Communication protocols

Quantum communication

G. Chênevert

September 2019

ISEN
ALL IS DIGITAL!
LILLE

yncréa

Communication protocols

Warm-up

Superdense coding

Quantum teleportation

Quantum cryptography

Recall

Consider an arbitrary state for a 2-level quantum system (qubit):

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \qquad \alpha, \beta \in \mathbb{C}, \qquad |\alpha|^2 + |\beta|^2 = 1.$$

When measured: $|\phi\rangle$ projects to a (random) classical state $\mathcal{M}|\phi\rangle$ with

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

Recall

Since $|0\rangle$ and $|1\rangle$ form an orthonormal base for the hermitian product:

$$\alpha = \langle 0|\phi\rangle \qquad \text{and} \qquad \beta = \langle 1|\phi\rangle.$$

Same reasoning applies to any other orthonormal basis.

Example

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

Compute

$$\mathbb{P}\big[\,\mathcal{M}|0\rangle = |\phi^+\rangle\,\big], \qquad \mathbb{P}\big[\,\mathcal{M}|0\rangle = |\phi^-\rangle\,\big].$$

Many ways to do it! Change of basis matrix may be useful...

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

2 qubits

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:

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

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

Exercise

Consider the 2-qubit state

$$|\phi\rangle = 0.48\,|0\rangle \otimes |0\rangle - 0.36\,|0\rangle \otimes |1\rangle + 0.64i\,|1\rangle \otimes |0\rangle - 0.48i\,|1\rangle \otimes |1\rangle.$$

a) Alice measures the first qubit. What is the probability she gets $|1\rangle$?

Answer: 64%

b) Bob then measures the second qubit. What is the probability he gets $|1\rangle$?

Answer: 36%

c) Is this state entangled ?

Answer: no ! it can be written as $(0.6\,|0\rangle + 0.8i\,|1\rangle) \otimes (0.8\,|0\rangle - 0.6\,|1\rangle)$

Exercise

Now Alice and Bob measure $|\phi\rangle$ in the Bell basis. What do they see?

Answer:

$$|\Phi^+\rangle : 23.04\%$$

$$|\Phi^-\rangle : 23.04\%$$

$$|\Psi^+\rangle : 26.96\%$$

$$|\Psi^-\rangle : 26.96\%$$

Reformulation

Apply

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix}$$

then measure in the $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ basis !

Communication protocols

Warm-up

Superdense coding

Quantum teleportation

Quantum cryptography

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 $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 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 $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 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 $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 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 operations X and Z (order doesn't 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

Encoding: summary

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

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

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

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

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 (hermitian) transformation for which

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

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

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

Superdense coding: discussion

- A compression factor of 2 can be achieved... (at a cost!)
- Could 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

Warm-up

Superdense coding

Quantum teleportation

Quantum cryptography

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 $|\phi\rangle_C = \alpha\,|0\rangle_C + \beta\,|1\rangle_C$ that she wants to send to Bob.

1) Preparation (can be done in advance)

Charlie prepares an entangled pair of qubits in Bell state

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

Superdense coding: the protocol

2) Sharing (can be done in advance)

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

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

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

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:

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

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

Quantum teleportation: the protocol

4) Communication

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

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

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

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

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)

Communication protocols

Warm-up

Superdense coding

Quantum teleportation

Quantum cryptography

Quantum key distribution (QKD)

Allows Alice and Bob to agree on a secret key

(that they will use for classical symmetric encryption, *e.g.* 128 bits for AES)

Two main protocols:

- **BB84** – Bennett & Brassard (1984)

  based on quantum superposition

- **E91** – Ekert (1991)

  based on entanglement

BB84: Idea

Prepare and measure qubits (photons) in two conjugate orthogonal bases,

e.g. **rectilinear**:

$$|+\rangle_0 = |H\rangle, \qquad |+\rangle_1 = |V\rangle$$

and **diagonal**:

$$|\times\rangle_0 = |D\rangle, \qquad |\times\rangle_1 = |A\rangle.$$

BB84: Basic step

- Alice randomly chooses a preparation basis $\mathcal{A} \in \{+, \times\}$ and a bit $a \in \{0, 1\}$.
- Alice prepares a qubit in state $|\mathcal{A}\rangle_a$ and sends it to Bob on a quantum channel.

- Bob randomly chooses a measurement basis $\mathcal{B} \in \{+, \times\}$ and measures the qubit :

$$b = \mathcal{M}_{\mathcal{B}} |\mathcal{A}\rangle_a.$$

BB84: Basic step

- Alice and Bob tell each other (over a classical channel) which bases $\mathcal{A}$ and $\mathcal{B}$ they chose.
- If $\mathcal{A} = \mathcal{B}$: they now share the common, secret value of $a = b$
- If $\mathcal{A} \neq \mathcal{B}$: they throw a and b away and start again.

On average, a new shared secret bit is obtained every 2 such exchanges.

BB84: Example

Alice randomly picks $\mathcal{A} = \times$ and $a = 0$.

She thus sends a $|\times\rangle_0 = |D\rangle$ photon to Bob.

- First case: Bob by chance chooses the same basis $\mathcal{B} = \times$. Measuring the received $|D\rangle$ in the diagonal basis, he gets (with probability 1) $|D\rangle = |\times\rangle_0$ thus finds $b = 0$.
- Second case: Bob unfortunately chooses the "wrong" basis $\mathcal{B} = +$. Measuring the received $|D\rangle$ in the rectilinear basis, he gets $|+\rangle_0 = |H\rangle$ or $|+\rangle_1 = |V\rangle$ with 50% probability each: the information about Alice's bit a is lost.

BB84: Security

No such thing as a passive attacker on a quantum channel! Necessarily "ActEve"

If she wants to learn something from the qubit in transit, she will:

- choose a measurement basis $\mathcal{E} \in \{+, \times\}$
- get $e = \mathcal{M}_{\mathcal{E}}|\mathcal{A}\rangle_a$ **leaving the qubit in state** $|\mathcal{E}\rangle_e$
- and Bob will in reality get $b = \mathcal{M}_{\mathcal{B}}|\mathcal{E}\rangle_e$.

BB84: Security

If Eve guesses correctly ($\mathbb{P} = \frac{1}{2}$): Alice and Bob have no way to know!

But when she picks the wrong basis: there is 50 % chance that $a \neq b$

So if Alice and Bob tell a and b to each other, they have $\frac{1}{4}$ chance of detecting Eve.

. . . but they just made their secret bits public

BB84: Security

Solution: exchange more bits than needed.

If Alice and Bob dislose the results of m successful exchanges, the probability that Eve goes undetected is $\left(\frac{3}{4}\right)^m \longrightarrow 0$ as $m \to \infty$.

With enough security bits, Eve will be detected with high probability.

Exercise

How many photons would Alice and Bob need to exchange on average if they want to establish a private 128-bit key with negligible ($< \frac{1}{2^{128}}$) probability that an eavesdropper would go undetected?

Answer: 874