Chapter 4
Circuit model for quantum computation

In quantum computation, the basic ingredients are qubits and gates. The composition of different gates acting on a series of qubits is what we called an algorithm. Here we introduce quantum gates and some algorithms.

4.1 Qubit gates

The single qubit algebra can be described in terms of the identity $\hat{\mathbb{1}}$ and Pauli $\hat{\sigma}_x$, $\hat{\sigma}_y$ and $\hat{\sigma}_z$ operators. All single qubit gates are a linear composition of these. In particular, they can be visualised as rotations of the state $|\psi\rangle$ on the Bloch sphere. The three elementary rotations by an angle θ around the Cartesian axes are defined as $\hat{R}^j(\theta) = e^{-i\theta\hat{\sigma}_j/2}$ for $j = x, y, z$. In particular, in the computational basis, which is the one mainly used in quantum computation, one has

$$R^x(\theta) = \begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix},$$
$$R^y(\theta) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}, \tag{4.1}$$
$$R^z(\theta) = \begin{pmatrix} \exp(-i\theta/2) & 0 \\ 0 & \exp(i\theta/2) \end{pmatrix}.$$

Then, the rotation of an angle θ around the unit axis $\mathbf{n}$ is given by

$$\hat{R}^{\mathbf{n}}(\theta) = e^{-i\theta\mathbf{n}\cdot\hat{\boldsymbol{\sigma}}/2} = \cos(\theta/2)\hat{\mathbb{1}} - i\sin(\theta/2)\mathbf{n}\cdot\hat{\boldsymbol{\sigma}}. \tag{4.2}$$

Beside the rotations, there are six important single-qubit gates that are standard. These are X, Y, Z and

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \tag{4.3}$$

In particular, X, Y and Z are respectively the Pauli operators $\hat{\sigma}_x$, $\hat{\sigma}_y$ and $\hat{\sigma}_z$ represented in the computational basis, and H is known as the Hadamard gate.

Eventually, the state of the qubit is measured. In particular, this is always the measurement of $\hat{\sigma}_z$ and one always obtains one of the two discrete outcomes: "0" or "1". Given the generic state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, with α and β being complex and $|\alpha|^2 + |\beta|^2 = 1$, then one has a probability $p_0 = |\alpha|^2$ to have the outcome "0" and $p_1 = |\beta|^2$ to have the outcome "1".

Example 4.1
The gate X flips states. Indeed,

$$X \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}. \tag{4.4}$$

Example 4.2
The Hadamard gate H generates uniform superpositions. In particular, one has

$$H \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$
$$H \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{4.5}$$

Namely, one has

$$\hat{H} |0\rangle = |+\rangle, \quad and \quad \hat{H} |0\rangle = |-\rangle, \tag{4.6}$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Notably, the Hadamard gate maps the basis of $\hat{\sigma}_z$ in that of $\hat{\sigma}_x$, and back.

Exercise 4.1
Express the Hadamard gate as a rotation.

Exercise 4.2
Prove that, given two fixed non-parallel normalised vectors $\mathbf{n}$ and $\mathbf{m}$, any unitary single qubit gate $\hat{U}$ can be expressed as

$$\hat{U} = e^{i\alpha} \hat{R}^{\mathbf{n}}(\beta) \hat{R}^{\mathbf{m}}(\gamma) \hat{R}^{\mathbf{n}}(\delta), \tag{4.7}$$

with $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.

It is common to represent quantum circuits with diagrams with the time running from left to right, where lines correspond to qubits and boxes to gates. For example, the following diagram

$$|0\rangle \;—\; \boxed{H} \;—\; \boxed{R_Z(\theta)} \;—\; \boxed{\not\!\nearrow} \tag{4.8}$$

corresponds to the following logical consecutive operations

0) Prepare the qubit in the ground state $|0\rangle$.
1) Apply the Hadamard gate H.
2) Apply a rotation of an angle θ around the z axis.
3) Measure the state of the qubit.

When one is working with more than one qubit, there is the need to construct the representation of the states the common computational basis. In the case of two qubits, the basis is given by $\{\, |00\rangle, |01\rangle, |10\rangle, |11\rangle \,\}$, whose representation in the common computational basis is

$$|00\rangle \sim \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle \sim \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle \sim \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle \sim \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \tag{4.9}$$

where the symbol $\sim$ indicates that the state $|\psi\rangle$ was represented on the computational basis. This is constructed through the tensor product, i.e.

$$|\psi\phi\rangle \sim \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} \otimes \begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix} = \begin{pmatrix} \psi_1\phi_1 \\ \psi_1\phi_2 \\ \psi_2\phi_1 \\ \psi_2\phi_2 \end{pmatrix}. \tag{4.10}$$

Owning the computational representation, we can introduce some 2-qubit gates. One of the most useful among these gates is the CNOT or control-NOT gate:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{4.11}$$

and is represented as

or equivalently as   (4.12)

It acts on a target qubit (qubit 1) in a way that depends on the state of a control qubit (qubit 0). Namely, it applies an X gate to the qubit 1 if the state of qubit 0 is 1, otherwise it does not change the state:

$$CNOT\,|00\rangle = |00\rangle\,, \quad CNOT\,|01\rangle = |01\rangle\,, \quad CNOT\,|10\rangle = |11\rangle\,, \quad CNOT\,|11\rangle = |10\rangle\,. \tag{4.13}$$

Exercise 4.3
Prove that CNOT can generate entanglement.

A second important 2-qubit gate is the SWAP, which swaps the state between two qubits. Namely

$$SWAP\,|a\rangle \otimes |b\rangle = |b\rangle \otimes |a\rangle\,. \tag{4.14}$$

A SWAP operation can be constructed using a concatenation of CNOT gates. In particular:

$$(4.15)$$

Similarly as the CNOT, one can construct a controlled unitary gate, where the state of the control qubit determines if a unitary gate $\hat{U}$ is applied to the target qubit:

$$C(U) \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{pmatrix} \sim \qquad \tag{4.16}$$

where U_{ij} are the matrix elements of $\hat{U}$.

4.1.1 Hadamard test

The Hadamard test is a useful tool for computing expectation values of a unitary, black-box operator $\hat{U}$ with respect to a state $|\psi\rangle$, which can be in principle a multi-qubit state. Since in general $\hat{U}$ is not Hermitian, one measures independently the real and immaginary part of $\langle\psi|\hat{U}|\psi\rangle$.

The circuit for the real Hadamard test is

$$
\begin{array}{c}
|0\rangle \!-\!\boxed{H}\!-\!\bullet\!-\!\boxed{H}\!-\!\boxed{\angle} \\
|\psi\rangle \!-\!/\!-\!\boxed{U}\!-
\end{array}
\tag{4.17}
$$

and it performs as follows. The first step is to generate a superposition in the first qubit (qubit 0):

$$
|0\rangle\,|\psi\rangle \xrightarrow{\hat{H}\otimes\hat{\mathbb{1}}} \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|\psi\rangle .
\tag{4.18}
$$

Then, we entangle the qubits with the $C(U)$ gate:

$$
\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|\psi\rangle \xrightarrow{C(U)} \tfrac{1}{\sqrt{2}}(|0\rangle\,|\psi\rangle + |1\rangle\,\hat{U}\,|\psi\rangle),
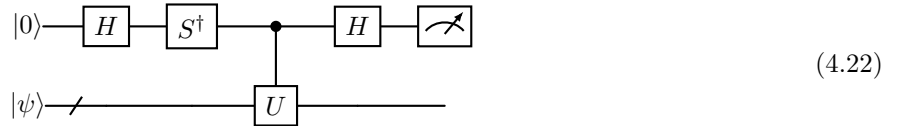\tag{4.19}
$$

and apply the Hadamard gate to qubit 0:

$$
\xrightarrow{\hat{H}\otimes\hat{\mathbb{1}}} \tfrac{1}{2}\left[(|0\rangle + |1\rangle)\,|\psi\rangle + (|0\rangle - |1\rangle)\hat{U}\,|\psi\rangle\right] = \tfrac{1}{2}\left[|0\rangle\,(\hat{\mathbb{1}} + \hat{U})\,|\psi\rangle + |1\rangle\,(\hat{\mathbb{1}} - \hat{U})\,|\psi\rangle\right] .
\tag{4.20}
$$

Finally, one measures qubit 0, and the probability of finding the qubit in $|0\rangle$ is

$$
P(|0\rangle) = \tfrac{1}{4}\,\langle\psi|\left(\hat{\mathbb{1}} + \hat{U}^\dagger\right)\left(\hat{\mathbb{1}} + \hat{U}\right)|\psi\rangle = \tfrac{1}{2}\left(1 + \Re\,\langle\psi|\hat{U}|\psi\rangle\right) .
\tag{4.21}
$$

Thus, by measuring only one qubit (qubit 0) one has an indication of the real part of $\langle\psi|\hat{U}|\psi\rangle$. To estimate the imaginary part, the circuit is modified as follows:

$$
\begin{array}{c}
|0\rangle \!-\!\boxed{H}\!-\!\boxed{S^\dagger}\!-\!\bullet\!-\!\boxed{H}\!-\!\boxed{\angle} \\
|\psi\rangle \!-\!/\!-\!\boxed{U}\!-
\end{array}
\tag{4.22}
$$

Then, the state before the measurement is

$$
\tfrac{1}{2}\left[|0\rangle\,(\hat{\mathbb{1}} - i\hat{U})\,|\psi\rangle + |1\rangle\,(\hat{\mathbb{1}} + i\hat{U})\,|\psi\rangle\right],
\tag{4.23}
$$

and correspondingly one has

$$
\tilde{P}(|0\rangle) = \tfrac{1}{2}\left(1 + \Im\,\langle\psi|\hat{U}|\psi\rangle\right) .
\tag{4.24}
$$

Notably, to well characterise these probabilities, there is the need to run the protocol several times to construct a statistics.

Exercise 4.4
Prove that the circuit in Eq. (4.22) provides the result in Eq. (4.24).