CO781 / QIC 890:

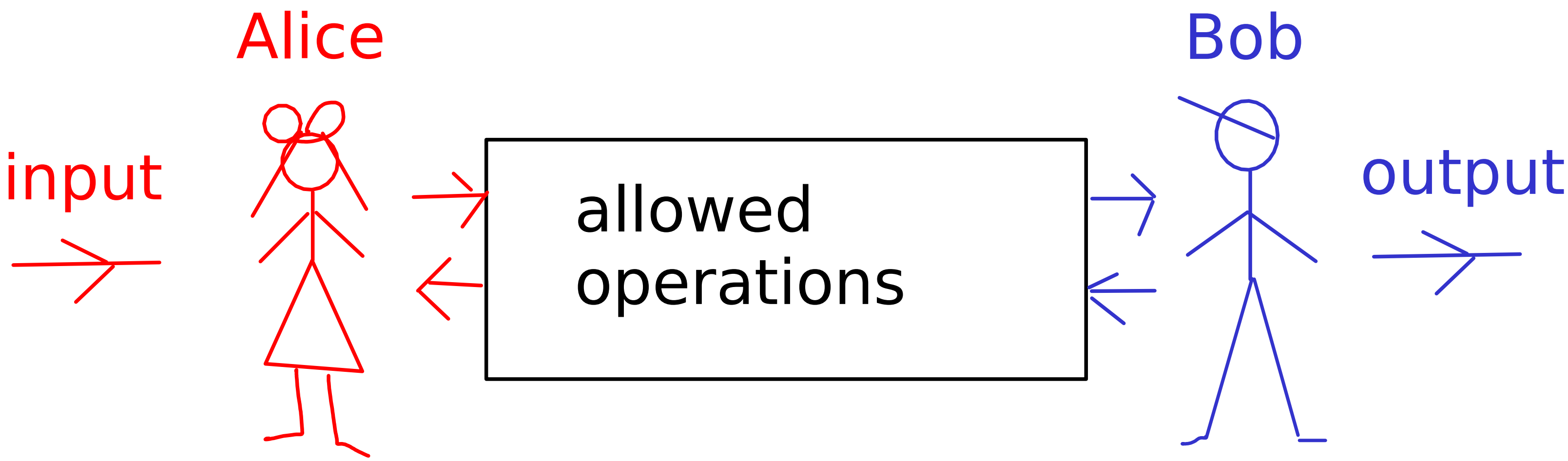
Theory of Quantum Communication

Topic 1, part 1

What is communication of data?

What is communication of data?

Simplest scenario: one sender, one receiver



Intuitively: if input data, output data are "similar" the data is communicated from Alice to Bob.

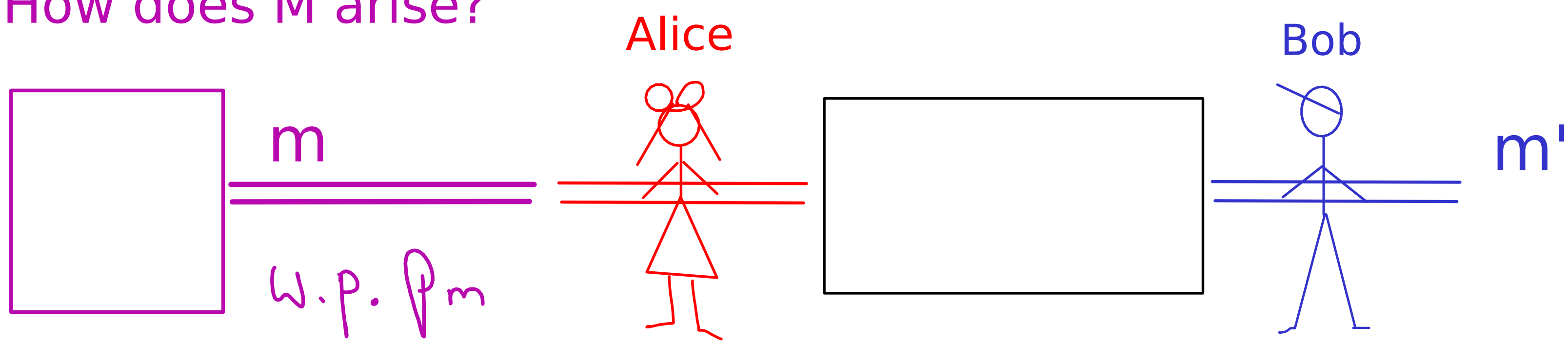
NB Local operations are "free".

What is communication of data?

e.g.1. Data: classical message m $\in \{0, 1\}$

outcome of some random variable (rv) M

How does M arise?



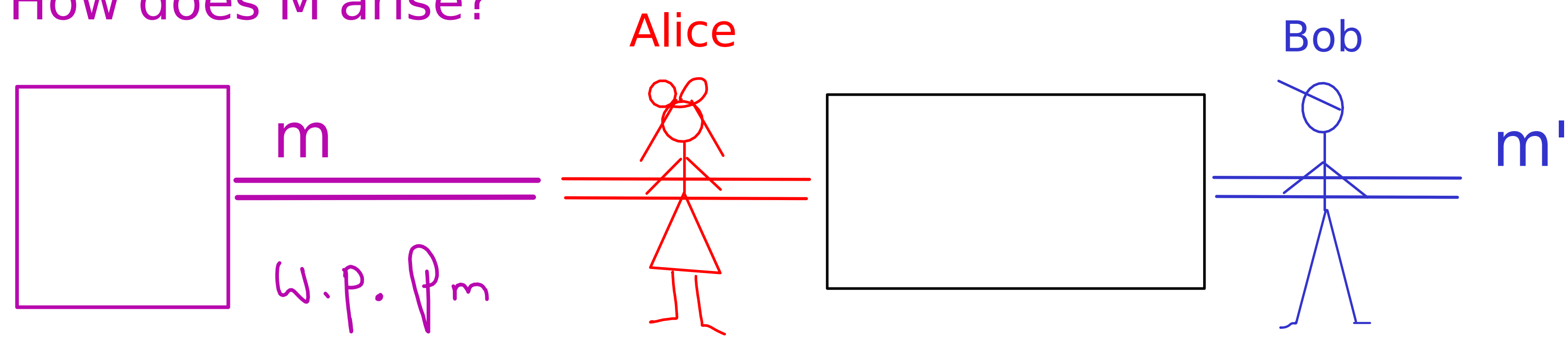
Rules: Alice and Bob do not know m before it arises, their initial state (shared or product) is independent of m. Only after Alice receives m may her operations depend on m. Bob's operations cannot depend on m, but they operate on "data coming from Alice that depends on m".

What is communication of data?

e.g.1. Data: classical message m $\in \{0,1\}$

outcome of some random variable (rv) M

How does M arise?



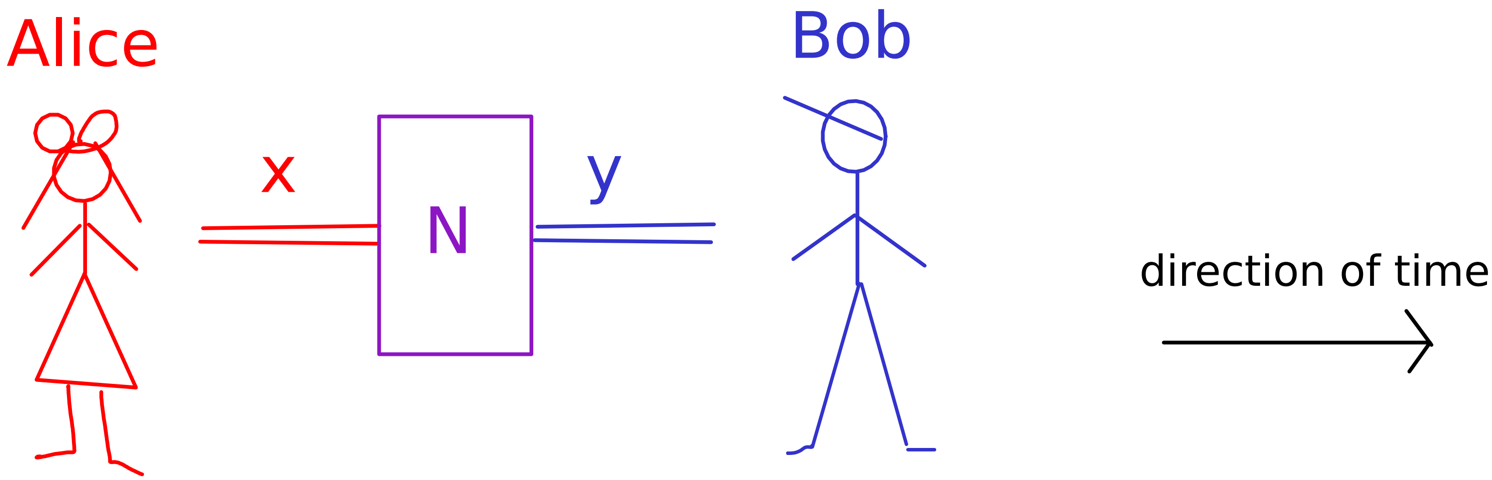
Intuitively: the data is communicated if for each possible m received by Alice, Bob's output m'=m.

Bob's output m' is a rv, call it M'.

If the data is communicated properly, necessary that:
(i) M' approx M, (ii) if a rv T correlates with M, then, T correlates with M' the same way.

What is communication of data?

Def: A noisy classical channel N from Alice to Bob with input alphabet X & output alphabet Y is specified by Pr(Y=y | X=x) for all possible x, y.



Def: the noiseless classical channel over X has X $\subseteq$ Y and Pr(Y=y | X=x) = δ_{xy}

i.e., Pr(Y=y | X=x) = $\begin{cases} 1 \text{ if } y=x, \\ 0 \text{ otherwise.} \end{cases}$

What is communication of data?

e.g.1. Data: classical message m $\in \{0, 1\}$

Concept: protocol. If Alice and Bob can use *once* a noiseless channel N of |X|=2, Alice can communicate M to Bob by choosing channel input x=m.

Concept: the channel N is a resource consumed in the above protocol. (Alice & Bob use 1 cbit.)

Concept: the ability to communicate M is a resource produced by the protocol (and can in turns be consumed as a subroutine elsewhere). (Alice & Bob create 1 cbit.)

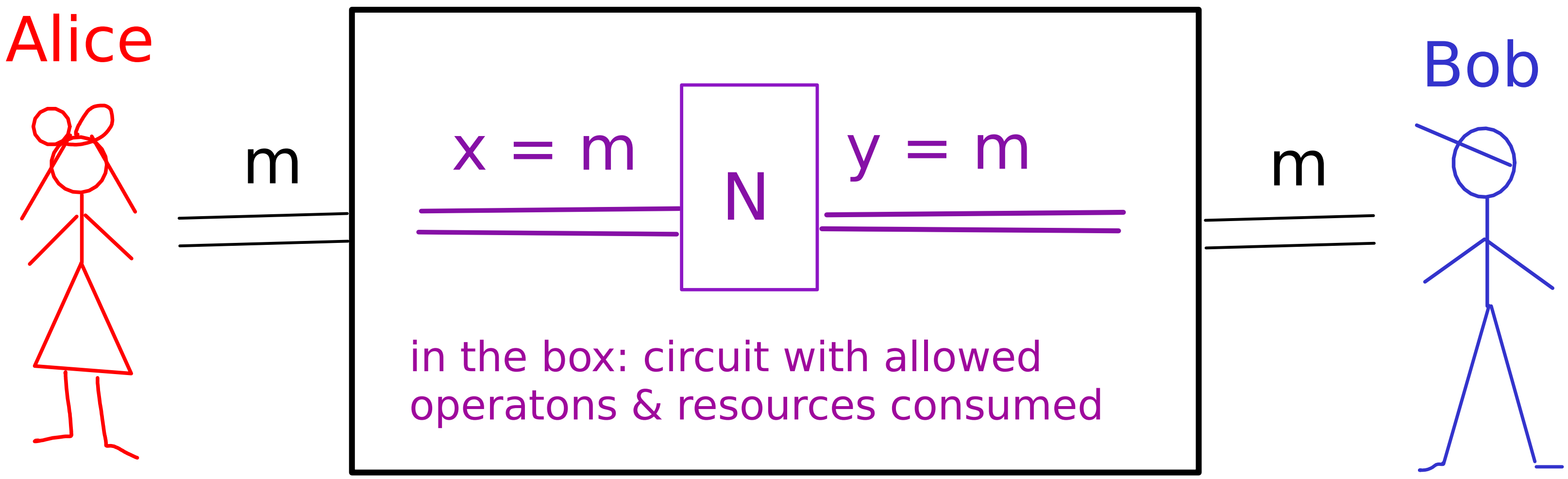
$\circledast$ the protocol simulates a noiseless channel (M->M')

Generalization: for |X| = d, log d cbits are consumed etc.
Sometimes add direction of comm to cbit. e.g., 1 cbit $\rightarrow$

What is communication of data?

e.g.1. Data: classical message $m \in \{0, 1\}$

Diagramatic representation of a protocol:



input (m) box w/ input & output output (m)

Convention: the diagram holds for all m
Formally : input is a mixture over m, apply linearity

What is communication of data?

e.g.1. Data: classical message $m \in \{0,1\}$

$$\forall m \qquad |m\rangle\langle m|_A \xrightarrow{\text{enc}} |m\rangle\langle m|_X \xrightarrow{N} |m\rangle\langle m|_Y \xrightarrow{\text{dec}} |m\rangle\langle m|_B$$

Question: is the following a reasonable description of communicating M to Bob?

$$\sum_{m=0}^{1} p_m |m\rangle\langle m|_A \xrightarrow{\text{enc}} \sum_{m=0}^{1} p_m |m\rangle\langle m|_X$$

$$\xrightarrow{N} \sum_{m=0}^{1} p_m |m\rangle\langle m|_Y$$

$$\xrightarrow{\text{dec}} \sum_{m=0}^{1} p_m |m\rangle\langle m|_B$$

It is necessary, but not sufficient.

What is communication of data?

e.g.1. Data: classical message $m \in \{0,1\}$

$$\forall m \quad |m\rangle\langle m|_A \xrightarrow{\text{enc}} |m\rangle\langle m|_X \xrightarrow{N} |m\rangle\langle m|_Y \xrightarrow{\text{dec}} |m\rangle\langle m|_B$$

Question: is the following a reasonable description of communicating M to Bob?

$$\sum_{m=0}^{1} p_m |m\rangle\langle m|_A \xrightarrow{\text{enc}} \sum_{m=0}^{1} p_m |m\rangle\langle m|_X$$

$$\xrightarrow{N} \sum_{m=0}^{1} p_m |m\rangle\langle m|_Y$$

$$\xrightarrow{\text{dec}} \sum_{m=0}^{1} p_m |m\rangle\langle m|_B$$

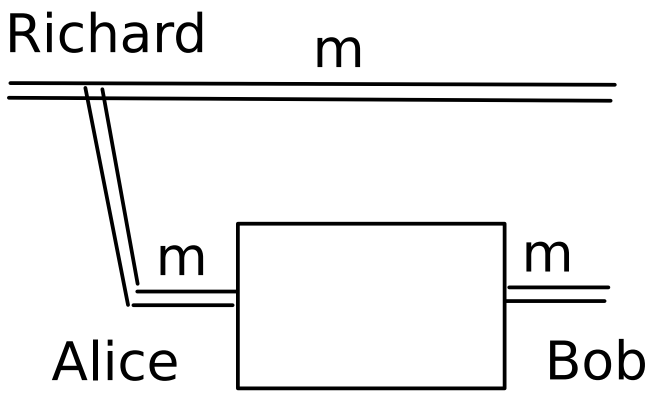
It is necessary, but not sufficient.

1. Bob could have created this without Alice.
2. Cannot impose correctness (e.g., p0 = p1 = 1/2, 0 <-> 1)

What is communication of data?

e.g.1. Data: classical message m $\in \{0,1\}$

Model: a reference Richard is holding a copy of m:



$$\sum_{m=0}^{1} p_m \, |m\rangle\langle m|_R$$

$$\xrightarrow{\text{forward to A}} \sum_{m=0}^{1} p_m \, |m\rangle\langle m|_R \otimes |m\rangle\langle m|_A$$

$$\xrightarrow{\text{enc}} \sum_{m=0}^{1} p_m \, |m\rangle\langle m|_R \otimes |m\rangle\langle m|_X$$

$$\xrightarrow{N} \sum_{m=0}^{1} p_m \, |m\rangle\langle m|_R \otimes |m\rangle\langle m|_Y$$

$$\xrightarrow{\text{dec}} \sum_{m=0}^{1} p_m \, |m\rangle\langle m|_R \otimes |m\rangle\langle m|_B$$

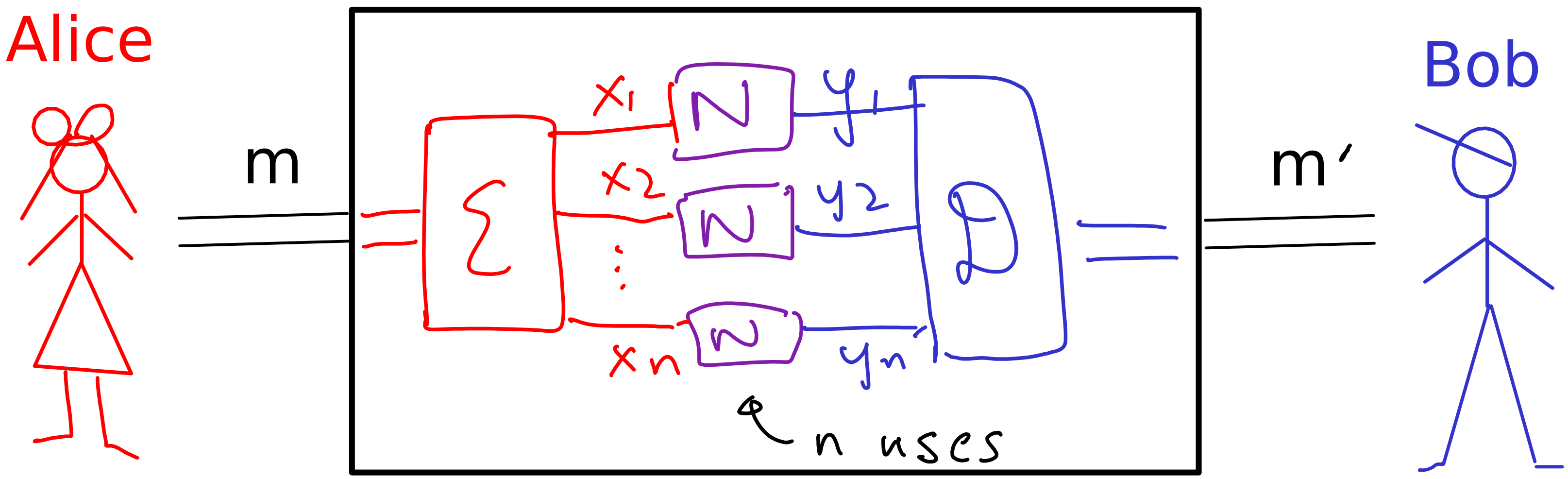
Ex: if T is correlated with M (as defined by a joint distribution pr(tm), how does T correlate with M'?

Ex: what if Alice also keeps a copy of m?

What is communication of data?

e.g.1++. Data: classical message m $\in \{1, 2, 3, \ldots, 2^{nr}\}$

A protocol to transmit data through a noisy channel:

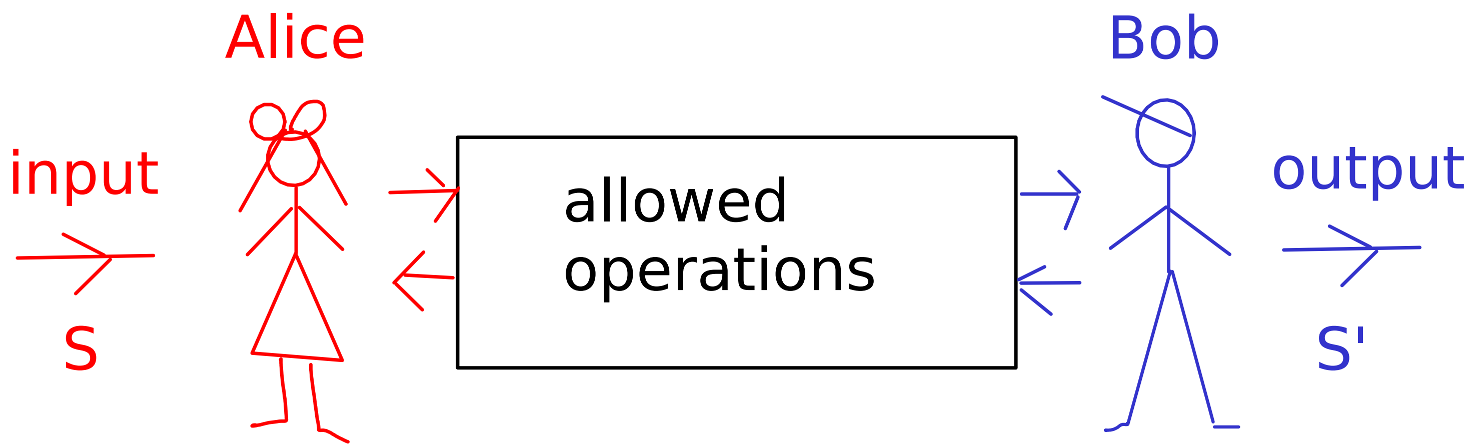


input (m) box w/ input & output output (m')

Shannon's noisy coding theorem: optimize r.

What is communication of data?

e.g.2. Quantum data: state (variable) on a system S



One definition of communication of quantum data:
for each input state ρ on S, the output on S' is ρ.

(or approximately so)

(We will see weaker definitions later, e.g., quantum data compression or remote state preparation.)

What is communication of data?

Def: A quantum channel N from a d1-dim system X to a d2-dim system Y is a function from d1xd1 matrices to d2xd2 matrices that are (1) linear, (2) trace-preserving, (3) completely positive. (aka TCP maps, Q ops etc)

Def: A noiseless quantum channel N on a d-dim sys is given by the identity map on dxd matrices (can also embed in an output space with dim bigger than d).

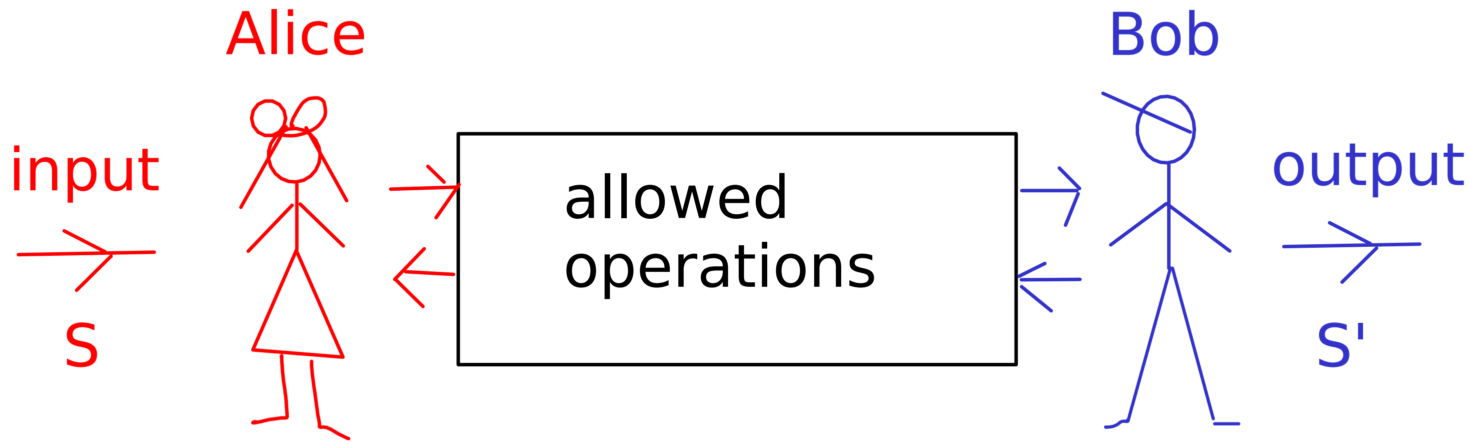
Similar to e.g.1, can communicate a 2-dim Q system (creating 1 qbit) by using a noiseless quantum channel on a 2-dim system (consuming 1 qbit).

(Extensions: log d qbits, adding direction)

Recall: quantum channels and their representations

What is communication of data?

e.g.2. Quantum data: state (variable) on a system S



Alternative definition of comm of quantum data:
each input in S is mapped to the output on S'
(approximately) by the noiseless quantum channel.

What is communication of data?

e.g.2. Quantum data: state (variable) on a system S

Def: the diamond norm distance between two channels $\mathcal{N}_1, \mathcal{N}_2$ is given by

$$\| \mathcal{N}_1 - \mathcal{N}_2 \|_\diamond := \max_{|\psi\rangle_{RS}} \| I \otimes \mathcal{N}_1 (|\psi\rangle\langle\psi|) - I \otimes \mathcal{N}_2 (|\psi\rangle\langle\psi|) \|_t$$

from S to S'

dim(R) = dim(S)

trace distance

NB M1, M2 same dim, Hermitian. Schatten 1-norm || M1 - M2 ||$_1$ is the sum of the absolute values of the eigenvalues of M1-M2.
|| ... ||_t = 1/2 || ... ||_1.
If M1, M2 are density matrices on sys S, referee draws one at random, prepares the state on S and gives the system S to Alice (she doesn't know which state), then, max prob for Alice to say whether the state is M1 or M2 is $\frac{1}{2} + \frac{1}{2} \| M_1 - M_2 \|_t$.

What is communication of data?

e.g.2. Quantum data: state (variable) on a system S

Def: the diamond norm distance between two channels $\mathcal{N}_1$, $\mathcal{N}_2$ is given by

$$\underbrace{\| \mathcal{N}_1 - \mathcal{N}_2 \|_\diamond}_{\text{from S to S'}} := \max_{\underbrace{|\psi\rangle_{RS}}_{\dim(R) = \dim(S)}} \underbrace{\| I \otimes \mathcal{N}_1 (|\psi\rangle\langle\psi|) - I \otimes \mathcal{N}_2 (|\psi\rangle\langle\psi|) \|_t}_{\text{trace distance}}$$

Consequence: If a communication protocol approximates the noiseless channel from S to S' to diamond norm distance $\leqslant \epsilon$, then,

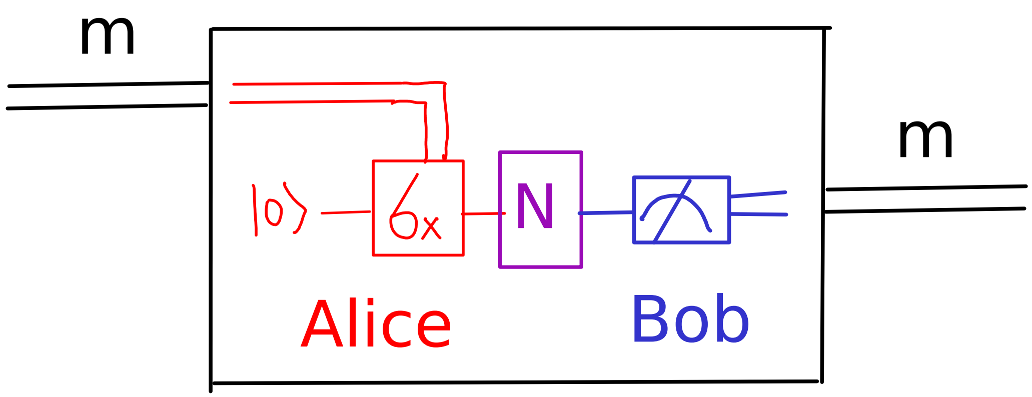
$\forall |\psi\rangle$ on system RS, the protocol yields a state on RS' with trace distance less than ϵ from $|\psi\rangle$.

i.e., this notion of approx preserves correlation with S.

What is communication of data?

e.g. 3. Alice can communicate 1 classical bit to Bob using a noiseless quantum channel N on a 2-dim sys.

Protocol:



This consumes "1 qbit" (the ability to send a 2-dim sys) and creates "1 cbit".

Concept: a resource inequality holds if there exists a protocol converting the resources (later: need approx).

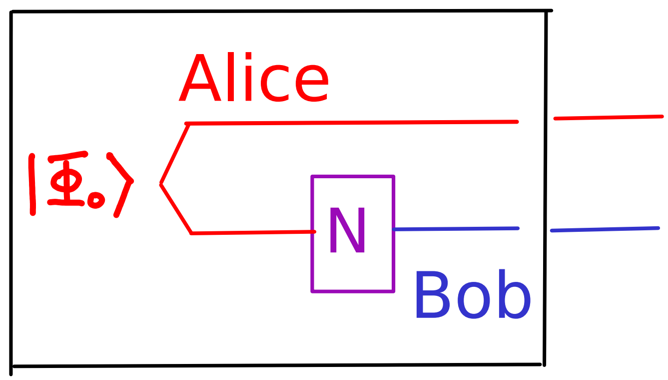
e.g. $\quad 1 \text{ qbit} \rightarrow \;\geqslant\; 1 \text{ cbit} \rightarrow$

resources consumed $\qquad\qquad$ resources created

What is communication of data?

e.g. 4. Alice and Bob can share $|\Phi_0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$
using a noiseless quantum channel N on a 2-dim sys.

Protocol:



NB output is shared by Alice & Bob

This consumes "1 qbit" and creates "1 ebit" (a maximally entangled state of local dim 2). Resource inequality:

$$1 \text{ qbit} \; \rightarrow \; \geq \; 1 \text{ ebit}$$

resources consumed

resources created

NB Above requires qbit to be entanglement preserving.

Exercise:

What is meant by the resource inequality

$$1 \text{ qbit} \longleftarrow \geqslant \quad 1 \text{ ebit} \qquad ?$$

Is it true?
If so, provide a protocol.
If not, provide a proof that no such protocol exists.

What is communication of data?

e.g 5 Superdense coding (SD) (Bennett-Wiesner "92")

Suppose Alice and Bob share the state $\frac{1}{\sqrt{s}}\sum_{i=1}^{s}|i\rangle\otimes|i\rangle$ and Alice can send an s-dimensional quantum system to Bob. Then, Alice can communicate any of $t=s^2$ messages to Bob.

Data: classical
Allowed resources: noiseless q channel, entanglement

Proof: for simplicity, first consider s=2.

Suppose Alice & Bob share the state $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

so that Alice (Bob) holds the first (second) qubit.

Recall the Pauli matrices:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Suppose Alice wants to communicate a message m from the set $\{0, x, y, z\}$.

If her message is m, she applies σ_m to A.

The shared state $|\Phi_0\rangle$ on AB is transformed by $\sigma_m \otimes I$.

For $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$|\Phi_0\rangle = \sigma_0 \otimes I \, |\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi_x\rangle = \sigma_x \otimes I \, |\Phi_0\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$

$$|\Phi_y\rangle = \sigma_y \otimes I \, |\Phi_0\rangle = \frac{1}{\sqrt{2}}(i|10\rangle - i|01\rangle)$$

$$|\Phi_z\rangle = \sigma_z \otimes I \, |\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

These 4 states are mutually orthogonal, and form the "Bell basis". NB Alice operates on a 2-dim system A, but the joint state on AB tranverses to 1 out of 4 possible distinguishable (ortho) states.

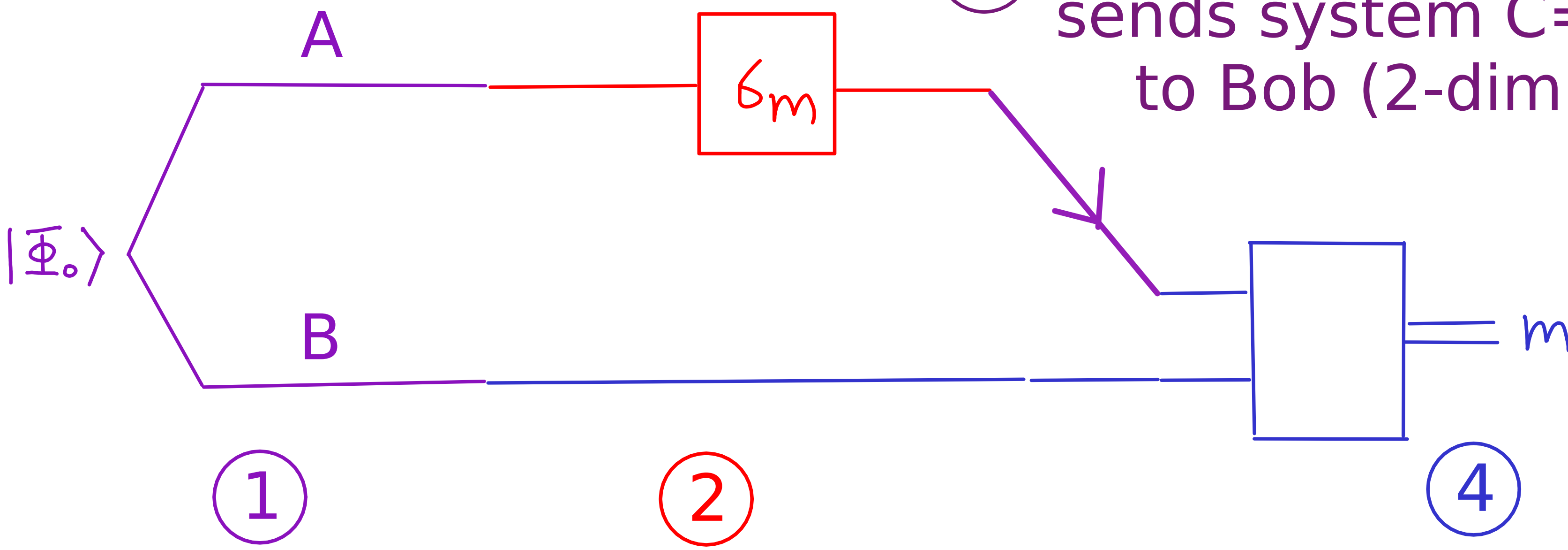
requires ent be preserved

If Alice sends C=A to Bob, he has AB in the state $|\Phi_v\rangle$.

He can measure AB along the Bell basis to find v !

Communication protocol:

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



Initial state shared between Alice and Bob. Alice is holding system A; Bob is holding system B.

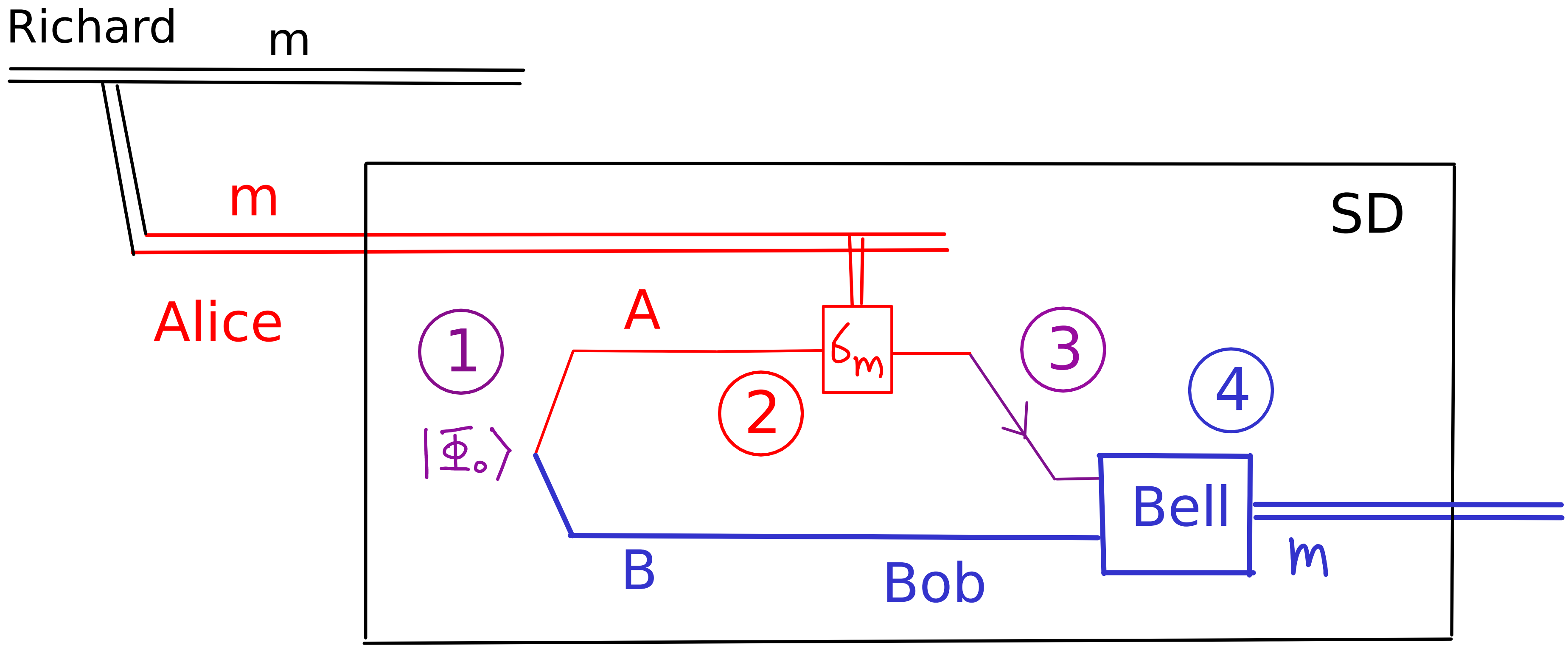
1 ebit

If Alice receives the message "m" $\in$ {0,x,y,z}, she applies σ_m to qubit A.

Having both A & B, Bob measures along the Bell basis; outcome is m.

Communication protocol:

recall circuit conventions



Resource inequality: 1 ebit + 1 qbit $\geq$ 2 cbits

NB the ebit can be pre-shared, or created by Bob through back communication. "Superdense" refers to the communication of 1 in s^2 distinguishable messages by sending an s-dim sys.

What is communication of data?

e.g 5 Teleportation (TP)
(Bennett-Brassard-Crepeau-Jozsa-Peres-Wootters 93)

In the language of resource inequality:

$$2 \text{ cbits} + 1 \text{ ebit} \geq 1 \text{ qbit}$$

given entanglement & ability to communicate classical bits

data is quantum

What is communication of data?

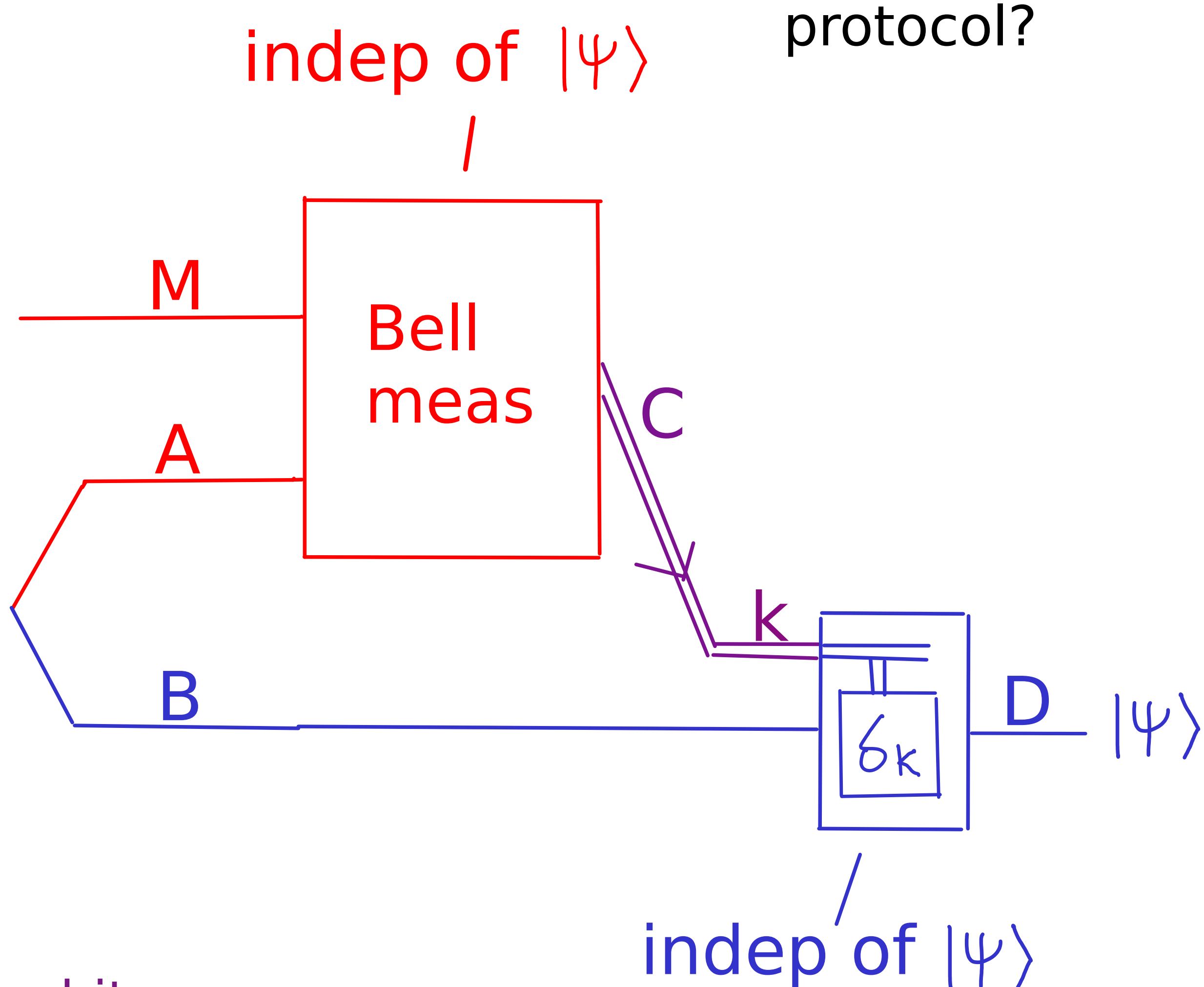
e.g 5 Teleportation (TP)

Ex: how to draw the box for this protocol?

Protocol:

$|\psi\rangle = a|0\rangle + b|1\rangle$

$|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



Red: Alice's

Blue: Bob's

Purple: cbits from Alice to Bob, entanglement

Proof: main mathematical tool:
Expressing an 8-dim quantum state in 2 ways.

$$(a|0\rangle + b|1\rangle)_M \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$$

$$= (a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)_{MAB} \frac{1}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{MA}(a|0\rangle + b|1\rangle)_B \frac{1}{2}$$

$$+ \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{MA}(a|0\rangle - b|1\rangle)_B \frac{1}{2}$$

no cross terms gives $a|000\rangle + b|111\rangle$

$$+ \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{MA}(a|1\rangle + b|0\rangle)_B \frac{1}{2}$$

$$+ \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{MA}(a|1\rangle - b|0\rangle)_B \frac{1}{2}$$

$= a|011\rangle + b|100\rangle$

$|\psi\rangle$ $\qquad\qquad$ $|\Phi_0\rangle$

$$(a|0\rangle + b|1\rangle)_M \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB} =$$

$|\Phi_0\rangle$ $\quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{MA}(a|0\rangle + b|1\rangle)_B \frac{1}{2}$ $\quad |\psi\rangle$

$|\Phi_z\rangle$ $\quad + \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{MA}(a|0\rangle - b|1\rangle)_B \frac{1}{2}$ $\quad \sigma_z|\psi\rangle$

$|\Phi_x\rangle$ $\quad + \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{MA}(a|1\rangle + b|0\rangle)_B \frac{1}{2}$ $\quad \sigma_x|\psi\rangle$

$i|\Phi_y\rangle$ $\quad + \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{MA}(a|1\rangle - b|0\rangle)_B \frac{1}{2}$ $\quad \sigma_y|\psi\rangle / i$

Pauli's: $\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Bell basis: $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\Phi_y\rangle = \frac{1}{\sqrt{2}}(i|10\rangle - i|01\rangle)$

$|\Phi_x\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$, $|\Phi_z\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

$$\underbrace{(a|0\rangle + b|1\rangle)_M}_{|\psi\rangle} \underbrace{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}}_{|\Phi_0\rangle} =$$

$$\underbrace{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{MA}}_{|\Phi_0\rangle} \underbrace{(a|0\rangle + b|1\rangle)_B}_{|\psi\rangle} \frac{1}{2}$$

$$+ \underbrace{\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{MA}}_{|\Phi_z\rangle} \underbrace{(a|0\rangle - b|1\rangle)_B}_{\sigma_z|\psi\rangle} \frac{1}{2}$$

$$+ \underbrace{\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{MA}}_{|\Phi_x\rangle} \underbrace{(a|1\rangle + b|0\rangle)_B}_{\sigma_x|\psi\rangle} \frac{1}{2}$$

$$+ \underbrace{\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{MA}}_{i|\Phi_y\rangle} \underbrace{(a|1\rangle - b|0\rangle)_B}_{\sigma_y|\psi\rangle / i} \frac{1}{2}$$

If Alice measures MA along the Bell basis, each outcome $k \in \{0,x,y,z\}$ occurs with prob 1/4, and postmeasurement state is $|\Phi_k\rangle_{MA} \otimes \sigma_k |\psi\rangle_B$.

If Alice sends k to Bob, he can apply σ_k to B, turning $\sigma_k |\psi\rangle_B$ to $|\psi\rangle_B$.

Remarks:

0. What is teleported, the body or the soul ?

1. $|\psi\rangle$ takes infintely many bits to describe. Also, given a copy, Alice cannot learn a description of $|\psi\rangle$

2. But Alice's operations are independent of $|\psi\rangle$ and only 2 bits of info need to be sent.

3. Generalizes to higher dimension.

4. Preserves global state / correlations

Ex: for any state $|\psi\rangle_{RM}$ where M is 2-dim, show that

$$|\psi\rangle_{RM} = a\,|\alpha_0\rangle\,|0\rangle + b\,|\alpha_1\rangle\,|1\rangle$$

for some unit vectors $|\alpha_0\rangle, |\alpha_1\rangle$ on R, and $|a|^2 + |b|^2 = 1$.

If Alice teleports M to Bob (with identity map on R), repeat the above analysis to show that the final state on RB is $|\psi\rangle$.

What is communication of data?

Summary: in each communication problem, need to clarify the data type, how it arises, what the output state should be (in terms of the input state), what resources are available to sender and receiver etc.

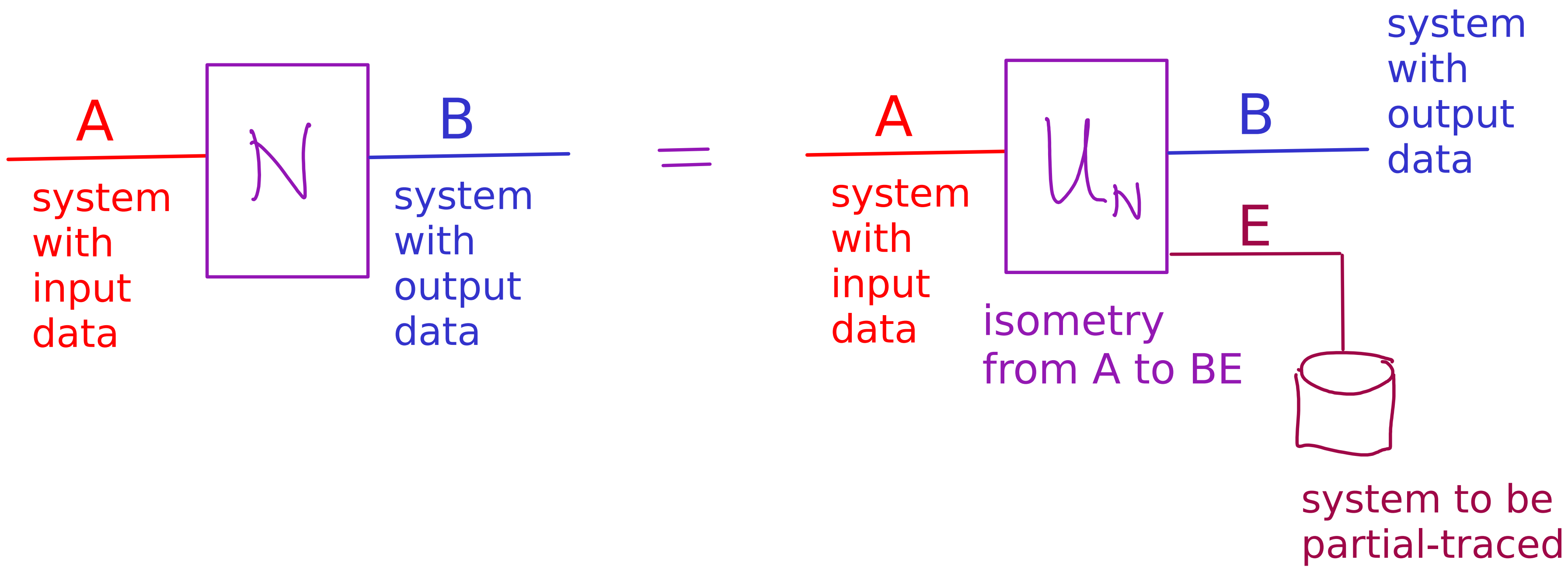
We saw examples how resources are used, and how various notions of "correct communication" are achieved.

We have considered resources cbits, qbits, ebits that satisfy all properties we want, and behave as we want as a component in any protocol.

Formalizing qbits and cbits

One can model the transformation from the input system to the output system as a quantum channel.

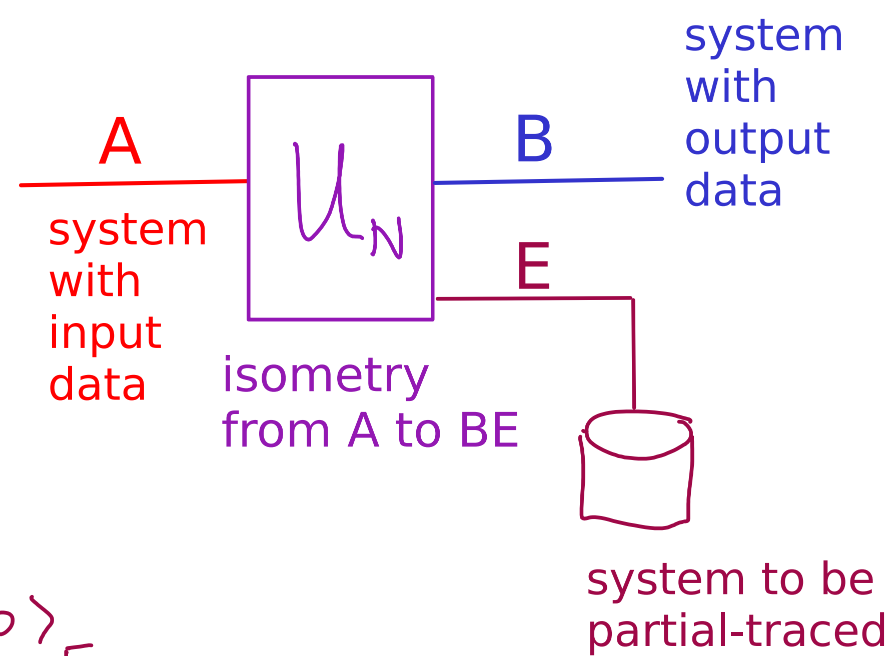
Recall that any quantum channel has a Stinespring dilation (also called the isometric extension or unitary representation):



Formalizing qbits and cbits

Let dim(A) = dim(B) = 2.

$\{|x\rangle\}_{x=0}^{1}$ basis for A,B.



qbit $\quad \forall x \quad |x\rangle_A \xrightarrow{U_N} |x\rangle_B |0\rangle_E$

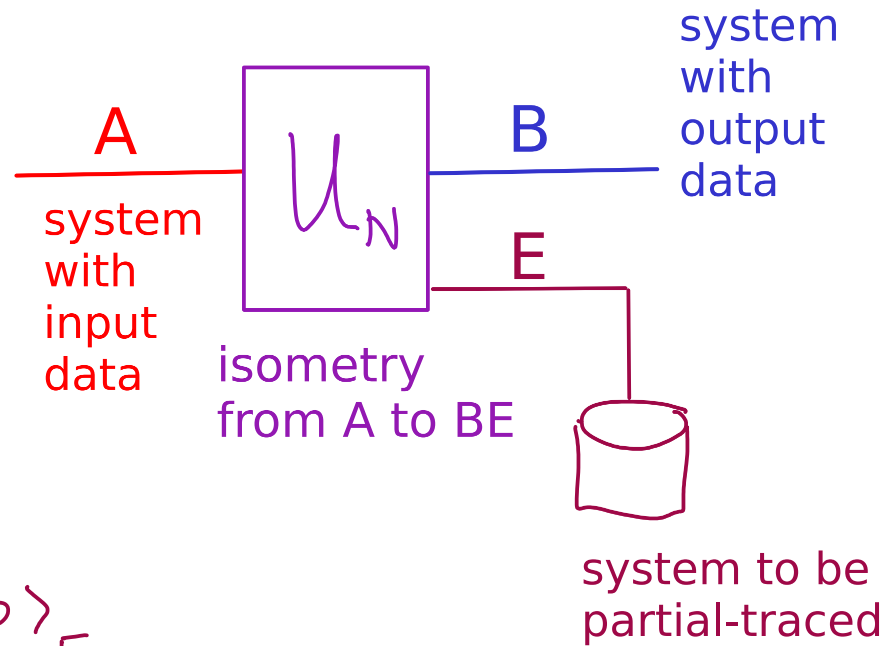
or $\quad \forall \rho \in B(A) \quad N(\rho) = \rho$

set of all bounded operators on A

Formalizing qbits and cbits

Let dim(A) = dim(B) = 2.

$\{|x\rangle\}_{x=0}^{1}$ basis for A,B.



qbit $\quad \forall x \quad |x\rangle_A \xrightarrow{U_N} |x\rangle_B |0\rangle_E$

cbit $\quad \forall x \quad |x\rangle_A \longrightarrow |x\rangle_B |x\rangle_E$

ie $N\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$

or $\quad \forall \rho \in B(A) \qquad N(\rho) =$ diag(ρ)

set of all bounded operators on A

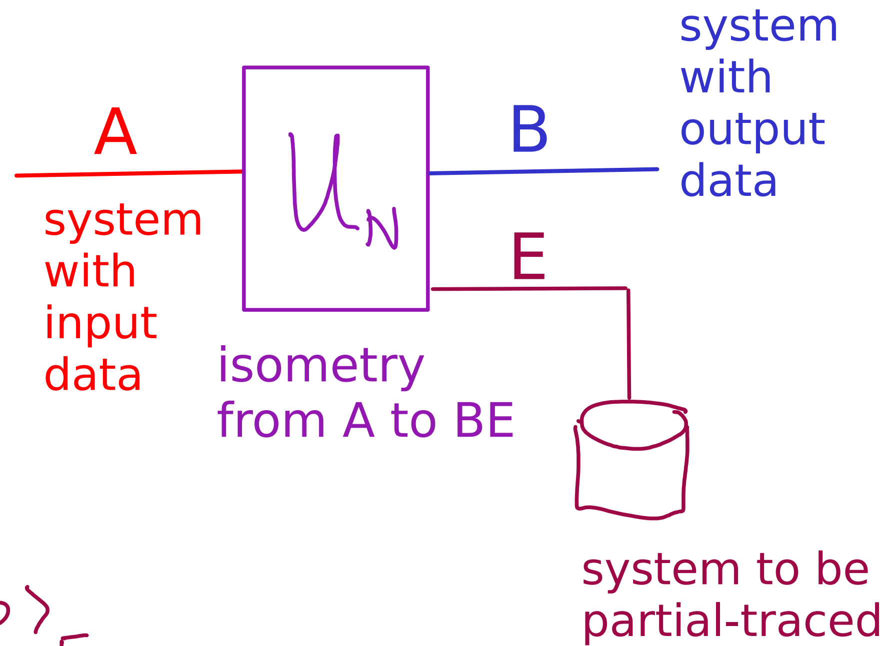
(Alice can also keep a copy of x in a cbit, or not)

(Crucial for Eve to have a copy that no one can take back -- def of being classical)

Formalizing qbits and cbits

Let dim(A) = dim(B) = 2.

$\{|x\rangle\}_{x=0}^{1}$ basis for A,B.



qbit $\quad \forall x \quad |x\rangle_A \xrightarrow{U_N} |x\rangle_B \, |0\rangle_E$

cbit $\quad \forall x \quad |x\rangle_A \longrightarrow |x\rangle_B \, |x\rangle_E$

Harrow 03

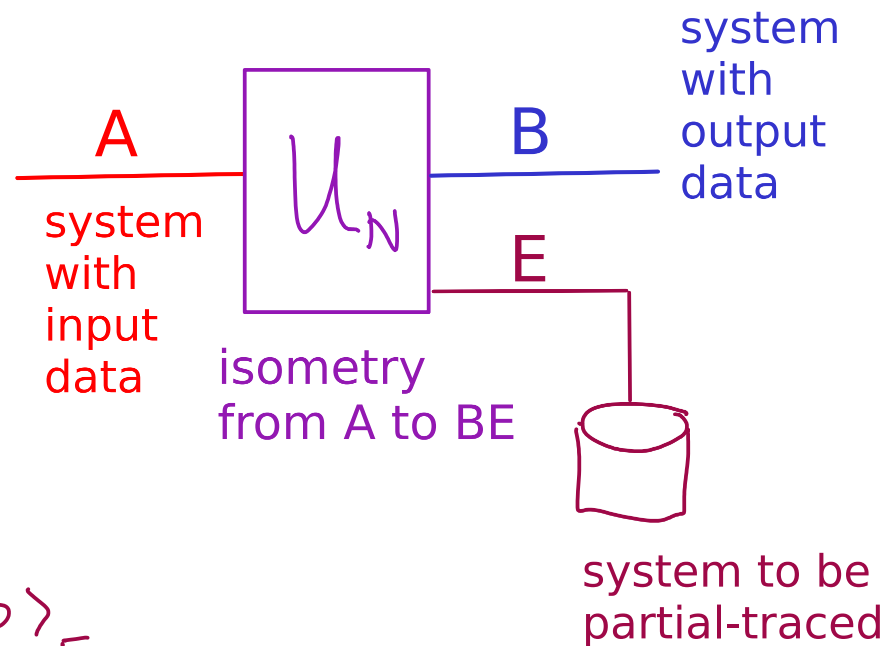
cobit $\quad \forall x \quad |x\rangle_A \longrightarrow |x\rangle_B \, |x\rangle_{A'} \, |0\rangle_E$

coherent classical communication
(no info lost to Eve, but the "x" must be shared between Alice and Bob)

Formalizing qbits and cbits

Let dim(A) = dim(B) = 2.

$\{|x\rangle\}_{x=0}^{1}$ basis for A,B.



$$\text{qbit} \quad \forall x \quad |x\rangle_A \xrightarrow{\mathcal{U}_N} |x\rangle_B |0\rangle_E$$

$$\text{cbit} \quad \forall x \quad |x\rangle_A \longrightarrow |x\rangle_B |x\rangle_E$$

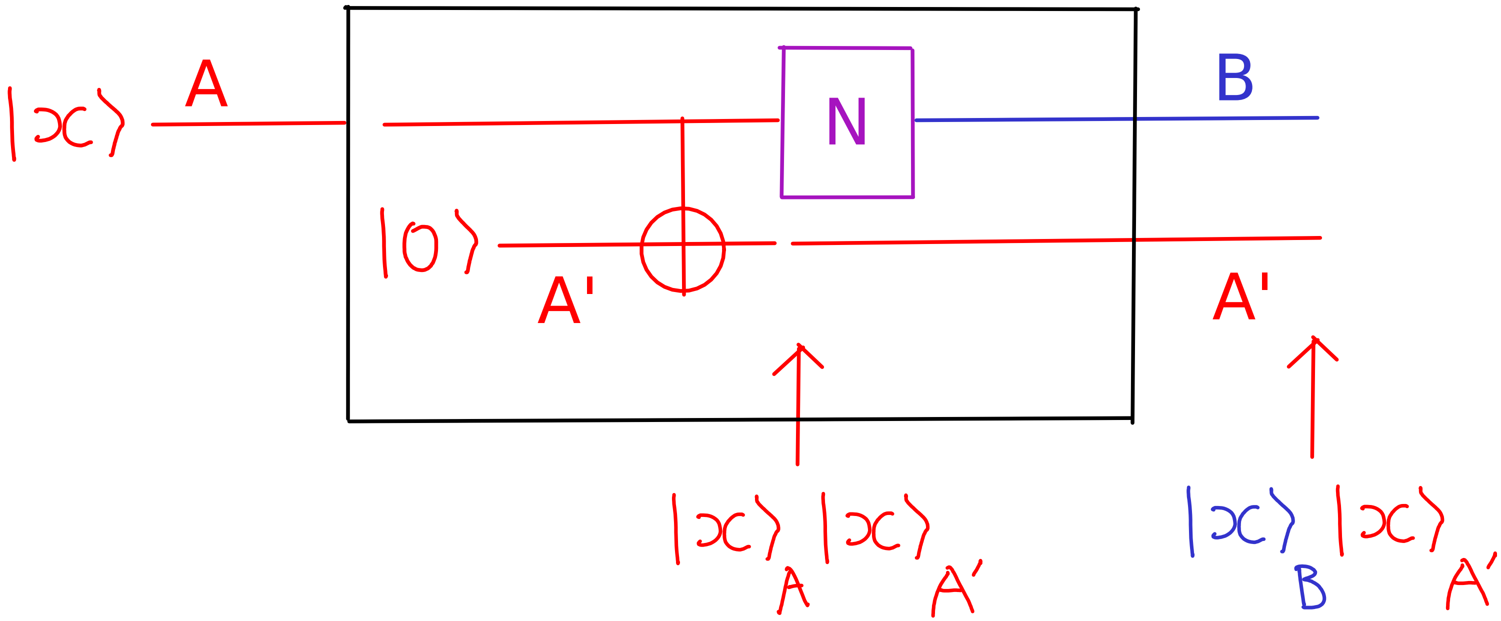
$$\text{cobit} \quad \forall x \quad |x\rangle_A \longrightarrow |x\rangle_B |x\rangle_{A'} |0\rangle_E$$

Ex: show that (i) qbit $\geq$ cobit $\geq$ cbit

(ii) cobit $\geq$ ebit

e.g., How to convert 1 qbit into 1 cobit?
In particular, how to get an additional output sys A' ?

Ans: local operations are allowed. Before applying the channel, Alice "makes a copy" of A onto A' "coherently"



and if input at A is in superposition
the state on AA' is in superposition

and final state on BA' in superposition

Composable communication:

Let Λ be a communication resource (e.g., qbit or cbit).

Let Π be a protocol approximately creating the resource (same input and output space).

If $\| \Lambda - \Pi \|_{\diamond} \leq \varepsilon$

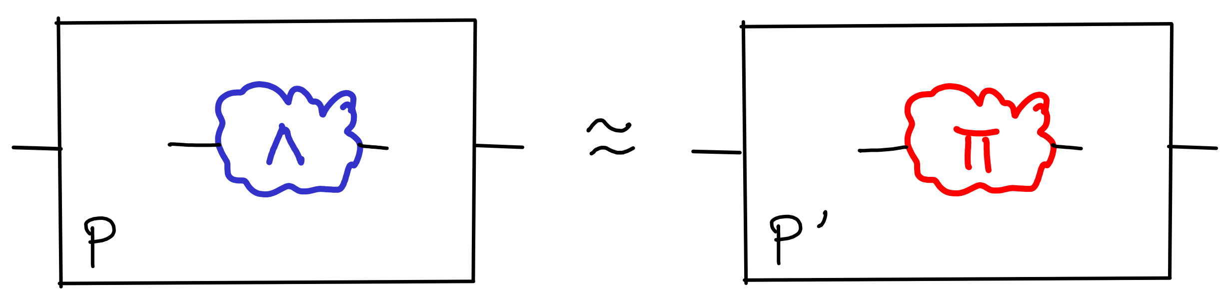
then, we have the following desirable composable property:

Let P be any protocol consuming Λ as a resource.
Replace Λ by Π in P, and call the resulting protocol P'.

Then, $\| P - P' \|_{\diamond} \leq \varepsilon$.

NB, Λ, Π, P, P' all TCP maps

ie $\Lambda \approx \Pi \Rightarrow$



Why?

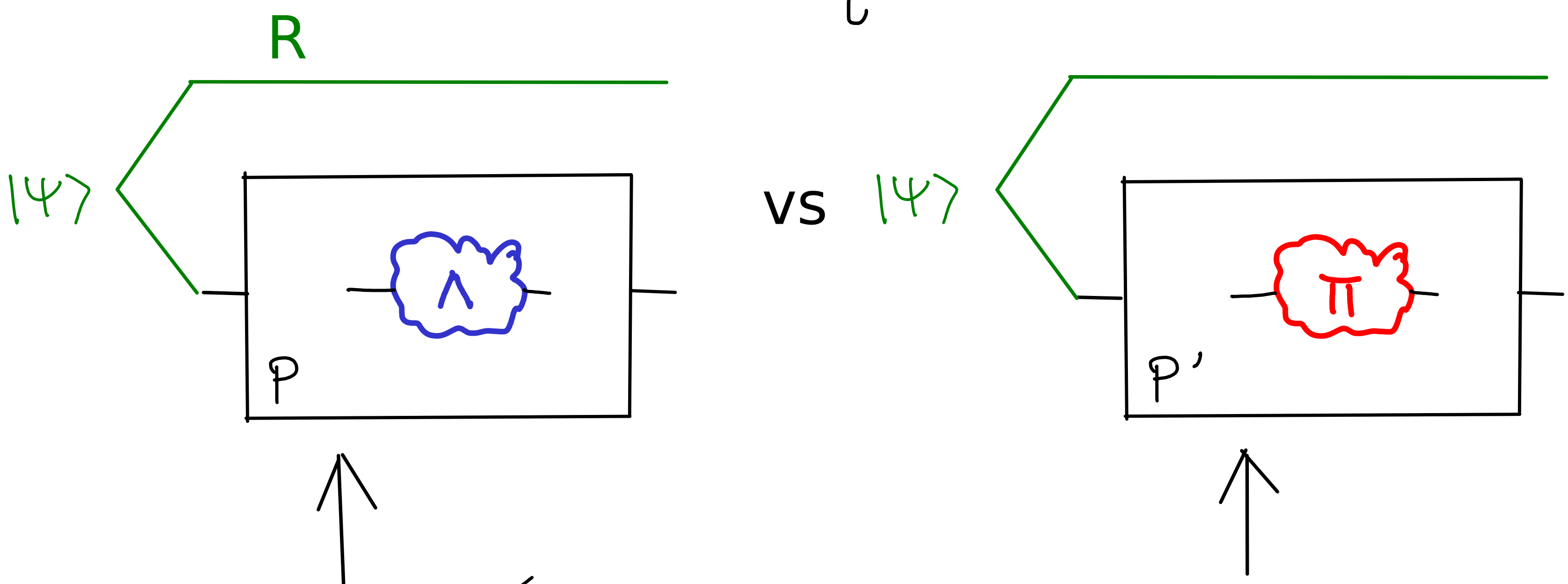
Proof sketch for composability of resources with approximation in diamond norm:

(1)
$$\| P - P' \|_\diamond = \max_{|\psi\rangle_{RS}} \| I \otimes P (|\psi\rangle\langle\psi|) - I \otimes P' (|\psi\rangle\langle\psi|) \|_t$$

input S, output T

same input + reference for both P, P'

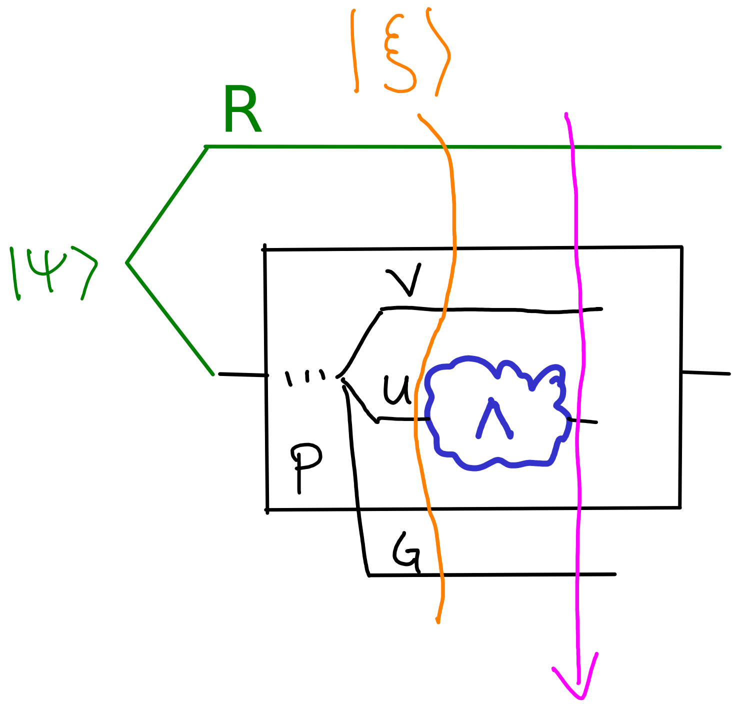
$\|\ \|_t$: difference between the outputs



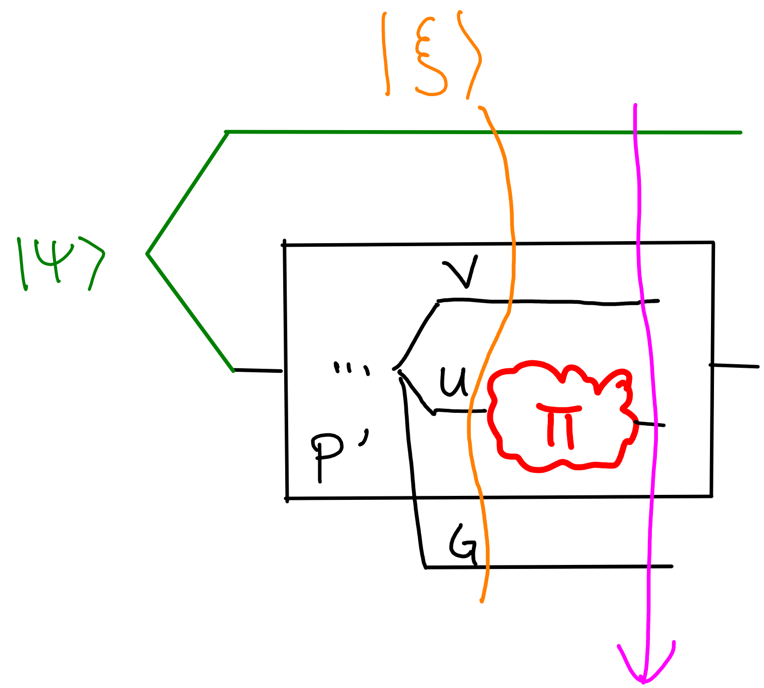
(2) same global state σ_{RW} right before Λ in P & before Π in P'

NB W includes input to Λ, Π. Let W = U V, U: input to Λ, Π

(3) Purify $\sigma_{RW} = \sigma_{RVU}$ and obtain $|\xi\rangle_{GRVU}$.



vs



$I_{RVG} \otimes \Lambda_U(|\xi\rangle\langle\xi|)$ $\qquad$ $I_{RVG} \otimes \Pi_U(|\xi\rangle\langle\xi|)$

(4) The subsequent operations of of P, P' are identical.

(5) $$\left\| I_{RVG} \otimes \Lambda_U(|\xi\rangle\langle\xi|) - I_{RVG} \otimes \Pi_U(|\xi\rangle\langle\xi|) \right\|_t$$

$$\geq \left\| I \otimes P(|\psi\rangle\langle\psi|) - I \otimes P'(|\psi\rangle\langle\psi|) \right\|_t$$

why? because

$$I_{RVG} \otimes \Lambda_u(|\xi\rangle\langle\xi|) \xrightarrow{\text{same op}} I \otimes P(|\psi\rangle\langle\psi|)$$

$$I_{RVG} \otimes \Pi_u(|\xi\rangle\langle\xi|) \longrightarrow I \otimes P'(|\psi\rangle\langle\psi|)$$

and trace distance is monotonic decreasing if the same operation is applied to the two states to be compared (cf Watrous lectures, or absorb the operation as the distinguishing measurement of the pre-operation state)

6 Since $\|\Lambda - \Pi\|_\diamond \leq \varepsilon$,

$$\| I_{RVG} \otimes \Lambda_u(|\xi\rangle\langle\xi|) - I_{RVG} \otimes \Pi_u(|\xi\rangle\langle\xi|) \|_t \leq \varepsilon$$

7 Combining the conclusions of (6) & (7) proves the claim.

Final remarks: composable resources are strong resources. They are harder to create, but are very useful if given. They're simpler to consider.

We will see both composable resources, and weaker form of communication in this course (the latter are easlier to obtain, but are less useful) so these tends to be "end goals" of our quantum information processing tasks. They are often more specific and awkward to define ...