Chapter 2

Computational Complexity

2.4 Landauer's Principle

Landauer, an IBM scientist, stated in 1960's the principle that energy is consumed in a computation only as a result of irreversible operations. The Landauer principle states that for every bit erased, at least $kT \ln 2$ units of energy dissipated into the environment, where T is the temperature of the environment. An equivalent statement is that the entropy of the environment increases by at least $k \ln 2$ units for every bit erased.

This principle naturally gives rise to the question: Can computation be carried out reversibly? It turns out reversible computation is possible using classical and also quantum circuits. We consider in this section classical reversible computation.

First, note that reversible gates must have the same number of inputs and outputs. There are altogether $(2^{2^n})^n$ gates from n bits to n bits. Of these, $(2^n)!$ are reversible.

For $n = 1$, the number of all gates is 4; and 2 are reversible. The NOT gate is the only non-trivial one-bit reversible gate.

For $n = 2$, there are 256 gates; 24 are reversible. All two-bit reversible gates turn out to be linear:

$$\begin{pmatrix} x \\ y \end{pmatrix} \to M \begin{pmatrix} x \\ y \end{pmatrix} \oplus \begin{pmatrix} a \\ b \end{pmatrix}$$

where M is one of the 6 matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

and $(a, b)^T$ is one of

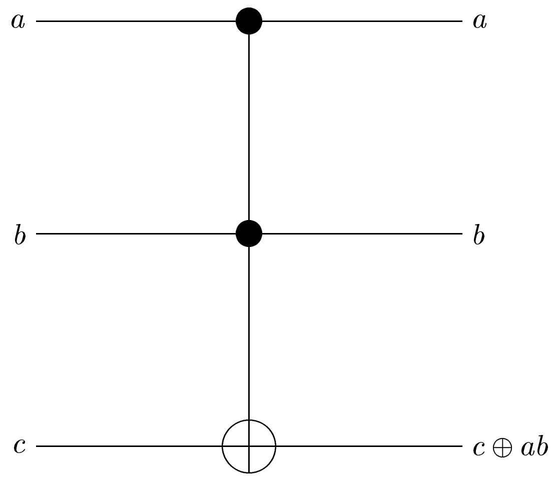
$$\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Using combinations of 1 and 2 bit reversible gates, we can only compute linear functions. So, unlike reversible computation, there is no universal set of gates using only 2 bit inputs.

2.4.1 The Toffoli Gate

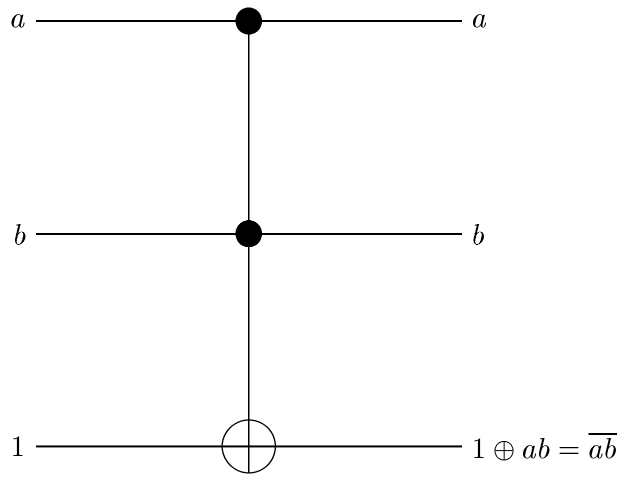
The Toffoli gate is a 3-bit to 3-bit gate defined by the following truth table.

Inputs			Outputs		
a	b	c	a'	b'	c'
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

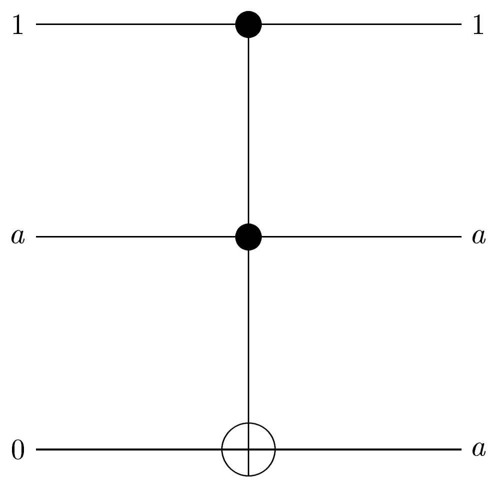


The Toffoli gate is reversible and nonlinear. It is also a universal gate for reversible computation. We can synthesize the NAND and COPY operations using the Toffoli gate as follows.

NAND



COPY



2.4.2 Garbage Bits and Cleaning Up

Reversible computation of a function $x \to f(x)$ generates some garbage bits $g(x)$:

$$(x, 0, 0) \to (x, f(x), g(x))$$

It is desirable to set these garbage bits back to 0 without destroying reversibility. Leaving garbage around in quantum computation may destroy coherence.

For safe-storage of result, we need another register, whose content y is arbitrary:

$$\begin{aligned} (x, 0, 0, y) &\to (x, f(x), g(x), y) \\ &\to (x, f(x), g(x), y \oplus f(x)) \\ &\to (x, 0, 0, y \oplus f(x)) \end{aligned}$$

Copying of $f(x)$ to the y register can be carried out by using CNOT gates. The *uncomputation* step can be carried out by simply running the reversible computation backwards.

We write

$$(x, y) \to (x, y \oplus f(x))$$

to denote such a composite operation. It is implicitly assumed that any garbage bits that may have been generated have been cleaned up.

2.5 Quantum Circuits

We begin by recalling that for a single qubit system we use the notation $|0\rangle$, $|1\rangle$ to denote the measurement (instrumentation) basis.

For two qubits, the state-space is 4 dimensional

$$\begin{aligned} |0\rangle &= |00\rangle = |0\rangle \otimes |0\rangle \\ |1\rangle &= |01\rangle = |0\rangle \otimes |1\rangle \\ |2\rangle &= |10\rangle = |1\rangle \otimes |0\rangle \\ |3\rangle &= |11\rangle = |1\rangle \otimes |1\rangle \end{aligned}$$

For n qubits, the state-space is 2^n dimensional with basis vectors

$$|i\rangle = |i_1 i_2 \cdots i_n\rangle = |i_1\rangle \otimes \cdots \otimes |i_n\rangle$$

where $0 \le i \le 2^n - 1$ is an integer and

$$i = 2^{n-1} i_1 + 2^{n-2} i_2 + \cdots + i_n$$

General state expansion in measurement basis:

$$|\Psi\rangle = \sum_{i=0}^{2^n - 1} a_i |i\rangle$$

where $\sum_i |a_i|^2 = 1$.

2.5.1 Single Qubit Gates

We give here a number of single-qubit gates which will serve as building blocks of larger gates.

The NOT gate or bit-flip operator X is defined by

$$\begin{aligned} X|0\rangle &= |1\rangle \\ X|1\rangle &= |0\rangle \end{aligned}$$

Matrix representation of X in the measurement basis is as follows

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The first row and first column correspond to basis vector $|0\rangle$, the second row and column to $|1\rangle$. For operators on n qubits we label the rows and columns beginning with $|0^n\angle$ and ending with $|1^n\rangle$ in alphabetical order.

As any quantum operator X acts linearly:

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle$$

In matrix notation,

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}.$$

The X operator together with the Y and Z operators defined next are known as Pauli operators.

Bit and Phase Flip:

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Phase Flip:

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

The following properties of the Pauli operators will be used in the sequel.

- $X^2 = Y^2 = Z^2 = I$.
- $XY = iZ$, $YZ = iX$, $ZX = iY$.
- $YX = -iZ$, $ZY = -iX$, $XZ = -iY$.
- $XYX = -X$, $YZY = -Z$, $ZXZ = -X$

Three other often used single-qubit operators are defined next.
Hadamard gate:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Phase gate:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

$\pi/8$ gate:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

A very useful set of operators are the *rotation* operators defined in terms of the Pauli operators.

$$\begin{aligned} R_x(\theta) &= e^{-i\theta X/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} X \\ &= \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \end{aligned}$$

$$\begin{aligned} R_y(\theta) &= e^{-i\theta Y/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y \\ &= \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \end{aligned}$$

$$\begin{aligned} R_z(\theta) &= e^{-i\theta Z/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Z \\ &= \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix} \end{aligned}$$

Some properties of the rotation operators are as follows.

- $R_x(\theta)R_x(-theta) = I$, and similarly for R_y and R_z.
- $XR_y(\theta)X = R_y(-\theta)$, and similarly for other combinations.

2.5.2 $Z - Y$ Decomposition of Single Qubit Operators

Theorem 1 *Any single qubit operator U can be expressed in the form*

$$
\begin{aligned}
U &= e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) \\
&= e^{i\alpha} \begin{bmatrix} e^{-i(\beta+\delta)/2}\cos(\gamma/2) & -e^{-i(\beta-\delta)/2}\sin(\gamma/2) \\ e^{i(\beta-\delta)/2}\sin(\gamma/2) & e^{i(\beta+\delta)/2}\cos(\gamma/2) \end{bmatrix}
\end{aligned}
$$

Proof. Exercise.

As a corollary we have the following very useful decomposition.

Corollary 1 *For any unitary single qubit operator U, there exist unitary A, B, C such that $ABC = I$ and $U = e^{i\alpha} AXBXC$.*

Proof. Let $U = e^{\imath\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$ and define

$$A = R_z(\beta) R_y(\gamma/2),$$

$$B = R_y(-\gamma/2) R_z(-(\delta+\beta)/2),$$

$$C = R_z((\delta-\beta)/2).$$

It is easily verified that

$$ABC = I.$$

Using the facts that $X^2 = I$,

$$XYX = -Y, \;\; XZX = -Z$$

or

$$XR_y(\theta)X = R_y(-\theta), \;\; XR_z(\theta)X = R_z(-\theta),$$

we get

$$
\begin{aligned}
XBX &= XR_y(-\gamma/2)XXR_z(-(\delta+\beta)/2)X \\
&= R_y(\gamma/2)R_z((\delta+\beta)/2).
\end{aligned}
$$

Using this, we have

$$AXBXC = R_z(\beta)R_y(\gamma)R_z(\delta).$$

2.5.3 Two-Qubit Gates

A two-qubit gate is the controlled-NOT gate, CNOT for short, which acts as follows.

$$|00\rangle \to |00\rangle;\ |01\rangle \to |01\rangle;\ |10\rangle \to |11\rangle;\ |11\rangle \to |10\rangle$$

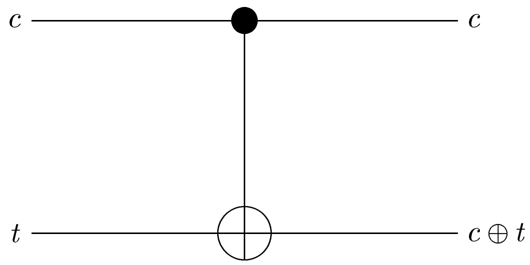
$$|c, t\rangle \to |c, c \oplus t\rangle$$

Qubit c is called the control qubit.

CNOT in matrix form:

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

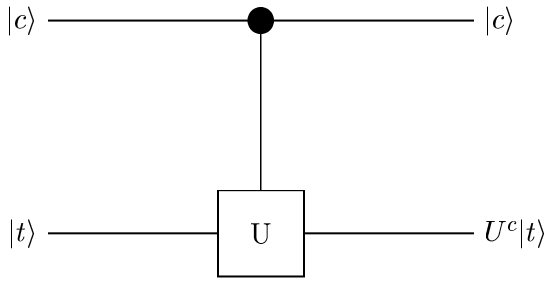
The circuit diagram for CNOT is shown below.



For an arbitrary single-qubit operation U, the controlled-U is defined by

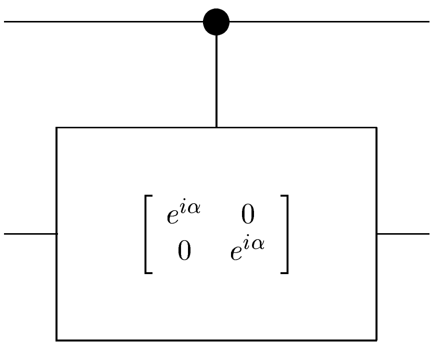
$$|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle.$$

Thus, if $|c\rangle = |0\rangle$, the target qubit $|t\rangle$ is unaltered. If $|c\rangle = |1\rangle$, the target undergoes the operation U.

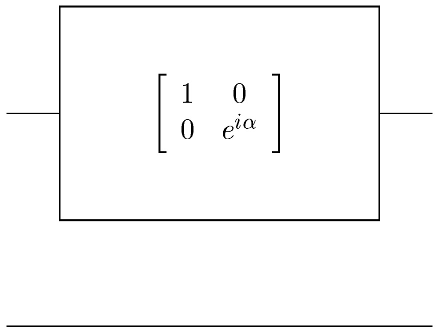


An often encountered operation is the controlled-phase operation:

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow e^{i\alpha}|10\rangle \\ |11\rangle &\rightarrow e^{i\alpha}|11\rangle \end{aligned}$$

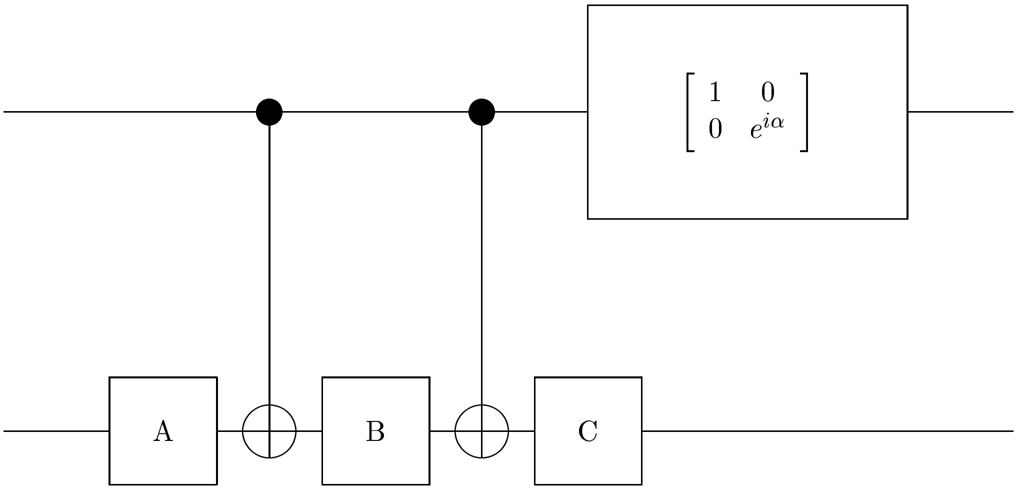


It is noteworthy that an equivalent circuit for controlled-phase operation is the following simpler circuit.



Theorem 2 *For any single-qubit operator U, the controlled-U operation $C(U)$ can be implemented using only single-qubit operators and CNOT gates.*

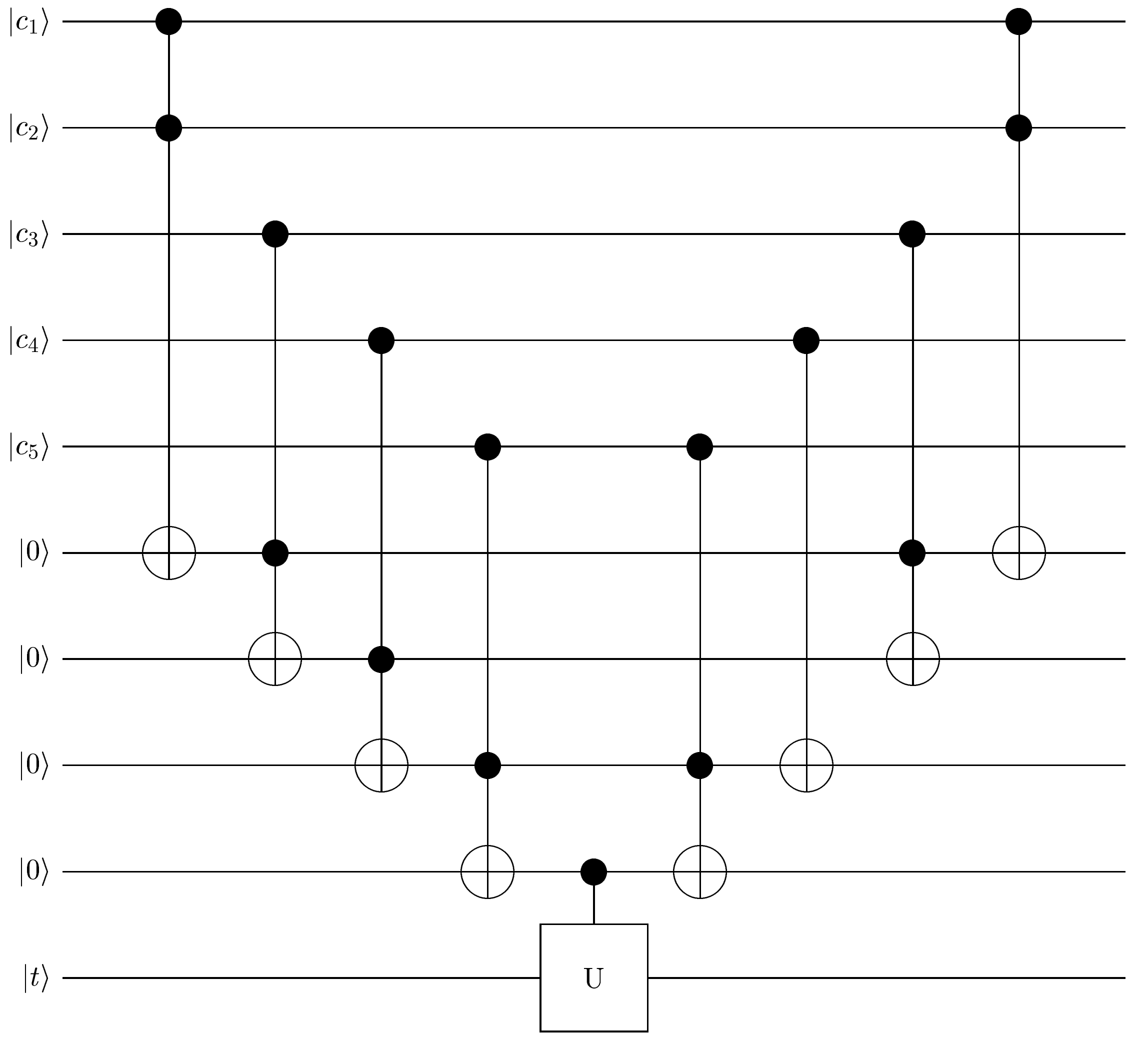
Proof. Using the $U = e^{i\alpha}AXBXC$ decomposition, $C(U)$ can be implemented as shown in the figure below. Recall that $ABC = I$.



Finally, we show how to implement $C^n(U)$, the controlled-U operation using n control qubits.

Theorem 3 *For any single-qubit operator U, $C^n(U)$ can be implemented using only single qubit gates and CNOT gates.*

Proof. The proof is by construction. For $n = 5$, an implementation satisfying the claim is given below. Recall that by the previous theorem $C(U)$ can be implemented using only CNOT and single-qubit gates.


$|c_1\rangle$
$|c_2\rangle$
$|c_3\rangle$
$|c_4\rangle$
$|c_5\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|t\rangle$
U