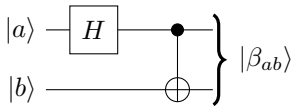
Christian B. Mendl, Pedro Hack, Keefe Huang, Irene López Gutiérrez

Exercise 7.1 (Bell states and superdense coding)
Recall that the *Bell states* are defined as

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

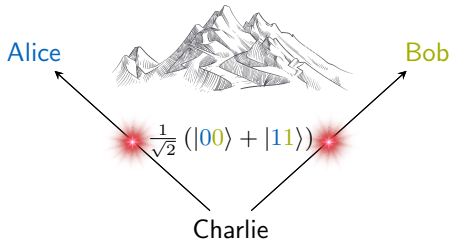
which can be summarized as $|\beta_{ab}\rangle = \frac{1}{\sqrt{2}}(|0, b\rangle + (-1)^a |1, 1-b\rangle)$ for $a, b \in \{0, 1\}$.

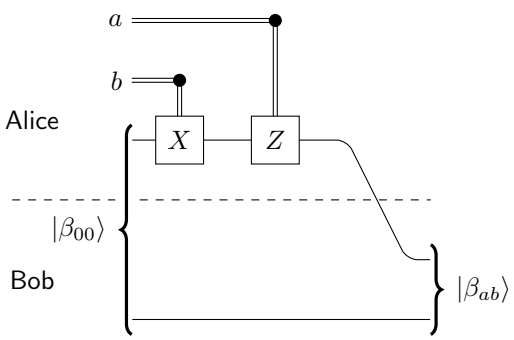
(a) Verify that the following quantum circuit creates the Bell states for inputs $|a, b\rangle$:



Note: this generalizes exercise 4.1(b). Since the circuit implements a unitary transformation of the standard basis states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, the Bell states form an orthonormal basis of the two qubit state space as well.

Superdense coding is a surprising use of entanglement to transmit two bits of classical information by sending just a single qubit! The setup agrees with quantum teleportation: two parties, usually referred to as Alice and Bob, live far from each other but share a pair of qubits in the entangled Bell state $|\beta_{00}\rangle$. They could have generated the pair during a visit in the past, or a common friend Charlie prepared it and sent one qubit to Alice and the other to Bob, as shown on the right.





Now Alice's task is to communicate two bits 'ab' of classical information to Bob. Alice can achieve that by applying X and/or Z gates to her qubit before sending it to Bob, depending on the information she wants to transmit: for '00', she does nothing to her qubit, for '01' she applies X, for '10' she applies Z, and for '11' she applies first X and then Z, i.e., $ZX = iY$. It turns out that the resulting states are precisely the Bell states, which Bob can distinguish by performing a measurement with respect to this basis. The diagram on the left summarizes the protocol.

(b) Verify for all combinations of $a, b \in \{0, 1\}$ that the output of the circuit is indeed the Bell state $|\beta_{ab}\rangle$.

(c) Suppose E is an operator on Alice's qubit (e.g., $E = M_m^\dagger M_m$ in the general measurement framework, with M_m a measurement operator). Show that $\langle\beta_{ab}|E \otimes I\,|\beta_{ab}\rangle$ takes the same value for all four Bell states. Assuming an adversarial "Eve" intercepts Alice's qubit on the way to Bob, can Eve infer anything about the classical information which Alice tries to send?

Solution

(a) For all $a, b \in \{0, 1\}$:

$$|a, b\rangle \overset{H\otimes I}{\mapsto} \frac{|0\rangle + (-1)^a |1\rangle}{\sqrt{2}} |b\rangle = \frac{1}{\sqrt{2}}\big(\,|0, b\rangle + (-1)^a |1, b\rangle\,\big) \overset{\text{CNOT}}{\mapsto} \frac{1}{\sqrt{2}}\big(\,|0, b\rangle + (-1)^a |1, 1-b\rangle\,\big) = |\beta_{ab}\rangle\,.$$

(b) We enumerate all four cases explicitly:

$ab = 00:$ $|\beta_{00}\rangle$ remains unchanged

$ab = 01:$ $(X \otimes I)\,|\beta_{00}\rangle = (X \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}((X\,|0\rangle)\,|0\rangle + (X\,|1\rangle)\,|1\rangle) = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = |\beta_{01}\rangle$

$ab = 10:$ $(Z \otimes I)\,|\beta_{00}\rangle = (Z \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}((Z\,|0\rangle)\,|0\rangle + (Z\,|1\rangle)\,|1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\beta_{10}\rangle$

$ab = 11:$ $(ZX \otimes I)\,|\beta_{00}\rangle = (ZX \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(-\,|10\rangle + |01\rangle) = |\beta_{11}\rangle$

Alternative solution: The operation of the classically-controlled gates can be summarized as $Z^a X^b$ for $a, b \in \{0, 1\}$. Note that X^b appears on the right since it is applied *first*. A matrix to the power of zero is the identity matrix, thus for example

$$X^b = \begin{cases} I & \text{if } b = 0 \\ X & \text{if } b = 1 \end{cases}.$$

A little thought confirms the following relations, for all $a, b \in \{0, 1\}$:

$$\begin{aligned} X^b\,|0\rangle &= |b\rangle\,, \quad X^b\,|1\rangle = |1-b\rangle\,, \\ Z^a\,|0\rangle &= |0\rangle\,, \quad Z^a\,|1\rangle = (-1)^a\,|1\rangle\,. \end{aligned}$$

With that, we can compute the output of the circuit:

$$\begin{aligned} (Z^a X^b \otimes I)\,|\beta_{00}\rangle &= (Z^a X^b \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= (Z^a \otimes I)\frac{1}{\sqrt{2}}\big((X^b\,|0\rangle)\,|0\rangle + (X^b\,|1\rangle)\,|1\rangle\big) \\ &= (Z^a \otimes I)\frac{1}{\sqrt{2}}\big(\,|b, 0\rangle + |1-b, 1\rangle\,\big) \\ &= (Z^a \otimes I)\frac{1}{\sqrt{2}}\big(\,|0, b\rangle + |1, 1-b\rangle\,\big) \\ &= \frac{1}{\sqrt{2}}\big((Z^a\,|0\rangle)\,|b\rangle + (Z^a\,|1\rangle)\,|1-b\rangle\,\big) \\ &= \frac{1}{\sqrt{2}}\big(\,|0, b\rangle + (-1)^a\,|1, 1-b\rangle\,\big) = |\beta_{ab}\rangle\,. \end{aligned}$$

The fourth equal sign follows from considering the two cases $b = 0$ and $b = 1$.

(c) $\langle\beta_{ab}|\,E \otimes I\,|\beta_{ab}\rangle$ turns out to be independent of a and b:

$$\begin{aligned} \langle\beta_{ab}|\,E \otimes I\,|\beta_{ab}\rangle &= \frac{1}{2}\Big(\,\langle 0, b| + (-1)^a\,\langle 1, 1-b|\,\Big)(E \otimes I)\Big(\,|0, b\rangle + (-1)^a\,|1, 1-b\rangle\,\Big) \\ &= \frac{1}{2}\Big(\,\langle 0, b|\,E \otimes I\,|0, b\rangle + (-1)^a\,\langle 0, b|\,E \otimes I\,|1, 1-b\rangle \\ &\qquad\qquad + (-1)^a\,\langle 1, 1-b|\,E \otimes I\,|0, b\rangle + \langle 1, 1-b|\,E \otimes I\,|1, 1-b\rangle\,\Big) \\ &= \frac{1}{2}\Big(\,\langle 0|\,E\,|0\rangle\,\underbrace{\langle b|b\rangle}_{=1} + (-1)^a\,\langle 0|\,E\,|1\rangle\,\underbrace{\langle b|1-b\rangle}_{=0} + (-1)^a\,\langle 1|\,E\,|0\rangle\,\underbrace{\langle 1-b|b\rangle}_{=0} + \langle 1|\,E\,|1\rangle\,\underbrace{\langle 1-b|1-b\rangle}_{=1}\,\Big) \\ &= \frac{1}{2}\big(\,\langle 0|\,E\,|0\rangle + \langle 1|\,E\,|1\rangle\,\big). \end{aligned}$$

Thus, whichever measurement (with operators $\{M_m\}$) Eve performs, the outcome probabilities $p(m) = \langle\beta_{ab}|\,M_m^\dagger M_m\,|\beta_{ab}\rangle$ are independent of $a, b \rightsquigarrow$ Eve cannot infer anything about the classical information.