Communication protocols

Quantum communication

G. Chênevert

October 2, 2020

Communication protocols

Review of formalism

Superdense coding

Quantum teleportation

Recall: qubit states

Quantum states of a 2-level quantum system (*qubit*):

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \in \mathcal{H}, \qquad \alpha, \beta \in \mathbb{C}.$$

Hermitian product: if $\quad |\psi\rangle = \delta\,|0\rangle + \varepsilon\,|1\rangle$,

$$\begin{aligned} \langle \phi \,|\, \psi \rangle &= \alpha^* \delta + \beta^* \varepsilon \\ &= [\,\alpha \;\; \beta\,]^* \begin{bmatrix} \delta \\ \varepsilon \end{bmatrix} \\ &= |\phi\rangle^\dagger |\psi\rangle \end{aligned}$$

Measurement

When $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ is measured:

$|\phi\rangle$ projects to a (random) classical state $\mathcal{M}|\phi\rangle \in \{|0\rangle, |1\rangle\}$ with

$$\mathbb{P}\big[\,\mathcal{M}|\phi\rangle = |0\rangle\,\big] = \frac{|\alpha|^2}{|\alpha|^2 + |\beta|^2}, \qquad \mathbb{P}\big[\,\mathcal{M}|\phi\rangle = |1\rangle\,\big] = \frac{|\beta|^2}{|\alpha|^2 + |\beta|^2}.$$

In particular: if $|\phi\rangle$ is *normalized*, this reduces to

$$\mathbb{P}\big[\,\mathcal{M}|\phi\rangle = |0\rangle\,\big] = |\alpha|^2, \qquad \mathbb{P}\big[\,\mathcal{M}|\phi\rangle = |1\rangle\,\big] = |\beta|^2.$$

More generally

$|\phi\rangle$ can be measured with respect to any orthonormal basis $|\varphi_1\rangle$, $|\varphi_2\rangle$

$$|\phi\rangle = \langle \varphi_1 \mid \phi \rangle \, |\varphi_1\rangle + \langle \varphi_2 \mid \phi \rangle \, |\varphi_2\rangle$$

$$\implies \mathbb{P}\big[\, \mathcal{M}|\phi\rangle = |\varphi_i\rangle \,\big] = |\langle \varphi_i \mid \phi \rangle|^2$$

Example:

$$|\phi^+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |\phi^-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \qquad \text{orthonormal basis}$$

2-qubit system

Orthonormal basis of the 4-dimensional space $\mathcal{H} \otimes \mathcal{H}$:

$$|0\rangle \otimes |0\rangle, \quad |0\rangle \otimes |1\rangle, \quad |1\rangle \otimes |0\rangle, \quad |1\rangle \otimes |1\rangle$$

But also the 4 Bell states:

$$|\Phi^+\rangle = \frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{\sqrt{2}}, \qquad |\Phi^-\rangle = \frac{|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle}{\sqrt{2}}$$

$$|\Psi^+\rangle = \frac{|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle}{\sqrt{2}}, \qquad |\Psi^-\rangle = \frac{|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle}{\sqrt{2}}$$

Entanglement

Recall that a state $|\Psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ is *entangled* if it cannot be written as a simple combination of two single qubit states:

$$\nexists_{|\varphi\rangle, |\psi\rangle \in \mathcal{H}} \quad |\Psi\rangle = |\varphi\rangle \otimes |\psi\rangle .$$

Exercise: is the following state entangled?

$$\frac{1}{2}\big(|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle\big)$$

No-cloning theorem

Theorem: *Quantum information cannot be copied.*

Precise statement: there exist no unitary operator $C : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ such that

$$\forall_{|\phi\rangle \in \mathcal{H}} \quad C|\phi\rangle = |\phi\rangle \otimes |\phi\rangle.$$

...of course! But even if you start with a blank qubit:

there is no unitary operator $C : \mathcal{H} \otimes \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ such that

$$\forall_{|\phi\rangle \in \mathcal{H}} \quad C(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle.$$

Reason

Suppose

$$\begin{cases} C(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle \\ C(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle \end{cases}$$

Then what is

$$C\big((|0\rangle + |1\rangle) \otimes |0\rangle\big) \ ?$$

A cloning operator cannot respect superposition of quantum states.

Communication protocols

Review of formalism

Superdense coding

Quantum teleportation

Superdense coding

- Bennett & Weisner (1992)
- **Two** classical bits can be transmitted on **one** quantum bit
- An entangled pair is used (and needed)
- A form of secure quantum communication
- Experimentally tested in various settings

Superdense coding: the protocol

Alice has two classical bits b_1 and b_2 that she wants to send to Bob.

$b_1 b_2$

Superdense coding: the protocol

1) Preparation (can be done in advance)

Charlie prepares an entangled pair of qubits in Bell state

$$|\Phi^+\rangle = \frac{|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B}{\sqrt{2}}.$$

2) Sharing (can be done in advance)

Charlie sends qubit A to Alice, qubit B to Bob.

Superdense coding: the protocol

3) Encoding

Alice modifies her qubit according to the two classical bits $b_1 b_2$ she wants to encode:

- if $b_1 b_2 = 00$ she does nothing, i.e. applies $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ to A

$$|\Phi^+\rangle = \frac{|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B}{\sqrt{2}}$$

Superdense coding: the protocol

- if $b_1 b_2 = 01$ she flips the phase of her qubit, i.e. applies $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ to A

$$|\Phi^-\rangle = \frac{|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B}{\sqrt{2}}$$

- if $b_1 b_2 = 10$ she negates her qubit, i.e. applies $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ to A

$$|\Psi^+\rangle = \frac{|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B}{\sqrt{2}}$$

- if $b_1 b_2 = 11$ she applies both X and Z (order doesn't really matter: why?)

$$|\Psi^-\rangle = \frac{|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B}{\sqrt{2}}$$

Superdense coding: the protocol

Summary of encoding: $b_1 b_2$ encoded as $Z^{b_2} X^{b_1} |\Phi^+\rangle$

$00 \mapsto |\Phi^+\rangle$

$01 \mapsto |\Phi^-\rangle$

$10 \mapsto |\Psi^+\rangle$

$11 \mapsto |\Psi^-\rangle$

Superdense coding: the protocol

4) Sending

Alice sends her qubit to Bob through a quantum channel; now Bob has the full entangled pair.

5) Decoding

Making a measurement in the orthonormal basis $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$ Bob is able to recover the initial pair of bits.

Superdense coding: the protocol

Reformulation: let T denote the unitary transformation for which

$$|0\rangle \otimes |0\rangle \mapsto |\Phi^+\rangle, \qquad |0\rangle \otimes |1\rangle \mapsto |\Phi^-\rangle, \qquad |1\rangle \otimes |0\rangle \mapsto |\Psi^+\rangle, \qquad |1\rangle \otimes |1\rangle \mapsto |\Psi^-\rangle$$

$$T = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 \end{bmatrix}$$

Then Bob can just perform $T^\dagger$ on the qubit pair to recover $|b_1\rangle \otimes |b_2\rangle$.

Superdense coding: discussion

- A compression factor of 2 can be achieved... (at a cost!)
- EPR pairs can be used to "store bandwidth" for future use
- If Eve measures Alice's qubit in transit: she will randomly get $|0\rangle$ or $|1\rangle$ no matter what the transmitted bits were
- Unfortunately Bob would then receive either a

$$|0\rangle \otimes |0\rangle, \quad |1\rangle \otimes |1\rangle, \quad |0\rangle \otimes |1\rangle \quad \text{or} \quad |1\rangle \otimes |0\rangle :$$

  b_1 survives but b_2 is lost (gets random output)

Communication protocols

Review of formalism

Superdense coding

Quantum teleportation

Quantum teleportation

Quantum teleportation

Quantum teleportation

- Bennett, Brassard, Crépeau, Jozsa, Peres, Wooters (1993)
- In superdense coding: 2 classical bits are sent using 1 quantum bit
- Quantum teleportation can be thought of as the reverse:

  1 quantum bit is sent using 2 classical bits of information
- No quantum system is physically transported: only its *state* is
- So: quantum information can be sent through a classical channel...

  provided both parties share an entangled pair.

Quantum teleportation: the protocol

Alice has a qubit in state $|\phi\rangle_A = \alpha\,|0\rangle_A + \beta\,|1\rangle_A$ that she wants to send to Bob.

1) Preparation (can be done in advance)

Charlie prepares an entangled pair of qubits in Bell state

$$|\Phi^+\rangle = \frac{|0\rangle_C \otimes |0\rangle_B + |1\rangle_C \otimes |1\rangle_B}{\sqrt{2}}.$$

Superdense coding: the protocol

2) Sharing (can be done in advance)

Charlie gives qubit C to Alice, qubit B to Bob.

Now Alice has two qubits A and C, Bob has qubit B; total state of the system is

$$|\phi\rangle_A \otimes |\Phi^+\rangle_{CB} = \frac{\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle}{\sqrt{2}}.$$

Superdense coding: the protocol

3) Measurement

Alice measures her two qubits in the Bell basis; the system degenerates equiprobably into one of the 4 states:

$$|\Phi^+\rangle_{AC} \otimes (\alpha\,|0\rangle_B + \beta\,|1\rangle_B), \qquad |\Phi^-\rangle_{AC} \otimes (\alpha\,|0\rangle_B - \beta\,|1\rangle_B)$$

$$|\Psi^+\rangle_{AC} \otimes (\alpha\,|1\rangle_B + \beta\,|0\rangle_B), \qquad |\Psi^-\rangle_{AC} \otimes (\alpha\,|1\rangle_B - \beta\,|0\rangle_B)$$

Quantum teleportation: the protocol

4) Communication

Alice tells Bob which of the 4 Bell states she measured using some (classical) binary encoding, *e.g.*

$$|\Phi^+\rangle_{AC} \mapsto 00 \qquad |\Psi^+\rangle_{AC} \mapsto 10$$

$$|\Phi^-\rangle_{AC} \mapsto 01 \qquad |\Psi^-\rangle_{AC} \mapsto 11$$

Quantum teleportation: the protocol

5) Correction

Bob is now able to correct his qubit in order to recover the initial quantum state $|\phi\rangle$:

- if 00 is received: $|\Phi^+\rangle_{AC} \otimes (\alpha |0\rangle_B + \beta |1\rangle_B)$, nothing to do
- if 01 is received: $|\Phi^-\rangle_{AC} \otimes (\alpha |0\rangle_B - \beta |1\rangle_B)$ he applies Z
- if 10 is received: $|\Psi^+\rangle_{AC} \otimes (\alpha |1\rangle_B + \beta |0\rangle_B)$ he applies X
- if 11 is received: $|\Psi^-\rangle_{AC} \otimes (\alpha |1\rangle_B - \beta |0\rangle_B)$ he applies $Y := ZX$.

Quantum teleportation: discussion

- No violation of the no-cloning theorem: A is not in state $|\phi\rangle$ anymore!
- Intercepting either half of the entangled pair or the classical bits does not give any information about $|\phi\rangle$
- Summary: entangled pair + 1 qubit = entangled pair + 2 bits
- Entanglement swapping: if Alice shares an entangled pair with Bob, he can teleport his qubit to Carol so that now Alice and Carol share an entangled pair
- 1400 km teleportation achieved with the Chinese Micius satellite (2017)