CO781 / QIC 890:

Theory of Quantum Communication

Topic 1, part 6

What is communication of data?

The no-signalling principle

Optimality of superdense coding and teleportation

Cobits, duality of SD and TP,
and unitary gates as bidirectional channels

Equivalence of generalized teleportation
& generalized encryption of quantum states

Non-composable qbit: remote state preparation
& approximation encryption of pure states

Beyond QM?

Beyond Quantum Mechanics?

The 5 axioms of QM lead to many equivalent ways to derive or to predict ...

e.g., for system AR in a state $|\psi\rangle_{AR}$

transformations & predictions on A can be derived either

- by analysing $\mathcal{E}_A \otimes \mathcal{I}_R (|\psi\rangle\langle\psi|)$
- or or analysing $\mathcal{E}_A (\mathrm{tr}_R |\psi\rangle\langle\psi|)$

e.g., for a density matrix ρ

without access to the purifying system, predictions do not depend on how we decompose $\rho = \sum_x p_x \rho_x = \sum_y q_y \sigma_y$

Furthermore, after evolution $\mathcal{E}$ output = $\sum_x p_x \mathcal{E}(\rho_x)$

i.e., can analyse the evolution by using linearity on any decomposition of the input

A significant body of work "extends" QM to find computational or information theoretic advantages beyond QM ...

e.g., PostBQP = PP, BQP(D-CTC) = PSPACE

Why study info processing in a non-physical model?

Main motivation: obtain insight on the physical model
Bonus: may get a result within the physical model

Problem: most extensions thus far does NOT contain QM as a special case. Most contradicts some element of QM.

Reassurances from QM,
e.g., linearity
e.g., the density matrix & a purification can't be used interchangeably (at least w/o justification).

Calculations, formulations etc must only use methods consistent with the extension.

Furthermore, one must be mindful of other trivializing consequences of the extensions ...

Some of this ties back to how we should define comm.
Will see some examples ...

Example 1 of extensions to QM -- postselection

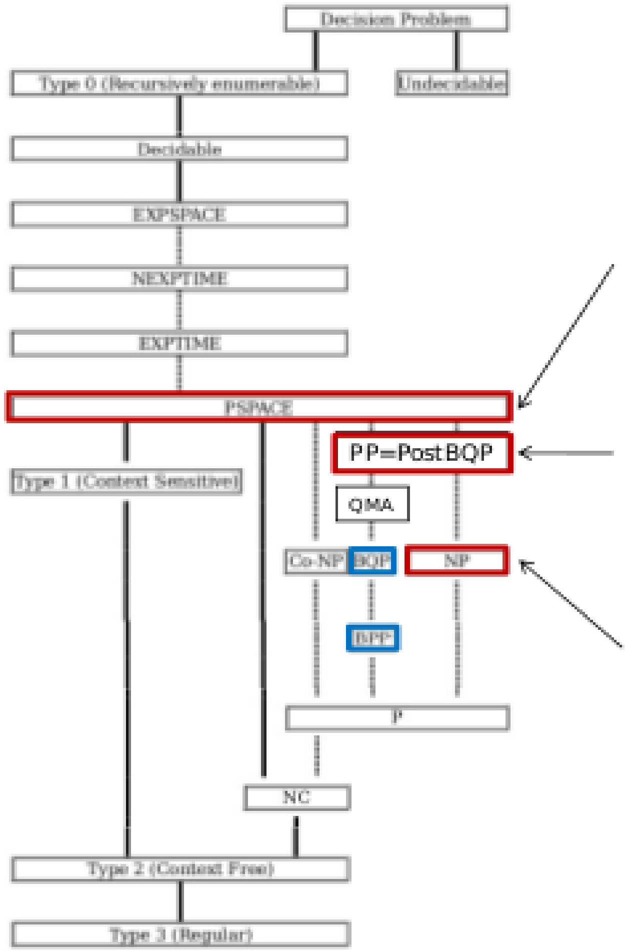
Postselection:

Allow a measurement along $\{|0\rangle, |1\rangle\}$ to postselect $|0\rangle$,

Then, renormalize postmeasurement state (nonlinear).

Studied and used by Aaronson 04:

PostBQP = PP

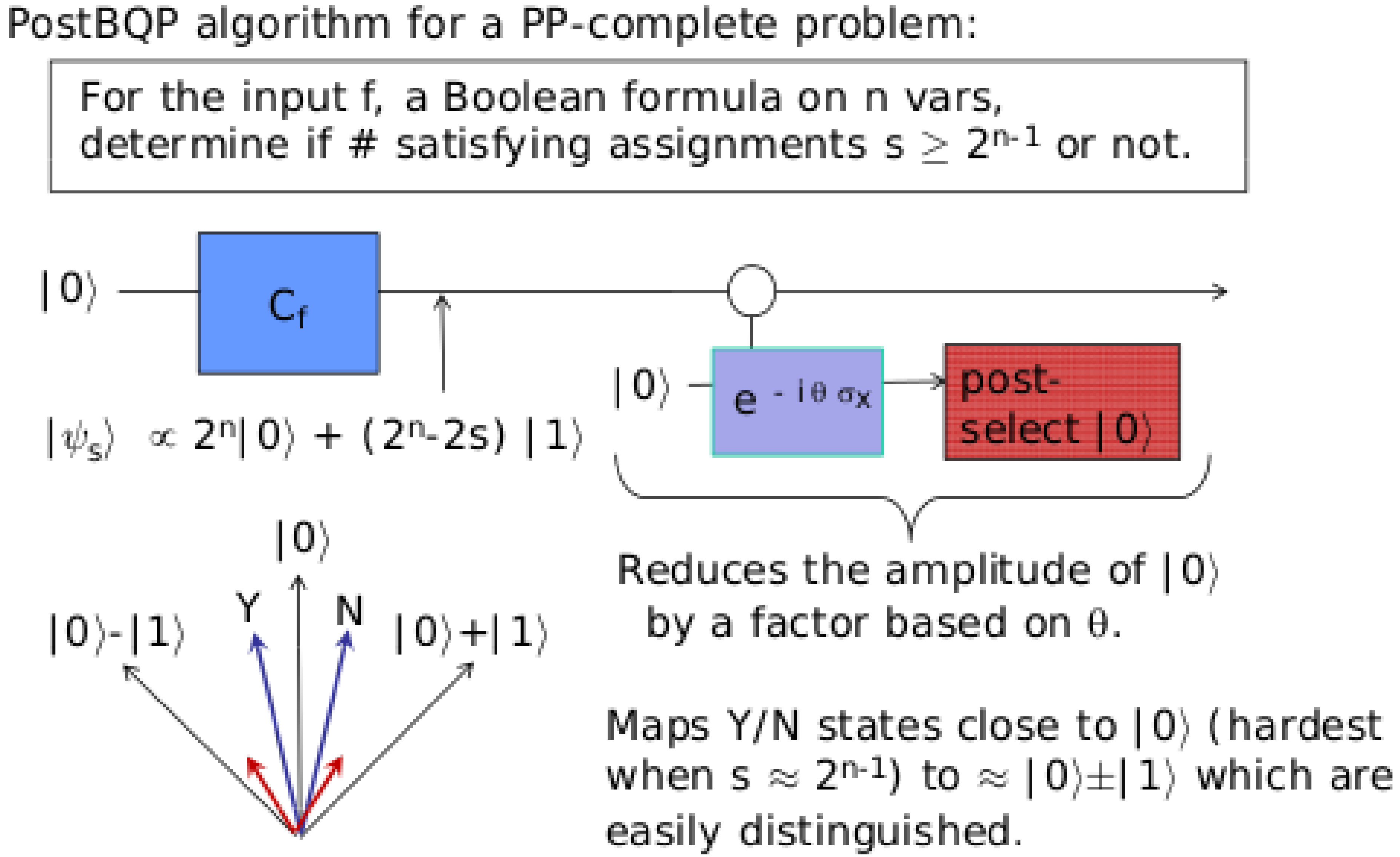


PSPACE: problems solvable by deterministic Turing machine in poly space

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

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

Skip in class, include for interested students ...



PostBQP algorithm for a PP-complete problem:

For the input f, a Boolean formula on n vars,
determine if # satisfying assignments s $\geq 2^{n-1}$ or not.

$|\psi_s\rangle \propto 2^n|0\rangle + (2^n-2s)\,|1\rangle$

Reduces the amplitude of $|0\rangle$
by a factor based on θ.

Maps Y/N states close to $|0\rangle$ (hardest when s $\approx 2^{n-1}$) to $\approx |0\rangle \pm |1\rangle$ which are easily distinguished.

Postselection:

Allow a measure along $\{|0\rangle, |1\rangle\}$ to postselect $|0\rangle$.

Then, renormalize postmeasurement state (nonlinear).

Studied and used by Aaronson 04:

PostBQP = PP

Decision problems solvable by probabilistic TM in poly time with error prob < 1/2

e.g., gives a short proof for PP being close.

Attractive features:

(1) postselected measurements can be delayed until the end so analysis follows usual QM

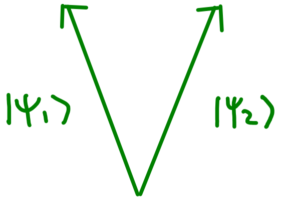
(2) can count such measurements & treat as a resource

(3) no hiding of complexity in the measurement basis

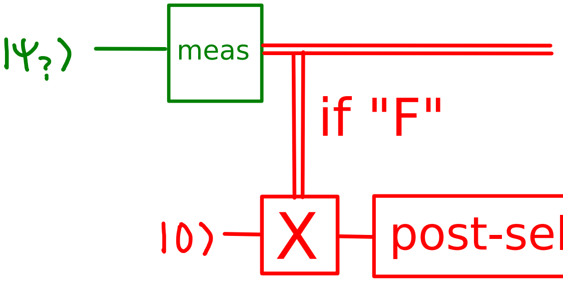
Consequences:

Can perfectly distinguish any two distinct pure states, which can be arbitrarily close to one another.

Idea (unambiguous state discrimination):



$$M_1 = c\,(I - |\psi_2\rangle\langle\psi_2|)$$
$$M_2 = c\,(I - |\psi_1\rangle\langle\psi_1|)$$
$$M_F = I - M_1 - M_2 \qquad (\text{small } c \Rightarrow M_F \geq 0)$$



if "F"

post-select "0"

← always get the correct answer

* can thus clone one of two unknown quantum states

Bad consequences:

1. violate no-signalling principle

2 post-selected meas + 1 ebit $\geqslant$ 1 qbit

Protocol: Alice shares 1 ebit with Bob. She "teleports" a qubit state -- with Bell meas replaced by change of Bell basis to computational basis, postselects "00".

- no correction needed by Bob
- Bob never hears from Alice

Is his state I/2 or what Alice tries to send to him?

What if Alice deviates from the protocol?

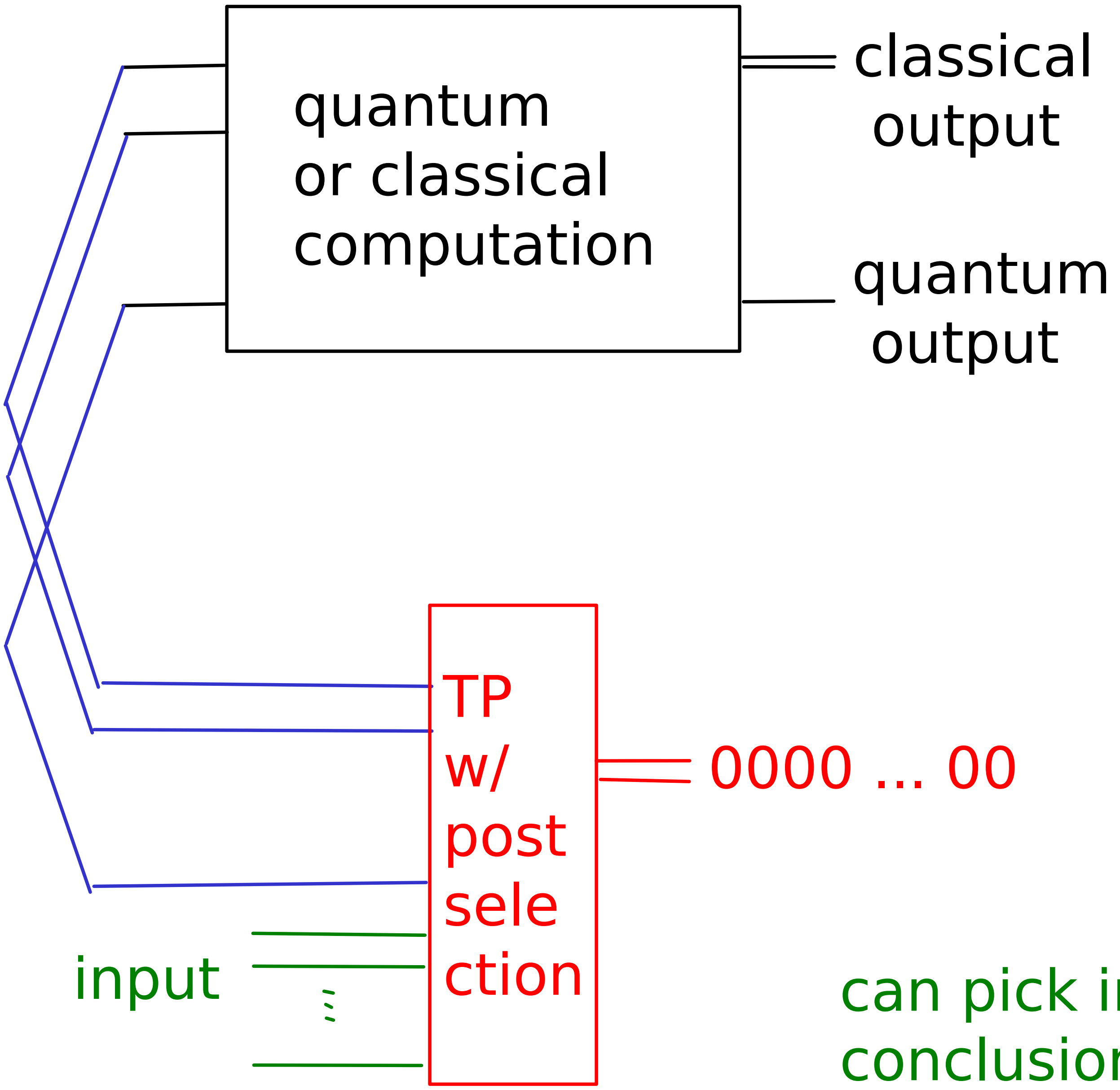
Is Bob's state well-defined?

Is part of a quantum state ever well-defined anymore?

Sadly, some are very excited by no-signalling ...

Bad consequences:

2. can compute before having an input



can pick input after conclusion of computation

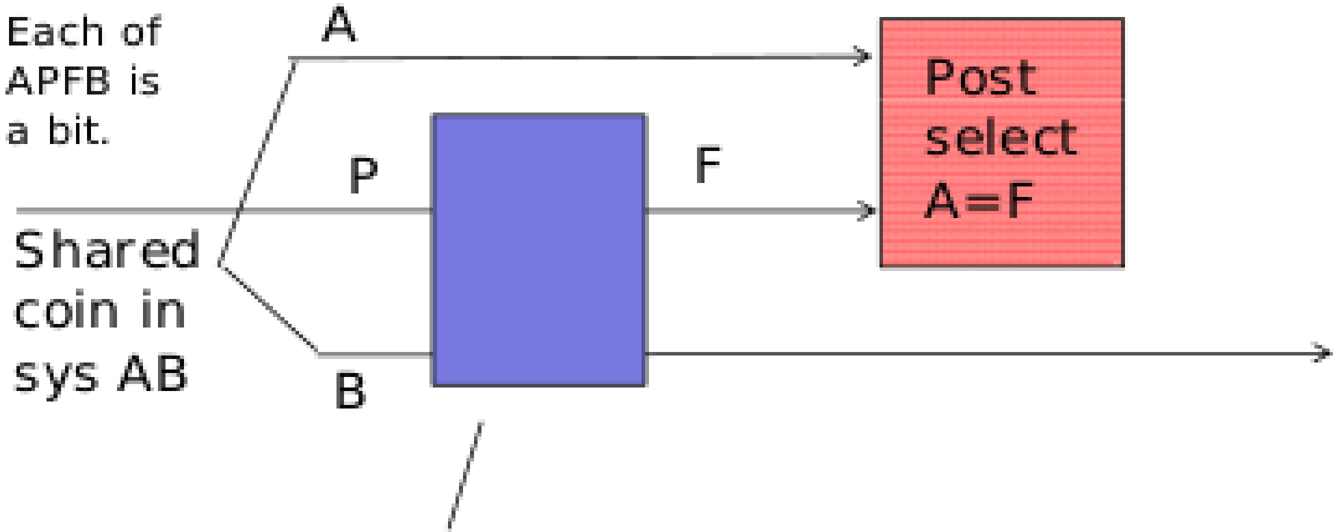
(reading for interested students)

Bad consequences:

3. time travel

Postselection implies time travel (Bennett-Schumacher 02):

Classical time traveler:



Interaction between system P and B

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

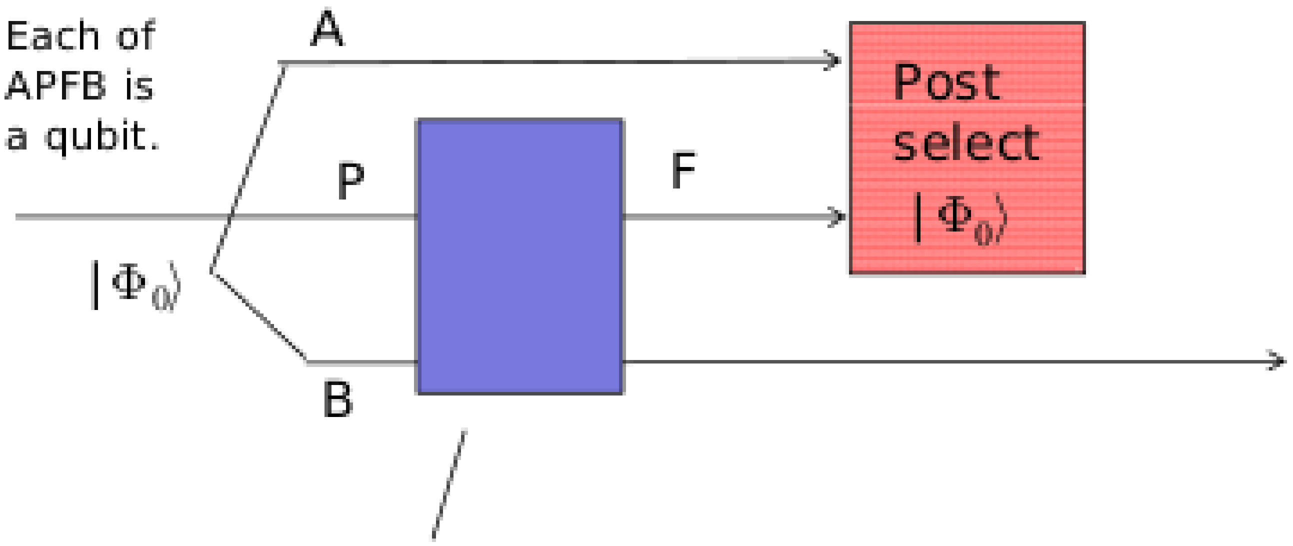
(reading for interested students)

Bad consequences:

3. time travel

Postselection implies time travel (Bennett-Schumacher 02):

Quantum time traveler:



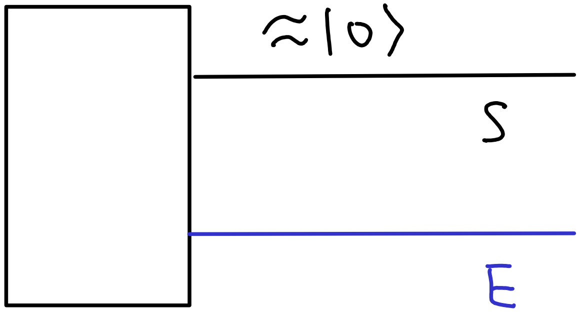
Each of APFB is a qubit.

Interaction between system P and B

Postselection teleports sys F to sys B !

Bad consequences:

4. Can't really define a state



Initial state preparation to error e, but state turns out:

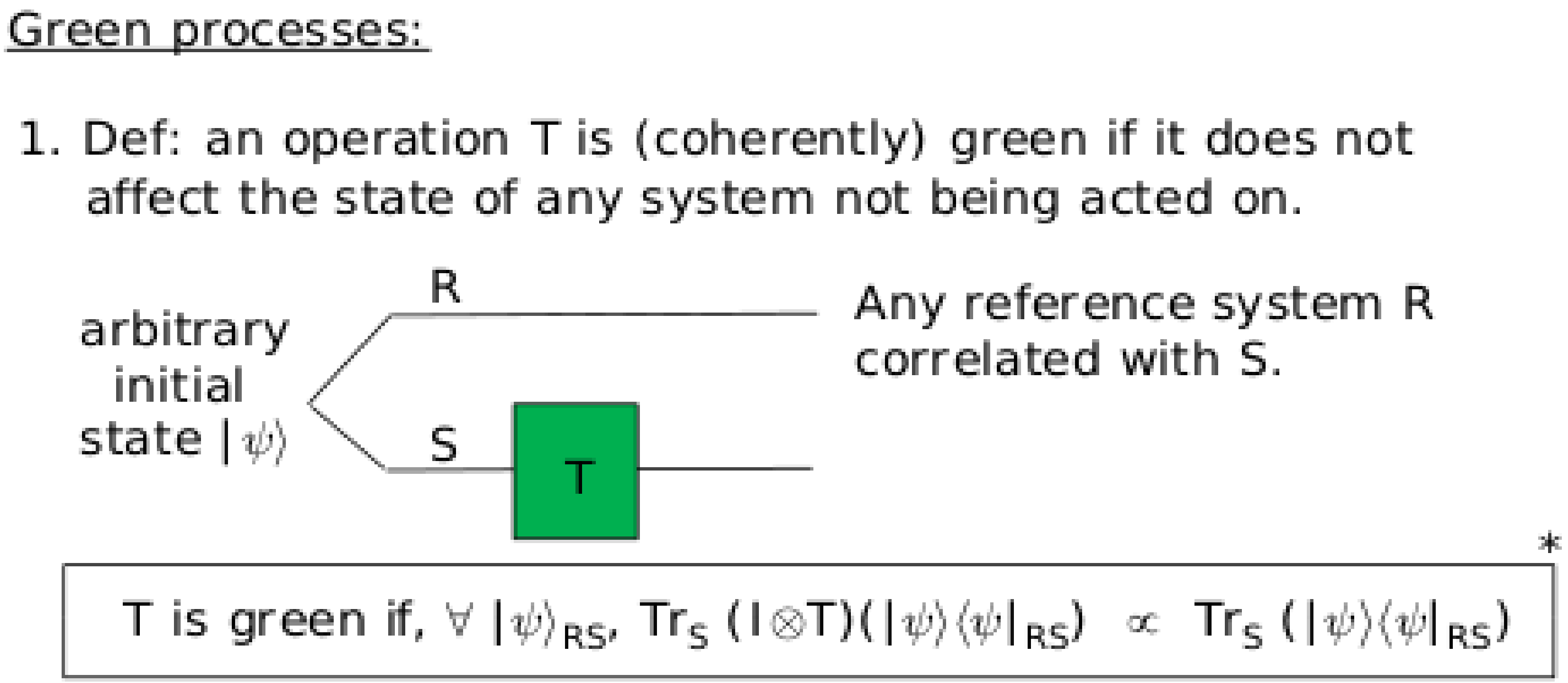
$$(1-e)\ |0\rangle\langle 0|_S \otimes |0\rangle\langle 0|_E \ + \ e\ |1\rangle\langle 1|_S \otimes |1\rangle\langle 1|_E$$

Someone can postselect "0" on E, thereby flipping the state on S ...

What if that register happens to be the final output of a long decision problem?

Resolution:

Restrict to green processes so that action from far away alone cannot change the local state ...



Green processes:

1. Def: an operation T is (coherently) green if it does not affect the state of any system not being acted on.

R
arbitrary initial state $|\psi\rangle$
S
T
Any reference system R correlated with S.

*

T is green if, $\forall\, |\psi\rangle_{RS}$, $\mathrm{Tr}_S\,(I\otimes T)(|\psi\rangle\langle\psi|_{RS}) \;\propto\; \mathrm{Tr}_S\,(|\psi\rangle\langle\psi|_{RS})$

But such process are implementable with regular QM so, no info theoretic advantage. (Open if computational advantages possible.)

Example 2 of extensions to QM -- cloning

Cloning:

Allow using a cloning machine $\forall \rho, \ \mathcal{E}(\rho) = \rho^{\otimes 2}$

Linearity of QM => no cloning

So, extension to allow cloning means we lose linearity.

But what does it mean to clone?

Say, Bob wants to clone. If he knows the state to be cloned, he just prepares them. So, someone else (Richard) determines the state, doesn't tell Bob, and presents Bob a copy.

$$\sum_x p_x \ |x\rangle\langle x|_R \otimes |\psi_x\rangle\langle\psi_x|_B$$

label of the state to be cloned the state to be cloned

Outcome of successful cloning:

$$\sum_x p_x \ |x\rangle\langle x|_R \otimes |\psi_x\rangle\langle\psi_x|_B \otimes |\psi_x\rangle\langle\psi_x|_{B'}$$

But without linearity, even though

$$\mathcal{E}(|\psi_x\rangle\langle\psi_x|) = |\psi_x\rangle\langle\psi_x|_B \otimes |\psi_x\rangle\langle\psi_x|_{B'}$$

it's not automatic that

$$I \otimes \mathcal{E}\Big(\sum_x p_x |x\rangle\langle x|_R \otimes |\psi_x\rangle\langle\psi_x|_B\Big) = \sum_x p_x |x\rangle\langle x|_R \otimes |\psi_x\rangle\langle\psi_x|_B \otimes |\psi_x\rangle\langle\psi_x|_{B'}$$

Furthermore, what is the input to the cloning machine?

Option 1: reduced state on B, $\sum_x p_x |\psi_x\rangle\langle\psi_x|_B$

Output = $\sum_x p_x |x\rangle\langle x|_R \otimes |\psi_x\rangle\langle\psi_x|_B \otimes \underbrace{\sum_{x'} p_{x'} |\psi_{x'}\rangle\langle\psi_{x'}|_{B'}}$

btw this can be known to Bob (e.g., BB84)
he doesn't even need the copy in B ...

So, the cloning machine is not useful ...

But without linearity, even though

$$\mathcal{E}(|\psi_x\rangle\langle\psi_x|) = |\psi_x\rangle\langle\psi_x|_B \otimes |\psi_x\rangle\langle\psi_x|_{B'}$$

it's not automatic that

$$I \otimes \mathcal{E}\Big(\sum_x p_x |x\rangle\langle x|_R \otimes |\psi_x\rangle\langle\psi_x|_B\Big) = \sum_x p_x |x\rangle\langle x|_R \otimes |\psi_x\rangle\langle\psi_x|_B \otimes |\psi_x\rangle\langle\psi_x|_{B'}$$

Furthermore, what is the input to the cloning machine?

Option 2: $|\psi_x\rangle\langle\psi_x|_B$ if system R is in state $|x\rangle\langle x|$

(Looks very nonlocal ...)

Now, for the same machine, what happens if input is half of a max ent state? (Warning: Choi-rep broken.)

$$\frac{1}{\sqrt{2}}(|00\overset{/}{\rangle}+|11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle+|{-}{-}\rangle) = |\Phi\rangle$$

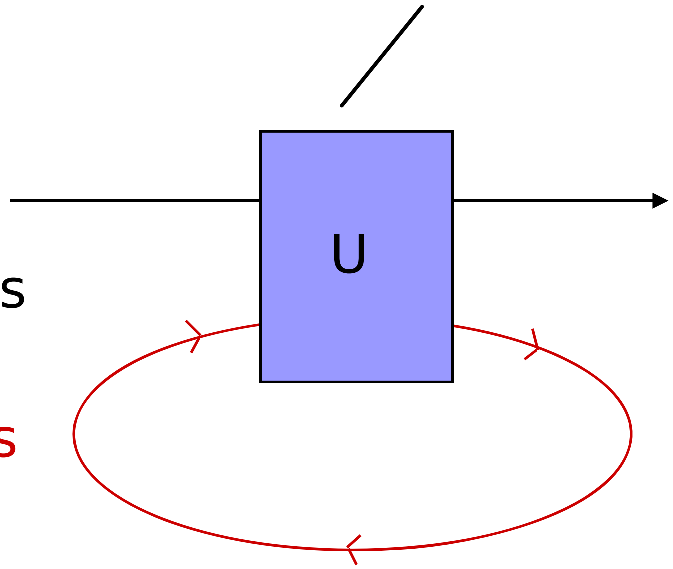
Should $I \otimes \mathcal{E}(|\Phi\rangle\langle\Phi|)$ be $\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)$ or $\frac{1}{\sqrt{2}}(|{+}{+}{+}\rangle+|{-}{-}{-}\rangle)$

or $\frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$ or $\frac{1}{2}(|{+}{+}{+}\rangle\langle{+}{+}{+}| + |{-}{-}{-}\rangle\langle{-}{-}{-}|)$?

Example 3 of extensions to QM
-- Deutsch closed-time-like curves

Deutsch CTCs

access to the CTC is via a certain interaction U between CR and CTC



Chronology respecting (CR) registers

CTC registers

in compact region, cannot be prepared, measured, or reused

No grandfather paradox if the state of the CTC is left invariant by the above interaction with the CR registers.

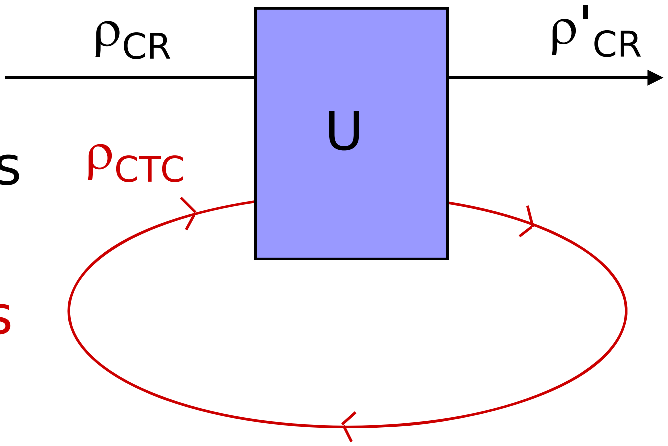
circuit diagrams vs spacetime diagrams

Deutsch CTCs

Such CTC state always exists;
can be mixed and not unique.

no grandfather paradox
reduces to QM far away
count complexity of U

Chronology respecting (CR) registers



CTC registers

State emerging from the interaction: $U \rho_{CR} \otimes \rho_{CTC} U^\dagger$

Consistency requirement:

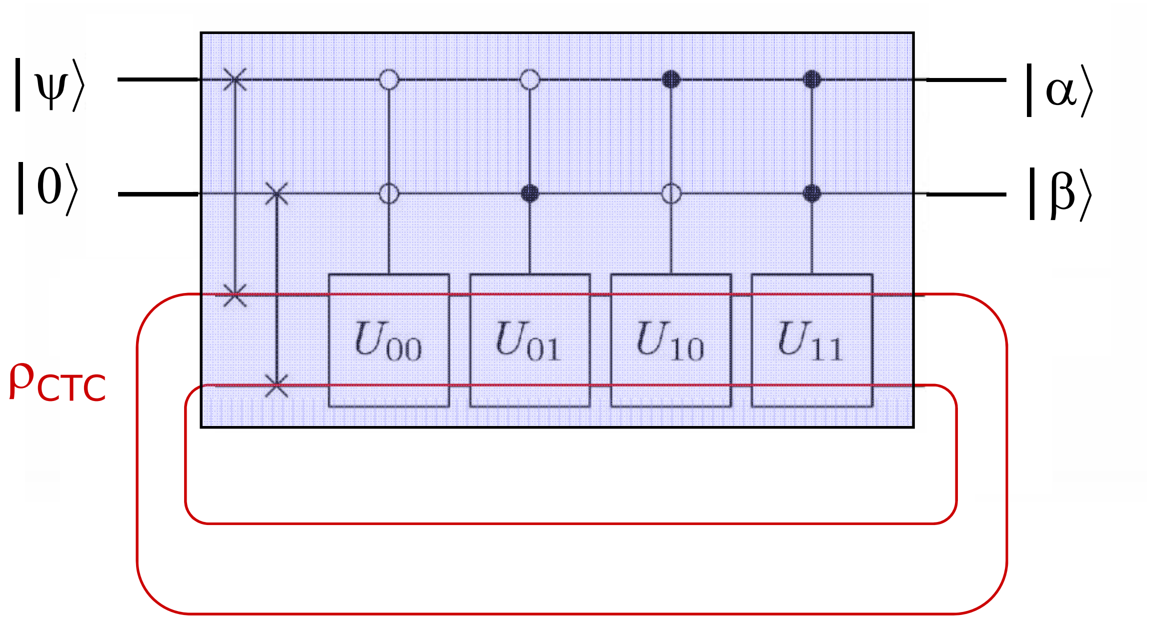
Output in CTC registers = $\mathrm{Tr}_{CR}\, U \rho_{CR} \otimes \rho_{CTC} U^\dagger = \rho_{CTC}$

The fixed point ρ_{CTC} depends on ρ_{CR}

Evolution of CR registers: $\rho'_{CR} = \mathrm{Tr}_{CTC}\, U \rho_{CR} \otimes \rho_{CTC} U^\dagger$

which is nonlinear !

Example (Brun, Harrington, Wilde 2008):



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

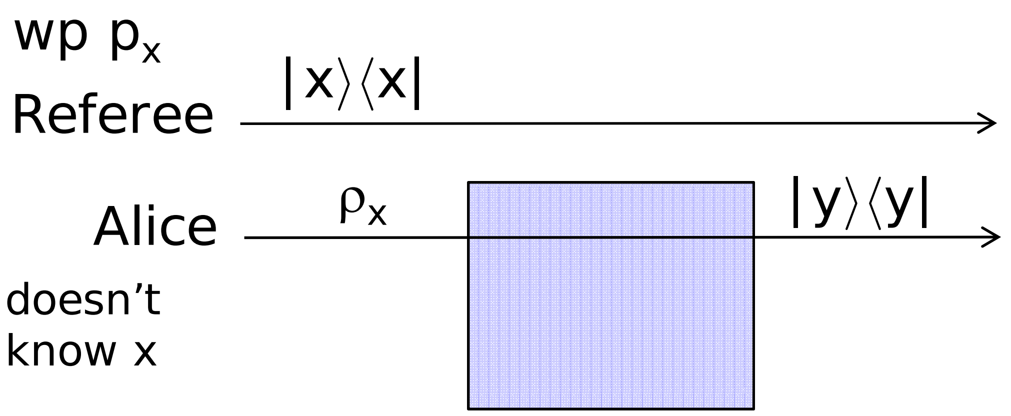
For $|\psi\rangle = \underbrace{|0\rangle, |1\rangle, |+\rangle, |-\rangle}_{\text{BB84 states !!}}$, $|\alpha\rangle|\beta\rangle = |00\rangle, |01\rangle, |10\rangle, |11\rangle$ resp.

cannot distinguish nonortho states in QM

What do mean by discriminating states? How do we describe the state in the CR register?

State discrimination

R: someone who knows ρ_x or where ρ_x originates



wp p_x

Referee $|x\rangle\langle x|$

Alice ρ_x $|y\rangle\langle y|$

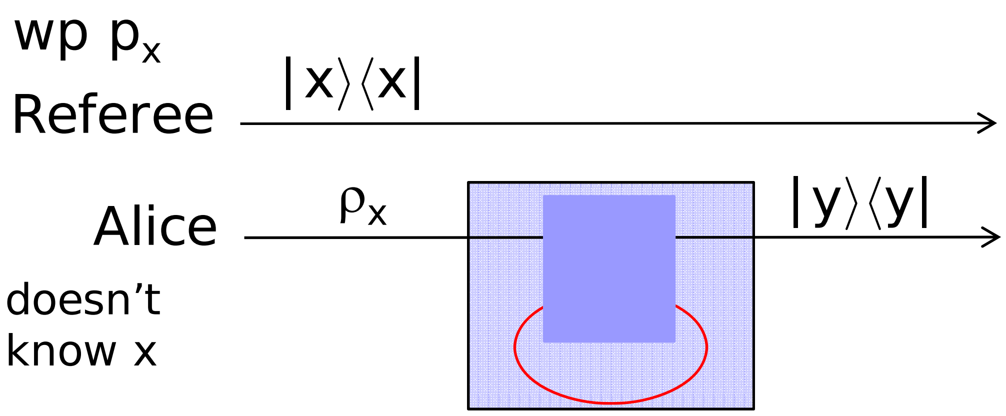
doesn’t know x

Initial state: $\sum_x p_x \, |x\rangle\langle x| \otimes \rho_x$

Final state: $\sum_x p_x \, |x\rangle\langle x| \otimes q(y|x) \, |y\rangle\langle y|$

succeeds if $\approx \sum_x p_x \, |x\rangle\langle x| \otimes |x\rangle\langle x|$

State discrimination with Deutsch CTCs



wp p_x

Referee $|x\rangle\langle x|$

Alice ρ_x $|y\rangle\langle y|$

doesn’t know x

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

Initial state: $\Sigma_x\, p_x\, |x\rangle\langle x| \otimes \rho_x$ (like option 1 in cloning example)

Thus, $\rho_{CR} = \Sigma_x\, p_x\, \rho_x = \mu$ (or equivalently $\Sigma_x\, p_x\, |x\rangle\langle x| \otimes \rho_x$)

Solving for: $\mathrm{Tr}_{CR}\, U\, \mu_{CR} \otimes \rho_{CTC}\, U^\dagger = \rho_{CTC}$ independent of x

gives $\rho'_{CR} = \mathrm{Tr}_{CTC}\, U\, \mu_{CR} \otimes \rho_{CTC}\, U^\dagger = \nu$ independent of x

Output state: $\Sigma_x\, p_x\, |x\rangle\langle x| \otimes \nu$

and the answer is independent of the question

For the Deutsch CTC, option 1 to interpret the input obeys locality and is pathology free, but does not offer advantages beyond QM.

Option 2 causes a lot of pathologies.

Concluding remarks:

Many of the extensions come with a big change to the physical model, and does not include QM as a special case.

Without standard QM, it's not obvious how to calculate, or even to falsify certain calculations.

When venturing outside of QM, one must NOT assume validity of QM (else a clear contradiction).

Rather, a new model with a clear, consistent, set of rules for calculations is needed before any derivation of consequences.

If the new model magically contains QM as a special case, we can start talk what's new in the extension. Else, comparisons may not be well-defined.