The Toffoli Gate

The Toffoli gate, invented by Tommaso Toffoli, has three inputs and three outputs. The first two inputs are control bits. They flip the third bit if they are both 1, otherwise the third bit remains the same. Since this gate is like the *CNOT* gate, but has two control bits, it is sometimes called a *CCNOT* gate. The function describing what this gate does is: $T(x,y,z) = (x,y,(x \wedge y) \oplus z)$.

This can also be given in tabular form.

Toffoli gate

Input			Output		
x	y	z	x	y	$(x \wedge y) \oplus z)$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

The standard diagram for this gate comes from the diagram of the *CNOT* gate (figure 6.14).

We can see from the table that the Toffoli gate is invertible—each triple of output values corresponds to exactly one triple of input values. Like the *CNOT* gate, this gate also has the property that it is its own inverse.

We know that $T(x,y,z) = (x,y,(x \wedge y) \oplus z)$. Now, using the output as the new input and applying T again gives:

$$T(x,y,(x \wedge y) \oplus z) = (x,y,(x \wedge y) \oplus (x \wedge y) \oplus z) = (x,y,z).$$

Here we use the facts that $(x \wedge y) \oplus (x \wedge y) = 0$ and $0 \oplus z = z$.

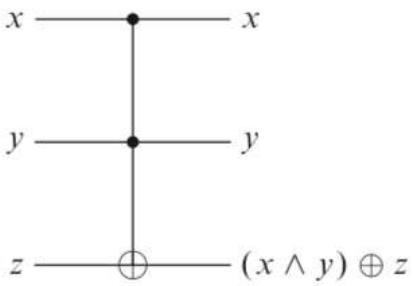

Figure 6.14
Toffoli gate.

The Toffoli gate is also universal. Recall that we can construct any boolean circuit using just *NAND* gates and fan-outs. To show that the Toffoli gate is universal, it is enough if we can show how to use it to compute both of these.

The *NAND* gate is described by $f(x,y) = \neg(x \wedge y)$, so we want a way of inputting x and y and getting an output of $\neg(x \wedge y)$. Since we are using the Toffoli gate, we will be inputting three values and getting an output of three values. Now $\neg(x \wedge y)$ is logically equivalent to $(x \wedge y) \oplus 1$. We can choose the third input value to always be 1, and we can ignore extra output values. We use

$$T(x,y,1) = (x,y,(x \wedge y) \oplus 1) = (x,y,\neg(x \wedge y))$$

to show that we can emulate the *NAND* gate by inputting x and y and reading off the third entry of the output.

We can use a similar idea for fan-out. We want to input just one value x and receive two outputs that are both x. Again, the Toffoli gate has three inputs and three outputs. We can choose the two other inputs apart from x to be fixed and as long as we get xs for two of the outputs we can ignore the third. This can be done by

$$T(x,1,0) = (x,1,x).$$

Consequently, any boolean circuit can be constructed using just Toffoli gates.

These constructions illustrate something that often arises when we use reversible gates. The number of inputs must equal the number of outputs, but often we want to compute things where the number of inputs and outputs differ. We can always do this by adding extra bits, often called ancilla bits, to the inputs, or by ignoring bits that are output. Output bits that are