Simple structure of a quantum computer (without error correction)

Unitary operation $U$ depends on what we need (e.g., a number to factor)

Idea: at the measurement stage some states are preferable (amplitudes of other states are $\approx 0$), the result tells us what we need

- We may need to measure only some qubits
- Still some randomness of the result (so mostly “hard to solve, easy to check” problems)
QC structure with error correction

Unitary operations $U_i$ do not necessarily involve all qubits

Technical issue: physical qubits can be reused

Unitary operations $U_i$ can be decomposed into simpler gates (usually 1-qubit or 2-qubit, sometimes 3-qubit gates).

Unitary operations are reversible, so QC is related to reversible computing (classically permutations, often permutations in QC as well); measurement is irreversible.
Language of quantum circuit diagrams
(more notations later when we need them)

qubit idling: thin line (“wire”)

several idling qubits  (Nielsen-Chuang’s book)  (Mermin’s book)

measurement  (N-C book)  (Mermin)  meas.

Read quantum circuit diagrams from left to right ( → )

|ψ⟩ ——— [U] ——— U|ψ⟩

|ψ⟩ ——— [U] ——— [V] ——— VU|ψ⟩

So  [U] [V] = [VU]
One-qubit logic gates

“gate” = “operation” = “function” = “map” = “transformation”

Classically, 4 one-bit functions:

\[
\begin{array}{cccc}
0 \to 0 & 0 \to 1 & 0 \to 0 & 0 \to 1 \\
1 \to 1 & 1 \to 0 & 1 \to 0 & 1 \to 1
\end{array}
\]

\((2^N) N\text{-bit} \to 1\text{-bit functions})

\[
\begin{array}{cccc}
\mathbb{I} & \text{NOT} & \text{erase} & \text{erase}'
\end{array}
\]

So, only 2 reversible 1-bit operations: NOT \((0 \leftrightarrow 1)\) and unity operation

Quantum 1-qubit gate: any \textbf{unitary} \(2 \times 2\) matrix

“Unitary” means \(UU^\dagger = UU^\dagger = \mathbb{I} (= \hat{1})\)

Actually, not U(2) group, but SU(2); “special” means \(\det(U) = 1\)

overall phase is not important for a 1-qubit gate

(though will be important for control-gates)

A unitary matrix has \(8 - 4 = 4\) degrees of freedom

\[UU^\dagger = \mathbb{I}\]

A matrix from SU(2) has 3 degrees of freedom, SU(2)\(\leftrightarrow\)SO(3) (3D rotation group)

A qubit state: direction of spin, a rotation is characterized by 3 Euler angles
Pauli matrices (digression)

\[ \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \]

Pauli matrices are Hermitian and unitary

\[ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \]

Language of Quantum Computing to a significant extent is based on Pauli matrices

\[ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \]

Together with unity matrix \( \mathbb{I} \), they form an (almost) orthonormal basis in the space of \( 2 \times 2 \) matrices

\[ \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \]

\[
\text{Tr} \left( \sigma_i^\dagger \sigma_j \right) = 2^1 \delta_{ij}
\]

Inner product for matrices is introduced as for vectors (matrix is “stretched” into vector):

\[
\langle \alpha | \beta \rangle = \sum_n \alpha_n^* \beta_n
\]

\[
\langle \hat{A} | \hat{B} \rangle = \sum_{ij} A_{ij}^* B_{ij} = \sum_{ij} A_{ji}^\dagger B_{ij} = \text{Tr}(A^\dagger B)
\]

(called Frobenius inner product)
Most important 1-qubit gates

1. Bit flip (NOT, X-gate, Pauli-X)

\[
\begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix} = X = \sigma_X = NOT
\]

\[
\begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix}
\begin{pmatrix}
\alpha \\
\beta
\end{pmatrix} =
\begin{pmatrix}
\beta \\
\alpha
\end{pmatrix} \quad \text{so} \quad \begin{pmatrix}
\alpha \\
\beta
\end{pmatrix} \rightarrow \begin{pmatrix}
\beta \\
\alpha
\end{pmatrix} \quad \begin{array}{c}
|0\rangle \\
|1\rangle
\end{array}
\]

\[
\alpha |0\rangle + \beta |1\rangle \rightarrow \beta |0\rangle + \alpha |1\rangle
\]

\[
X |0\rangle = |1\rangle
\]

\[
X |1\rangle = |0\rangle
\]

2. Phase flip (Z-gate)

\[
\begin{pmatrix}
1 & 0 \\
0 & -1
\end{pmatrix} = Z = \sigma_Z
\]

\[
\begin{pmatrix}
\alpha \\
\beta
\end{pmatrix} \rightarrow \begin{pmatrix}
\alpha \\
-\beta
\end{pmatrix}
\]

\[
\alpha |0\rangle + \beta |1\rangle \rightarrow \alpha |0\rangle - \beta |1\rangle
\]

\[
Z [\alpha |0\rangle + \beta |1\rangle] = \alpha |0\rangle - \beta |1\rangle
\]

\[
Z |0\rangle = |0\rangle
\]

\[
Z |1\rangle = -|1\rangle
\]
Most important 1-qubit gates (cont.)

3. Phase & bit flip (Y-gate)

\[
\begin{pmatrix}
0 & -i \\
i & 0
\end{pmatrix} = Y = \sigma_Y
\]

\[
\begin{pmatrix}
\alpha \\
\beta
\end{pmatrix} \rightarrow \begin{pmatrix}
-i \beta \\
i \alpha
\end{pmatrix}
\]

\[
Y|0\rangle = i|1\rangle
\]

\[
Y|1\rangle = -i|0\rangle
\]

\[
Y[\alpha|0\rangle + \beta|1\rangle] = -i\beta|0\rangle + i\alpha|1\rangle
\]

Very often defined differently:

\[
Y = \begin{pmatrix}
0 & -1 \\
1 & 0
\end{pmatrix} \quad \text{or} \quad Y = \begin{pmatrix}
0 & 1 \\
-1 & 0
\end{pmatrix}
\]

Mermin-web (Eqs. 1.48, 1.49)

In Mermin-book the usual definition (Eq. 1.51), except in Ch. 5 (error correction)

4. Hadamard

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

\[
H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}
\]

\[
\begin{pmatrix}
\alpha + \beta \\
\frac{\sqrt{2}}{\alpha - \beta}
\end{pmatrix} \rightarrow \begin{pmatrix}
\alpha + \beta \\
\frac{\sqrt{2}}{\alpha - \beta}
\end{pmatrix}
\]
Most important 1-qubit gates (cont.)

5. Phase gate

\[
\begin{pmatrix}
1 & 0 \\
0 & i
\end{pmatrix}
= \begin{pmatrix}
1 & 0 \\
0 & e^{i\pi/2}
\end{pmatrix}
= \begin{pmatrix}
1 & 0 \\
0 & e^{i\pi/2}
\end{pmatrix}
\]

\[
S \quad \text{Notation from N-C book}
\]

\[
S = \sqrt{Z} \quad \text{since} \quad Z = \begin{pmatrix}
1 & 0 \\
0 & e^{i\pi}
\end{pmatrix}
\]

Do not confuse with Mermin’s notation \(S_{ij}\) for SWAP

6. “\(\pi/8\)”-gate or T-gate

\[
\begin{pmatrix}
1 & 0 \\
0 & e^{i\pi/4}
\end{pmatrix}
= T \quad \text{Notation from N-C book}
\]

\[
T = \sqrt{S}
\]

Called \(\pi/8\) because equivalent to \(\exp(-i \frac{\pi}{8} Z)\)
Sequential gates

Possible confusion: left-to-right in quantum circuit diagrams, right-to-left in matrix notations

\[ UV = VU \]

Example

\[ |0\rangle S Z H \]

means

\[ H Z S |0\rangle = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} (1) (0) \]

\[ H \quad Z \quad S \quad |0\rangle \]
Summary for main 1-qubit gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{bit flip}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{phase flip}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{phase & bit flip}$$

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

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

$$T = \sqrt{S}$$
Some useful relations

\[ X^2 = Y^2 = Z^2 = \mathbb{I} \]

\[ H^2 = \mathbb{I} \]

\[
X = \begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix} \\
Y = \begin{pmatrix}
0 & -i \\
i & 0
\end{pmatrix} \\
Z = \begin{pmatrix}
1 & 0 \\
0 & -1
\end{pmatrix}
\]

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

\[ XY = -YX = iZ \]
\[ YZ = -ZY = iX \]
\[ ZX = -XZ = iY \]

The factor \( i \) is not important (overall phase), therefore sufficient to consider \( X \) and \( Z \).

\[ HXH = Z, \quad HZH = X \]

Check

\[
\frac{1}{\sqrt{2}} \begin{pmatrix}
1 & 1 \\
1 & -1
\end{pmatrix} \begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix}
1 & 1 \\
1 & -1
\end{pmatrix} = \frac{1}{2} \begin{pmatrix}
1 & 1 \\
1 & -1
\end{pmatrix} \begin{pmatrix}
1 & -1 \\
1 & 1
\end{pmatrix} = \frac{1}{2} \begin{pmatrix}
2 & 0 \\
0 & -2
\end{pmatrix} = \begin{pmatrix}
1 & 0 \\
0 & -1
\end{pmatrix}
\]

\[ XA = A_{\text{EXCHANGED ROWS}} \quad AX = A_{\text{EXCHANGED COLUMNS}} \]

The second equation \( HXH = Z \Rightarrow HHXHH = HZH \)
Same relations in the language of circuit diagrams

\[ X \otimes X = \quad \]
\[ Y \otimes Y = \quad \]
\[ Z \otimes Z = \quad \]
\[ H \otimes H = \quad \]
\[ H \otimes X \otimes H = \quad Z \quad \]
\[ H \otimes Z \otimes H = \quad X \quad \]
Bloch sphere (some physical meaning)

\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle = e^{i\gamma} \left( \cos\frac{\theta}{2} |0\rangle + e^{i\varphi} \sin\frac{\theta}{2} |1\rangle \right) \]

irrelevant

\[ \theta : \text{zenith (polar) angle, } 0 \leq \theta \leq \pi \]

\[ \varphi : \text{azimuth angle, } \text{mod } 2\pi \]

(often \(|0\rangle\) at the bottom, \(|1\rangle\) at the top)

Corresponds to direction of a spin in real space

\[ Z \text{ axis } \rightarrow |0\rangle \]
\[ -Z \text{ axis } \rightarrow |1\rangle \]
\[ Y \text{ axis } \rightarrow \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \]
\[ -Y \text{ axis } \rightarrow \frac{|0\rangle - i|1\rangle}{\sqrt{2}} \]
\[ X \text{ axis } \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \]
\[ -X \text{ axis } \rightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}} \]
\[ \text{equator } \rightarrow \frac{|0\rangle + e^{i\varphi}|1\rangle}{\sqrt{2}} \]

Orthogonal vectors in Hilbert space correspond to opposite directions on Bloch sphere
Unitary 1-qubit transformations

Physical evolution leads to a unitary transformation of wavefunctions

\[ |\dot{\psi}\rangle = -\frac{i}{\hbar} \hat{H} |\psi\rangle \implies |\psi(t)\rangle = \hat{U} |\psi(0)\rangle, \quad \hat{U} = e^{-(i/\hbar)\hat{H}t} \]

Since \( \hat{H} \) is Hermitian, \( \hat{U} \) is unitary

\[ \hat{U} \hat{U}^\dagger = e^{-(i/\hbar)\hat{H}t} e^{(i/\hbar)\hat{H}^\dagger t} = \mathbb{1} \]

\( U(2) \): group of unitary transformations in 2D

\( SU(2) \): subgroup of \( U(2) \) with \( \det = 1 \)

(since overall phase in not important, \( S \) means special)

\[ SU(2) \leftrightarrow SO(3) \]

(almost isomorphism; actually homomorphism \( 2 \to 1 \), kernel \( \pm \mathbb{1} \))

1-qubit unitary operations correspond to rotations of the Bloch sphere
Main 1-qubit operations on the Bloch sphere

\[ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \]

Rotation about X-axis by angle \( \pi \) (180°)

(rotation counterclockwise looking from the axis end, but not important since \( \pi \))

X-axis does not move:

\[
\frac{|0\rangle + |1\rangle}{\sqrt{2}} \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}
\]

Note that

\[
\frac{|0\rangle - |1\rangle}{\sqrt{2}} \rightarrow -\frac{|0\rangle - |1\rangle}{\sqrt{2}}
\]

(be careful with overall phase)

Larmor rotation (precession) of a real spin by a magnetic field along X

(this is a physical picture, often used in QC; \( \omega = \gamma B \), \( \gamma \) is gyromagnetic ratio)
Main 1-qubit operations on the Bloch sphere (cont.)

\[ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \]  
Rotation about Z-axis by \( \pi \) (180°)

\[ Y = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \]  
Rotation about Y-axis by \( \pi \) (180°)

\[ H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \]  
Rotation by \( \pi \) about axis in XZ plane, which is at angle \( \pi/4 \) from Z and X

Now it is obvious why \( X^2 = Y^2 = Z^2 = H^2 = \hat{1} \), just a rotation by 2\( \pi \)

\[ S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \]  
Rotation about Z-axis by \( \pi/2 \) (90°)

\[ T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \]  
Rotation about Z-axis by \( \pi/4 \) (45°)
Main 1-qubit operations on the Bloch sphere (cont.)

\[
H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
\]

Rotation by \(\pi\) about axis in XZ plane, which is at angle \(\pi/4\) from Z and X

Another rotation realization for Hadamard

\[
H = R_Y(\pi/2) R_Z(\pi)
\]

(rotation about Z by \(\pi\) and rotation about Y by \(\pi/2\))

Check:

\[
\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}
\]

\[
|0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}
\]

Counterclockwise rotation about Y by \(\pi/2\)

\[
|1\rangle \rightarrow \frac{-|0\rangle + |1\rangle}{\sqrt{2}}
\]
Arbitrary 1-qubit unitary transformation

An arbitrary 1-qubit unitary can be parametrized as

$$U = e^{i\alpha} \exp\left(-i \frac{\theta}{2} (\vec{n}\vec{\sigma})\right)$$

where $$\vec{n}\vec{\sigma} = n_x\sigma_x + n_y\sigma_y + n_z\sigma_z$$,

$$\alpha, \theta, n_x, n_y, n_z$$ are real numbers, $$n_x^2 + n_y^2 + n_z^2 = 1$$

$$\alpha$$ is irrelevant (overall phase), so 3 real parameters

Counterclockwise rotation about axis $$\vec{n}$$ by angle $$\theta$$
(this is why $$\theta/2$$ and “−” sign)

Useful relation:

$$\exp\left(-i \frac{\theta}{2} (\vec{n}\vec{\sigma})\right) = \cos \frac{\theta}{2} \hat{1} - i \sin \frac{\theta}{2} (\vec{n}\vec{\sigma})$$

follows from $$(\vec{n}\vec{\sigma})^2 = \hat{1}$$
Two-qubit states

\[ |\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \]

\[
\begin{aligned}
|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 &= 1 \\
\text{Overall phase is not important } \Rightarrow \text{ can choose } \alpha_0 \text{ real}
\end{aligned}
\]

\[ 8 - 2 = 6 \text{ degrees of freedom} \quad (2 \cdot 2^k - 2 \text{ degrees of freedom for } k \text{ qubits}) \]
Two-qubit states

\[ |\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \]

\[ 8 - 2 = 6 \text{ degrees of freedom} \]

Tensor-product states (outer-product, direct-product): each qubit is some state

\[ (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) = \]

\[ = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix} \]

\[ 2 + 2 = 4 \text{ degrees of freedom} \]

A general 2-qubit state is a tensor-product state only if \( \alpha_{00}\alpha_{11} = \alpha_{10}\alpha_{01} \). Otherwise – entangled.
Notations for multi-qubit computational-basis states

\[ |x_3, x_2, x_1, x_0\rangle \equiv |x_3\rangle |x_2\rangle |x_1\rangle |x_0\rangle \equiv |x_3\rangle \otimes |x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle \]

Computational-basis state, represents classical state \( \sum x_n 2^n \)

- \( |x_3\rangle \) ____________ (most significant bit at the top)
- \( |x_2\rangle \) ____________
- \( |x_1\rangle \) ____________
- \( |x_0\rangle \) ____________

However, people often say in opposite order: first qubit, second qubit, etc.
Two-qubit gates

Any unitary $4 \times 4$ matrix
(overall phase is not important)

Can be defined by transformation of the basis vectors:

- $|00\rangle \rightarrow \ldots \ (4 \text{ complex numbers})$
- $|01\rangle \rightarrow \ldots \ (4)$
- $|10\rangle \rightarrow \ldots \ (4)$
- $|11\rangle \rightarrow \ldots \ (4)$

Then linearity

Degrees of freedom: $32 - 16 - 1 = 15 \quad \text{(for } k \text{ qubits } 4^k - 1)$

Reversible: $UU^\dagger = \underline{\text{_________}}$
Examples of two-qubit gates

1. Trivial: tensor-product gates

\[
\mathbf{U} \otimes \mathbf{V} = \begin{pmatrix}
\mathbf{U}_{00} \begin{pmatrix} V_{00} & V_{01} \\ V_{10} & V_{11} \end{pmatrix} & \mathbf{U}_{01} \begin{pmatrix} V_{00} & V_{01} \\ V_{10} & V_{11} \end{pmatrix} \\
\mathbf{U}_{10} \begin{pmatrix} V_{00} & V_{01} \\ V_{10} & V_{11} \end{pmatrix} & \mathbf{U}_{11} \begin{pmatrix} V_{00} & V_{01} \\ V_{10} & V_{11} \end{pmatrix}
\end{pmatrix}
\]

Math structure: tensor-product of matrices

2–5. Many gates are of controlled type: one qubit controls the other one (consider next)
2. Controlled-NOT (CNOT)

Generalizes classical CNOT: target bit is flipped if control bit is 1

|00⟩ → |00⟩
|01⟩ → |01⟩
|10⟩ → |11⟩
|11⟩ → |10⟩

Unitary matrix; can be checked, but actually trivial, because a permutation of computational basis

\[ α_0 |00⟩ + α_1 |01⟩ + α_2 |10⟩ + α_3 |11⟩ \rightarrow α_0 |00⟩ + α_1 |01⟩ + α_3 |10⟩ + α_2 |11⟩ \]
CNOT (cont.)

Notation: CNOT\textsubscript{ij} or \( C_{ij} \) (Mermin’s book)

\[
\text{control} \quad \text{CNOT} \quad \text{target}
\]

\[
\text{CNOT}_{10} |x\rangle |y\rangle = |x\rangle |y \oplus x\rangle \quad \text{for computational basis}
\]

qubit 1 \quad qubit 0 \quad \text{addition modulo 2}

(again, transformation for other states defined by linearity)

\[
\text{CNOT}_{01} |x\rangle |y\rangle = |x \oplus y\rangle |y\rangle
\]

Actually, not possible to say that nothing happens to the control qubit; this is true only if it is \(|0\rangle\) or \(|1\rangle\). If control qubit is in a superposition state, it gets entangled with the target qubit. Then it will not have a state by itself, and it may depend on what happens next with the target qubit.

Example

\[
\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2} \quad \rightarrow \quad |0\rangle - |1\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}
\]

Control changes, while target the same!
3. Controlled-Z (CZ)

```
control
|   |
|   |
|   | Z
|   |
|   |
|   |
```

Phase-flip of target if control is $|1\rangle$

|00⟩ → |00⟩
|01⟩ → |01⟩
|10⟩ → |10⟩
|11⟩ → −|11⟩

Somewhat surprisingly, symmetric

Matrix

\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & -1
\end{pmatrix}
\]

(Nielsen-Chuang)
4. Controlled-phase (C-phase)

Phase-S gate if control is $|1\rangle$

\[
\begin{align*}
|00\rangle &\rightarrow |00\rangle \\
|01\rangle &\rightarrow |01\rangle \\
|10\rangle &\rightarrow |10\rangle \\
|11\rangle &\rightarrow i|11\rangle
\end{align*}
\]

Also symmetric

Matrix
\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & i
\end{pmatrix}
\]

Note that often controlled-phase means
\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & e^{i\varphi}
\end{pmatrix}
\]
Examples of two-qubit gates (cont.)

5. Any controlled-$U$

\[
\begin{array}{c}
|00\rangle \rightarrow |00\rangle \\
|01\rangle \rightarrow |10\rangle \\
|10\rangle \rightarrow |01\rangle \\
|11\rangle \rightarrow |11\rangle \\
\end{array}
\]

\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
\end{pmatrix}
\]

Notation \(\text{SWAP}_{ij}\)

\(S_{ij}\) (Mermin)

Symmetric

\[\alpha |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle \rightarrow \alpha |00\rangle + \alpha_2 |01\rangle + \alpha_1 |10\rangle + \alpha_3 |11\rangle\]
Useful relations between two-qubit gates

1. \((\text{CNOT}_{ij})^2 = (\text{CZ}_{ij})^2 = (\text{SWAP}_{ij})^2 = \hat{1}\)

2. \(\text{CNOT}_{ij} = (H_i H_j) \text{CNOT}_{ji} (H_i H_j)\)

So, who controls whom is a matter of preference!

Proof

because \(HZH = X\) (if control=1) 
while \(H^2 = \hat{1}\) (if control=0)

symmetric CZ

similar to the first step: \(H X H = Z, H^2 = \hat{1}\)

Sufficient to prove only for basis states!
\[
\text{CNOT}_{ij} = \left( H_i H_j \right) \text{CNOT}_{ji} \left( H_i H_j \right) \quad \text{(cont.)}
\]

Another proof

\[
\text{CNOT}_{ij} = \frac{1}{2} (I_i + Z_i) I_j + \frac{1}{2} (I_i - Z_i) X_j =
\]

\[
\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{selects state } |0\rangle \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \text{selects state } |1\rangle
\]

\[
= I_i \frac{1}{2} (I_j + X_j) + Z_i \frac{1}{2} (I_j - X_j) =
\]

\[
\text{(note that } X \leftrightarrow Z \text{ corresponds to } i \leftrightarrow j) \]

now exchange order and multiply by \( \hat{1} \) from both sides

\[
= \left( H_i H_j \right) \left( H_i H_j \right) \left[ \frac{1}{2} (I_j + X_j) I_i + \frac{1}{2} (I_j - X_j) Z_i \right] \left( H_i H_j \right) \left( H_i H_j \right) =
\]

\[
\left( HXH = Z, \quad HZH = X \right) \quad = \left( H_i H_j \right) \left[ \frac{1}{2} (I_j + Z_j) I_i + \frac{1}{2} (I_j - Z_j) X_i \right] \left( H_i H_j \right) =
\]

\[
\text{CNOT}_{ji}
\]

\[
= \left( H_i H_j \right) \text{CNOT}_{ji} \left( H_i H_j \right)
\]
\[
\text{CNOT}_{ij} = \left( H_i H_j \right) \text{CNOT}_{ji} \left( H_i H_j \right) \quad \text{(cont.)}
\]

One more (direct) proof

Let us prove the opposite (equivalent) relation

\[
|00\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \rightarrow \text{CNOT}_{ij} \left( H_i H_j \right)
\]

\[
|01\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \rightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) \rightarrow \text{CNOT}_{ij} \left( H_i H_j \right)
\]

Two more initial states

\[
|11\rangle \quad \text{(as should be)}
\]

since \( H^2 = \hat{1} \)
$$CNOT_{ij} = \left( H_i H_j \right) CNOT_{ji} \left( H_i H_j \right)$$  (cont.)

We proved the relation for 4 initial basis states $$\Rightarrow$$ should hold for any initial state.

Important example, it shows that CNOT is not a one-way action, this is an interaction (has “quantum back-action”).

\[
\begin{align*}
|10\rangle & \rightarrow \frac{0 - 1}{\sqrt{2}} \frac{0 + 1}{\sqrt{2}} \\
|11\rangle & \rightarrow \frac{0 - 1}{\sqrt{2}} \frac{0 - 1}{\sqrt{2}}
\end{align*}
\]
Useful relations between two-qubit gates (cont.)

3. \( \text{SWAP}_{ij} = \text{CNOT}_{ij} \text{CNOT}_{ji} \text{CNOT}_{ij} \)

\[
\begin{array}{cccccc}
\text{证明} \\
\text{Again, consider only (computational) basis states for initial state} \\
\text{CNOT}_{ij} \quad \text{CNOT}_{ji} \\
|x_i \rangle |y_j \rangle \rightarrow |x_i \rangle |x \oplus y \rangle_j \rightarrow |x \oplus x \oplus y \rangle_i |x \oplus y \rangle_j = |y_i \rangle |x \oplus y \rangle_j \rightarrow \\
\text{CNOT}_{ij} \\
\rightarrow |y_i \rangle |x \oplus y \oplus y \rangle_j = |y_i \rangle |x \rangle_j
\end{array}
\]
Three-qubit gates

Any unitary $8 \times 8$ matrix
(overall phase is not important)

In general characterized by $4^3 - 1 = 63$ real numbers

Two most important 3-qubit gates: Toffoli and Fredkin


Toffoli gate

Flip target if both controls are 1

\[
\begin{pmatrix}
1 & 1 & 0 \\
1 & 1 & 1 \\
0 & 1 & 1 \\
0 & 1 & 0 \\
\end{pmatrix}
\]

|110⟩ ↔ |111⟩
other basis states do not change

Can be constructed with CNOTs and 1-qubit gates (6 CNOTs needed)

Classical Toffoli gate is sufficient for classical reversible computation (to beat informational limit for energy dissipation in computation). Cannot be decomposed into 2-bit gates (in contrast to the quantum case), minimal gate for reversible computation. Realizes AND if target 0, NAND if target 1.
Fredkin gate

Fredkin gate: controlled-SWAP

Classical Fredkin realizes AND (in lower target) if lower target is initially 0.
No fan-out gate (no-cloning theorem)

**Theorem:** impossible to realize fan-out gate

\[ |\psi\rangle \quad \underbrace{U\quad|\psi\rangle} \quad |\psi\rangle \]

\[ |0\rangle \quad \underbrace{U\quad|\psi\rangle} \quad |\psi\rangle \]

**Proof**

Assume \( U |0\rangle|0\rangle = |0\rangle|0\rangle \)
\( U |1\rangle|0\rangle = |1\rangle|1\rangle \)

Then \( U (\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha |0\rangle|0\rangle + \beta |1\rangle|1\rangle \), while for desired cloning

\[
(\alpha|0\rangle + \beta|1\rangle)|0\rangle \rightarrow (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) = \\
= \alpha^2 |0\rangle|0\rangle + \beta^2 |1\rangle|1\rangle + \alpha\beta |0\rangle|1\rangle + \alpha\beta |1\rangle|0\rangle \\
\text{(a different state!)}
\]

**More general proof**

Assume \( U |\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \)
\( U |\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle \)

Unitary operation preserves inner product, therefore \( \langle \phi|\psi \rangle = (\langle \phi|\psi \rangle)^2 \).

This is possible only when \( \langle \phi|\psi \rangle = 0 \) or 1 (i.e., can clone only orthogonal states)