Lecture 12: Superdense Coding & Quantum Teleportation

Scribed by: Sebastian Bauer

Department of Mathematics, MIT

October 14, 2003

1 Superdense Coding & Quantum Teleportation

1.1 Repetition

1. EPR pair: $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$,
   which is in some sense (as we will soon see) equivalent to
2. $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Think of this EPR pair as shared between two people, Alice and Bob. Alice owns the first qubit, Bob the second.
Alice can change from 1) to 2) without Bob's help:

$$\begin{aligned} & \sigma_y(1) \cdot \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \qquad \left(\sigma_y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \right) && (1) \\ = \; & \frac{1}{\sqrt{2}}(i\,|11\rangle + i\,|00\rangle) && (2) \\ = \; & \frac{i}{\sqrt{2}}(|11\rangle + |00\rangle) && (3) \end{aligned}$$

Recall the Bell basis:

$$\begin{aligned} & & & \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) && (4) \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \quad \sigma_x(1) \cdot \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) & = & \frac{1}{\sqrt{2}}(|11\rangle - |00\rangle) && (5) \\ \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} & \quad \sigma_y(1) \cdot \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) & = & \frac{i}{\sqrt{2}}(|11\rangle + |00\rangle) && (6) \\ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & \quad \sigma_z(1) \cdot \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) & = & \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) && (7) \end{aligned}$$

Any pair of the Bell basis states has inner product 0, e.g.

$$\frac{1}{2}(\langle 01| - \langle 10|) \cdot (|01\rangle + |10\rangle) = \frac{1}{2}(\langle 01|01\rangle - \langle 10|01\rangle + \langle 01|10\rangle - \langle 10|10\rangle) = \frac{1}{2}(1 - 0 + 0 - 1) = 0$$

$\Rightarrow$ The 4 Bell states (4)-(7) constitute an orthonormal basis for the space of state for 2 qubits.

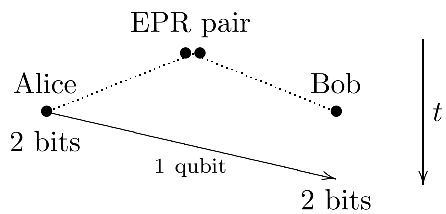
1.2 Superdense Coding

Theorem 1. *The amount of information extractable from one qubit is 1 bit.*

Theorem 2. *An EPR pair cannot carry any information.*

We won't prove these theorems now; perhaps in a later lecture.

So if Alice sends 1 qubit to Bob, can she only encode 1 bit of information?



Alice and Bob have shared an EPR pair in the past, and now Alice sends a qubit. This can transmit 2 bits of info.

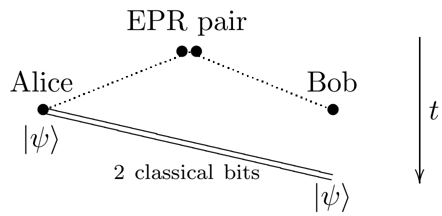
Explanation:

- Alice and Bob start with an EPR pair $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, where Alice owns the first and Bob the second qubit.
- Alice applies one of the operations $\{id, \sigma_x, \sigma_y, \sigma_z\}$ to her qubit and sends it to Bob. Thus she can create one of four orthogonal states, which corresponds to 2 classical bits of information.
- Bob can now measure the 2 qubits in the Bell basis and thereby learn which of the 4 operations Alice has used, hence what 2-bit information she wanted to transmit.

So it is not really a paradox, as 2 qubits contain 2 bits of information; but when discovered it was quite surprising.

Although it might look like we've found a way of superluminal communication, this is not possible: Bob cannot tell which operation Alice has performed on her half of the EPR pair by just measuring his half. He needs either Alice's qubit, or the information about the operation Alice performed, which would have to be transmitted to him classically, i.e. at maximum with the speed of light.

1.3 Quantum Teleportation



We have the same setup:

Alice and Bob have shared an EPR pair in the past. After receiving two classical bits, Bob can exactly reproduce Alice's qubit state $|\psi\rangle$.

This seems paradox at first sight, because $|\psi\rangle$ can be in any of the continuous states and therefore it contains in some sense an infinite amount of information, that could not possibly be transmitted in only two classical bits.

Explanation:

It works exactly like in superdense coding, except that Alice measures her half of the EPR pair and submits the result classically to Bob via 2 classical bits.

- Alice has a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- Alice and Bob share 2 qubits in state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. We use this state instead of the usual EPR state, as the Algebra becomes a little bit easier that way.
- The product state is $\frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) \otimes (|00\rangle + |11\rangle)$
- Alice measures her qubits in the Bell basis $\left\{\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)\right\}$ and gets

$$\begin{aligned}
&\frac{1}{2\sqrt{2}}\left[(\alpha|00\rangle + \alpha|11\rangle)|0\rangle + (\alpha|00\rangle - \alpha|11\rangle)|0\rangle + (\alpha|01\rangle + \alpha|10\rangle)|1\rangle + (\alpha|01\rangle - \alpha|10\rangle)|1\rangle\right.\\
&\quad\left. + (\beta|10\rangle + \beta|01\rangle)|0\rangle + (\beta|10\rangle - \beta|01\rangle)|0\rangle + (\beta|11\rangle + \beta|00\rangle)|1\rangle + (\beta|11\rangle - \beta|00\rangle)|1\rangle\right]\\
= &\frac{1}{2\sqrt{2}}\left[(|00\rangle + |11\rangle)(\alpha|0\rangle + \beta|1\rangle) + (|00\rangle - |11\rangle)(\alpha|0\rangle - \beta|1\rangle)\right.\\
&\quad\left. + (|01\rangle + |10\rangle)(\alpha|1\rangle + \beta|0\rangle) + (|01\rangle - |10\rangle)(\alpha|1\rangle - \beta|0\rangle)\right]
\end{aligned} \tag{8}$$

- When Bob receives the result of Alice's measurement, he can apply the corresponding of the 4 Pauli matrices to revert this back into the state $\alpha|0\rangle + \beta|1\rangle$.

Note by the way, that the teleportation also doesn't work faster than light:
The two classical bits need time to be transmitted from Alice to Bob.

2 Interlude: Communication Complexity

Alice	Bob
x	y

Alice and Bob want to compute $f(x, y)$.

How much communication between them does it require?

If x, y are of length n $\Longrightarrow$ classically: $\propto \sqrt{n}$
quantum bits: $\propto \log n$

$\Longrightarrow$ $\exists$ situations where qubits are much better than classical bits.

3 Models of Quantum Computation

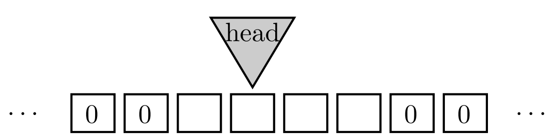
- **Quantum Turing Machine**
- **Quantum Gate Array**
- **Quantum Cellular Automata**
- **Adiabatic Quantum Computer** (see next lecture)
- **Linear Optics Quantum Computer** (beam splitters, phase shifters, mirrors etc.; only a few years ago the devices got sophisticated enough to produce and count single photons efficiently)
- **Quantum Computation by Anyons** (particles that live in two dimensions, e.g. surface of metals)
- **Modular Functors** (Quantum Field Theory)
- **Measurements on Cluster States** (two-dimensional grid; measure qubits one at a time in proper order; the computation should be quite easy, but the hard part is preparing such a cluster state: you have to switch the interaction between neighboring qubits on and off)

3.1 Quantum Turing Machine & Equivalency to Quantum Gate Array

3.1.1 Classical Turing Machine

Recall the properties of a classical Turing Machine (TM):

- infinite tape (with a finite number of non-zero spots)
- head at some position on tape
- table which maps head state & tape symbol to head action



head state	tape symbol		head state	tape symbol	direction
a	0		c	0	L
a	1		e	0	R
b	0	$\longrightarrow$	f	1	stay
b	1		a	0	stay
⋮	⋮		⋮	⋮	⋮

3.1.2 Classical Reversible Turing Machine

In order to be reversible, the table has to have the same number of columns on both sides.

head state	tape symbol	direction (from)		head state	tape symbol	direction (to)
a	0	L		c	0	L
a	0	R				
a	0	-				
a	1	L	$\longrightarrow$			
a	1	R				
a	1	-				
b	0	L				
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$

This kind of reversible TM can do any computation that a normal TM can do (proof: simulate a gate array).

3.1.3 Quantum Turing Machine

TM is in (a subset of) superpostition of states:

$$|\text{head state}\rangle \otimes |\text{direction}\rangle \otimes |\text{tape position}\rangle \otimes \bigotimes_{i=-\infty}^{\infty} |\text{tape symbol at position } i\rangle \tag{9}$$

The process of reading the tape, changing the symbol on the tape and moving the head to another position is split into two separate operations that change the state of the TM in the following ways:

- Movement transition:

$$\begin{aligned} |\text{to L}\rangle \otimes |i\rangle &\longrightarrow |\text{from R}\rangle \otimes |i-1\rangle \\ |\text{to R}\rangle \otimes |i\rangle &\longrightarrow |\text{from L}\rangle \otimes |i+1\rangle \\ |\text{stay}\rangle \otimes |i\rangle &\longrightarrow |\text{stay}\rangle \otimes |i\rangle \end{aligned} \tag{10}$$

- Transition function (corresponding to table in previous TM's)[1]:

$$|\text{head state}\rangle \otimes |\text{"from" direction}\rangle \otimes |i\rangle \otimes |\text{symbol } i\rangle \longrightarrow |\text{head state}'\rangle \otimes |\text{"to" direction}'\rangle \otimes |i\rangle \otimes |\text{symbol } i'\rangle \tag{11}$$

$\Longrightarrow$ unitary map U on the vector space $V_{\text{head state}} \otimes V_{\text{direction}} \otimes V_{\text{symbols}}$

[1] In this operation no head movement happens. This is taken care of separately by the movement transition; hence here the tape position i stays the same

How do we know when the TM is finished?

There are two possibilities:

1. We have a special stopping state (HALT), which is perpendicular to all other states, so that no collapse of the superposition can occur by measuring projection on HALT state subspace); we measure after each time step to see if the head is in HALT state.

2. Once we compute the answer, we start counting, so the tape looks like

$$|\text{answer}\rangle \otimes |i\rangle \quad \longrightarrow \quad \underbrace{|\text{answer}\rangle}_{k \text{ cells}} \otimes \underbrace{|i+1\rangle}_{\text{rest of tape}} \tag{12}$$

   After some time, the probability that the answer is in the first part of the tape hopefully reaches 1.

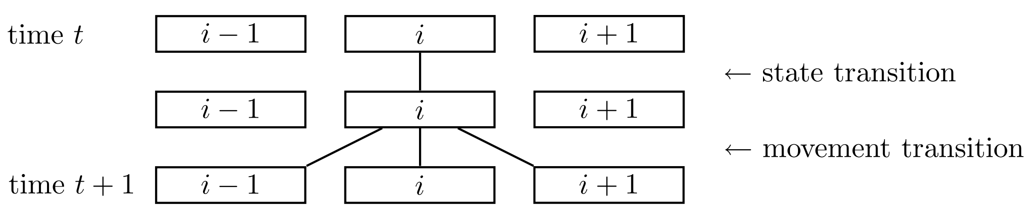
Theorem 3. *A quantum gate array with $\mathcal{O}(n)$ qubits and $\mathcal{O}(n^2)$ gates can simulate a quantum TM for n steps.*

Proof:

We're gonna use some registers

symbol at i	head state at i	direction	$\|0\dots 0\rangle$	symbol at $i+1$	head state at $i+1$	direction
	($\|0\rangle$ if head is not here)		work qubits			

Between time t and $t+1$ both state and movement transition take place and can change the contents of the registers i and (if the head moves) the neighboring registers.



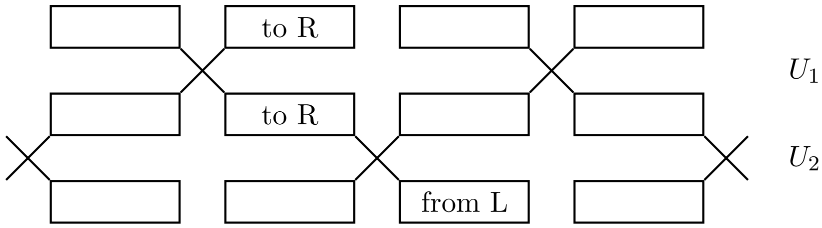
The state transition is no problem, since only the registers corresponding to position i need to be changed, and the change only depends on the contents of these registers.

In the movement transition only the head and direction registers are changed. The two possible head movements to the right and to the left correspond to the following operations:

$$\underbrace{|\text{head}\rangle\,|\text{to R}\rangle}_{\text{position } i} \quad \underbrace{|0\rangle\,|0\rangle}_{\text{position } i+1} \quad \longrightarrow \quad |0\rangle\,|0\rangle \quad |\text{head}\rangle\,|\text{from L}\rangle \tag{13}$$

$$\underbrace{|0\rangle\,|0\rangle}_{\text{position } i-1} \quad \underbrace{|\text{head}\rangle\,|\text{to L}\rangle}_{\text{position } i} \quad \longrightarrow \quad |\text{head}\rangle\,|\text{from R}\rangle \quad |0\rangle\,|0\rangle \tag{14}$$

This can be achieved with a unitary transformation on all pairs of registers on positions $2k, 2k+1$, followed by a unitary transformation on all pairs on positions $2k-1, 2k$:



The effect of either U operation on the different possible states of the head and direction registers can be seen in the following table. Marked with U_1 and U_2 is the above example.

	$\lvert\text{head}\rangle\lvert\text{to L}\rangle \quad \lvert 0\rangle\lvert 0\rangle$ $\downarrow$ $\lvert\text{head}\rangle\lvert\text{to L}\rangle \quad \lvert 0\rangle\lvert 0\rangle$	$\lvert 0\rangle\lvert 0\rangle \quad \lvert\text{head}\rangle\lvert\text{to L}\rangle$ $\downarrow$ $\lvert\text{head}\rangle\lvert\text{from R}\rangle \quad \lvert 0\rangle\lvert 0\rangle$	
$U_2 \rightarrow$	$\lvert\text{head}\rangle\lvert\text{to R}\rangle \quad \lvert 0\rangle\lvert 0\rangle$ $\downarrow$ $\lvert 0\rangle\lvert 0\rangle \quad \lvert\text{head}\rangle\lvert\text{from L}\rangle$	$\lvert 0\rangle\lvert 0\rangle \quad \lvert\text{head}\rangle\lvert\text{to R}\rangle$ $\downarrow$ $\lvert 0\rangle\lvert 0\rangle \quad \lvert\text{head}\rangle\lvert\text{to R}\rangle$	$\leftarrow U_1$
	$\lvert\text{head}\rangle\lvert\text{stay}\rangle \quad \lvert 0\rangle\lvert 0\rangle$ $\downarrow$ $\lvert\text{head}\rangle\lvert\text{stay}\rangle \quad \lvert 0\rangle\lvert 0\rangle$	$\lvert 0\rangle\lvert 0\rangle \quad \lvert\text{head}\rangle\lvert\text{stay}\rangle$ $\downarrow$ $\lvert 0\rangle\lvert 0\rangle \quad \lvert\text{head}\rangle\lvert\text{stay}\rangle$	