Landauer's Principle

Only irreversible operations consume energy. For every bit erased, $kT \ln 2$ units of energy dissipated into the environment. Equivalently, the entropy of the environment increases by $k \ln 2$ units.

Reversible computation does not use up energy.

Reversible computation is possible using classical circuits.

Quantum computation is reversible until the time of measurement.

Classical Reversible Circuits

Reversible gates must have the same number of inputs and outputs.

There are $(2^{2^n})^n$ gates from n bits to n bits.

The number of reversible n-bit gates is $(2^n)!$.

For $n = 1$, the number of all gates is 4; 2 are reversible.

The NOT gate is the only non-trivial one-bit reversible gate.

Two-Bit Reversible Circuits

For $n = 2$, there are 256 gates; 24 are reversible.

All two-bit reversible gates are 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

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

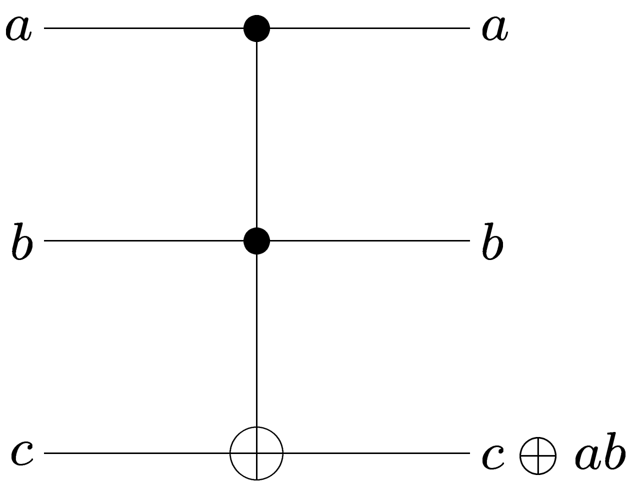
$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

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

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

The Toffoli Gate

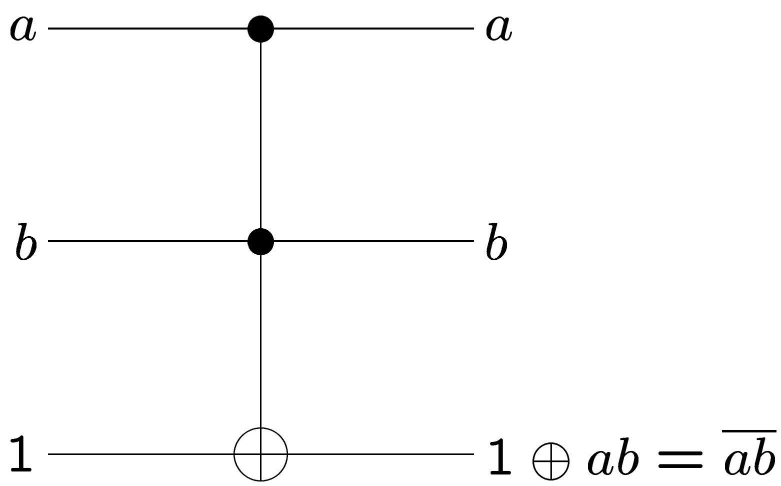
Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



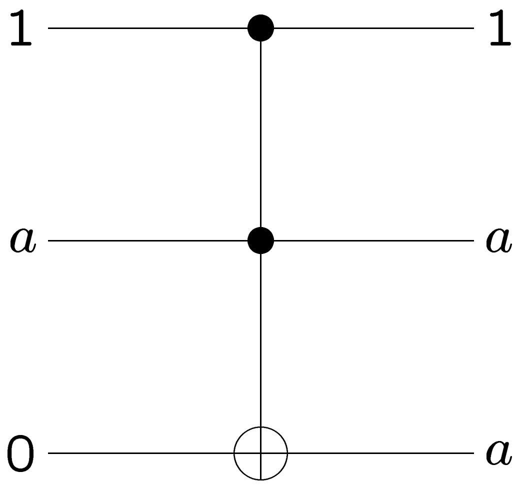
Reversible. Nonlinear, hence cannot be synthesized by 2-bit reversible gates, which are linear.

Universality of the Toffoli Gate

NAND



COPY



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, need another register, whose content y is arbitrary:

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

We write

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

to denote such a composite operation.

Quantum Gates

Recall that for single qubit $|0\rangle$, $|1\rangle$ are the measurement 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, 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 $0 \leq i \leq 2^n - 1$ 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 $\sum_i |a_i|^2 = 1$.

Single Qubit Gates

NOT or Bit-Flip operator X

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

Matrix representation of in the measurement basis

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

Linearity:

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

In matrix notation,

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

Pauli Matrices

Bit Flip:

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

Bit and Phase Flip:

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

Phase Flip:

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

Some Other Single Qubit Gates

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:

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

Rotation Operators

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

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

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

$Z - Y$ Decomposition

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.

A Useful Decomposition

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 $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$ 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

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

Controlled–NOT

CNOT is a two-qubit gate:

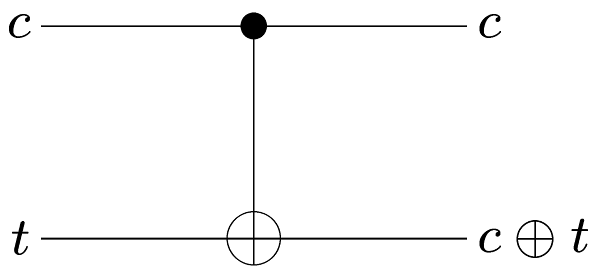
$|00\rangle \to |00\rangle$; $|01\rangle \to |01\rangle$; $|10\rangle \to |11\rangle$; $|11\rangle \to |10\rangle$

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

Qubit c is called the control qubit.

CNOT in matrix form:

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

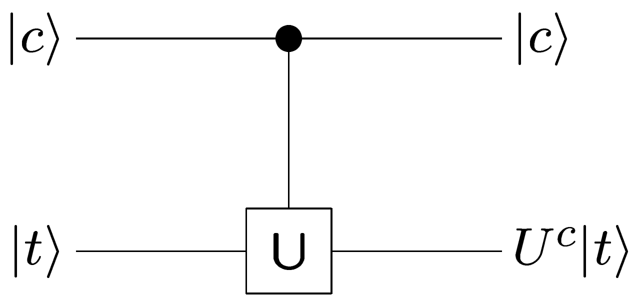


Contolled-U

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

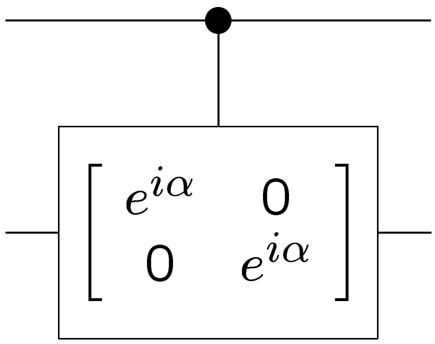
$$|c\rangle|t\rangle \to |c\rangle U^c|t\rangle.$$

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

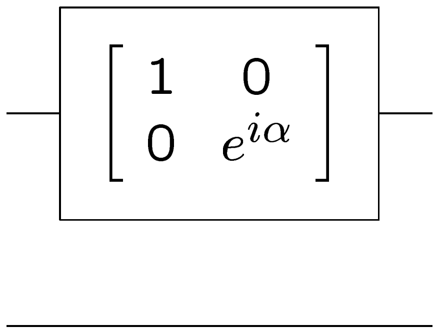


Controlled Phase

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

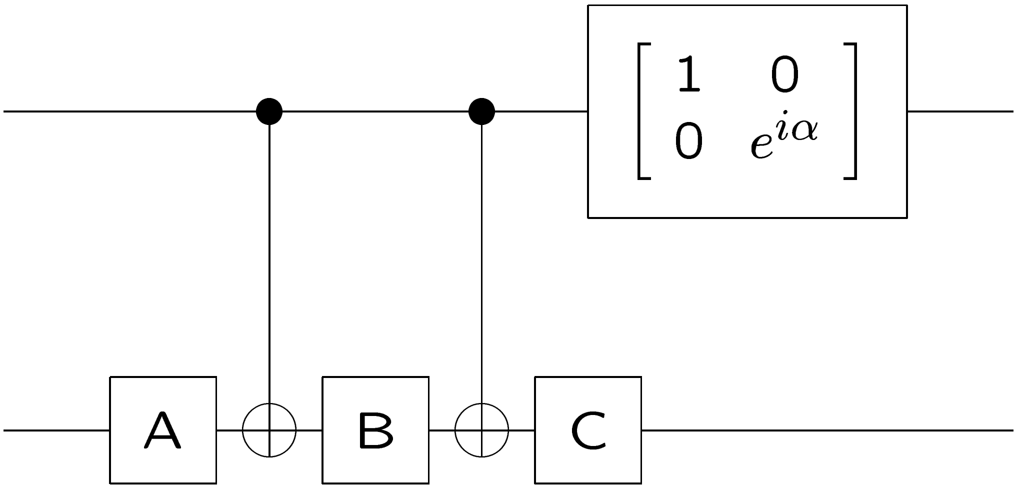


An equivalent circuit:



Controlled-U Implementation

Using the $U = e^{i\alpha} AXBXC$ decomposition, $C-U$ can be implemented as follows. Recall that $ABC = I$.



Multiple Contols

$C^n(U)$ with n controls may be implemented using CNOT and $C(U)$ gates, as illustrated for $n = 5$ below.