Chapter 5: Complete set of quantum gates

Arbitrary quantum gates acting on any number of qubits can be constructed (approximated to arbitrary precision) from a small number of one-and two-bit gates.

Single-qubit gates

General single-qubit state is a point on the Bloch sphere

$$|\theta, \varphi\rangle = \exp\left(-i\frac{\varphi}{2}\right)\cos\frac{\theta}{2}|\uparrow\rangle + \exp\left(i\frac{\varphi}{2}\right)\sin\frac{\theta}{2}|\downarrow\rangle \qquad (0 \le \theta \le \pi; 0 \le \varphi \le 2\pi).$$

General single-qubit gate $\mathbf{U}|\theta, \varphi\rangle = |\theta', \varphi'\rangle$ is a rotation about an arbitrary axis.

Experimentalists do not like arbitrary axes!

Decomposition into products of rotations about a small number of different axes is possible, at least approximately. Precision depends on the number of factors in the product,

- The $\frac{\pi}{8}$ gate:

$$\mathbf{T} = \begin{pmatrix} 1 & 0 \\ 0 & \exp i\frac{\pi}{4} \end{pmatrix} = \exp i\frac{\pi}{8} \begin{pmatrix} \exp -i\frac{\pi}{8} & 0 \\ 0 & \exp i\frac{\pi}{8} \end{pmatrix} = \exp\left(i\frac{\pi}{8}\right) \exp\left(-i\frac{\pi}{8}\mathbf{Z}\right)$$

$$\mathbf{S} = \mathbf{T}^2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad \mathbf{S}^2 = \mathbf{Z}$$

- The NOT and $\sqrt{\text{NOT}}$ gates:

$$\exp(i\phi\mathbf{X}) = \mathbf{1}\cos\phi + i\mathbf{X}\sin\phi = \begin{pmatrix} \cos\phi & i\sin\phi \\ i\sin\phi & \cos\phi \end{pmatrix}$$

$\sim$ NOT for $\phi = \frac{\pi}{2}$; $\sim \sqrt{\text{NOT}}$ for $\phi = \frac{\pi}{4}$.

- The Hadamard gate (Jacques Salomon Hadamard, 1865-1963)

$$\mathbf{H} = \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Z}) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

$$\mathbf{H}|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\downarrow\rangle + |\uparrow\rangle); \quad \mathbf{H}|\downarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle)$$

Basis states $\rightarrow$ symmetric and antisymmetric linear combinations.

Is a very efficient tool for creating entangled states $\rightarrow$ quantum algorithms.

$\mathbf{H}^2 = \mathbf{1} \Rightarrow \mathbf{H}$ is unitary $\Rightarrow \mathbf{H}$ is a rotation. Axis?

- The Hadamard gate (Jacques Salomon Hadamard, 1865-1963)

$$\mathbf{H} = \frac{1}{\sqrt{2}}(\mathbf{X}+\mathbf{Z}) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

$$\mathbf{H}|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\downarrow\rangle + |\uparrow\rangle); \quad \mathbf{H}|\downarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle)$$

Basis states $\rightarrow$ symmetric and antisymmetric linear combinations.

Is a very efficient tool for creating entangled states $\rightarrow$ quantum algorithms.

$\mathbf{H}^2 = \mathbf{1} \Rightarrow \mathbf{H}$ is unitary $\Rightarrow \mathbf{H}$ is a rotation. Axis?

Every single qubit operation can be approximated to arbitrary precision using only the $\frac{\pi}{8}$ and (square root of) Hadamard gates.

Two-qubit gates

- The CNOT gate (controlled not) flips the target qubit when the control qubit is 1.

As a truth table:

control-qubit	target-qubit	result
0	0	00
0	1	01
1	0	11
1	1	10

In matrix notation with respect to the usual computational basis $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{X} \end{pmatrix}$$

Note that $\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the single-qubit NOT gate.

The CNOT gate and the single-qubit gates discussed above suffice to perform any unitary operation on a finite number of qubits.

Universal set of gates

Three steps of the proof:

1. Two-level gates are universal. Any $d \times d$ unitary matrix $\mathbf{U}$ can be written (exactly) as a product of $\frac{d(d-1)}{2}$ two level unitary matrices (affecting only two vector components).

2. CNOT and single-qubit gates are universal. Any two-level matrix can be expressed (exactly) by these building blocks.

3. Single-qubit gates can be approximated using $\mathbf{H}^{\frac{1}{2}}$ and $\frac{\pi}{8}$ gates.

$$\mathbf{H}_{\pm}^{\frac{1}{2}} = \frac{\exp \mp i\frac{\pi}{4}}{\sqrt{2}}(\mathbf{1} \pm i\mathbf{H}) = \mathbf{H}_{\pm}^{-\frac{1}{2}}$$

Be careful:

$$\mathbf{H} = \mathbf{H}^{-1} \Rightarrow \mathbf{H}^{\frac{1}{2}} = \left(\mathbf{H}^{-1}\right)^{\frac{1}{2}}$$

and so

$$\mathbf{H}^{-\frac{1}{2}} \neq \left(\mathbf{H}^{\frac{1}{2}}\right)^{-1} \text{ since } \mathbf{H}^{-\frac{1}{2}}\mathbf{H}^{\frac{1}{2}} = \mathbf{H}.$$

The true inverse is obtained from

$$\mathbf{H}_{+}^{\frac{1}{2}}\mathbf{H}_{-}^{-\frac{1}{2}} = \mathbf{1}$$

Step 2 of the proof: constructing two-level gates

Rearrange the computational basis such that the two levels of interest are the basis states of one qubit, apply arbitrary single-qubit operation, rearrange the basis back to original order.

Step 2 of the proof: constructing two-level gates

Rearrange the computational basis such that the two levels of interest are the basis states of one qubit, apply arbitrary single-qubit operation, rearrange the basis back to original order.

Example: How to achieve operation $\mathbf{U}$ between basis vectors $|ABC\rangle = |000\rangle$ and $|111\rangle$:

- Apply the Toffoli gate $\theta^{(3)}$ (CCNOT):
  $\theta^{(3)}(\text{NOT}A, \text{NOT } B, C)$: $|000\rangle \leftrightarrow |001\rangle$; all other states unaffected.

- $\theta^{(3)}(\text{NOT}A, C, B)$: $|001\rangle \leftrightarrow |011\rangle$; all other states unaffected.

- Apply $\text{C}^2\mathbf{U}$ to A, with B and C as control qubits.
  $\mathbf{U}$ thus acts only on the first qubit of $|011\rangle$ and $|111\rangle$ as desired.

- Reshuffle to original order.

All controlled or doubly controlled gates can be built using CNOT.