

Introduction to Quantum Computing

Gabriel Ribeiro Fernandes

October 2025

1 Introduction

2 Section 2

2.1 Section 2.1

2.2 Single qubit gates

(Nielsen and Chang sections 1.3.1, 2.1.8, 4.2)

Principle of time evolution: the quantum state $|\psi\rangle$ at current time point t transitions to a new quantum state $|\psi'\rangle$ at a later time $t' \geq t$.

The transition will always be described by a complex unitary matrix U .

$$|\psi'\rangle = U \cdot |\psi\rangle$$

Circuit notation:



Notes:

- The circuit is read from left to right, but the matrix time vector ($U \cdot |\psi\rangle$) from right to left.
- U preserves normalisation.

Examples:

- quantum analogue of classical NOT-gate ($0 \leftrightarrow 1$) flip $|0\rangle \leftrightarrow |1\rangle \rightsquigarrow$ Pauli-X gate:

$$X \equiv \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\text{(check: } x |0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \text{)}$$

analogue for 1 to 0.

- Pauli-Y gate:

$$Y \equiv \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

- Pauli-Z gate:

$$Z \equiv \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Z leaves $|0\rangle$ unchanged, but flips the sign of the coefficient of $|1\rangle$.

Recall the Bloch sphere representation of a general quantum state:

$$|\psi\rangle = \cos\left(\frac{\varphi}{2}\right) |0\rangle + ie^{i\varphi} \sin\left(\frac{\varphi}{2}\right) |1\rangle$$

Then:

$$Z |\psi\rangle = \cos\left(\frac{\varphi}{2}\right) |0\rangle - e^{i\varphi} \sin\left(\frac{\varphi}{2}\right) |1\rangle \quad (1)$$

$$= \cos\left(\frac{\varphi}{2}\right) |0\rangle + e^{i(\varphi+\pi)} \sin\left(\frac{\varphi}{2}\right) |1\rangle \quad (\text{with } e^{i\pi} = -1) \quad (2)$$

\rightsquigarrow new Bloch sphere angles: $\theta' = \theta$, $\varphi' = \varphi + \pi$
(rotation by $\pi = 180^\circ$ around z-axis)

x, y and z gates are called Pauli matrices.

The Pauli vector $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3) = (x, y, z)$ is a vector of 2x2 matrices.

- Hadamard gate:

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

$$\alpha |0\rangle + \beta |1\rangle \longrightarrow \boxed{H} \longrightarrow \alpha \frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

- Phase gate:

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

- T gate:

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

Note: $T^2 = S$ (since $(e^{i\frac{\pi}{4}})^2 = e^{i\frac{\pi}{2}} = i$)

Pauli matrices satisfy:

$$\sigma_j^2 = \text{identity}.$$

$$\sigma_j \cdot \sigma_k = -\sigma_k \cdot \sigma_j \text{ for all } j \neq k$$

Commutator: $[\sigma_j, \sigma_k] := \sigma_j \sigma_k - \sigma_k \sigma_j = 2i \sigma_l$ for (j, k, l) — which is a cyclic permutation of (1,2,3)

Matrix exponential and rotation gates $R_x(\theta)$, $R_y(\theta)$, $R_z(\theta)$ (pdf in Moodle) Z-Y decomposition of an arbitrary 2x2 matrix:

For any unitary matrix $U \in \mathbb{C}^{2 \times 2}$ there exists real numbers $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ such that:

$$U = e^{i\alpha} \cdot R_z(\beta) \cdot R_y(\gamma) \cdot R_z(\delta) = e^{i\alpha} \begin{pmatrix} e^{-i\frac{\beta}{2}} & 0 \\ 0 & e^{i\frac{\beta}{2}} \end{pmatrix} \cdot \begin{pmatrix} \cos(\frac{\gamma}{2}) & -\sin(\frac{\gamma}{2}) \\ \sin(\frac{\gamma}{2}) & \cos(\frac{\gamma}{2}) \end{pmatrix} \cdot \begin{pmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{pmatrix}$$

2.3 Multiple qubit

(Nielsen and Chang sections 1.2.1, 2.1.7)

So far: single qubits, superposition of basis states $|0\rangle$ and $|1\rangle$.

For two qubits, this generalises to:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

as computational basis states: all combinations (bitstrings) of 0s and 1s.

General two-qubit state:

$$|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$$

with amplitudes $\alpha_{ij} \in \mathbb{C}$ such that:

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \quad (\text{normalization})$$

Can identify the basis states with unit vectors:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Thus:

$$|\psi\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \in \mathbb{C}^4$$

What happens if we measure only one qubit of a two-qubit state?
 Say we measure the first qubit: obtain the result.

0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$

1 with probability $|\alpha_{10}|^2 + |\alpha_{11}|^2$

Wavefunction directly after measurement:

if we measured 0: $|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$

if we measured 1: $|\psi'\rangle = \frac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$

Mathematical formalism for constructing two-qubit states:

Tensor product of vector spaces can combine two (arbitrary) vector spaces V and W to form the tensor product $V \otimes W$.

(Look into the "Tensor products of vector spaces" — Moodle)

Generalisation to n qubits: 2^n computational basis states

$\{|0, \dots, 0\rangle, |0, \dots, 0, 1\rangle, |0, \dots, 1, 0\rangle, \dots, |1, \dots, 1\rangle\}$ (all bit strings of length n)

Thus, a general n -qubit quantum state, also denoted as "quantum register", is given by:

$$|\psi\rangle = \sum_{x_0=0}^1 \sum_{x_1=0}^1 \dots \sum_{x_{n-1}=0}^1 \alpha_{x_{n-1}, \dots, x_1, x_0} |x_{n-1} \dots x_1 x_0\rangle \quad (3)$$

$$= \sum_{x=0}^{2^n-1} \alpha_x |x\rangle \quad \text{binary representation} \quad (4)$$

with $\alpha_x \in \mathbb{C}$ for all $x \in \{0, \dots, 2^n - 1\}$ such that:

$$\| |\psi\rangle \|^2 = \sum_{x=0}^{2^n-1} |\alpha_x|^2 \stackrel{!}{=} 1 \quad (\text{normalisation})$$

\rightsquigarrow in general "hard" to simulate on a classical computer (for large n) due to this "curse of dimensionality".

Vector space as tensor products: $\underbrace{\mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2}_{n \text{ times}} = (\mathbb{C}^2)^{\otimes n} \approx \mathbb{C}^{(2^n)}$

2.4 Multiple qubit gates

(Nielsen and Chuang sections 1.3.2, 1.3.4, 2.17)

As for single qubits, an operation on multiple qubits is described by an unitary matrix U .

For n qubits: $U \in \mathbb{C}^{2^n \times 2^n}$

Example: Controlled-NOT gate (also denoted CNOT)

two qubits: control and target

target qubit gets flipped if control is 1:

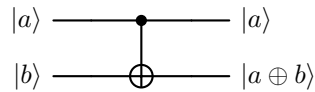
$$\underbrace{|00\rangle}_{\text{control}|target} \mapsto |00\rangle,$$

$$|01\rangle \mapsto |01\rangle, |10\rangle \mapsto |11\rangle, |11\rangle \mapsto |10\rangle$$

Can be expressed as:

$$|ab\rangle \mapsto |a, a \oplus b\rangle, \forall a, b \in \{0, 1\} \quad |a \oplus b \text{ defined as "addition modulo 2"}$$

Circuit notation:

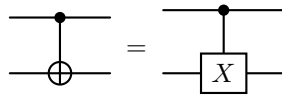


Matrix Representation:

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{Pauli-X}$$

This matrix is unitary.

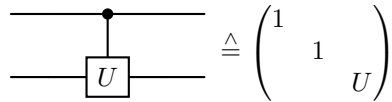
Alternative notation:



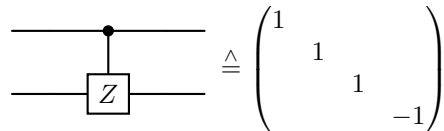
We can generalise Pauli-X to any unitary single-qubit gate U acting on the target qubit \rightsquigarrow controlled U -gate:

$$|00\rangle \mapsto |00\rangle, |01\rangle \mapsto |01\rangle, |10\rangle \mapsto |1\rangle \otimes (U|0\rangle), |11\rangle \mapsto (|1\rangle \otimes (U|1\rangle))$$

Generalisation:

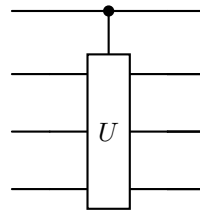


Example: controlled-z:



Exercise: show that controlled-z gate is invariant when flipping control and target qubits.

Controlled-U gate for multiple target qubits:

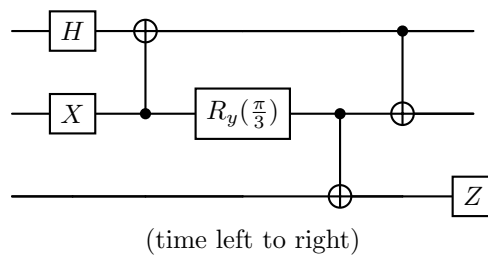


Note: single qubit and CNOT gates are universal: they can be used to implement an arbitrary unitary operation on n qubits.

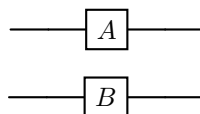
(Quantum analogue of universality of classical NAND gate)

proof in Nielsen and Chang section 4.5

Example of a circuit consisting only of single qubit gates and CNOTs:



Matrix Kronecker products: matrix representation of single qubit gates acting in parallel:



Operation on basis states: $a, b \in \{0, 1\}$

$$\underbrace{|a, b\rangle}_{|a\rangle \otimes |b\rangle} \mapsto (A|a\rangle) \otimes (B|b\rangle) = (A \otimes B)|a, b\rangle$$

Example: $A = I$ (identity), $B = Y$:

$$|00\rangle \mapsto |0\rangle \otimes \underbrace{(Y|0\rangle)}_{i|1\rangle} = i|01\rangle$$

$$|01\rangle \mapsto |0\rangle \otimes \underbrace{(Y|1\rangle)}_{-i|0\rangle} = -i|00\rangle$$

$$|10\rangle \mapsto |1\rangle \otimes (Y|0\rangle) = i|11\rangle$$

$$|11\rangle \mapsto |1\rangle \otimes (Y|1\rangle) = -i|10\rangle$$

Matrix Representation:

(ket on the left of map to represents column and resulting one on the row)

$$\begin{array}{c} \text{---} \boxed{I} \text{---} \\ \text{---} \boxed{Y} \text{---} \end{array} \triangleq \begin{pmatrix} 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix} \text{Pauli-Y} = \begin{pmatrix} Y & 0 \\ 0 & Y \end{pmatrix} = I \otimes Y$$

General formula: Kronecker product (matrix representation of tensor products of operators)

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{pmatrix} \in \mathbb{C}^{mp \times nq}$$

$\forall A \in \mathbb{C}^{m \times n}, B \in \mathbb{C}^{p \times q}$ (NumPy `np.kron(A, B)`)

Generalise to arbitrary number of tensor factors, e.g.

$$\begin{array}{c} \text{---} \boxed{A} \text{---} \\ \text{---} \boxed{B} \text{---} \\ \text{---} \boxed{C} \text{---} \end{array} \triangleq A \otimes B \otimes C = (A \otimes B) \otimes C = A \otimes (B \otimes C)$$

Basic properties:

(a) $(A \otimes B)^* = A^* \otimes B^*$ (elementwise complex conjugation)

(b) $(A \otimes B)^T = A^T \otimes B^T$ (transposition)

(c) $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$

(d) $(A \otimes B) \otimes C = A \otimes (B \otimes C)$ (associative property)

(e) $\underbrace{(A \otimes B) \cdot (C \otimes D)}_{\text{matrix-matrix multiplication}} = (A \cdot B) \otimes (C \cdot D)$

for matrices of compatible dimensions.

$$\begin{array}{ccc} \text{---} \boxed{C} \text{---} \boxed{A} \text{---} & & \text{---} \boxed{A \cdot C} \text{---} \\ & = & \\ \text{---} \boxed{D} \text{---} \boxed{B} \text{---} & & \text{---} \boxed{B \cdot D} \text{---} \end{array}$$

(side exchange because its read from left to right)

(f) Kronecker product of Hermitian matrices is Hermitian

(g) Kronecker product of unitary matrices is unitary (follows from (c) & (e))