C Quantum information

C.1 Qubits

C.1.a Single qubits

Just as the bits 0 and 1 are represented by distinct physical states in a conventional computer, so the *quantum bits* (or qubits) $|0\rangle$ and $|1\rangle$ are represented by distinct quantum states. We call $|0\rangle$ and $|1\rangle$ the *computational* or *standard* measurement basis. What distinguishes qubits from classical bits is that they can be in a superposition of states, $a_0|0\rangle + a_1|1\rangle$, for $a_0, a_1 \in \mathbb{C}$, where $|a_0|^2 + |a_1|^2 = 1$. If we measure this state in the computational basis, we will observe $|0\rangle$ with probability $|a_0|^2$ and likewise for $|1\rangle$; after measurement the qubit is in the observed state. This applies, of course, to measurement in any basis. I will depict the measurement possibilities this way:

$$\begin{aligned} a_0|0\rangle + a_1|1\rangle &\xrightarrow{|a_0|^2} |0\rangle, \\ a_0|0\rangle + a_1|1\rangle &\xrightarrow{|a_1|^2} |1\rangle. \end{aligned}$$

The following *sign basis* is often useful:

$$|+\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{III.8}$$

$$|-\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{III.9}$$

Notice that $|+\rangle$ is "halfway" between $|0\rangle$ and $|1\rangle$, and likewise $|-\rangle$ is halfway between $|0\rangle$ and $-|1\rangle$. Draw them to be sure you see this. As a consequence (Exer. III.29):

$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), \\ |1\rangle &= \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle). \end{aligned}$$

To remember this, think $(+x) + (-x) = 0$ and $(+x) - (-x) = (+2x)$, which is nonzero (this is just a mnemonic).

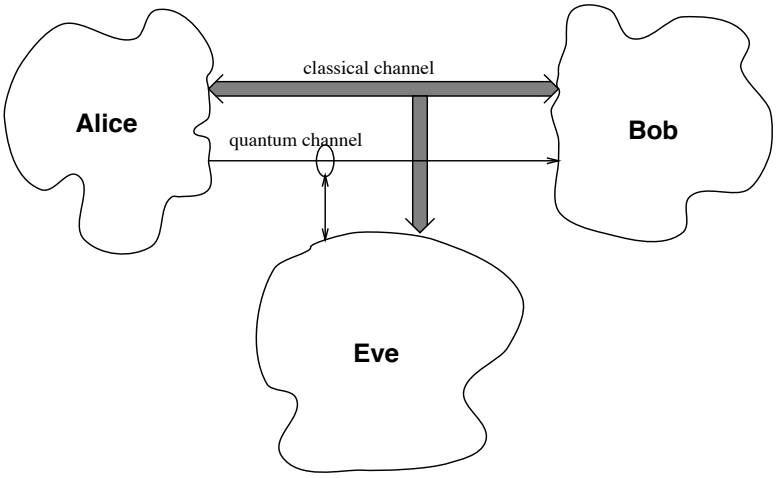

Figure III.6: Quantum key distribution [from Rieffel & Polak (2000)].

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

Figure III.7: Example if QKD without interference. [fig. from wikipedia]

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✘			✓		✓

Figure III.8: Example if QKD with eavesdropping. [fig. from wikipedia]

C.1.b Quantum key distribution

In 1984 Bennett and Brassard showed how sequences of qubits could be used to distribute an encryption key securely.[3] This is called the "BB84 protocol." Ironically, the idea was proposed initially by Stephen Wiesner in the 1970s, but he couldn't get it published.

We are supposing that Alice is transmitting a key to Bob over two channels, one classical and one quantum. Eve may eavesdrop on both channels and even replace the signals in them. Over the quantum channel Alice will send the photons to Bob that encode the key bits in two different bases, either $\{|\uparrow\rangle, |\rightarrow\rangle\}$, which I'll call the "+ basis," or $\{|\nearrow\rangle, |\searrow\rangle\}$ (the "× basis") (respectively 0, 1 in each basis). Alice chooses randomly the basis in which to encode her bits (see Fig. III.7). Bob will measure the photons according to these two bases, also chosen randomly and independently of Alice. After the transmission, Alice and Bob will communicate over the classical channel and compare their random choices; where they picked the same basis, they will keep the bit, otherwise they will discard it. (They will have agreed on about 50% of the choices.)

Suppose Eve is eavesdropping on the quantum channel, measuring the qubits and retransmitting them to Bob (see Fig. III.8). About 50% of the time, she will guess the wrong basis, and will also resend it in this same incorrect basis. If this is one of the times Alice and Bob chose the same basis, the bit will nevertheless be incorrect about half of the time (the times

[3] This section is based on Rieffel & Polak (2000), which is also the source for otherwise unattributed quotes.

Eve chose the wrong basis). That is, about 50% of the time Eve picks the same basis as Alice, so she reads the bit correctly and transmits it to Bob correctly. About 50% of the time Eve guesses the wrong basis. She will know this, if she is listening in on the classical channel, but she has already transmitted it to Bob in the wrong basis. If this is a case in which Alice and Bob used the same basis (and so Bob should get it correct), he will get it incorrect 50% of the time, since Eve transmitted it in the other basis. So 25% of the bits that should be correct will be wrong. This high error rate will be apparent to Alice and Bob if they have been using an error-detecting code for the key. (In effect Eve is introducing significant, detectable noise into the channel.) Furthermore, Eve's version of the key will be about 25% incorrect. Therefore Bob knows that the key was not transmitted securely and Eve gets an incorrect key.

This is only the most basic technique, and it has some vulnerabilities, and so other techniques have been proposed, but they are outside the scope of this book. "The highest bit rate system currently demonstrated exchanges secure keys at 1 Mbit/s (over 20 km of optical fibre) and 10 kbit/s (over 100 km of fibre)"[4] "As of March 2007 the longest distance over which quantum key distribution has been demonstrated using optic fibre is 148.7 km, achieved by Los Alamos National Laboratory/NIST using the BB84 protocol." In Aug. 2015 keys were distributed over a 307 km optical cable, with 12.7 kbps key generation rate. "The distance record for free space QCD [quantum key distribution] is 144 km between two of the Canary Islands, achieved by a European collaboration using entangled photons (the Ekert scheme) in 2006,[7] and using BB84 enhanced with decoy states[8] in 2007.[9] The experiments suggest transmission to satellites is possible, due to the lower atmospheric density at higher altitudes." At least three companies offer commercial QKD. "Quantum encryption technology provided by the Swiss company Id Quantique was used in the Swiss canton (state) of Geneva to transmit ballot results to the capitol in the national election occurring on October 21, 2007." Four QKD networks have been in operation since mid-late 2000s. Among them,

> [t]he world's first computer network protected by quantum key distribution was implemented in October 2008, at a scientific conference in Vienna. The name of this network is SECOQC (**Se**cure **Co**mmunication Based on **Q**uantum **C**ryptography) and

[4] `https://en.wikipedia.org/wiki/Quantum_key_distribution` (accessed 12-09-18).

EU funded this project. The network used 200 km of standard fibre optic cable to interconnect six locations across Vienna and the town of St Poelten located 69 km to the west.

C.1.c Multiple qubits

We can combine multiple qubits into a *quantum register*. By Postulate 4, if $\mathcal{H}$ is the state space of one qubit, then the tensor power $\mathcal{H}^{\otimes n}$ will be the state space of an n-qubit quantum register. The computational basis of this space is the set of all vectors $|b_1 b_2 \cdots b_n\rangle$ with $b_k \in \mathbf{2}$. (I define $\mathbf{2} \stackrel{\text{def}}{=} \{0,1\}$ to be the set of bits, and in general I use a boldface integer $\mathbf{N}$ for the set integers $\{0,1,\ldots,N-1\}$.) Therefore the dimension of the space $\mathcal{H}^{\otimes n}$ is 2^n, and the set of states is the set of normalized vectors in $\mathbb{C}^{2^n}$. For 10 qubits we are dealing with 1024-dimensional complex vectors (because each of the 2^{10} basis vectors has its own complex amplitude). This is a huge space, exponentially larger than the 2^n classical n-bit strings. This is part of the origin of *quantum parallelism*, because we can compute on all of these qubit strings in parallel. Consider a quantum computer with 500 qubits; it could be very small (e.g., 500 atoms), but it is computing in a space of 2^{500} complex numbers. Note that 2^{500} is more than the number of particles in the universe times the age of the universe in femtoseconds! That is, a 500-qubit quantum computer is equivalent to a universe-sized computer working at high speed since the Big Bang.

Whereas an ordinary direct product has dimension $\dim(S \times T) = \dim S + \dim T$, a tensor product has dimension $\dim(S \otimes T) = \dim S \times \dim T$. Hence if $\dim S = 2$, $\dim S^{\otimes n} = 2^n$.

Measuring some of the qubits in a register causes partial collapse of the quantum state. Suppose we have a composite state

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle,$$

and we measure just the first bit. We will get 0 with probability $|a_{00}|^2 + |a_{01}|^2$ and it will collapse into the state $a_{00}|00\rangle + a_{01}|01\rangle$, but we must renormalize it:

$$|\psi'\rangle = \frac{a_{00}|00\rangle + a_{01}|01\rangle}{\sqrt{|a_{00}|^2 + |a_{01}|^2}}.$$

Do this by striking out all terms in $|\psi\rangle$ that have 1 in the first qubit.

$$|\psi\rangle \stackrel{|a_{00}|^2+|a_{01}|^2}{\longrightarrow} a_{00}|00\rangle + a_{01}|01\rangle \cong \frac{a_{00}|00\rangle + a_{01}|01\rangle}{\sqrt{|a_{00}|^2 + |a_{01}|^2}}.$$

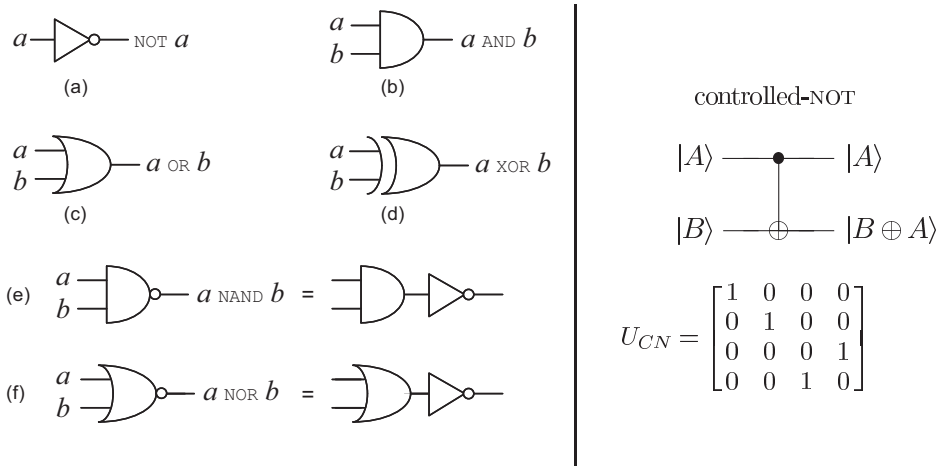

Figure III.9: Left: classical gates. Right: controlled-NOT gate. [from Nielsen & Chuang (2010, Fig. 1.6)]

C.2 Quantum gates

Quantum gates are analogous to ordinary logic gates (the fundamental building blocks of circuits), but they must be unitary transformations (see Fig. III.9, left, for ordinarty logic gates). Fortunately, Bennett, Fredkin, and Toffoli have already shown how all the usual logic operations can be done reversibly. In this section you will learn the most important quantum gates.

C.2.a Single-qubit gates

The NOT gate is simple because it is reversible: $\text{NOT}|0\rangle = |1\rangle$, $\text{NOT}|1\rangle = |0\rangle$. Its desired behavior can be represented:

$$\begin{aligned} \text{NOT}: \quad |0\rangle &\mapsto |1\rangle \\ |1\rangle &\mapsto |0\rangle. \end{aligned}$$

Note that defining it on a basis defines it on all quantum states. Therefore it can be written as a sum of dyads (outer products):

$$\text{NOT} = |1\rangle\langle 0| + |0\rangle\langle 1|.$$

You can read this, "return $|1\rangle$ if the input is $|0\rangle$, and return $|0\rangle$ if the input is $|1\rangle$." Recall that in the standard basis $|0\rangle = (1\ 0)^{\mathrm{T}}$ and $|1\rangle = (0\ 1)^{\mathrm{T}}$.

Therefore NOT can be represented in the standard basis by computing the outer products:

$$\text{NOT} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} (1\ 0) + \begin{pmatrix} 1 \\ 0 \end{pmatrix} (0\ 1) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The first column represents the result for $|0\rangle$, which is $|1\rangle$, and the second represents the result for $|1\rangle$, which is $|0\rangle$.

Although NOT is defined in terms of the computational basis vectors, it applies to any qubit, in particular to superpositions of $|0\rangle$ and $|1\rangle$:

$$\text{NOT}(a|0\rangle + b|1\rangle) = a\text{NOT}|0\rangle + b\text{NOT}|1\rangle = a|1\rangle + b|0\rangle = b|0\rangle + a|1\rangle.$$

Therefore, NOT exchanges the amplitudes of $|0\rangle$ and $|1\rangle$.

In quantum mechanics, the NOT transformation is usually called X. It is one of four useful unitary operations, called the *Pauli matrices*, which are worth remembering. In the standard basis:

$$I \stackrel{\text{def}}{=} \sigma_0 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{III.10}$$

$$X \stackrel{\text{def}}{=} \sigma_x \stackrel{\text{def}}{=} \sigma_1 \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{III.11}$$

$$Y \stackrel{\text{def}}{=} \sigma_y \stackrel{\text{def}}{=} \sigma_2 \stackrel{\text{def}}{=} \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \tag{III.12}$$

$$Z \stackrel{\text{def}}{=} \sigma_z \stackrel{\text{def}}{=} \sigma_3 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{III.13}$$

We have seen that X is NOT, and I is obviously the identity gate. Z leaves $|0\rangle$ unchanged and maps $|1\rangle$ to $-|1\rangle$. It is called the phase-flip operator because it flips the phase of the $|1\rangle$ component by π relative to the $|0\rangle$ component. (Recall that global/absolute phase doesn't matter.) The Pauli matrices span the space of 2×2 complex matrices (Exer. III.18).

Note that $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$. It is thus the analog in the sign basis of X (NOT) in the computational basis. What is the effect of Y on the computational basis vectors? (Exer. III.12)

Note that there is an alternative definition of Y that differs only in global phase:

$$Y \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

This is a $90° = \pi/2$ counterclockwise rotation: $Y(a|0\rangle + b|1\rangle) = b|0\rangle - a|1\rangle$. Draw a diagram to make sure you see this.

Note that the Pauli operations apply to *any* state, not just basis states. The X, Y, and Z operators get their names from the fact that they reflect state vectors along the x, y, z axes of the Bloch-sphere representation of a qubit, which we will not use in this book. Since they are reflections, they are Hermitian (their own inverses).

C.2.b Multiple-qubit gates

We know that any logic circuit can be built up from NAND gates. Can we do the same for quantum logic, that is, is there a universal quantum logic gate? We can't use NAND, because it's not reversible, but we will see that there are universal sets of quantum gates.

The *controlled-NOT* or CNOT gate has two inputs: the first determines what it does to the second (negate it or not).

$$\begin{array}{lcl} \text{CNOT}: & |00\rangle & \mapsto & |00\rangle \\ & |01\rangle & \mapsto & |01\rangle \\ & |10\rangle & \mapsto & |11\rangle \\ & |11\rangle & \mapsto & |10\rangle. \end{array}$$

Its first argument is called the *control* and its second is called the *target*, *controlled*, or *data* qubit. It is a simple example of conditional quantum computation. CNOT can be translated into a sum-of-dyads representation (Sec. A.2.d), which can be written in matrix form (Ex. III.21, p. 194):

$$\begin{array}{rcl} \text{CNOT} & = & |00\rangle\langle 00| \\ & + & |01\rangle\langle 01| \\ & + & |11\rangle\langle 10| \\ & + & |10\rangle\langle 11| \end{array}$$

We can also define it (for $x, y \in \mathbf{2}$), $\text{CNOT}|xy\rangle = |xz\rangle$, where $z = x \oplus y$, the exclusive OR of x and y. That is, $\text{CNOT}|x, y\rangle = |x, x \oplus y\rangle$ CNOT is the only non-trivial 2-qubit reversible logic gate. Note that CNOT is unitary since obviously $\text{CNOT} = \text{CNOT}^\dagger$ (which you can show using its dyadic representation or its matrix representation, Ex. III.21, p. 194). See the right

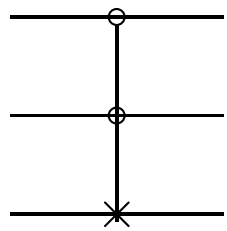

Figure III.10: Diagram for CCNOT or Toffoli gate [fig. from Nielsen & Chuang (2010)]. Sometimes the $\times$ is replaced by $\oplus$ because $\mathrm{CCNOT}|xyz\rangle = |x, y, xy \oplus z\rangle$.

panel of Fig. III.9 (p. 104) for the matrix and note the diagram notation for CNOT.

CNOT can be used to produce an entangled state:

$$\mathrm{CNOT}\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]|0\rangle = \mathrm{CNOT}\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\beta_{00}\rangle.$$

Note also that $\mathrm{CNOT}|x, 0\rangle = |x, x\rangle$, that is, FAN-OUT, which would seem to violate the No-cloning Theorem, but it works as expected only for $x \in \mathbf{2}$. In general $\mathrm{CNOT}|\psi\rangle|0\rangle \neq |\psi\rangle|\psi\rangle$ (Exer. III.22).

Another useful gate is the three-input/output *Toffoli gate* or *controlled-controlled-NOT*. It negates the third qubit if and only if the first two qubits are both 1. For $x, y, z \in \mathbf{2}$,

$$\begin{aligned} \mathrm{CCNOT}|1, 1, z\rangle &\stackrel{\text{def}}{=} |1, 1, \neg z\rangle, \\ \mathrm{CCNOT}|x, y, z\rangle &\stackrel{\text{def}}{=} |x, y, z\rangle, \quad \text{otherwise.} \end{aligned}$$

That is, $\mathrm{CCNOT}|x, y, z\rangle = |x, y, xy \oplus z\rangle$. All the Boolean operations can be implemented (reversibly!) by using Toffoli gates (Exer. III.25). For example, $\mathrm{CCNOT}|x, y, 0\rangle = |x, y, x \wedge y\rangle$. Thus it is a universal gate for quantum logic.

In Jan. 2009 CCNOT was implemented successfully using trapped ions.[5]

[5] Monz, T.; Kim, K.; Hänsel, W.; Riebe, M.; Villar, A. S.; Schindler, P.; Chwalla, M.; Hennrich, M. et al. (Jan 2009). "Realization of the Quantum Toffoli Gate with Trapped Ions." *Phys. Rev. Lett.* **102** (4): 040501. `arXiv:0804.0082`.

C.2.c Walsh-Hadamard transformation

Recall that the sign basis is defined $|+\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The *Hadamard transformation* or *gate* is defined:

$$H|0\rangle \stackrel{\text{def}}{=} |+\rangle, \tag{III.14}$$

$$H|1\rangle \stackrel{\text{def}}{=} |-\rangle. \tag{III.15}$$

In sum-of-dyads form: $H \stackrel{\text{def}}{=} |+\rangle\langle 0| + |-\rangle\langle 1|$. In matrix form (with respect to the standard basis):

$$H \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{III.16}$$

Note that H is self-adjoint, $H^2 = I$ (since $H^\dagger = H$). H can be defined also in terms of the Pauli matrices: $H = (X + Z)/\sqrt{2}$ (Exer. III.33).

The H transform can be used to transform the computational basis into the sign basis and back (Exer. III.32):

$$\begin{aligned} H(a|0\rangle + b|1\rangle) &= a|+\rangle + b|-\rangle, \\ H(a|+\rangle + b|-\rangle) &= a|0\rangle + b|1\rangle. \end{aligned}$$

Alice and Bob could use this in quantum key distribution.

When applied to a $|0\rangle$, H generates an (equal-amplitude) superposition of the two bit-values, $H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. This is a useful way of generating a superposition of both possible input bits, and the Walsh transform, a tensor power of H, can be applied to a quantum register to generate a superposition of all possible register values. Consider the $n = 2$ case:

$$\begin{aligned} H^{\otimes 2}|\psi, \phi\rangle &= (H \otimes H)\,(|\psi\rangle \otimes |\phi\rangle) \\ &= (H|\psi\rangle) \otimes (H|\phi\rangle) \end{aligned}$$

In particular,

$$\begin{aligned} H^{\otimes 2}|00\rangle &= (H|0\rangle) \otimes (H|0\rangle) \\ &= |+\rangle^{\otimes 2} \\ &= \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^{\otimes 2} \\ &= \left(\frac{1}{\sqrt{2}}\right)^2 (|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle). \end{aligned}$$

Notice that this is an equal superposition of all possible values of the 2-qubit register. (I wrote the amplitude in a complicated way, $1/\sqrt{2^2}$, to help you see the general case.) In general,

$$\begin{aligned}
H^{\otimes n}|0\rangle^{\otimes n} &= \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)^{\otimes n} \\
&= \frac{1}{\sqrt{2^n}} \overbrace{(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle)}^{n} \\
&= \frac{1}{\sqrt{2^m}} (|00\ldots00\rangle + |00\ldots01\rangle + \cdots + |11\ldots11\rangle) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\mathbf{2}^n} |\mathbf{x}\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\mathbf{x}\rangle.
\end{aligned}$$

Note that "$2^n - 1$" represents a string of n 1-bits, and that $\mathbf{2} = \{0, 1\}$. Hence, $H^{\otimes n}|0\rangle^{\otimes n}$ generates an equal superposition of all the 2^n possible values of the n-qubit register. We often write $W_n = H^{\otimes n}$ for the Walsh transformation.

An linear operation applied to such a superposition state in effect applies the operation simultaneously to all 2^n possible input values. This is *exponential* quantum parallelism and suggests that quantum computation might be able to solve exponential problems much more efficiently than classical computers. To see this, suppose $U|x\rangle = |f(x)\rangle$. Then:

$$U(H^{\otimes n}|0\rangle^{\otimes n}) = U\left[\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle\right] = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} U|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |f(x)\rangle$$

This is a superposition of the function values $f(x)$ for all of the 2^n possible values of x; it is computed by one pass through the operator U.

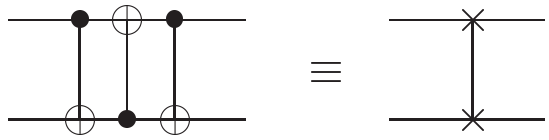

Figure III.11: Diagram for swap [from Nielsen & Chuang (2010)].

C.3 Quantum circuits

A *quantum circuit* is a sequential series of quantum transformations on a quantum register. The inputs are usually computational basis states (all $|0\rangle$ unless stated otherwise). *Quantum circuit diagrams* are drawn with time going from left to right, with the quantum gates crossing one or more "wires" (qubits) as appropriate. The circuit represents a sequence of unitary operations on a quantum register rather than physical wires.

These "circuits" are different in several respects from ordinary sequential logic circuits. First, loops (feedback) are not allowed, but you can apply transforms repeatedly. Second, Fan-In (equivalent to OR) is not allowed, since it it not reversible or unitary. Fan-Out is also not allowed, because it would violate the No-cloning Theorem. (N.B.: This does not contradict the universality of the Toffoli or Fredkin gates, which are universal only with respect to logical or classical states.)

Fig. III.9 (right) on page 104 shows the symbol for CNOT and its effect.

The swap operation is defined $|xy\rangle \mapsto |yx\rangle$, or explicitly

$$\text{SWAP} = \sum_{x,y\in\mathbf{2}} |yx\rangle\langle xy|.$$

We can put three CNOTs in series to swap two qubits (Exer. III.35). Swap has a special symbol as shown in Fig. III.11.

In general, any unitary operator U (on any number of qubits) can be conditionally controlled (see Fig. III.12); this is the quantum analogue of an if-then statement. If the control bit is 0, this operation does nothing, otherwise it does U. This is implemented by $|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes U$. Effectively, the *operators* are entangled.

Suppose the control bit is in superposition, $|\chi\rangle = a|0\rangle + b|1\rangle$. The effect

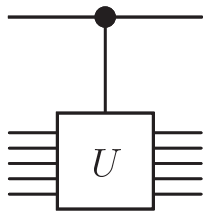

Figure 1.8. Controlled-U gate.

Figure III.12: Diagram for controlled-U [from Nielsen & Chuang (2010)].

of the conditional operation is:

$$\begin{aligned}
&(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U)|\chi, \psi\rangle \\
&\quad = (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U)(a|0\rangle + b|1\rangle) \otimes |\psi\rangle \\
&\quad = |0\rangle\langle 0|(a|0\rangle + b|1\rangle) \otimes I|\psi\rangle + |1\rangle\langle 1|(a|0\rangle + b|1\rangle) \otimes U|\psi\rangle \\
&\quad = a|0\rangle \otimes |\psi\rangle + b|1\rangle \otimes U|\psi\rangle \\
&\quad = a|0, \psi\rangle + b|1, U\psi\rangle.
\end{aligned}$$

The result is a superposition of entangled outputs. Notice that CNOT is a special case of this construction, a controlled X.

We also have a quantum analogue for an if-then-else construction. If U_0 and U_1 are unitary operators, then we can make the choice between them conditional on a control bit as follows:

$$|0\rangle\langle 0| \otimes U_0 + |1\rangle\langle 1| \otimes U_1.$$

For example,

$$\text{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X. \tag{III.17}$$

In quantum circuit diagrams, the symbol for the CCNOT gate is show in Fig. III.10, or with $\bullet$ for top two connections and $\oplus$ for bottom, suggesting $\text{CCNOT}|x, y, z\rangle = |x, y, xy \oplus z\rangle$. Alternately, put "CCNot" in a box. Other operations may be shown by putting a letter or symbol in a box, for example "H" for the Hadamard gate.

The Hadamard gate can be used to generate Bell states (Exer. III.34):

$$\text{CNOT}(H \otimes I)|xy\rangle = |\beta_{xy}\rangle. \tag{III.18}$$

In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$

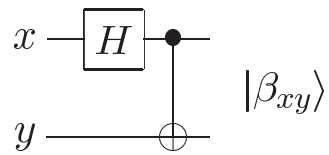

Figure III.13: Quantum circuit for generating Bell states. [from Nielsen & Chuang (2010, fig. 1.12)]

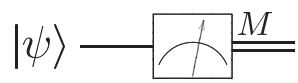

Figure III.14: Symbol for measurement of a quantum state (from Nielsen & Chuang (2010)).

The circuit for generating Bell states (Eq. III.18) is shown in Fig. III.13.

It's also convenient to have a symbol for quantum state measurement, such as Fig. III.14.

C.4 Quantum gate arrays

Fig. III.15 shows a quantum circuit for a 1-bit full adder. As we will see (Sec. C.7), it is possible to construct reversible quantum gates for any classically computable function. In particular the Fredkin and Toffoli gates are universal.

Because quantum computation is a unitary operator, it must be reversible. You know that an irreversible computation $x \mapsto f(x)$ can be embedded in a reversible computation $(x, c) \mapsto (g(x), f(x))$, where c are suitable ancillary constants and $g(x)$ represents the garbage qubits. Note that throwing away the garbage qubits (dumping them into the environment) will collapse the quantum state (equivalent to measurement) by entangling them in the many degrees of freedom of the environment. Typically these garbage qubits will be entangled with other qubits in the computation, collapsing them as well, and interfering with the computation. Therefore the garbage

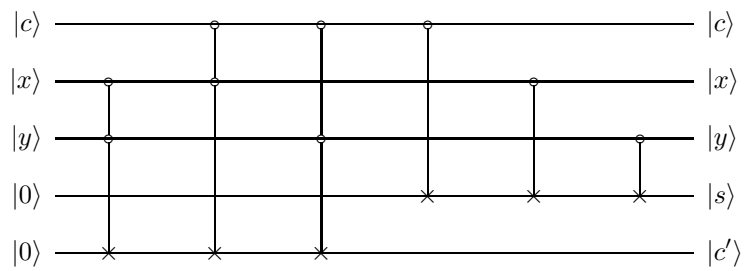

Figure III.15: Quantum circuit for 1-bit full adder [from Rieffel & Polak (2000)]. "x and y are the data bits, s is their sum (modulo 2), c is the incoming carry bit, and c' is the new carry bit."

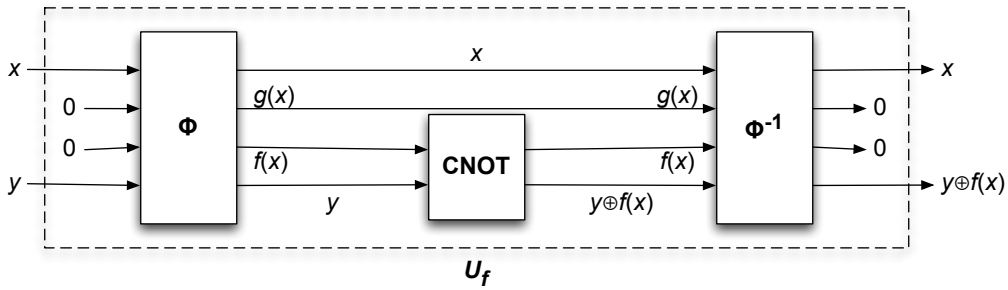

Figure III.16: Quantum gate array for reversible quantum computation.

must be produced in a *standard state* independent of x. This is accomplished by uncomputing, as we did in classical reversible computing (Ch. II, Sec. C.6, p. 57).

Since NOT is reversible, each 1 bit in c can be replaced by a 0 bit followed by a NOT, so we need only consider computations of the form $(x, 0) \mapsto (g(x), f(x))$; that is, all the constant bits can be zero.

Therefore, we begin by embedding our irreversible computation of f in a reversible computation Φ, which we get by providing 0 constants and generating garbage $g(x)$; see Fig. III.16. That is, Φ will perform the following computation on four registers (*data, workspace, result, target*):

$$(x, 0, 0, y) \mapsto (x, g(x), f(x), y).$$

The result $f(x)$ is in the result register and the garbage $g(x)$ is in the workspace register. Notice that x and y (data and target) are passed through. Now use CNOTs between corresponding places in the result and target registers to compute $y \oplus f(x)$, where $\oplus$ represents bitwise exclusive-or, in the target register. Thus we have computed:

$$(x, 0, 0, y) \mapsto (x, g(x), f(x), y \oplus f(x)).$$

Now we uncompute with Φ^{-1}, but since the data and target registers are passed through, we get $(x, 0, 0, y \oplus f(x))$ in the registers. We have restored the data, workspace, and result registers to their initial values and have $y \oplus f(x)$ in the target register. Ignoring the result and workspace registers, we write

$$(x, y) \mapsto (x, y \oplus f(x)).$$

This is the standard approach we will use for embedding a classical computation in a quantum computation.

Therefore, for any computable $f : \mathbf{2}^m \to \mathbf{2}^n$, there is a reversible *quantum gate array* $U_f : \mathcal{H}^{m+n} \to \mathcal{H}^{m+n}$ such that for $x \in \mathbf{2}^m$ and $y \in \mathbf{2}^n$,

$$U_f|x, y\rangle = |x, y \oplus f(x)\rangle,$$

See Fig. III.17. In particular, $U_f|x, \mathbf{0}\rangle = |x, f(x)\rangle$. The first m qubits are called the *data register* and the last n are called the *target register*.

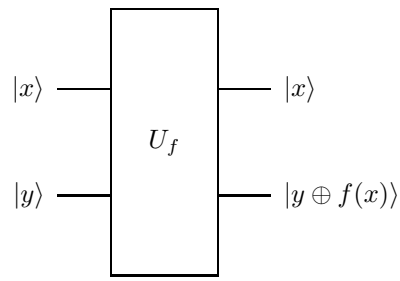

Figure III.17: Computation of function by quantum gate array (Rieffel & Polak, 2000).

C.5 Quantum parallelism

Since U_f is linear, if it is applied to a superposition of bit strings, it will produce a superposition of the results of applying f to them in parallel (i.e., in the same time it takes to compute it on one input):

$$U_f(c_1|\mathbf{x}_1\rangle + c_2|\mathbf{x}_2\rangle + \cdots + c_k|\mathbf{x}_k\rangle) = c_1 U_f|\mathbf{x}_1\rangle + c_2 U_f|\mathbf{x}_2\rangle + \cdots + c_k U_f|\mathbf{x}_k\rangle.$$

For example, if we have a superposition of the inputs $\mathbf{x}_1$ and $\mathbf{x}_2$,

$$U_f\left(\frac{\sqrt{3}}{2}|\mathbf{x}_1\rangle + \frac{1}{2}|\mathbf{x}_2\rangle\right) \otimes |\mathbf{0}\rangle = \frac{\sqrt{3}}{2}|\mathbf{x}_1, f(\mathbf{x}_1)\rangle + \frac{1}{2}|\mathbf{x}_2, f(\mathbf{x}_2)\rangle.$$

The amplitude of a result y will be the sum of the amplitudes of all x such that $y = f(x)$.

If we apply U_f to a superposition of all possible 2^m inputs, it will compute a superposition of all the corresponding outputs *in parallel* (i.e., in the same time as required for one function evaluation)! The Walsh-Hadamard transformation can be used to produce this superposition of all possible inputs:

$$\begin{aligned} W_m|00\ldots0\rangle &= \frac{1}{\sqrt{2^m}}\left(|00\ldots0\rangle + |00\ldots1\rangle + \cdots + |11\ldots1\rangle\right) \\ &= \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x}\in\mathbf{2}^m} |\mathbf{x}\rangle \\ &= \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle. \end{aligned}$$

In the last line we are obviously interpreting the bit strings as natural numbers. Hence,

$$U_f W_m|\mathbf{0}\rangle = U_f\left(\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x,0\rangle\right) = \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}U_f|x,0\rangle = \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x,f(x)\rangle.$$

A single circuit does all 2^m computations simultaneously! "Note that since n qubits enable working simultaneously with 2^n states, quantum parallelism circumvents the time/space trade-off of classical parallelism through its ability to provide an exponential amount of computational space in a linear amount of physical space." (Rieffel & Polak, 2000)

This is amazing, but not immediately useful. If we measure the input bits, we will get a random value, and the state will be projected into a superposition of the outputs for the inputs we measured. If we measure an output bit, we will get a value probabilistically, and a superposition of all the inputs that can produce the measured output. Neither of the above is especially useful, so most quantum algorithms transform the state in such a way that the values of interest have a high probability of being measured. The other thing we can do is to extract common properties of all values of $f(x)$. Both of these require different programming techniques than classical computing.

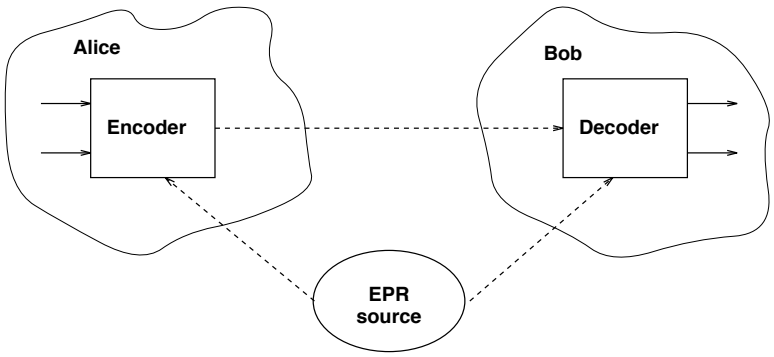

Figure III.18: Superdense coding. (Rieffel & Polak, 2000)

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

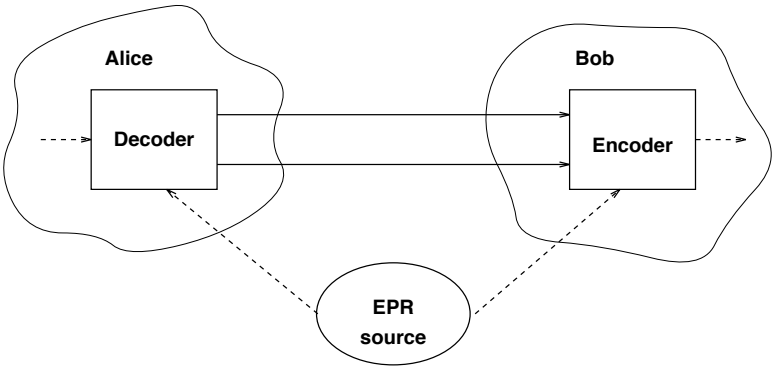

Figure III.19: Quantum teleportation. (Rieffel & Polak, 2000)

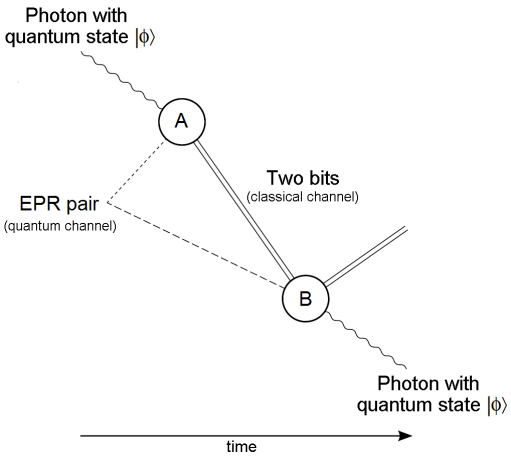

Figure III.20: Possible setup for quantum teleportation. [from wikipedia commons]

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 (leaving Bob's qubit alone) the resulting composite state is:

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

Notice that the amplitude a of $|\psi\rangle$ has been transferred to the components of the shared pair having the same parity ($|00\rangle$ and $|11\rangle$), whereas the amplitude b has been transferred to the components having the opposite parity ($|10\rangle$ and $|01\rangle$). When Alice applies $H \otimes I$ to her qubits the result is:

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

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 to separate Alice's qubits from Bob's, we have:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2}\left[|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle)\right. \\ &\quad \left. +|10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)\right]. \end{aligned}$$

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 qubits. In fact you can see that the amplitudes are transformed by the Pauli matrices, and Bob can restore the quantum state by applying the correct Pauli matrix. 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, which includes 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 with an entangled pair, two bits can be interchanged with one qubit. This is one example of a method of *interchanging resources*. However, quantum teleportation does

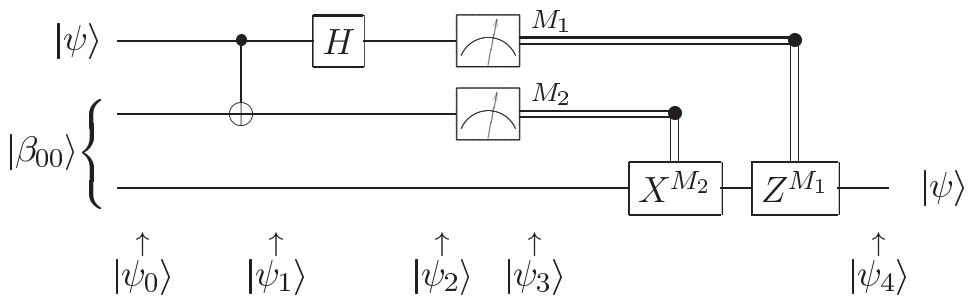

Figure III.21: Circuit for quantum teleportation. [from Nielsen & Chuang (2010)]

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 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

[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).

defined:

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

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

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