

Lecture 8

①

Unit quantum protocols. Let us now consider three ^(or four!) noiseless protocols that illustrate several of the important concepts of QIT:

- ① Resource inequalities.
- ② Interconversion of resources
- ③ Rate regions and tradeoffs.

These protocols are also building blocks that we will draw on later in the course. These are called unit protocols, because they interchange discrete units of our resources—these are like “atoms” of QIT.

- I. Entanglement distribution.
- II. Elementary coding.
- III. Superdense coding.
- IV. Q teleportation.

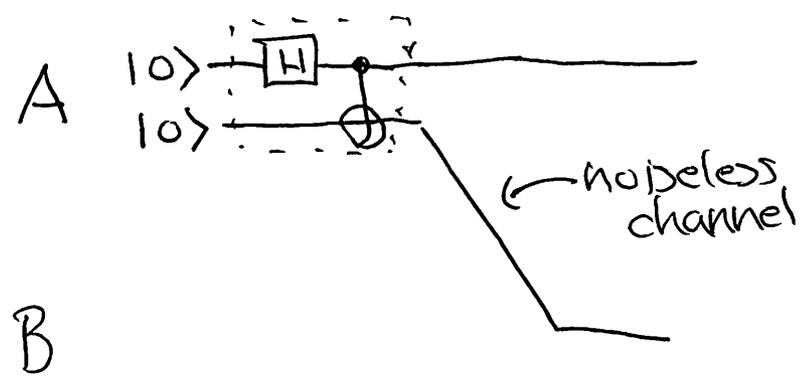
The unit resources involved in these protocols are:

- shared entanglement $[qq]$
- noiseless qubit channel $[q \rightarrow q]$
- noiseless bit channel $[c \rightarrow c]$

I. Entanglement distribution.

②

This protocol is quite elementary. To create a shared ebit between Alice & Bob, Alice can prepare an EPR pair locally and send half of it to Bob:



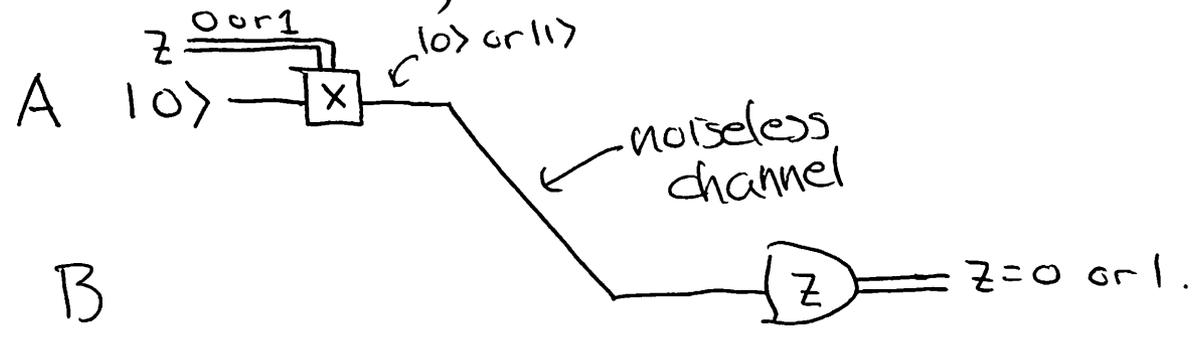
The output is $|\Phi_+\rangle^{AB}$.

The resource inequality is $[q \rightarrow q] \geq [qq]$.
 (Note, this is not true the other way around!)

II. Elementary coding.

A qubit channel can be used to send a classical bit. The 2 bit values, 0 or 1, can be encoded as 2 orthogonal qubit states:

$$0 \rightarrow |0\rangle, \quad 1 \rightarrow |1\rangle.$$



$$[q \rightarrow q] \geq [c \rightarrow c]$$

Again, the reverse is not true.

III. Superdense coding. ③

Remember that we can interconvert among the 4 Bell states by acting on just one of the 2 qubits:

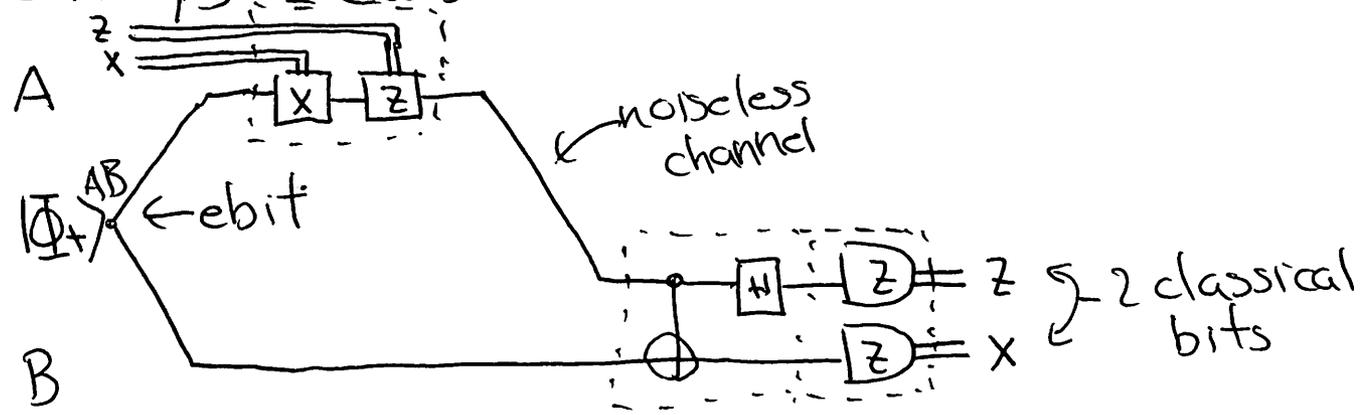
$$(I \otimes I) |\Phi_+\rangle = |\Phi_+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

$$(X \otimes I) |\Phi_+\rangle = |\Psi_+\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$$

$$(Z \otimes I) |\Phi_+\rangle = |\Phi_-\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$$

$$(ZX \otimes I) |\Phi_+\rangle = |\Psi_-\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$$

Because these 4 states are orthogonal, they can be reliably distinguished by measurements. Distinguishing 4 possibilities conveys 2 classical bits of info.



$$[q \rightarrow q] + [qq] \geq 2 [c \rightarrow c]$$

So even though entanglement by itself cannot produce communication, it can enhance communication.

IV. Q teleportation.

(4)

This is by far the most subtle of the four elementary protocols. We can see it by considering the following state:

$$|\psi\rangle^A |\Phi_+\rangle^{A'B} \leftarrow \begin{array}{l} 2 \text{ qubits on A's side,} \\ 1 \text{ " on B's " .} \end{array}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \leftarrow \text{arbitrary state.}$$

$$\begin{aligned} |\psi\rangle^A |\Phi_+\rangle^{A'B} &= \frac{\alpha}{\sqrt{2}} (|000\rangle^{AA'B} + |011\rangle^{AA'B}) \\ &+ \frac{\beta}{\sqrt{2}} (|100\rangle^{AA'B} + |111\rangle^{AA'B}). \end{aligned}$$

Now let's rewrite Alice's 2 qubits in the

Bell basis: $|00\rangle = \frac{1}{\sqrt{2}} (|\Phi_+\rangle + |\Phi_-\rangle)$

$$|11\rangle = \frac{1}{\sqrt{2}} (|\Phi_+\rangle - |\Phi_-\rangle)$$

$$|01\rangle = \frac{1}{\sqrt{2}} (|\Psi_+\rangle + |\Psi_-\rangle)$$

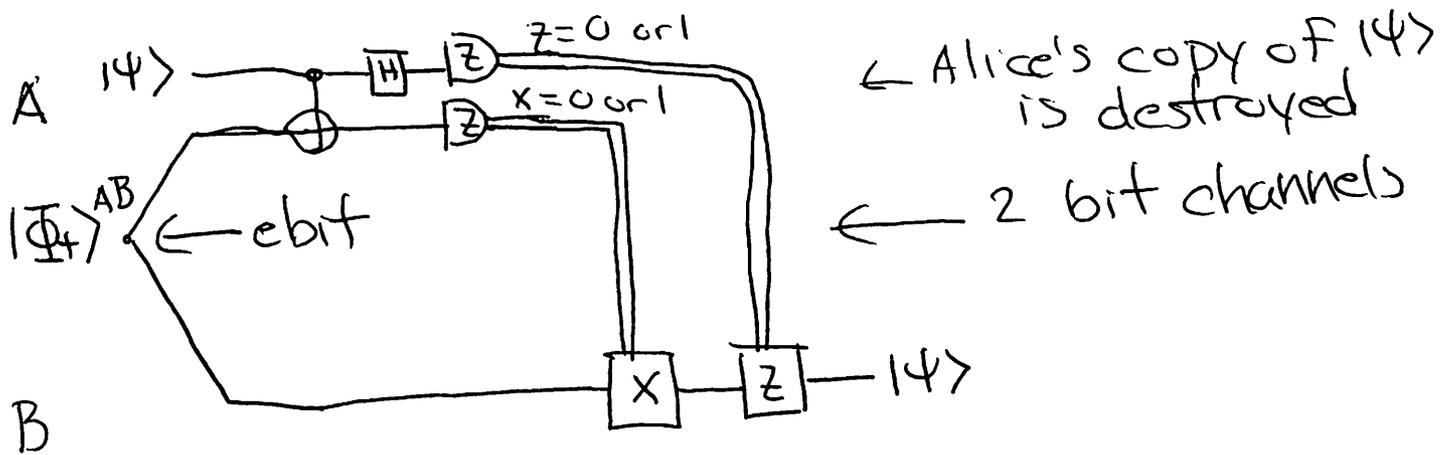
$$|10\rangle = \frac{1}{\sqrt{2}} (|\Psi_+\rangle - |\Psi_-\rangle)$$

$$\begin{aligned} \Rightarrow |\psi\rangle^A |\Phi_+\rangle^{A'B} &= \frac{1}{2} \left[|\Phi_+\rangle^{AA'} (\alpha|0\rangle + \beta|1\rangle)^B \right. \\ &+ |\Psi_+\rangle^{AA'} (\alpha|1\rangle + \beta|0\rangle)^B + |\Phi_-\rangle^{AA'} (\alpha|0\rangle - \beta|1\rangle)^B \\ &\left. + |\Psi_-\rangle^{AA'} (\alpha|1\rangle - \beta|0\rangle)^B \right] \end{aligned}$$

This was just algebra—nothing has been done! ⑤
 But if Alice measures A & A' in the Bell basis, we see that

- ① The 4 outcomes are all equally likely, and
- ② Bob's qubit is left in one of 4 possible states: $|\psi\rangle$, $X|\psi\rangle$, $Z|\psi\rangle$, or $XZ|\psi\rangle$.

If Bob knows the measurement outcome, he can apply one of 4 unitaries to recover $|\psi\rangle$. And note: this protocol works even if A & B do not know what $|\psi\rangle$ is! This is an oblivious protocol.



$$[qq] + 2[c \rightarrow e] \geq [q \rightarrow q].$$

Private resources

For cryptographic applications we sometimes want to ensure that information transmitted and/or shared is private—i.e., secret from any eavesdroppers. For this reason we sometimes want to define private versions of resources:

$[cc]_{\text{priv}} = \text{shared random secret bit (key bit)}$ ⑥

$[c \rightarrow c]_{\text{priv}} = \text{private bit channel}$

Note that

$$[cc]_{\text{priv}} \geq [cc]$$

$$[c \rightarrow c]_{\text{priv}} \geq [c \rightarrow c]$$

One-time pad:

$$[c \rightarrow c] + [cc]_{\text{priv}} \geq [c \rightarrow c]_{\text{priv}}$$

A bit like teleportation!

but not the other way around.

Also, $[c \rightarrow c]_{\text{priv}} \geq [cc]_{\text{priv}}$, but

$[c \rightarrow c] \not\geq [cc]_{\text{priv}} \leftarrow \text{can't share secret keys through a public channel.}$

Quantum protocols can be used to produce private classical resources:

$$[qq] \geq [cc]_{\text{priv}} \leftarrow \text{secret key generation}$$

$$[qq] + [q \rightarrow q] \geq 2[c \rightarrow c]_{\text{priv}} \leftarrow \text{superdense coding.}$$

Next time we will see that by combining these unit protocols, we can achieve all noiseless resource conversions, by showing that the achievable rate regions correspond to "time sharing" these unit protocols.