CO781 / QIC 890:

Theory of Quantum Communication

Topic 1, part 2

What is communication of data?

The no-signalling principle

Optimality of superdense coding and teleportation

Locality of quantum mechanics

Suppose Alice and Bob each holds one quantum system, and they share a joint initial state.

If Alice measures her system A, the GLOBAL state (and Bob's state on B) post-measurement may depend her measurement outcome.

e.g., sharing $\frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$

Alice measures along the $\{|0\rangle, |1\rangle\}$ basis.

If her outcome is "0" Bob's state is $|0\rangle$.

If her outcome is "1" Bob's state is $|1\rangle$.

Question: can Alice signal to Bob (transmitting a message) by measuring her system?

Question: can Alice signal to Bob (transmitting a message) by measuring her system?

Better not!

1. Alice cannot control the outcome, so, even though Bob can find out Alice's measurement outcome, the net result is the sharing of a random bit.

   Resource inequality: ebit $\geqslant$ rbit

2. Bob doesn't even know if Alice has made the meas or if she ever would. Any measurement Bob can perform depends on his local state, WHETHER Alice has measured or not. Bob's state is $\frac{I}{2}$.

The no-signalling principle

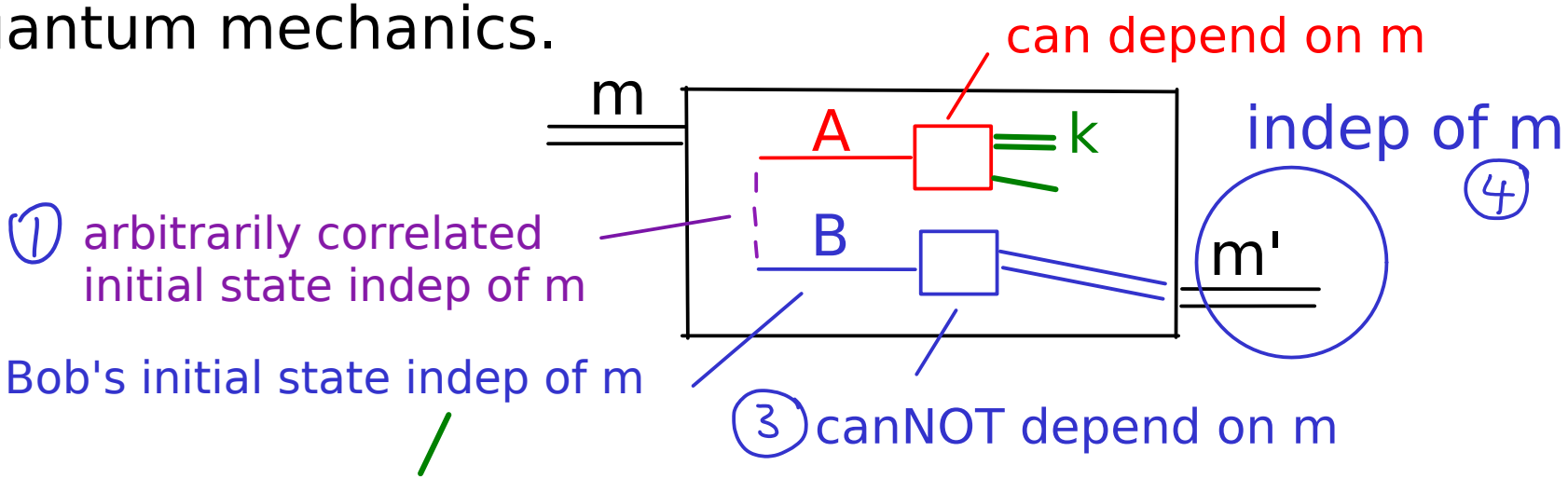
Alice cannot communicate 1 classical bit to Bob if no system physically moves from Alice to Bob.

Implied by any of the following:

1. Without a system moving between Alice and Bob, their operations commute -- neither can affect the other.

2. Bob's state is well defined. (Comm causes state change.)

3. Quantum mechanics.



for each k can depend on m, but need to average over k (then no dependence on m)

Consequences of the no-signalling principle:

C1. No-signalling principle holds even if we allow unlimited amount of entanglement and back comm (from Bob-to-Alice)

there is no free lunch ...

C2. Cannot communicate 1 out of s+t messages using a noiseless classical channel with input size s, even with unlimited entanglement for any t, s $\in \mathbb{Z}^+$.

C3. Cannot communicate an (s+t)-dim system using a noiseless quantum channel with input dim s, even with unlimited entanglement for any t, s $\in \mathbb{Z}^+$.

there is no discounted lunch ...

Qns: do C2, C3 hold if unlimited back communication from Bob to Alice is available? (Do not discuss ...)

Proof:

For C1, argument 3 for no-signalling principle still hold

For C2, we use a useful proof technique:

To disprove the possibility of certain task using suspiciously little comm, assume a protocol exists, replace the comm by a random guess of the message, get a contradiction.

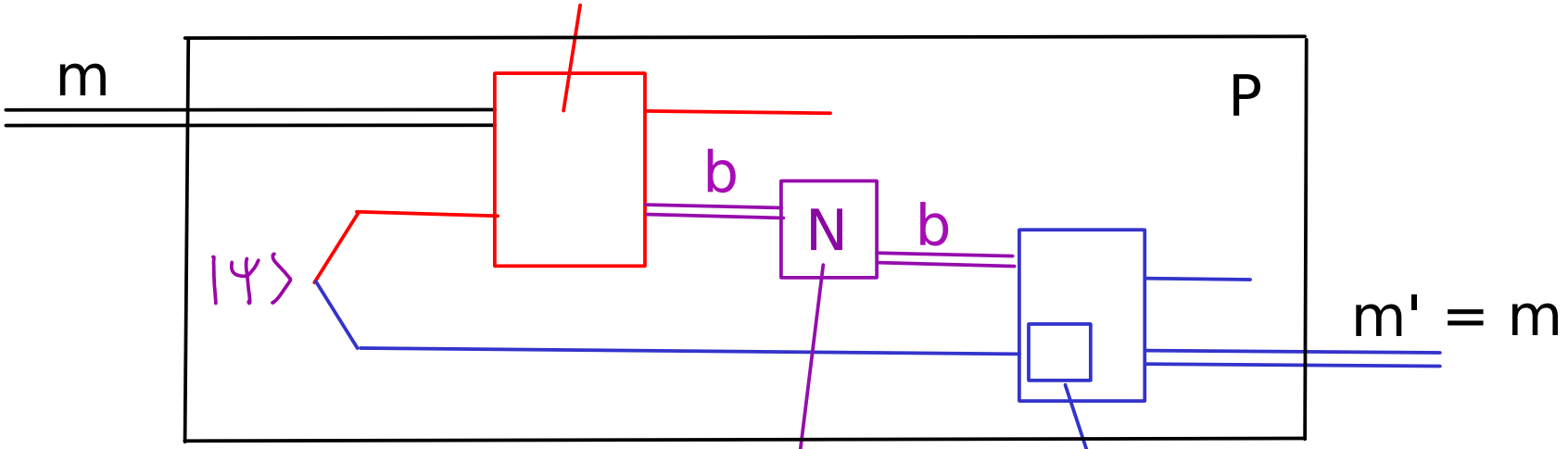
PS for quantum comm, we sometimes replace Bob's channel output by the max mixed state.

C2. Cannot communicate 1 out of s+t messages using a noiseless classical channel with input size s, even with unlimited entanglement for any t, $s \in \mathbb{Z}^+$.

Pf: suppose the opposite. So, there is a protocol P using a noiseless classical channel N with input size s and consuming some state $|\psi\rangle$, and $\forall\, m \in \{1,2,\ldots,s+t\}$ Bob outputs m' = m.

WLOG pure -- purify in Alice's lab

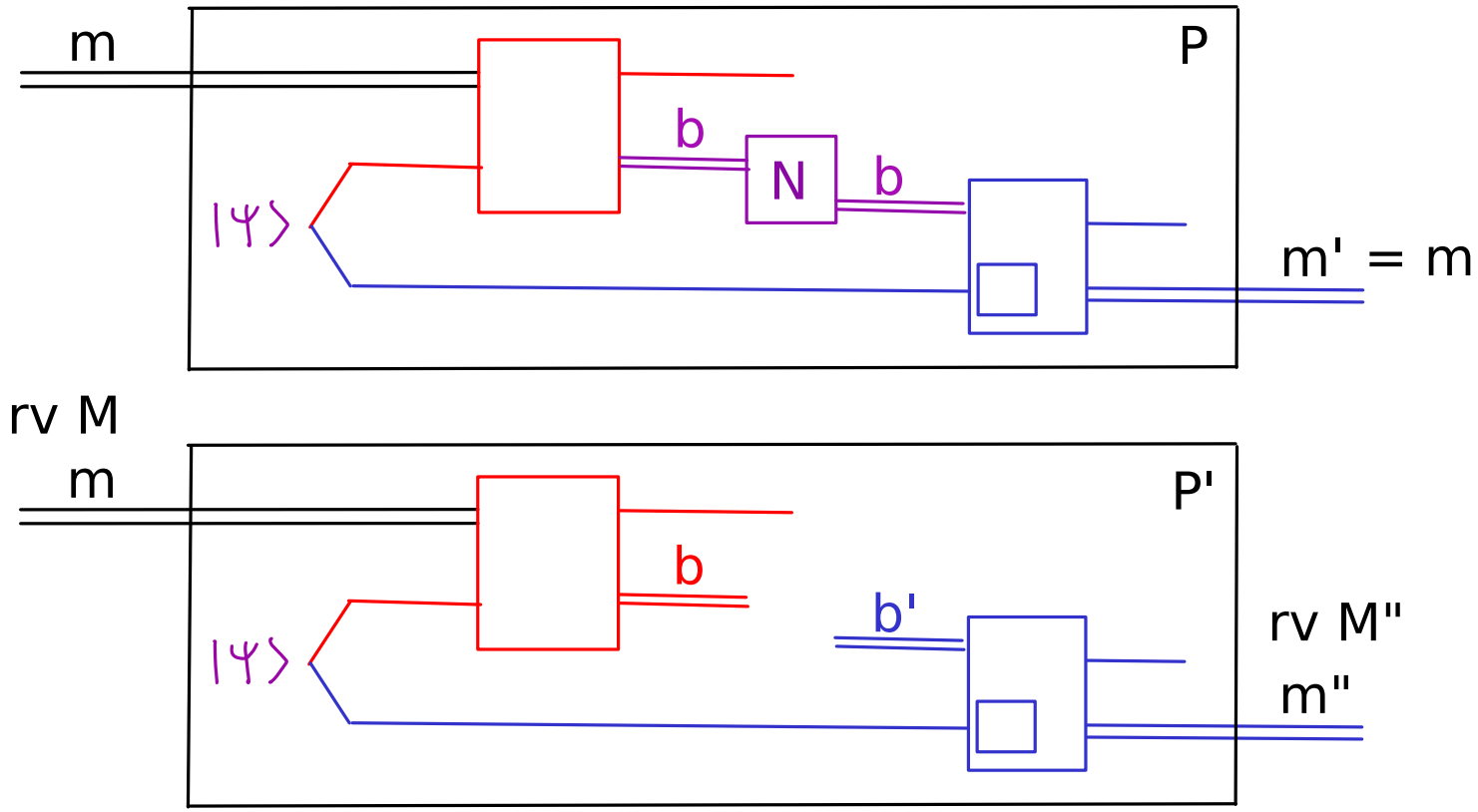
most generally, Alice operates on m and her share of $|\psi\rangle$ obtains the channel input b (+remaining sys) & sends it



no back comm
sole transmission in P

absorb Bob's earlier operations into here

Modify P to P' by removing N, Alice not sending b, and Bob choosing a random b' from {1,2,...,s}.



For P', with prob 1/s, b'=b and m"=m'=m.
* This holds for arbitrary M. In particular, take M to be the uniformly distributed over (s+t) values, so does M". * Meanwhile m=m" with prob 1/s. So, M, M" not independent, contradicting the conclusion from argument 3 to show the no-signalling principle.

Alternatively, given I(M:M")>0, we can view P' as a "noisy channel" from Alice to Bob with positive capacity so with many uses can communicate nearly noiselessly (wk 4).

We can use protocol P' many times -- this consumes more entangled states and still requires no communication. The conclusion still contradict the no-signalling principle.

We proved C1, C2 from more elementary principles.

For C3, we use a central idea in this course --
that of composition of protocols -- to prove our claim.

(Many of the results in this course have multiple,
non-equivalent proofs.)

C3. Cannot communicate an (s+t)-dim system using a noiseless quantum channel with input dim s, even with unlimited entanglement for any t, s $\in \mathbb{Z}^+$.

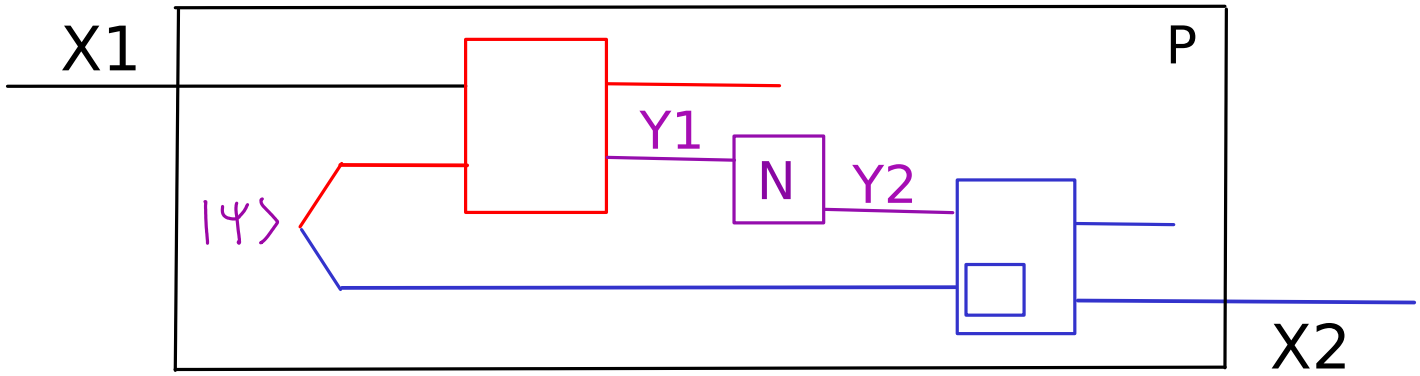
Pf: Useful fact, if entanglement is free, 1 qbit = 2 cbits

Reason: SD implies 1 qbit + 1 ebit $\geq$ 2 cbits

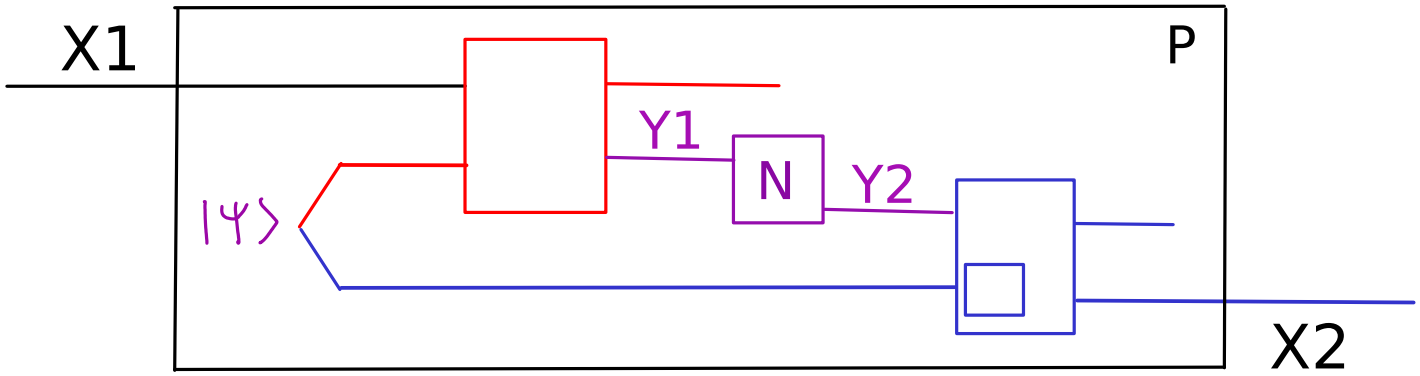
TP implies 2 cbits + 1 ebit $\geq$ 1 qbit

Expect C3 reduces to C2. Again, proof by contradiction.

Suppose there is a protocol P approximating the identity map from X1 to X2 in diamond norm by consuming an s-dim noiseless quantum channel.



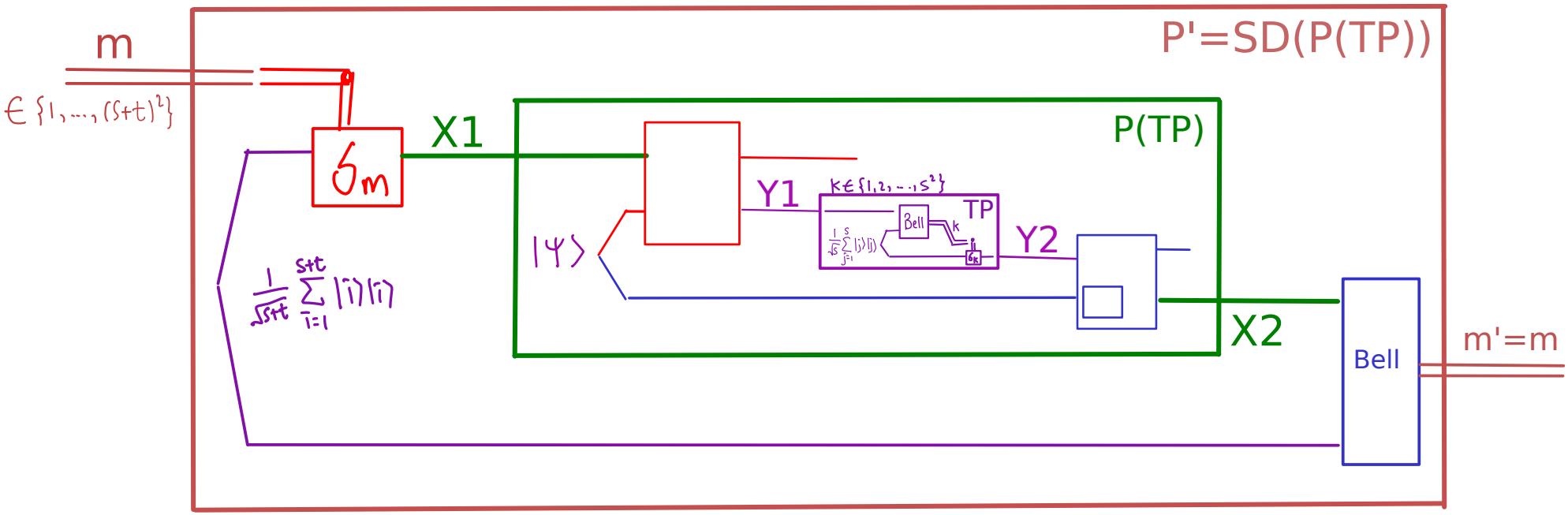
dim(X1) = dim(X2) = s+t , dim(Y1) = dim(Y2) = s



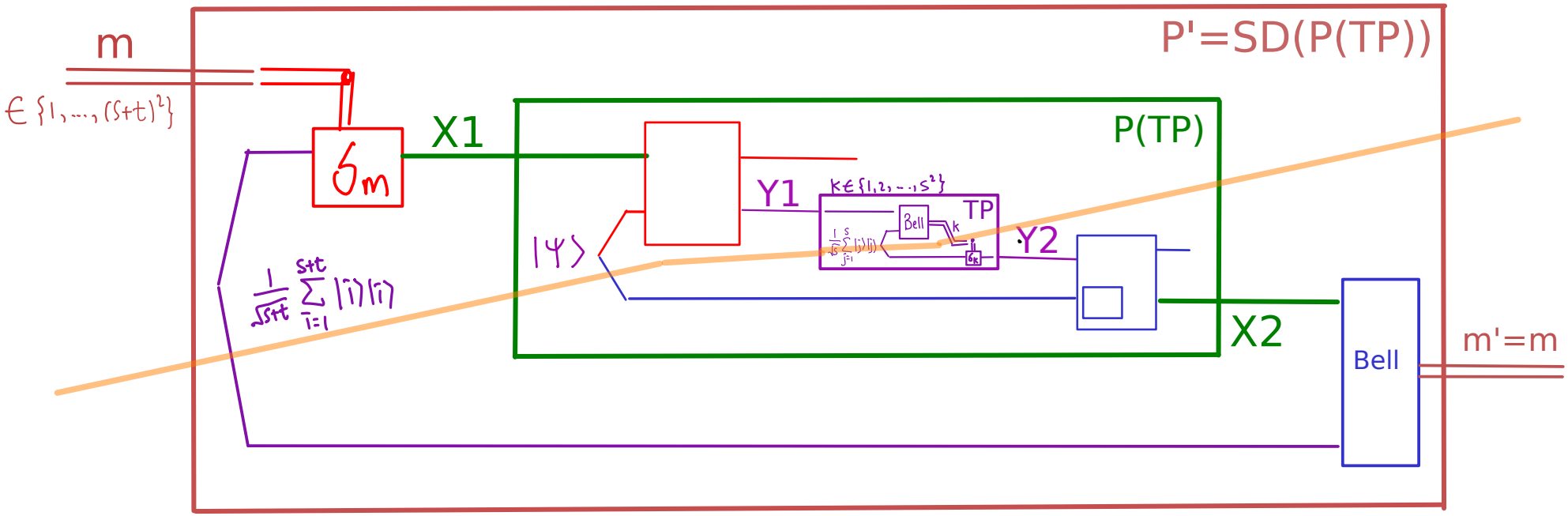
$\dim(X1) = \dim(X2) = s+t$, $\dim(Y1) = \dim(Y2) = s$

Modify P in 2 ways to get P': (+entanglement)

1. simulate N with TP using a noiseless classical channel with s^2 inputs
2. use P (+entanglement) in SD to communicate 1-of-$(s+t)^2$ messages



Overall, SD(P(TP)) uses a noiseless classical channel to transmit $k \in \{1,2,\ldots, s^2\}$ and 3 entangled states. It communicates $m \in \{1,2,\ldots,(s+t)^2\}$. This contradicts C1 if t>0.



In the language of resource inequalities:

C1: $\forall r > 0 \quad \neg (\infty \text{ cbits}_{\leftarrow} + \text{ ent} \geq r \text{ cbits}_{\rightarrow})$

C2: $\forall r, s > 0 \quad \neg (s \text{ cbits} + \text{ ent} \geq (r+s) \text{ cbits})$

C3: $\forall r, s > 0 \quad \neg (s \text{ qbits} + \text{ ent} \geq (r+s) \text{ qbits})$

We proved C3 using SD, TP, and C2:

By contradiction, if C3 holds for some r, s > 0 & $|\Psi\rangle$, then,

$$s \text{ qbits} + |\Psi\rangle \geq (r+s) \text{ qbits} \qquad (*)$$

By TP: $s \text{ ebits} + 2s \text{ cbits} \geq s \text{ qbits}$

Substitute TP into $(*)$ (meaning using TP to simulate qbit consumed in $(*)$)
(note arithmetic in RI corr to protocol compositions)

$$s \text{ ebits} + 2s \text{ cbits} + |\Psi\rangle \geq (r+s) \text{ qbits} \qquad (\dagger)$$

$$s \text{ ebits} + 2s \text{ cbits} + |\Psi\rangle + (r+s) \text{ ebits} \geq (r+s) \text{ qbits} + (r+s) \text{ ebits}$$

$$\geq 2(r+s) \text{ cbits} \quad (\text{by SD})$$

so contradicts C2 ...

Other useful results in QM:

- Unlimited classical comm cannot produce 1 ebit or 1 cbit.
- Cannot comm 1 out of (s+t) messages by physically moving an s-dim system (Holevo's Theorem)

CO781 / QIC 890:

Theory of Quantum Communication

Topic 1, part 2

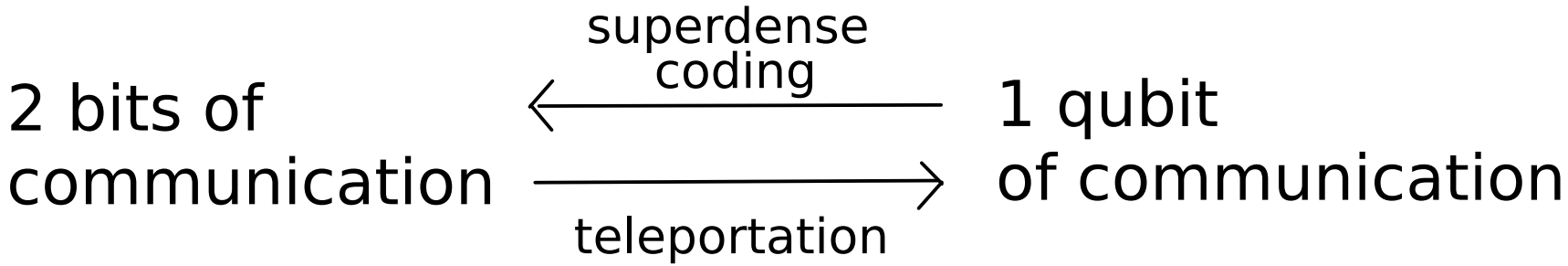
What is communication of data?

The no-signalling principle

Optimality of superdense coding and teleportation

Superdense coding and teleportation:

If entanglement is free, these two communication protocols are inverses of one another:



Furthemore, each protocol is optimal, because of the other protocol !

Optimality of teleportation:

approx in diamond norm distance
asymptotic (2c cbits + ent $\geqslant$ qbits)

Any method to communicate one qubit using unlimited entanglement must send at least 2 bits.

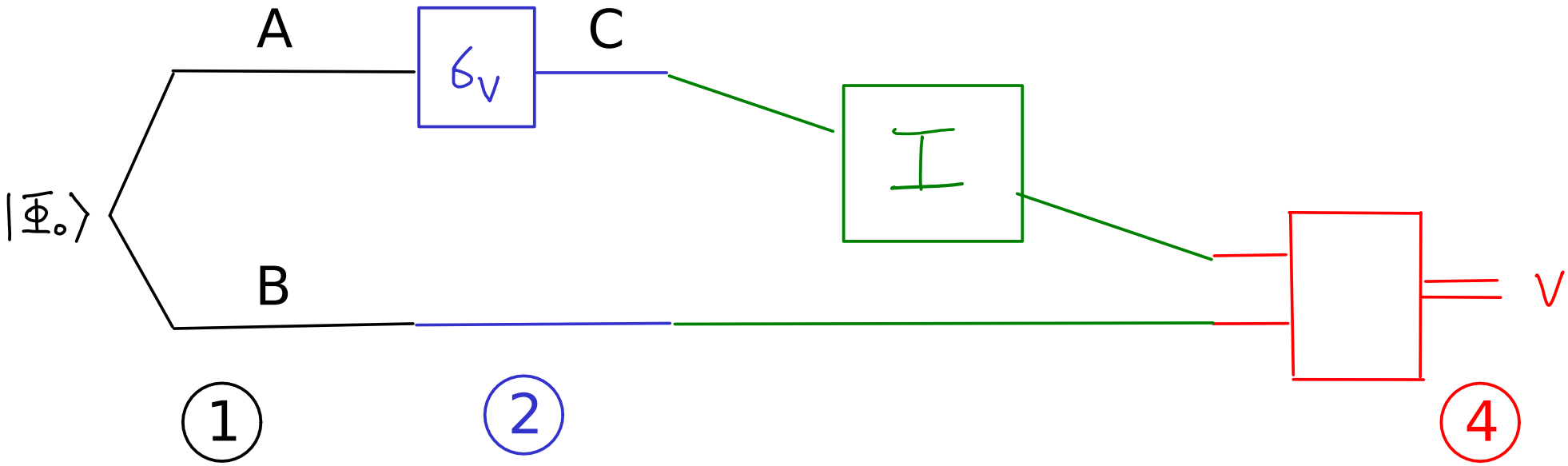
Proof:
Suppose, by contradiction, there is a protocol T that communicates a qubit while consuming an entangled state $|\psi\rangle$ and sending c < 2 classical bits.

Idea: if X is suspiciously too good to be true, compose X with a known protocol Y to get Z so good that it gives a contradiction.

X: protocol T sending fewer than 2 classical bits
Y: superdense coding
Composition: use T to comm the qubit in Y
Z: sending too much classical data with entanglement

Superdense coding (this holds):

③ Alice sends system C to Bob (2-dim).

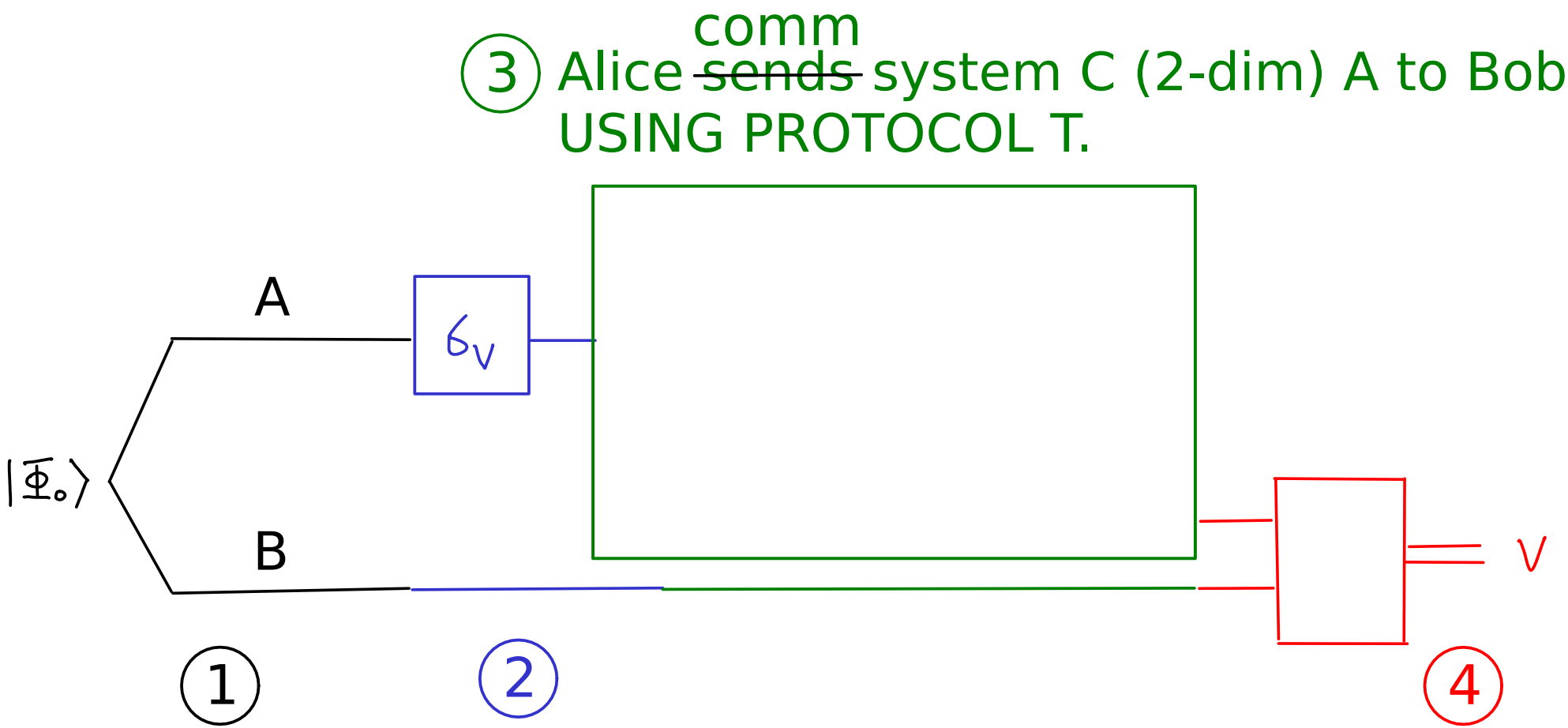


① ebit shared by Alice (A) and Bob (B)

② To comm "v" Alice applies Pauli-v, for v in {0,x,y,z}.

④ Bob measures along the Bell basis to get v.

Superdense coding (still holds IF protocol T exists):

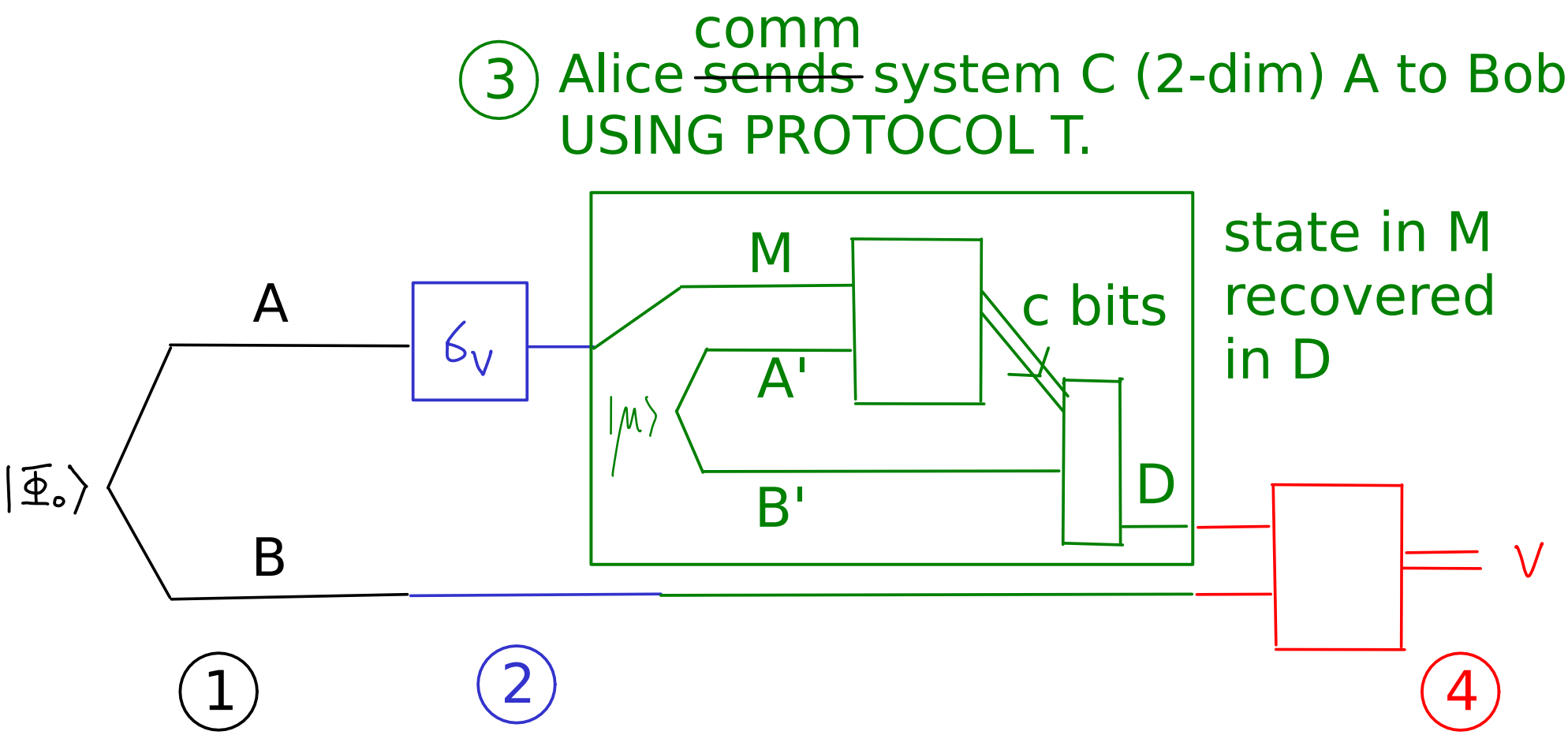


ebit shared by Alice (A) and Bob (B)

To comm "v" Alice applies Pauli-v, for v in {0,x,y,z}.

Bob measures along the Bell basis to get v.

Superdense coding (still works if method T exists):

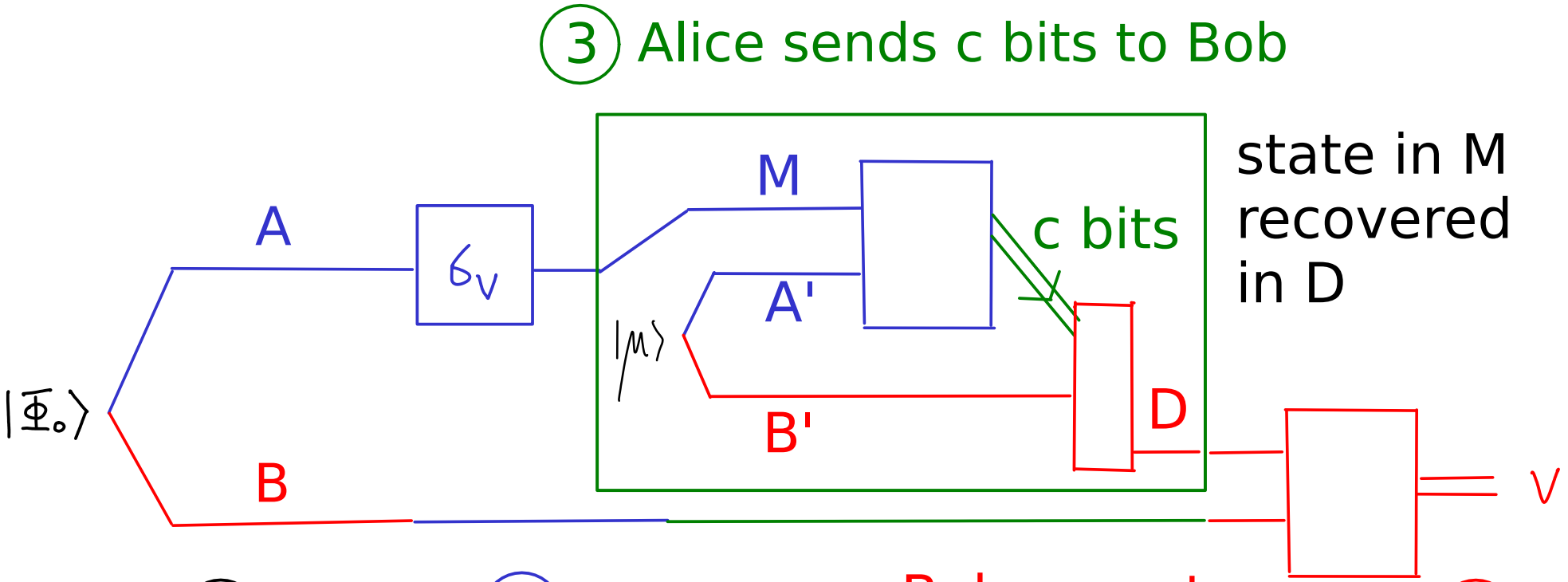


ebit shared by Alice (A) and Bob (B)

To comm "v" Alice applies Pauli-v, for v in {0,x,y,z}.

Bob measures along the Bell basis to get v.

Z: method to send 2 classical bits v using c bits & entanglement



1

ebit shared by Alice (A) and Bob (B)

2

To comm "v" Alice applies Pauli-v, for v in {0,x,y,z}.

Alice also operates on M and A'.

Bob operates on D, then

4

Bob measures along the Bell basis to get v.

Optimality of teleportation:

Any method to communicate one qubit using entanglement must send at least 2 bits.

Proof summary:
Suppose, by contradiction, there is a protocol T to communicate a qubit while consuming some entangled state $|M\rangle$ and sending $c < 2$ classical bits.

Then, take superdense coding scheme, and send the qubit in SD coding by method T.

New scheme now communicates 2 bits using $|M\rangle$, $|\Phi_0\rangle$ and by sending $c < 2$ bits.

This contradicts C2. So, protocol T cannot exist.

In resource inequalities:

If $|\psi\rangle$ + c bits $\geq$ 1 qbit

then $|\psi\rangle$ + c bits $\geq$ 1 qbit $\geq$ 2 cbits by SD

+ 1 ebit + 1 ebit

Thus c $\geq$ 2. (due to C2)

From the original teleportation paper:

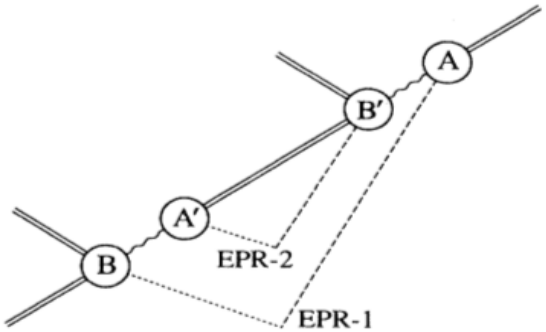


figure drawn as a postscript file by the late Asher Peres

FIG. 2. Spacetime diagram of a more complex 4-way coding scheme in which the modulated EPR particle (wavy line) is teleported rather than being transmitted directly. This diagram can be used to prove that a classical channel of two bits of capacity is necessary for teleportation. To do so, assume on the contrary that the teleportation from A' to B' uses an internal classical channel of capacity $C < 2$ bits, but is still able to transmit the wavy particle's state accurately from A' to B', and therefore still transmit the external two-bit message accurately from B to A. The assumed lower capacity $C < 2$ of the internal channel means that if B' were to guess the internal classical message superluminally instead of waiting for it to arrive, his probability 2^{-C} of guessing correctly would exceed 1/4, resulting in a probability greater than 1/4 for successful superluminal transmission of the external two-bit message from B to A. This in turn entails the existence of two distinct external two-bit messages, r and s, such that $P(r|s)$, the probability of superluminally receiving r if s was sent, is less than 1/4, while $P(r|r)$, the probability of superluminally receiving r if r was sent, is greater than 1/4. By redundant coding, even this statistical difference between r and s could be used to send reliable superluminal messages; therefore reliable teleportation of a two-state particle cannot be achieved with a classical channel of less than two bits of capacity. By the same argument, reliable teleportation of an N-state particle requires a classical channel of $2\log_2(N)$ bits capacity.

superdense coding

no discounted lunch principle C2

Optimality of superdense coding:

Any method to communicate 2 bits using entanglement must send at least 1 qubit.

Proof: exercise / self-study.