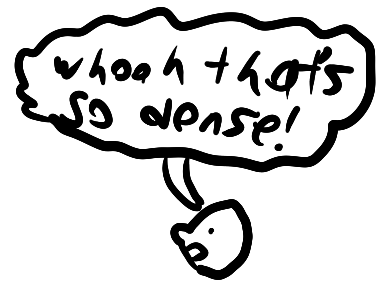
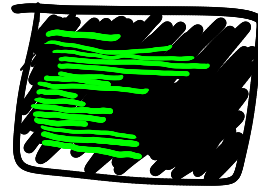


# Lecture II

## Superdense coding



At this point we have (more or less) all the components of **quantum information theory** that we'll need. To recap:

- Pure states: unit vectors  $|\psi\rangle \in \mathbb{C}^d$
- Mixed states: Trace 1 operators  $\rho \in \mathcal{H} \rightarrow \mathcal{H}$
- Gates: unitary matrices  $U: \mathcal{H} \rightarrow \mathcal{H}$
- Measurement:  $\{P_i\}$  s.t.  $\sum_i P_i = I$

$$P_i P_j = 0 \quad \forall i \neq j$$

$$P_i^2 = P_i \quad \forall i$$

Before we move on to **general quantum computation**, let's work through a few **quantum communication protocols** as a warm up. Today we'll see how to send **2 bits** of classical data by sending **a single (entangled) qubit**.

# (The Bell basis)

We've previously used the **entangled state**

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

in our protocols, but this is not the only 2-qubit entangled state. In fact there exists an orthonormal basis of  $\mathbb{C}^2 \otimes \mathbb{C}^2$  which consists of entangled states. This is called the **Bell basis**, consisting of the **Bell states**

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

$$| B_{01} \rangle = \frac{1}{\sqrt{2}} (| 01 \rangle + | 10 \rangle)$$

$$| B_{10} \rangle = \frac{1}{\sqrt{2}} (| 00 \rangle - | 11 \rangle)$$

$$| B_{11} \rangle = \frac{1}{\sqrt{2}} (| 01 \rangle - | 10 \rangle)$$

It can be readily verified that these 4 states are orthonormal and non-separable (i.e. entangled). As an entangled basis of  $\mathbb{C}^2 \otimes \mathbb{C}^2$ , these states arise frequently in quantum computation.

Ex.

Recall that the circuit



$$(\text{= CNOT}(H \otimes I))$$

generates the EPR pair or Bell state  $| B_{00} \rangle$  from the  $| 00 \rangle$  initial state. We can ask what states it maps the other 3 computational basis states to:

$$\begin{aligned} \text{CNOT}(H \otimes I) | 01 \rangle &= \text{CNOT} \left( \frac{1}{\sqrt{2}} | 01 \rangle + \frac{1}{\sqrt{2}} | 11 \rangle \right) \\ &= \frac{1}{\sqrt{2}} | 01 \rangle + \frac{1}{\sqrt{2}} | 10 \rangle \\ &= | B_{01} \rangle \end{aligned}$$

$$\begin{aligned} \text{CNOT}(H \otimes I) | 10 \rangle &= \text{CNOT} \left( \frac{1}{\sqrt{2}} | 00 \rangle - \frac{1}{\sqrt{2}} | 10 \rangle \right) \\ &= | B_{10} \rangle \end{aligned}$$

$$\begin{aligned} \text{CNOT}(H \otimes I)|11\rangle &= \text{CNOT}\left(\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle\right) \\ &= |B_{11}\rangle \end{aligned}$$

So this circuit implements a **change of basis** from the computational basis to the Bell basis. Since the circuit is unitary, it follows that its dagger

$$(\text{CNOT}(H \otimes I))^\dagger = (H \otimes I)\text{CNOT}$$

maps the Bell basis back to the computational basis.

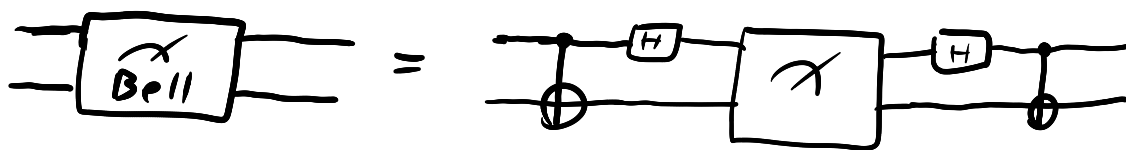
$$\begin{aligned} (H \otimes I)\text{CNOT}|B_{00}\rangle &= (H \otimes I)\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) \\ &= \frac{1}{2}(|00\rangle + |10\rangle + |00\rangle - |10\rangle) \\ &= |00\rangle \end{aligned}$$

### (Bell basis measurement)

We denote measurement in the Bell basis by



Observe that Bell basis measurement is equivalent to a change of basis followed by a computational basis measurement and a change back to the Bell basis.



We've used this trick before to measure in the  $\{|+\rangle, |-\rangle\}$  basis. So far it's just a mathematical convenience, but soon we'll see that it's important for building a real quantum computer. In general, for **any orthonormal basis**  $\{|e_i\rangle\}$ , the matrix  $U = [|e_1\rangle \dots |e_n\rangle]$  is unitary, and



The ability to measure in the Bell basis leads to some surprising consequences. The first one we will discuss is **superdense coding**.

## (Superdense coding)

Suppose **Alice** wants to send **Bob** two bits of information over a telephone line. Basic information theory states that **Alice** actually needs to send both bits (*is this obvious?*)

What if **Alice** can also send **qubits** over the telephone line? If **Alice** and **Bob** share an entangled pair, it turns out that **Alice** only needs to send a **single qubit** to send two (classical) bits of information. Let's see how this works.

Recall the definitions of the  $X$  &  $Z$  gates:

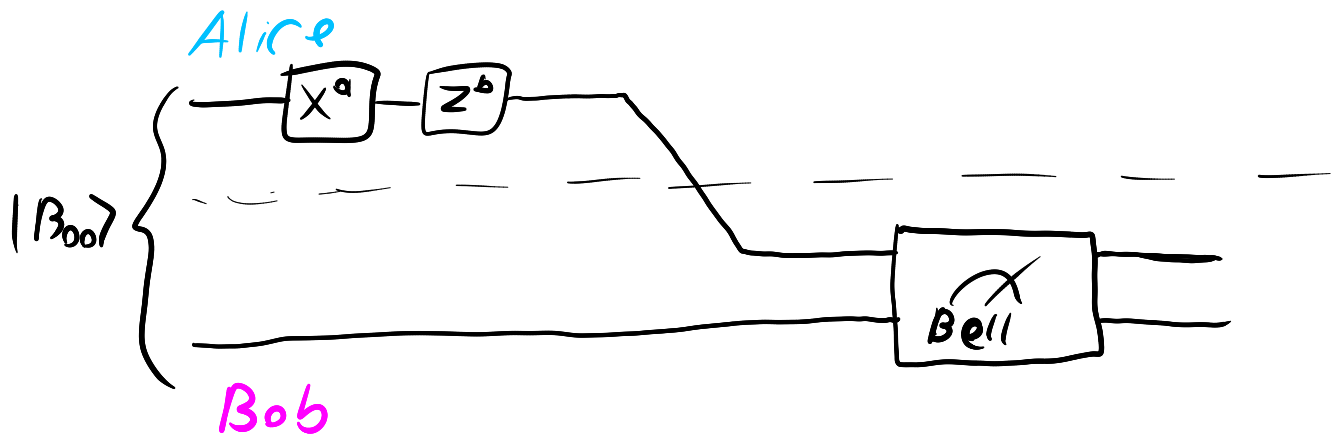
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

**Alice** and **Bob** share a pre-entangled  **$|B_{00}\rangle$**  state. To send the bits  **$a$**  and  **$b$** , **Alice** applies the following transformation to her qubit

$a$	$b$	transformation
0	0	$I$
0	1	$X$
1	0	$Z$
1	1	$ZX$

Alternately, we can write the transformation as  $Z^a X^b$ . **Alice** then sends her qubit to **Bob** who measures both qubits in the Bell basis to get  $|B_{ab}\rangle$ .

The protocol can be summarized as below:



To see why this works, observe that

$$\begin{aligned} (X \otimes I) |B_{00}\rangle &= \frac{1}{\sqrt{2}} ((X \otimes I) |00\rangle + (X \otimes I) |11\rangle) \\ &= \frac{1}{\sqrt{2}} (|10\rangle + |01\rangle) \\ &= |B_{01}\rangle \end{aligned}$$

Likewise,

$$\begin{aligned} (Z \otimes I) |B_{00}\rangle &= \frac{1}{\sqrt{2}} ((Z \otimes I) |00\rangle + (Z \otimes I) |11\rangle) \\ &= \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) \\ &= |B_{10}\rangle \end{aligned}$$

$$\begin{aligned} (ZX \otimes I) |B_{00}\rangle &= \frac{1}{\sqrt{2}} ((ZX \otimes I) |00\rangle + (ZX \otimes I) |11\rangle) \\ &= \frac{1}{\sqrt{2}} (-|10\rangle + |01\rangle) \\ &= |B_{11}\rangle \end{aligned}$$

In short,

$$(Z^a X^b \otimes I) |B_{00}\rangle = |B_{ab}\rangle$$

So when Bob measures in the Bell basis, his result is  $B_{ab}$  which tells him Alice's bits  $a$  &  $b$ .

## (Relationship to mixed states & EPR paradox)

At first glance superdense coding seems to contradict the fact that local operations **Alice** performs can't alter **Bob's** reduced density matrix. The key here is that while local operations don't impact **Bob's** reduced density matrix, which accounts for all **local measurements** of **Bob's** qubit, they can change the joint (entangled) state, which is observable through a joint measurement.

You may wonder whether we really **need** the two entangled qubits — that is, could **Alice** just send a state encoding her bits like

$$(-1)^a |b\rangle$$

and then have **Bob** "decode" the state? The answer is a resounding **NO** by **Holevo's Theorem** which states, roughly, that you can't get more than one bit of information out of a qubit.