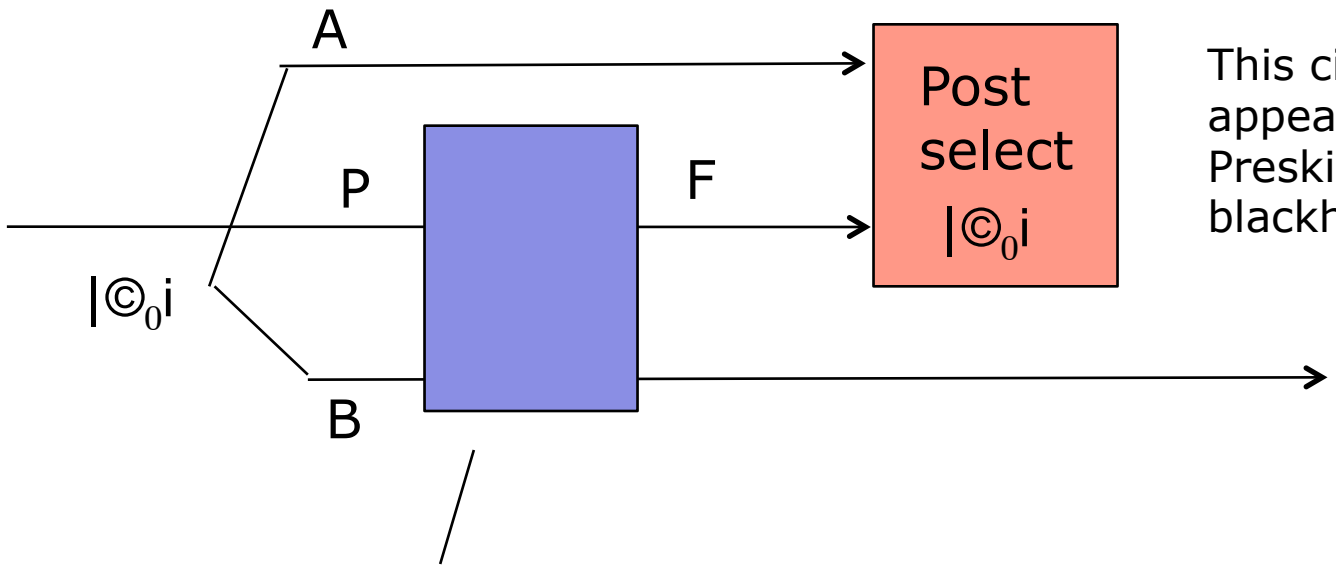
1. Teleportation



After postselection, system F is teleported to system B !

Consequences of postselection:

1. Quantum simulation of time travel (Bennett & Schumacher 02)



This circuit has also appeared in Gottesman-Preskill 2003 concerning blackhole final states.

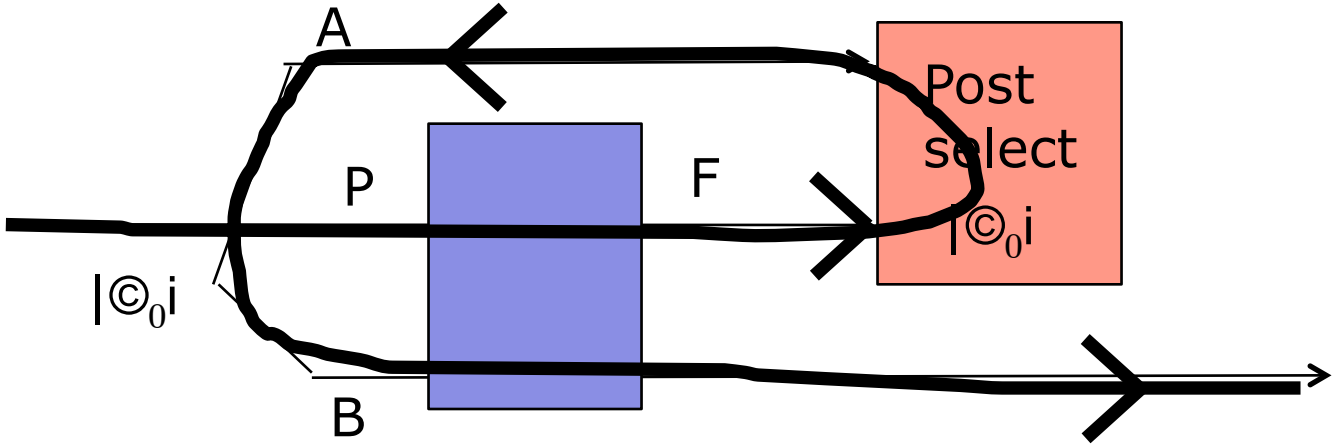
Interaction between system P and B

After postselection, system F is teleported to system B !

Again, the future F state (reincarnated as B) has interacted with its past P !

Consequences of postselection:

1. Quantum simulation of time travel (Bennett & Schumacher 02)



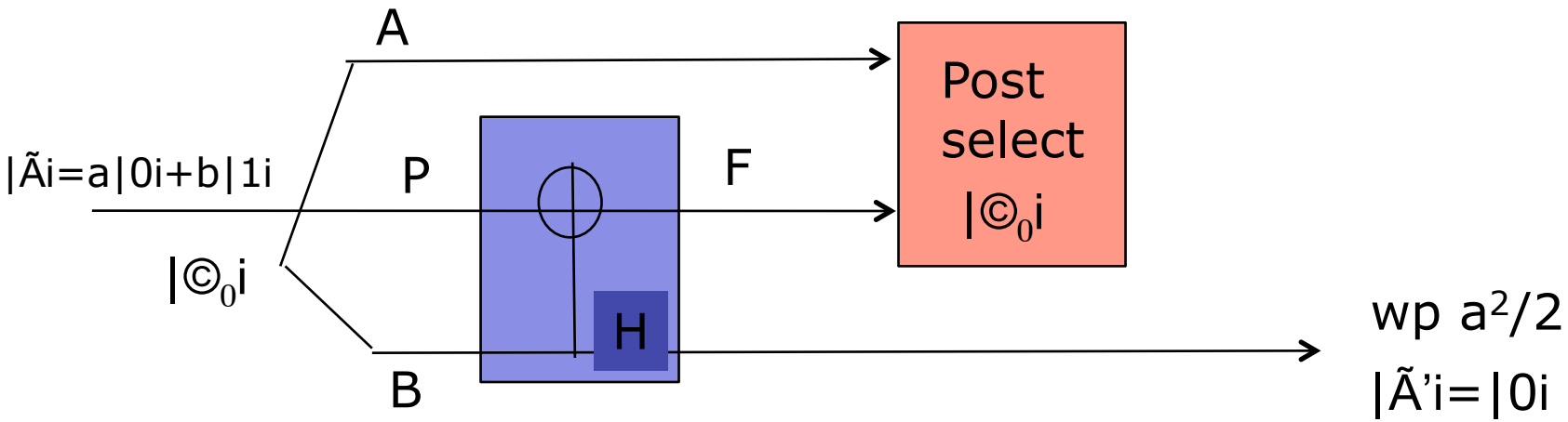
Q: Is it time travel?
A: It depends on what your definition of "is" is.

Q: Does it clone?
A: No. F is only reincarnated in B ...

Q: What about grand father paradox?
A: Only happens on a set of state of measure 0!

Consequences of postselection:

Example how the grandfather paradox manifest itself:



The grand father paradox occurs if the initial state is |Ãi=|1i (i.e., a=0) . Thus, this circuit postselects |0i.

Conversely, knowing how to postselect |0i enables postselection of |©0i and thus times travel as shown above.

Thus, postselection and postselected CTCs are interchangeable computational primitives.

Consequences of postselection:

2. Perfect discrimination of linearly independent pure states $\{|\psi_x i\}$ (Brun, Wilde 10)

It's known how to perfectly discriminate such states if the answer "I don't know" is allowed to occur some times (unambiguous state discrimination).

"Postreject" "I don't know" –

take a |0i state, conditioned on "I don't know", turn apply a bit flip, then postselect |0i.

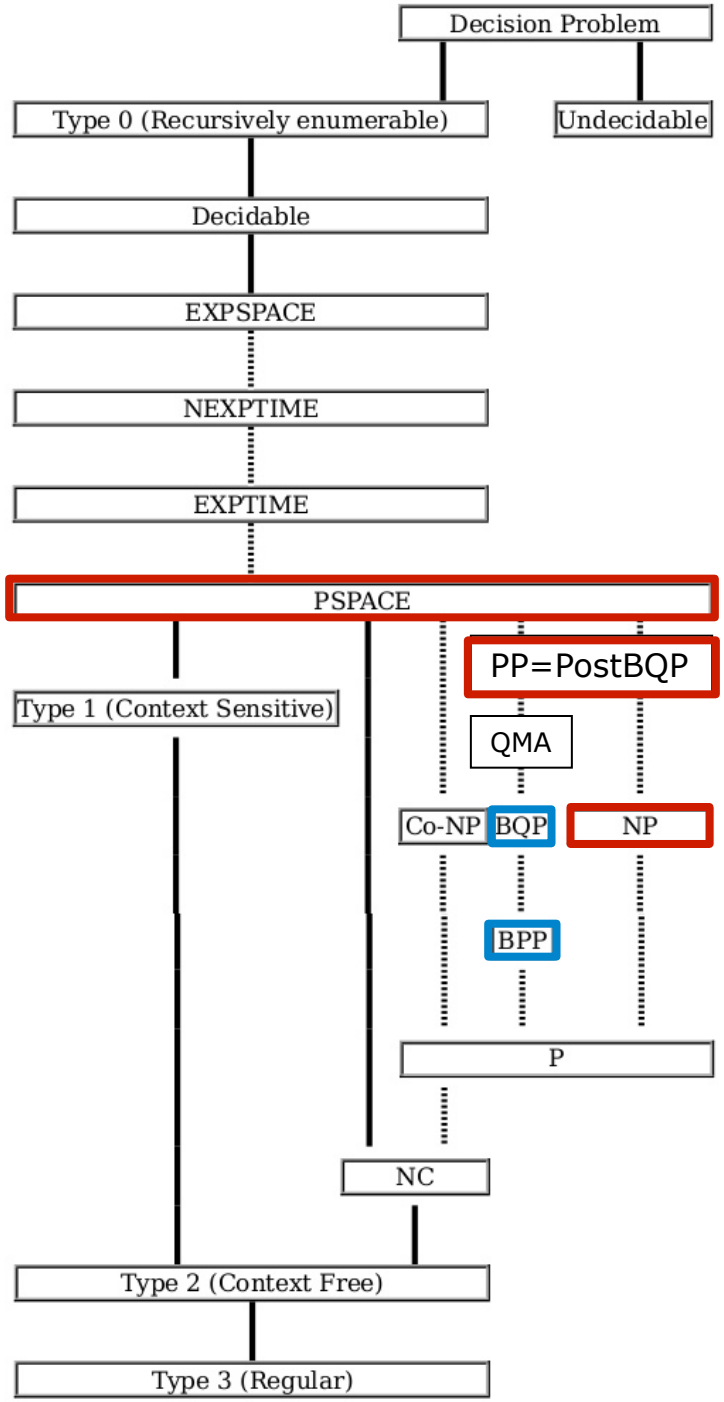
Consequences of postselection:

3. PostBQP = PP (Aaronson04)

Problems solvable by poly-time quantum computer given post-selected measurements

Problems for which 9 a probabilistic poly-time Turing machine that accepts with prob ¸ ½ iff answer is "yes."

NB this gives simple proof for closure of PP since closure of PostBQP is simple to show.



check if PP \subset PSPACE
NP \subset QMA

PSPACE: problems solvable by deterministic Turing machine in poly space

PP: problems solvable by a probabilistic poly-time Turing machine (accepting wp ¸ ½ iff answer is yes)

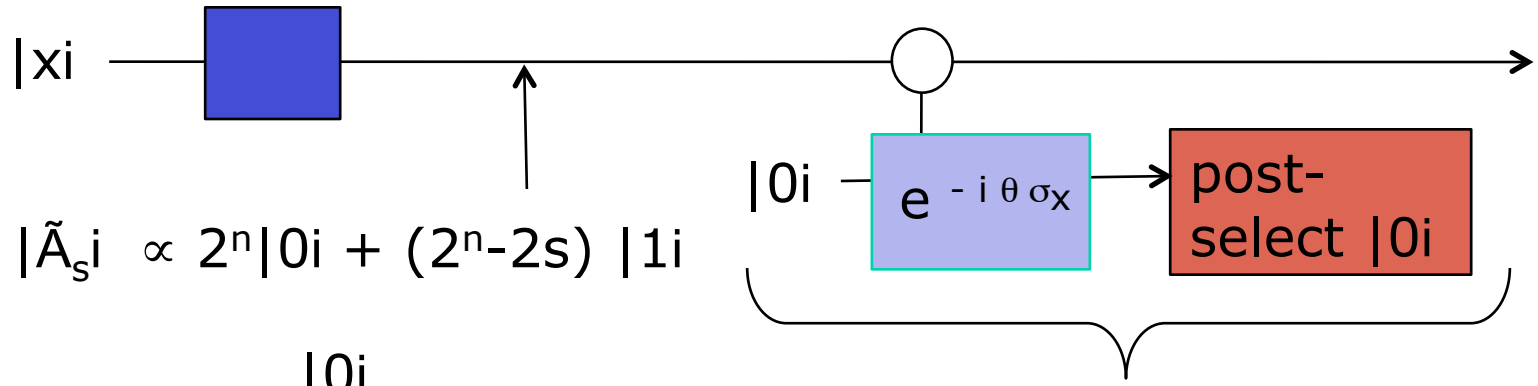
NP: problems solvable by non-deterministic Turing machine in poly time

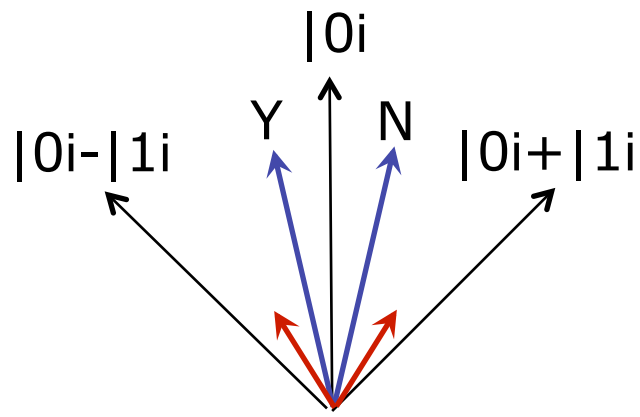
Consequences of postselection:

3. PostBQP = PP (Aaronson04)

Idea behind a PostBQP algorithm for a PP-complete problem:

Let s be # satisfying assignments for a Boolean formula with n variables. Determine whether $s \gtrless 2^{n-1}$ (1/2 of all possibilities).





Reduces the amplitude of |0i by an amount depending on θ.

States close to |0i (the hardest case when $s = 2^{n-1}$) is mapped to $= |0i \S |1i$ so the Y/N ans can be distinguished.

1. How physical is postselection?

2. Is it possible to make the computation model fault-tolerant?

   Note the algorithm to solve PP complete problems requires accuracy exponential in the input size.

Consequences of postselection:

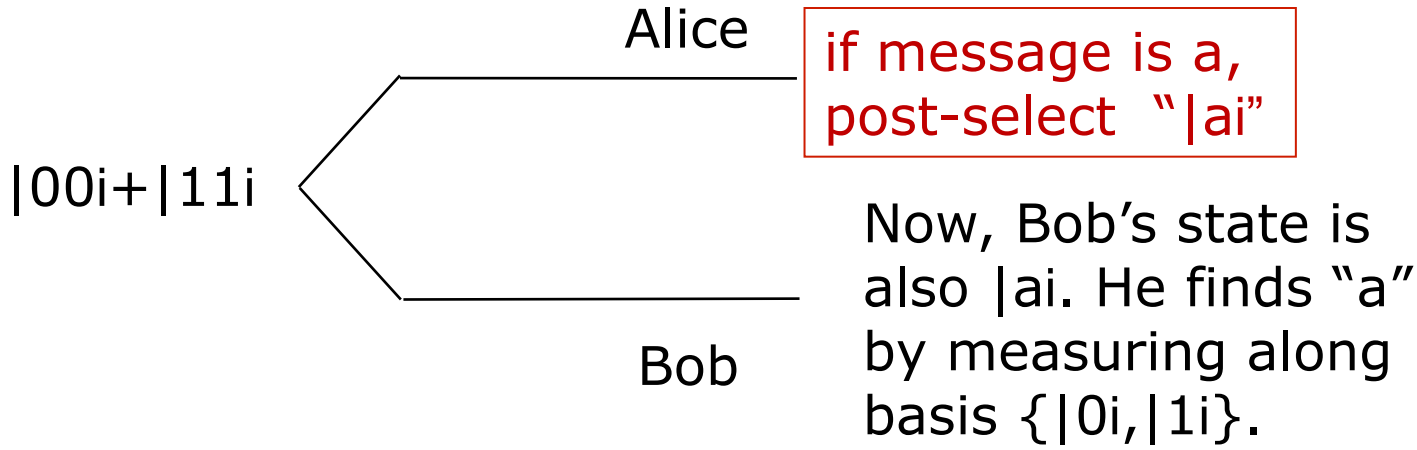
4. Environmental destruction

(a) faster than light communication

(b) state change in remote system

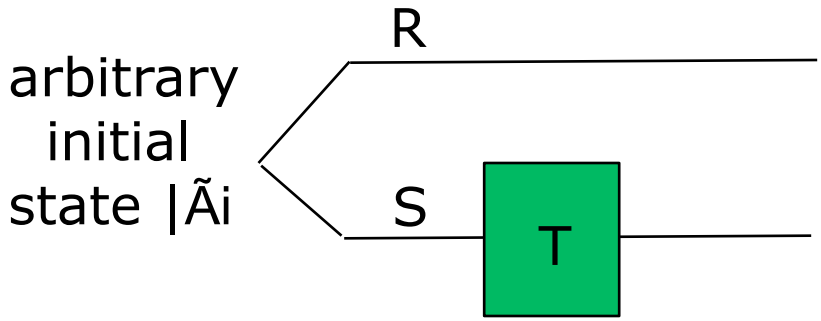
Are these features or bugs?

(c) inconsistency in defining Bob's state ...
Is it |0i or |1i or I/2?
NB no temporal ordering between Alice's & Bob's steps!



Green processes:

1. We say that an operation T is (coherently) green if it does not affect the state of any other systems not being acted on.



$$\text{T is green if, } 8\ |\tilde{A}i_{RS},\ \mathrm{Tr}_S\,(I-T)(|\tilde{A}ih\tilde{A}|_{RS}) \propto \mathrm{Tr}_S\,(|\tilde{A}ih\tilde{A}|_{RS}) \qquad *$$

2. T is discretely green if R is classical above

3. T is approximately green if the condition * holds approx.

Results:

1. Exactly coherently or discretely green CTCs can be implemented exactly using regular quantum mechanics.

   So, they cannot improve our information theoretic ability to perform state discrimination.

   Whether there is a computational advantage or not is still open (known algorithms use very nongreen CTCs)

2. For approx green CTCs, if enough are used together, they're not green at all. If few are allowed, they can be well approximated by regular QM.

NB: very easy to show the above since we can use the Kraus decomposition and linearity.

5. What about noise?

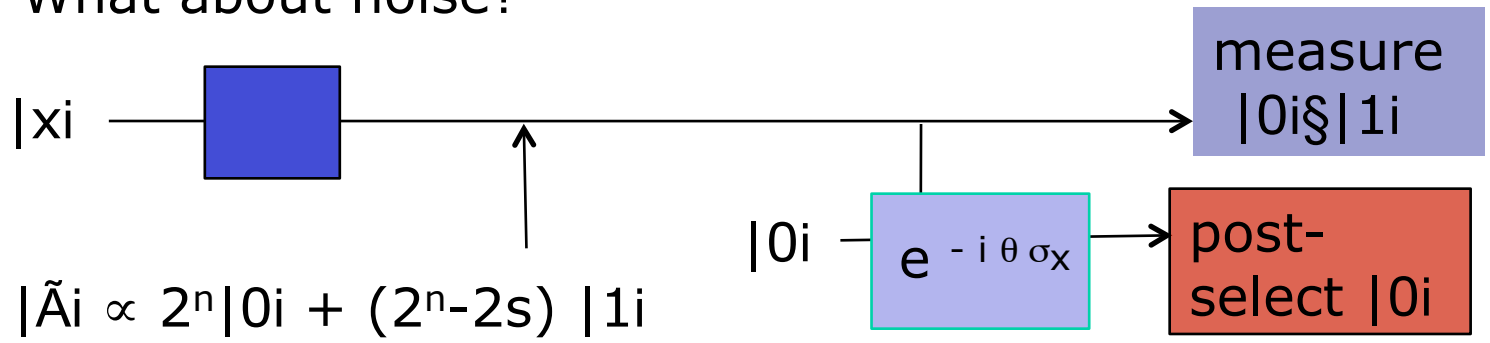
Algorithm to solve PP problems using postselection requires error rate · $O(2^{-n})$.

Are fault-tolerant protocols and threshold analysis applicable in PostBQP?

Thanks to John (and many others – Daniel Gottesman, Panos Aliferis, Peter Shor, Andrew Steane, Manny Knill, ...)
we know that if we recursively replace physical operations by fault-tolerant gadgets, and if the physical noise model is sufficiently benign, k levels of concatenation allows simulation of a logical computation at an effective noise rate $O(^{2}2^{k})$ if the physical noise rate is ^{2} .

Thus k ¼ O(log n) levels are sufficient to maintain the desired accuracy, and the resource overhead is poly(n).

5. What about noise?



We know how to fault-tolerantly simulate the above logical circuit to high accuracy, except for the postselected meas.

What doesn't work:

a. decoding first, which incurs too much physical noise

Suppose we're postselecting |0i from a|0i+ b|1i where a ¼ 2^{-n}, b ¼ 1. Let the bit flip prob be ².
There are 2 ways to postselect |0i:
With prob (1-²) $|a|^2$: "there's no bit flip and state was|0i"
With prob ² $|b|^2$: "there's a bit flip and state was |1i"
The second event is much more likely ... for large n.

5. What about noise?

What doesn't work (to enable fault tolerant postselection):

b. Perform one level of coding and measure the logical |0i.

All known fault tolerant measurements deduce the logical measurement outcomes based on parities of measurement outcomes of multiple qubits.

To postselect an unlikely outcome, a physical error followed by post-selection of the wrong outcome is much more likely than post-selection of the correct outcome.

Such encoded measurement amplifies (not reduces) the effective error rate on inputs of the most interest.

... not sure how to make fault-tolerant gadget for postselected measurement.

5. What about noise?

What doesn't work (to enable fault tolerant postselection):

c. Level reduction cannot be applied due to the lack of fault tolerant gadget for postselected measurement.

Without level reduction, little hope to lower effective error rate.

No eggs, and no chicken.

d. Direct analysis of a level-k logical measurement yields similarly negative results ...

We emphasize that our analysis are case studies, rather than no-go proof for fault tolerance in PostBQP.

Conclusion

1. Deutsch CTCs (closed timelike curves)
   - Method to discriminate non-orthogonal states X
   - Algorithms for solving NP or PSPACE problems X ?
   - Nonlinearity trap

2. Postselected CTCs
   - Method to discriminate non-orthogonal states
   - Algorithms for solving PP problems
   - Environmental concerns
   - Fault-tolerance ??

Physics of CTCs

Stockum, Proc. Roy. Soc. Edinburgh A, 57:135 (1937)
Godel, Rev. Mod. Phys., 21:447 (1949)
Morris, Thorne and Yurtsever, PRL 61, 1446 (1988)
Gott, PRL 66, 1126 (1991)
Deser, Jackiw and 'tHooft, PRL 68, 267 (1992)
Hawking, Phys. Rev. D 46, 603 (1992)
Thorne (1993) [first hit in google for "closed timed curves]
Ori, PRL 95, 021101 (2005)

Deutsch Model

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

Post-selected Model

Bennett & Schumacher (lecture, TIFR Mumbai 2002)
Horowitz and Maldacena hep-th/0310281 (2003)
Gottesman and Preskill hep-th/0311269 (2003)
Aaronson quant-ph/0412187
G. Svetlichny arXiv/0902.4898 (2009)
S. Lloyd et al arXiv/1005.2219, 1007.2615

Consequences for state discrimination & computation

Abrams and Lloyd quant-ph/9801041
Bacon quant-ph/0309189
Aaronson (op cit 2004)
Aaronson & Watrous arXiv/0808.2669
Brun, Harrington & Wilde arXiv/0811.1209
Bennett, Leung, Smith & Smolin arXiv:0908.3023
Brun and Wilde arXiv/1008.0433