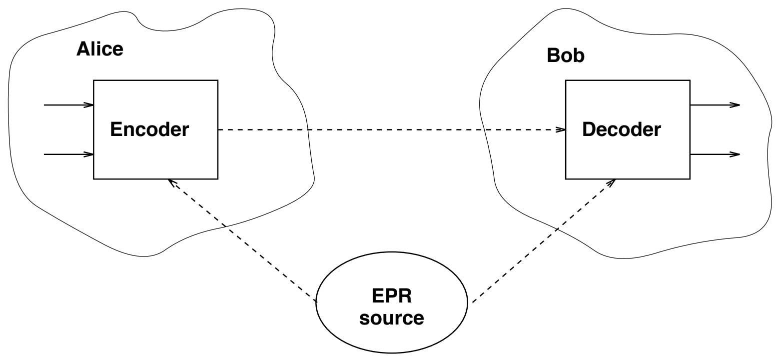

Figure III.18: Superdense coding. (Rieffel & Polak, 2000)

C.6 Applications

C.6.a Superdense coding

We will consider a couple simple applications of these ideas. The first is called *superdense coding* or (more modestly) *dense coding*, since it is a method by which one quantum particle can be used to transmit two classical bits of information. It was described by Bennett and Wiesner in 1992, and was partially validated experimentally by 1998.

Here is the idea. Alice and Bob share an entangled pair of qubits. To transmit two bits of information, Alice applies one of four transformations to her qubit. She then sends her qubit to Bob, who can apply an operation to the entangled pair to determine which of the four transformations she applied, and hence recover the two bits of information.

Now let's work it through more carefully. Suppose Alice and Bob share the entangled pair $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Since the four Bell states are a basis for the quantum state of the pair of qubits, Alice's two bits of information can be encoded as one of the four Bell states. For example, Alice can use the state $|\beta_{zx}\rangle$ to encode the bits z, x (the correspondence is arbitrary so long as we are consistent, but this one is easy to remember). Recall the circuit for generating Bell states (Fig. III.13, p. 112). Its effect is $\text{CNOT}(H \otimes I)|zx\rangle = |\beta_{zx}\rangle$. This cannot be used by Alice for generating the Bell states, because she doesn't have access to Bob's qubit. However, the Bell states differ from each other only in the relative parity and phase of their component qubits (i.e., whether they have the same or opposite bit values and the same or opposite signs). Therefore, Alice can alter the parity and phase of just her qubit to transform the entangled pair into any of the Bell states. In particular, if she uses zx to select I, X, Z, or $ZX = Y$ (corresponding to $zx = 00, 01, 10, 11$ respectively) and applies it to just her qubit, she can generate the corresponding Bell state $|\beta_{zx}\rangle$. I've picked this correspondence because of the simple relation between the bits z, x and the application of the operators Z, X, but this is not necessary; any other 1-1 correspondence between the two bits and the four operators could be used. When Alice applies this transformation to her qubit, Bob's qubit is unaffected, and so the transformation on the entangled pair is $I \otimes I$, $X \otimes I$, $Z \otimes I$, or $ZX \otimes I$. We can check the results as follows:

bits	transformation	result	
00	$I \otimes I$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$= \|\beta_{00}\rangle$
01	$X \otimes I$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$	$= \|\beta_{01}\rangle$
10	$Z \otimes I$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$= \|\beta_{10}\rangle$
11	$ZX \otimes I$	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$	$= \|\beta_{11}\rangle$

For example, in the second-to-last case, since $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$, we see $Z \otimes I \left[\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right] = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. Make sure you can explain the results in the other cases (Exer. III.39).

When Alice wants to send her information, she applies the appropriate operator to her qubit and sends her single transformed qubit to Bob, which he uses with his qubit to recover the information by measuring the pair of qubits in the Bell basis. This can be done by inverting the Bell state generator, which, since the CNOT and H are self-adjoint, is simply:

$$(H \otimes I)\text{CNOT}|\beta_{zx}\rangle = |zx\rangle.$$

This translates the Bell basis into the computational basis, so Bob can measure the bits exactly.

C.6.b Quantum teleportation

Quantum teleportation is not quite as exciting as it sounds! Its goal is to transfer the exact quantum state of a particle from Alice to Bob by means a classical channel (Figs. III.19, III.20). Of course, the No Cloning Theorem says we cannot copy a quantum state, but we can "teleport" it by destroying

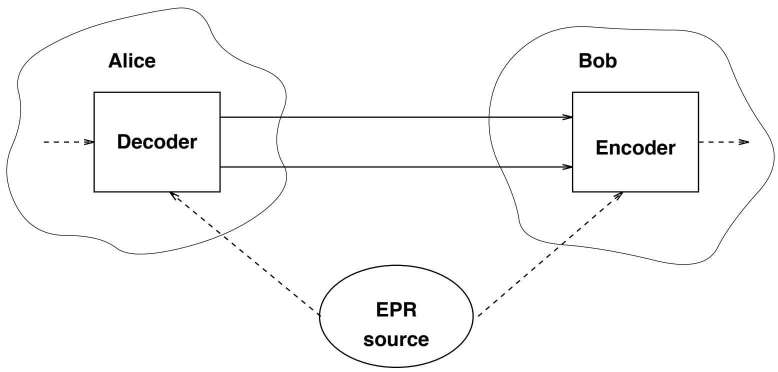

Figure III.19: Quantum teleportation. (Rieffel & Polak, 2000)

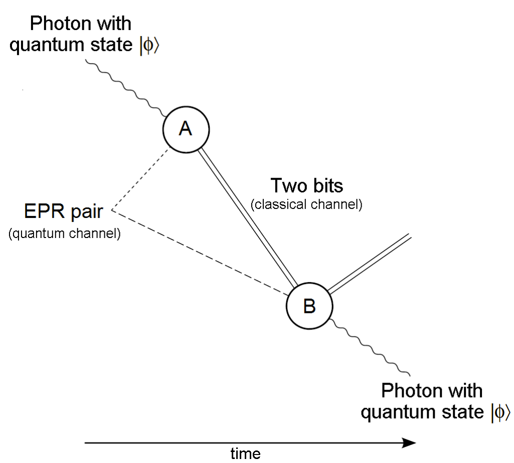

Figure III.20: Possible setup for quantum teleportation. [from wikipedia commons] the original and recreating it elsewhere. Single-qubit quantum teleportation was described by Bennett in 1993 and first demonstrated experimentally in the late 1990s.

This is how it works. Alice and Bob begin by sharing the halves of an entangled pair, $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Suppose that the quantum state that Alice wants to share is $|\psi\rangle = a|0\rangle + b|1\rangle$. The composite system comprising the unknown state and the Bell state is

$$\begin{aligned}
|\psi_0\rangle &\stackrel{\text{def}}{=} |\psi, \beta_{00}\rangle \\
&= (a|0\rangle + b|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
&= \frac{1}{\sqrt{2}}[a|0\rangle(|00\rangle + |11\rangle) + b|1\rangle(|00\rangle + |11\rangle)] \\
&= \frac{1}{\sqrt{2}}(a|0,00\rangle + a|0,11\rangle + b|1,00\rangle + b|1,11\rangle).
\end{aligned}$$

Alice applies the decoding circuit used for superdense coding to the unknown state and her qubit from the entangled pair. This function is $(H \otimes I)$CNOT; it measures her two qubits in the Bell basis. When Alice applies CNOT to her two qubits (leaviing Bob's qubit alone) the resulting composite state is:

$$\begin{aligned}
|\psi_1\rangle &\stackrel{\text{def}}{=} (\text{CNOT} \otimes I)|\psi_0\rangle \\
&= (\text{CNOT} \otimes I)\left[\frac{1}{\sqrt{2}}(a|00,0\rangle + a|01,1\rangle + b|10,0\rangle + b|11,1\rangle)\right] \\
&= \frac{1}{\sqrt{2}}(a|00,0\rangle + a|01,1\rangle + b|11,0\rangle + b|10,1\rangle).
\end{aligned}$$

When she applies $H \otimes I$ to her qubits the result is:

$$\begin{aligned}
|\psi_2\rangle &\stackrel{\text{def}}{=} (H \otimes I \otimes I)|\psi_1\rangle \\
&= (H \otimes I \otimes I)\frac{1}{\sqrt{2}}(a|0,00\rangle + a|0,11\rangle + b|1,10\rangle + b|1,01\rangle) \\
&= \frac{1}{2}\left[a(|0,00\rangle + |1,00\rangle + |0,11\rangle + |1,11\rangle)\right. \\
&\quad \left. + b(|0,10\rangle - |1,10\rangle + |0,01\rangle - |1,01\rangle)\right].
\end{aligned}$$

This is because $H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Rearranging and factoring, we have:

$$|\psi_2\rangle = \frac{1}{2}[|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle)$$

$$+|10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)] \,.$$

Thus the unknown amplitudes have been transferred from the first qubit (Alice's) to the third (Bob's), which now incorporates the amplitudes a and b, but in different ways depending on the first two bits. In fact you can see that the amplitudes are transformed by the Pauli matrices. Therefore Alice measures the first two bits (completing measurement in the Bell basis) and sends them to Bob over the classical channel. This measurement partially collapses the state, including Bob's qubit, but in a way that is determined by the first two qubits.

When Bob receives the two classical bits from Alice, he uses them to select a transformation for his qubit, which restores the amplitudes to the correct basis vectors. These transformations are the Pauli matrices (which are their own inverses):

bits	gate	input	
00	I	$a\|0\rangle + b\|1\rangle$	(identity)
01	X	$a\|1\rangle + b\|0\rangle$	(exchange)
10	Z	$a\|0\rangle - b\|1\rangle$	(flip)
11	ZX	$a\|1\rangle - b\|0\rangle$	(exchange–flip)

In each case, applying the specified gate to its input yields $|\psi\rangle = a|0\rangle + b|1\rangle$, Alice's original quantum state. This is obvious in the 00 case, but you should verify the others (Exer. III.40). Notice that since Alice had to measure her qubits, the original quantum state of her particle has collapsed. Thus it has been "teleported," not copied.

The quantum circuit in Fig. III.21 is slightly different from what we've described, since it uses the fact that the appropriate transformations can be expressed in the form $Z^{M_1}X^{M_2}$, where M_1 and M_2 are the two classical bits. You should verify that $ZX = Y$ (Exer. III.41).

Both superdense coding and teleportation indicate that under some circumstances two bits and an entangled pair can be interchanged with one qubit. This is one example of a method of *interchanging resources*. However, quantum teleportation does not allow faster-than-light communication, since Alice has to transmit her two classical bits to Bob.

Entangled states can be teleported in a similar way. Free-space quantum teleportation has been demonstrated over 143 km between two of the Canary

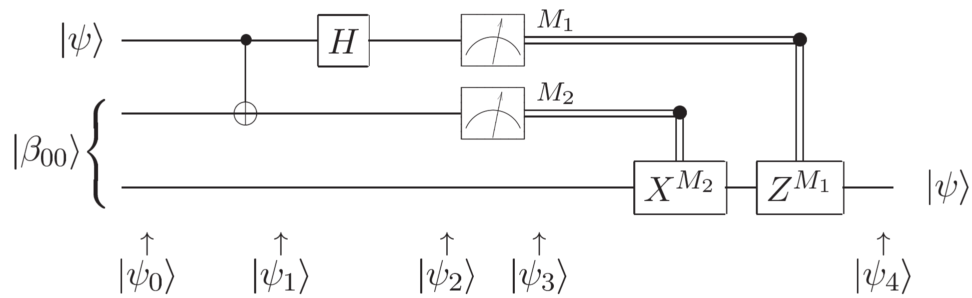

Figure III.21: Circuit for quantum teleportation. [from Nielsen & Chuang (2010)]

Islands (*Nature*, 13 Sept. 2012).[6] In Sept. 2015 teleportation was achieved over 101 km through supercooled nanowire. For teleporting material systems, the current record is 21 m.

C.7 Universal quantum gates

We have seen several interesting examples of quantum computing using gates such as CNOT and the Hadamard and Pauli operators.[7] Since the implementation of each of these is a technical challenge, it raises the important question: What gates are sufficient for implementing *any* quantum computation?

Both the Fredkin (controlled swap) and Toffoli (controlled-controlled-NOT) gates are sufficient for classical logic circuits. In fact, they can operate as well on qubits in superposition. But what about other quantum operators?

It can be proved that single-qubit unitary operators can be approximated arbitrarily closely by the Hadamard gate and the T ($\pi/8$) gate, which is defined:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \cong \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix} \qquad \text{(III.19)}$$

(ignoring global phase). To approximate within ϵ any single-qubit unitary

[6] `http://www.nature.com/nature/journal/v489/n7415/full/nature11472.html` (accessed 12-09-18).

[7] This lecture follows Nielsen & Chuang (2010, §4.5).

operation, you need $\mathcal{O}(\log^c(1/\epsilon))$ gates, where $c \approx 2$. For an m-gate circuit (of CNOTs and single-qubit unitaries) and an accuracy of ϵ, $\mathcal{O}(m \log^c(m/\epsilon))$, where $c \approx 2$, gates are needed (Solovay-Kitaev theorem).

A *two-level operation* is a unitary operator on a d-dimensional Hilbert space that non-trivially affects only two qubits out of n (where $d = 2^n$). It can be proved that any two-level unitary operation can be computed by a combination of CNOTs and single-qubit operations. This requires $\mathcal{O}(n^2)$ single-qubit and CNOT gates.

It also can be proved that an arbitrary d-dimensional unitary matrix can be decomposed into a product of two-level unitary matrices. At most $d(d-1)/2$ of them are required. Therefore a unitary operator on an n-qubit system requires at most $2^{n-1}(2^n - 1)$ two-level matrices.

In conclusion, the H (Hadamard), CNOT, and $\pi/8$ gates are sufficient for quantum computation. For fault-tolerance, either the *standard set* — H (Hadamard), CNOT, $\pi/8$, and S (phase) — can be used, or H, CNOT, Toffoli, and S. The latter *phase gate* is defined:

$$S = T^2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{III.20}$$