Quantum Algorithms

Definitions, Measurement, Uncomputation, Intro to Phase Kickback

Anish Ghosh

Tensor Product of Vectors

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \in \mathbb{C}^3 \quad \otimes \quad y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} \in \mathbb{C}^3 \quad \longrightarrow \quad \begin{bmatrix} x_1 y \\ x_2 y \\ x_3 y \end{bmatrix} \quad \longrightarrow \quad x \otimes y = \begin{bmatrix} x_1 y_1 \\ x_1 y_2 \\ x_1 y_3 \\ x_2 y_1 \\ x_2 y_2 \\ x_2 y_3 \\ x_3 y_1 \\ x_3 y_2 \\ x_3 y_3 \end{bmatrix}.$$

Each component of x multiplies the entire vector y.

$$\boxed{\dim\left(\mathbb{C}^3 \otimes \mathbb{C}^3\right) = 9}$$

Tensor Product of Vectors: Binary Example

$$x = \begin{bmatrix}1\\0\\1\end{bmatrix} \in \mathbb{C}^3 \quad \otimes \quad y = \begin{bmatrix}0\\1\\1\end{bmatrix} \in \mathbb{C}^3 \quad \longrightarrow \quad \begin{bmatrix}1\,y\\0\,y\\1\,y\end{bmatrix} \quad \longrightarrow \quad x \otimes y = \begin{bmatrix}1\cdot 0\\1\cdot 1\\1\cdot 1\\0\cdot 0\\0\cdot 1\\0\cdot 1\\1\cdot 0\\1\cdot 1\\1\cdot 1\end{bmatrix} = \begin{bmatrix}0\\1\\1\\0\\0\\0\\0\\1\\1\end{bmatrix}.$$

Each component of x multiplies the entire vector y.

$$\boxed{\dim\left(\mathbb{C}^3 \otimes \mathbb{C}^3\right) = 9}$$

Formal Definition

Definition 1 (Tensor Product)

Let V and W be vector spaces over a field K with bases

$$e_1, \ldots, e_m \qquad \text{and} \qquad f_1, \ldots, f_n,$$

respectively.
The **tensor product** $V \otimes W$ is a vector space over K of dimension mn, equipped with a bilinear operation

$$\otimes : V \times W \longrightarrow V \otimes W.$$

The tensor product space $V \otimes W$ has basis

$$\boxed{e_i \otimes f_j, \qquad i = 1, \ldots, m, \quad j = 1, \ldots, n.}$$

Definition adapted from Nannicini, *Quantum Algorithms for Optimizers* [1].

Kronecker Product (Matrix Version of Tensor Product)

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Each entry of A multiplies the entire matrix B.

$$A \otimes B = \begin{bmatrix} 1B & 0B \\ 1B & 1B \end{bmatrix}$$

$$\Downarrow$$

$$A \otimes B = \left[\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{array}\right].$$

Dimensions

$$A, B \in \mathbb{C}^{2\times 2}$$
$$\Downarrow$$
$$A \otimes B \in \mathbb{C}^{4\times 4}$$

Formal Definition: Kronecker Product

Definition 2 (Kronecker Product)

Let

$$A \in \mathbb{C}^{m \times n}, \qquad B \in \mathbb{C}^{p \times q}.$$

The **Kronecker product** of A and B is

$$D := A \otimes B \in \mathbb{C}^{mp \times nq},$$

defined by

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ a_{21}B & \cdots & a_{2n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}.$$

Relation to Definition 1. The Kronecker product is a generalization of the tensor product from vectors to matrices. For column vectors, the Kronecker product reduces to the usual vector tensor product.

Source: Nannicini, *Quantum Algorithms for Optimizers*, Definition 1.2; see Definition 1.1 for the tensor product [1].

Hermitian Conjugate and Tensor-Power Notation

Notation:

$$A \in \mathbb{C}^{m\times n}, \qquad \mathbb{S} \text{ is a vector space.}$$

Conjugate Transpose or Hermitian conjugate

$$\boxed{A^\dagger := \overline{A}^{\,T}}$$

Also written as A^H; here we use $A^\dagger$.

Repeated tensor products

$$A^{\otimes n} = \underbrace{A \otimes A \otimes \cdots \otimes A}_{n \text{ times}}, \qquad \mathbb{S}^{\otimes n} = \underbrace{\mathbb{S} \otimes \mathbb{S} \otimes \cdots \otimes \mathbb{S}}_{n \text{ times}}.$$

Notation from Nannicini, *Quantum Algorithms for Optimizers* [1].

Binary Strings

Example

$$\vec{j} = (1, 0, 1, 1) \in \{0, 1\}^4.$$

- A binary string of length q is written as

$$\vec{j} \in \{0, 1\}^q, \qquad q \in \mathbb{Z}_{>0}.$$

- The arrow indicates that $\vec{j}$ is a **string of binary digits**.
- The k-th digit of $\vec{j}$ is written

$$\vec{j}_k \in \{0, 1\}, \qquad k = 1, \ldots, q.$$

For

$$\vec{j} = (1, 0, 1, 1),$$

we have

$$\vec{j}_1 = 1, \qquad \vec{j}_2 = 0, \qquad \vec{j}_3 = 1, \qquad \vec{j}_4 = 1.$$

Binary String and Its Integer Value

We use j without the arrow to denote the **decimal integer represented by** $\vec{j}$.

$$\boxed{j = \sum_{k=1}^{q} \vec{j}_k \, 2^{\,q-k}}$$

Example

$$\vec{j} = (1, 0, 1, 1)$$

$$\begin{aligned} j &= \vec{j}_1 2^3 + \vec{j}_2 2^2 + \vec{j}_3 2^1 + \vec{j}_4 2^0 \\ &= 1(2^3) + 0(2^2) + 1(2^1) + 1(2^0) \\ &= 8 + 0 + 2 + 1 \\ &= \boxed{11}. \end{aligned}$$

Most Significant Bit and Least Significant Bit

Consider a binary string

$$\vec{j} = (\vec{j}_1, \vec{j}_2, \ldots, \vec{j}_q).$$

Most Significant Bit (MSB)

The bit associated with the **largest power of** 2.

For

$$1011,$$

the leftmost bit contributes

$$1 \cdot 2^3 = 8.$$

$$\boxed{\text{MSB} = 1}$$

Least Significant Bit (LSB)

The bit associated with the **smallest power of** 2.

For

$$1011,$$

the rightmost bit contributes

$$1 \cdot 2^0 = 1.$$

$$\boxed{\text{LSB} = 1}$$

Big-Endian and Little-Endian Ordering

Big-endian

MSB comes first.

$$\vec{j} = (1,0,1,1)$$

$$\boxed{j = \sum_{k=1}^{q} \vec{j}_k \, 2^{q-k}}$$

$$j = 1(2^3) + 0(2^2) + 1(2^1) + 1(2^0) = 11.$$

$$\underbrace{1}_{\text{MSB}}\;0\;1\;\underbrace{1}_{\text{LSB}}$$

Little-endian

LSB comes first.

$$\vec{j} = (1,1,0,1)$$

$$\boxed{j = \sum_{k=1}^{q} \vec{j}_k \, 2^{k-1}}$$

$$j = 1(2^0) + 1(2^1) + 0(2^2) + 1(2^3) = 11.$$

$$\underbrace{1}_{\text{LSB}}\;1\;0\;\underbrace{1}_{\text{MSB}}$$

Same integer, different ordering convention.

Classical Bit vs Quantum Qubit

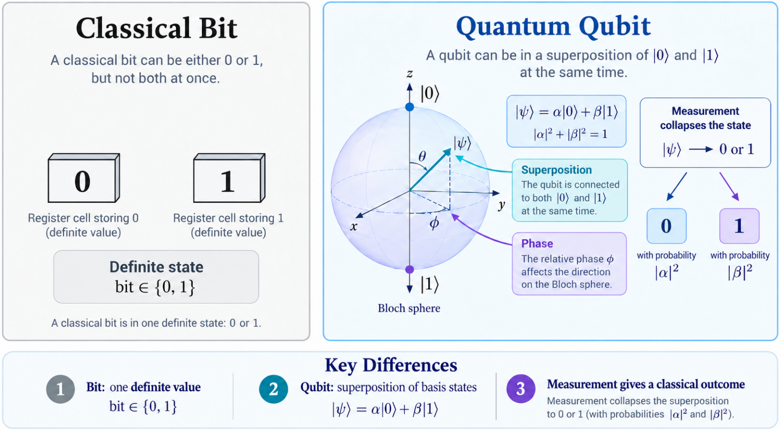


Figure 1: Comparison of a classical bit and a quantum qubit.

What is a Quantum State?

- A **quantum state** is the mathematical description of a quantum system.
- Mathematically, it is represented by a **complex vector**

$$\psi \in \mathbb{C}^n.$$

- A valid quantum state must be a **unit vector**:

$$\boxed{\|\psi\|_2 = 1}$$

- Equivalently,

$$\boxed{\sum_{j=1}^{n} |\psi_j|^2 = 1.}$$

A quantum state is therefore a normalized complex vector.

Working with Quantum States Mathematically

Now that we know that a quantum state is a normalized complex vector, two natural questions arise:

1. **How do we represent and work with quantum states in a mathematical setting?**

2. **How do we extend the description of a single qubit to a general *n*-qubit quantum system?**

General Qubit State

A qubit state is written as a linear combination of the basis states

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Hence,

$$\boxed{|\psi\rangle = \alpha|0\rangle + \beta|1\rangle}$$

with

$$\alpha, \beta \in \mathbb{C}, \qquad |\alpha|^2 + |\beta|^2 = 1.$$

Equivalently,

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

α and β are the amplitudes of the qubit state.

Hadamard Basis

Besides the standard basis $\{|0\rangle, |1\rangle\}$, we will also use the **Hadamard basis**.

$$\boxed{H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \qquad H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)}$$

Using the standard basis vectors,

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \qquad H|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}.$$

Thus, the Hadamard basis is

$$\boxed{\{H|0\rangle,\ H|1\rangle\}.}$$

Quantum State Notation

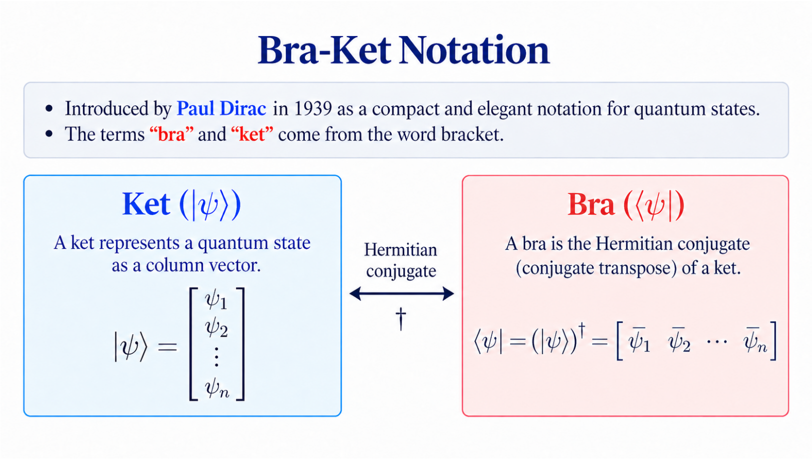


Figure 2: Bra-ket notation for representing quantum states.

Formal Definition: Basis State

Let

$$\mathcal{B} = \{|j\rangle\}_{j\in J}$$

be a chosen basis for the space of quantum states, where J is the **index set** labeling the basis vectors.

Definition 3 (Basis State)

A quantum state $|\psi\rangle$ is called a **basis state** if

$$\boxed{|\psi\rangle = \alpha_k|k\rangle}$$

for some $k \in J$, where

$$\alpha_k \in \mathbb{C}, \qquad |\alpha_k|^2 = 1.$$

Here, k is simply an index in J. When the basis is indexed by binary strings, we write $\vec{k}$ for the binary string and k for its corresponding decimal integer.

Example: Binary and Decimal Basis Indices

Consider the binary index set

$$J = \{0,1\}^2.$$

Its elements are the four binary strings

$$\boxed{\vec{k} \in \{00, 01, 10, 11\}.}$$

Each binary string $\vec{k}$ has a corresponding decimal integer k:

Binary string $\vec{k}$	**Decimal** k	**Basis vector**
00	0	$\lvert 00\rangle$
01	1	$\lvert 01\rangle$
10	2	$\lvert 10\rangle$
11	3	$\lvert 11\rangle$

For example,

$$\boxed{\vec{k} = 10 \qquad \Longleftrightarrow \qquad k = 2.}$$

Thus,

$$|\vec{k}\rangle = |10\rangle, \qquad \alpha_k = \alpha_2.$$

Example: Basis State

For the basis

$$\mathcal{B} = \{|00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle\},$$

a general state is written as

$$|\psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle.$$

If $|\psi\rangle$ is a **basis state**, then exactly one amplitude is nonzero.
For example, if the basis state is $|10\rangle$, then

$$\boxed{\alpha_0 = 0, \qquad \alpha_1 = 0, \qquad |\alpha_2|^2 = 1, \qquad \alpha_3 = 0.}$$

Thus,

$$|\psi\rangle = \alpha_2|10\rangle.$$

Superposition of Basis States

Let

$$\mathcal{B} = \{|j\rangle\}_{j \in J}$$

be a chosen basis, where J is the index set.

Any quantum state can be written as a **linear combination** of the basis states:

$$|\psi\rangle = \sum_{j \in J} \alpha_j |j\rangle.$$

Definition 4 (Superposition of Basis States)

The state $|\psi\rangle$ is in a **superposition of basis states** if more than one coefficient α_j is nonzero.

Superposition of Quantum States

Given two quantum states $|\psi\rangle$ and $|\phi\rangle$, form a **linear combination**

$$|\widetilde{\chi}\rangle = \alpha|\psi\rangle + \beta|\phi\rangle, \qquad \alpha, \beta \in \mathbb{C}.$$

If $|\widetilde{\chi}\rangle \neq 0$, normalize it:

$$\boxed{|\chi\rangle = \frac{\alpha|\psi\rangle + \beta|\phi\rangle}{\left\|\alpha|\psi\rangle + \beta|\phi\rangle\right\|_2}.}$$

Then $|\chi\rangle$ is a valid quantum state and is called a **superposition of $|\psi\rangle$ and $|\phi\rangle$**.

Superposition of Quantum States

Given two quantum states $|\psi\rangle$ and $|\phi\rangle$, form a **linear combination**

$$|\widetilde{\chi}\rangle = \alpha|\psi\rangle + \beta|\phi\rangle, \qquad \alpha, \beta \in \mathbb{C}.$$

If $|\widetilde{\chi}\rangle \neq 0$, normalize it:

$$\boxed{|\chi\rangle = \frac{\alpha|\psi\rangle + \beta|\phi\rangle}{\|\alpha|\psi\rangle + \beta|\phi\rangle\|_2}}.$$

Then $|\chi\rangle$ is a valid quantum state and is called a **superposition of $|\psi\rangle$ and** $|\phi\rangle$.

Remark 1

*The states $|\psi\rangle$ and $|\phi\rangle$ must belong to the **same state space**; in particular, their vector representations must have the same dimension.*

n-Qubit State

Definition 5 (General n-Qubit State)

An n-qubit quantum state is a unit vector in

$$\left(\mathbb{C}^2\right)^{\otimes n}.$$

Using the 2^n computational basis states

$$\left\{|\vec{j}\rangle : \vec{j} \in \{0,1\}^n\right\},$$

a general state is written as a superposition (linear combination)

$$\boxed{|\psi\rangle = \sum_{\vec{j}\in\{0,1\}^n} \alpha_j |\vec{j}\rangle}$$

with amplitudes $\alpha_j \in \mathbb{C}$ satisfying

$$\boxed{\sum_{\vec{j}\in\{0,1\}^n} |\alpha_j|^2 = 1.}$$

State Vector Representation: Two Qubits

A two-qubit state can be written as the linear combination

$$|\psi\rangle_2 = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle.$$

Collect the amplitudes into the vector

$$\boxed{\boldsymbol{\alpha} = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix}}$$

with

$$\alpha_j \in \mathbb{C}, \qquad \sum_{j=0}^{3} |\alpha_j|^2 = 1.$$

Thus, the state is completely determined by the amplitudes

$$\alpha_0, \alpha_1, \alpha_2, \alpha_3.$$

State Vector as a Matrix-Vector Product

For the two-qubit computational basis,

$$\mathcal{B} = \{|00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle\}.$$

The state

$$|\psi\rangle_2 = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$$

can be written as

$$\boxed{|\psi\rangle_2 = \begin{bmatrix}|00\rangle & |01\rangle & |10\rangle & |11\rangle\end{bmatrix}\begin{bmatrix}\alpha_0\\ \alpha_1\\ \alpha_2\\ \alpha_3\end{bmatrix}.}$$

State of a Generic n-Qubit System

For n qubits, the computational basis is

$$\mathcal{B} = \left\{ |\vec{j}\rangle : \vec{j} \in \{0,1\}^n \right\},$$

which contains 2^n basis states.

By Definition 4, a general n-qubit state is a **superposition of these basis states**:

$$\boxed{|\psi\rangle_n = \sum_{\vec{j} \in \{0,1\}^n} \alpha_j |\vec{j}\rangle}$$

with

$$\alpha_j \in \mathbb{C}, \qquad \sum_{\vec{j} \in \{0,1\}^n} |\alpha_j|^2 = 1.$$

State vector

$$\boxed{|\psi\rangle_n = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{2^n-1} \end{bmatrix} \in \mathbb{C}^{2^n}}$$

Inner and Outer Products

Let $|\psi\rangle$ and $|\phi\rangle$ be two quantum states belonging to the same state space. Recall that

$$\langle\psi| := |\psi\rangle^\dagger, \qquad \langle\phi| := |\phi\rangle^\dagger.$$

Definition 6 (Inner Product)

The **inner product** of $|\psi\rangle$ and $|\phi\rangle$ is

$$\boxed{\langle\psi|\phi\rangle = |\psi\rangle^\dagger|\phi\rangle \in \mathbb{C}.}$$

Thus, the inner product produces a **scalar**.

Definition 7 (Outer Product)

The **outer product** of $|\psi\rangle$ and $|\phi\rangle$ is

$$\boxed{|\psi\rangle\langle\phi| = |\psi\rangle|\phi\rangle^\dagger.}$$

Thus, the outer product produces a **matrix**.

Formal Definition: Entanglement

Definition 8 (Entangled State)

An n-qubit state $|\psi\rangle_n$ is called **entangled** if there do not exist single-qubit states

$$|\psi_1\rangle, \ldots, |\psi_n\rangle$$

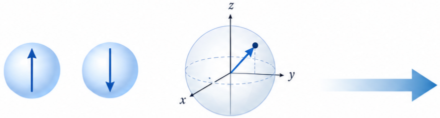
such that

$$\boxed{|\psi\rangle_n = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle.}$$

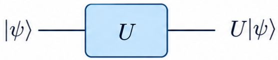
If such a decomposition exists, then the state is called **separable** or a **product state**.

From Understanding Qubits to Operations on Qubits

From states to quantum gates



$|0\rangle$ $|1\rangle$ $\alpha|0\rangle + \beta|1\rangle$



$$U = \begin{bmatrix} u_{00} & u_{01} & \cdots & u_{0,2^q-1} \\ u_{10} & u_{11} & \cdots & u_{1,2^q-1} \\ \vdots & \vdots & & \vdots \\ u_{2^q-1,0} & u_{2^q-1,1} & \cdots & u_{2^q-1,2^q-1} \end{bmatrix}$$

Postulate 2. A quantum operation (or gate) acting on q qubits is represented by a unitary matrix in $C^{2^q \times 2^q}$.

Adapted from Giacomo Nannicini, *Quantum Algorithms for Optimizers*.

Why Are Quantum Gates Unitary?

A quantum operation, or **gate**, transforms a state as

$$|\psi\rangle \longmapsto U|\psi\rangle.$$

A valid quantum state must remain normalized after the operation:

$$\|U|\psi\rangle\|_2^2 = \langle\psi|U^\dagger U|\psi\rangle = 1.$$

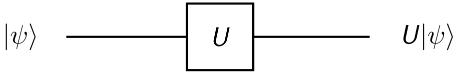
Since this must hold for every normalized state $|\psi\rangle$,

$$\boxed{U^\dagger U = I.}$$

Hence, U must be a **unitary matrix**.

Introduction to a Single-Qubit Circuit

A single-qubit circuit shows how a qubit state changes when a **single-qubit gate** is applied.



The circuit is read from **left to right**:

$$\boxed{|\psi\rangle \;\longmapsto\; U|\psi\rangle}$$

where

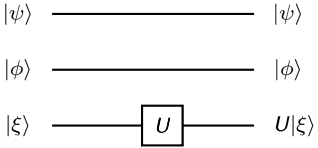
$$U \in \mathbb{C}^{2\times 2}$$

is a unitary matrix representing the single-qubit gate.

Multi-Qubit Circuit: Product State

Consider three qubits in the product state

$$|\psi\rangle \otimes |\phi\rangle \otimes |\xi\rangle.$$



Only the third qubit is acted on:

$$\boxed{|\psi\rangle \otimes |\phi\rangle \otimes |\xi\rangle \longmapsto |\psi\rangle \otimes |\phi\rangle \otimes U|\xi\rangle.}$$

Equivalently,

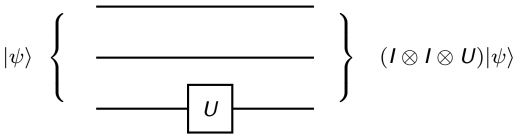
$$\boxed{I \otimes I \otimes U.}$$

Multi-Qubit Circuit: Entangled State

As mentioned earlier an entangled state, cannot factored into individual qubit states:

$$|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle.$$

Therefore, the action of a gate on one qubit must be described through the **full state**.



Hence,

$$\boxed{|\psi\rangle \longmapsto (I \otimes I \otimes U)|\psi\rangle.}$$

For entangled states, we evolve the entire joint state, not the qubits independently.

What is Quantum Measurement?

A quantum state is described by its **amplitudes**. For a state

$$|\psi\rangle = \sum_j \alpha_j |j\rangle,$$

the amplitude α_j tells us the contribution of the basis state $|j\rangle$ to $|\psi\rangle$.

When the state is measured, the squared magnitude of the amplitude gives the probability of observing that basis state:

$$\boxed{\Pr(\text{observe } |j\rangle) = |\alpha_j|^2.}$$

For a single qubit,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

so measurement produces one classical outcome

$$\boxed{x \in \{0, 1\}}$$

with

$$\Pr(x = 0) = |\alpha|^2, \qquad \Pr(x = 1) = |\beta|^2.$$

Formal Definition: Single-Qubit Measurement

Let $|\psi\rangle_n$ be an n-qubit state as in Definition 5:

$$|\psi\rangle_n = \sum_{\vec{j} \in \{0,1\}^n} \alpha_j |\vec{j}\rangle.$$

Definition 9 (Measurement of Qubit k)

Let Q_k denote the **random variable corresponding to the measurement outcome of the k-th qubit**, with sample space

$$Q_k \in \{0, 1\}.$$

Its probability distribution is

$$\boxed{\Pr(Q_k = 0) = \sum_{\substack{\vec{j} \in \{0,1\}^n \\ \vec{j}_k = 0}} |\alpha_j|^2, \qquad \Pr(Q_k = 1) = \sum_{\substack{\vec{j} \in \{0,1\}^n \\ \vec{j}_k = 1}} |\alpha_j|^2.}$$

Post-Measurement State

Suppose measuring qubit k gives the observed value

$$x \in \{0, 1\}.$$

Only the basis states satisfying

$$\vec{j}_k = x$$

remain. The post-measurement state is

$$\boxed{|\psi'\rangle = \sum_{\substack{\vec{j} \in \{0,1\}^n \\ \vec{j}_k = x}} \frac{\alpha_j}{\sqrt{\displaystyle\sum_{\substack{\vec{\ell} \in \{0,1\}^n \\ \vec{\ell}_k = x}} |\alpha_\ell|^2}} |\vec{j}\rangle}$$

The denominator renormalizes the remaining amplitudes so that

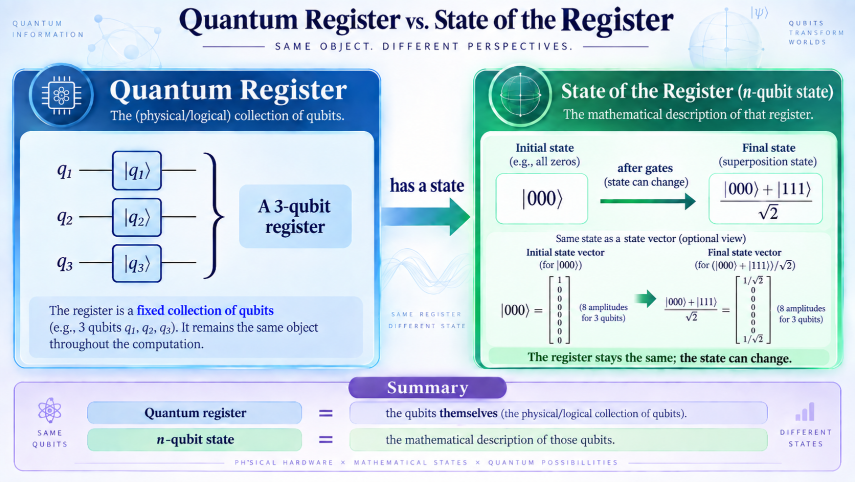
$$\| \, |\psi'\rangle \, \|_2 = 1.$$

Remark 2

Since the only possible outcomes are 0 and 1,

$$\Pr(Q_k = 0) + \Pr(Q_k = 1) = 1,$$

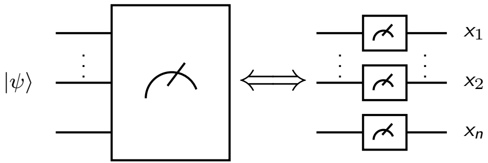
so knowing one probability immediately determines the other.


QUANTUM INFORMATION
Quantum Register vs. State of the Register
SAME OBJECT. DIFFERENT PERSPECTIVES.
QUBITS TRANSFORM WORLDS
Quantum Register
The (physical/logical) collection of qubits.
q_1 $|q_1\rangle$
q_2 $|q_2\rangle$
q_3 $|q_3\rangle$
A 3-qubit register
The register is a fixed collection of qubits (e.g., 3 qubits q_1, q_2, q_3). It remains the same object throughout the computation.
has a state
SAME REGISTER DIFFERENT STATE
State of the Register (n-qubit state)
The mathematical description of that register.
Initial state (e.g., all zeros)
$|000\rangle$
after gates (state can change)
Final state (superposition state)
$\frac{|000\rangle + |111\rangle}{\sqrt{2}}$
Same state as a state vector (optional view)
Initial state vector (for $|000\rangle$)
$|000\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$
(8 amplitudes for 3 qubits)
Final state vector (for $(|000\rangle + |111\rangle)/\sqrt{2}$)
$\frac{|000\rangle + |111\rangle}{\sqrt{2}} = \begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1/\sqrt{2} \end{bmatrix}$
(8 amplitudes for 3 qubits)
The register stays the same; the state can change.
Summary
SAME QUBITS
Quantum register = the qubits themselves (the physical/logical collection of qubits).
n-qubit state = the mathematical description of those qubits.
DIFFERENT STATES
PH'SICAL HARDWARE × MATHEMATICAL STATES × QUANTUM POSSIBILLITIES

Measurement of an n-Qubit System

Measuring an n-qubit state means measuring each qubit in the computational basis. The outcome is a classical bit string

$$\vec{x} = (x_1, \dots, x_n) \in \{0,1\}^n.$$



Measuring the full register is equivalent to measuring all qubits and collecting the classical outcomes:

$$\boxed{|\psi\rangle \longmapsto \vec{x} \in \{0,1\}^n.}$$

Amplitude and Phase of a Qubit

A generic single-qubit state is

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad \alpha, \beta \in \mathbb{C}, \qquad |\alpha|^2 + |\beta|^2 = 1.$$

The complex amplitudes can be written in polar form:

$$\alpha = r_0 e^{i\phi_0}, \qquad \beta = r_1 e^{i\phi_1}.$$

Quantity	**Meaning**
$r_0 = \lvert\alpha\rvert$	Magnitude of the amplitude of $\lvert 0\rangle$
$r_1 = \lvert\beta\rvert$	Magnitude of the amplitude of $\lvert 1\rangle$
ϕ_0, ϕ_1	Phases of the two amplitudes
$r_0^2,\ r_1^2$	Measurement probabilities of 0 and 1

The physically important phase is the **relative phase**

$$\phi = \phi_1 - \phi_0.$$

After removing the common global phase, the state can be written as

$$\boxed{|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle.}$$

From Complex Amplitudes to Relative Phase

Since $\alpha, \beta \in \mathbb{C}$, each amplitude has a **magnitude** and a **phase**.

Derivation

$$\alpha = r_0 e^{i\phi_0}, \qquad \beta = r_1 e^{i\phi_1},$$

$$\begin{aligned} |\psi\rangle &= r_0 e^{i\phi_0}|0\rangle + r_1 e^{i\phi_1}|1\rangle \\ &= r_0 e^{i\phi_0}|0\rangle + r_1 e^{i\phi_0} e^{i(\phi_1 - \phi_0)}|1\rangle \\ &= e^{i\phi_0}\left(r_0|0\rangle + r_1 e^{i(\phi_1 - \phi_0)}|1\rangle\right). \end{aligned}$$

Define the **relative phase**

$$\boxed{\phi = \phi_1 - \phi_0}.$$

Then

$$|\psi\rangle = e^{i\phi_0}\left(r_0|0\rangle + r_1 e^{i\phi}|1\rangle\right).$$

Ignoring the global phase gives

$$\boxed{|\psi\rangle = r_0|0\rangle + r_1 e^{i\phi}|1\rangle.}$$

Reasoning

$r_0 = |\alpha|$ and $r_1 = |\beta|$ are the **magnitudes** of the amplitudes.

Using
$$e^{i\phi_1} = e^{i\phi_0} e^{i(\phi_1 - \phi_0)},$$
we rewrite the second amplitude so that $e^{i\phi_0}$ can be factored from the state.

After factorization, $e^{i\phi_0}$ multiplies the **entire state vector**. Hence it is called the **global phase**.

A global phase does not change the physical predictions of the state, so it can be ignored [2].

The remaining phase difference
$$\phi = \phi_1 - \phi_0$$
is the physically relevant **relative phase**.

From Relative Phase to the Standard Qubit Form

Derivation
From the previous slide,

$$|\psi\rangle = r_0|0\rangle + r_1 e^{i\phi}|1\rangle.$$

Since $|\psi\rangle$ is normalized,

$$r_0^2 + r_1^2 = 1, \qquad r_0, r_1 \geq 0.$$

Using

$$\cos^2 x + \sin^2 x = 1,$$

we parameterize

$$r_0 = \cos x, \qquad r_1 = \sin x, \qquad 0 \leq x \leq \frac{\pi}{2}.$$

Now write

$$x = \frac{\theta}{2}, \qquad 0 \leq \theta \leq \pi.$$

Therefore,

$$\boxed{|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle}$$

with

$$0 \leq \theta \leq \pi, \qquad 0 \leq \phi < 2\pi.$$

Reasoning
The normalization condition

$$r_0^2 + r_1^2 = 1$$

matches the identity

$$\cos^2 x + \sin^2 x = 1.$$

Hence r_0 and r_1 can be represented by **cosine and sine**.
We then define

$$\theta = 2x,$$

so that

$$r_0 = \cos\left(\frac{\theta}{2}\right), \qquad r_1 = \sin\left(\frac{\theta}{2}\right).$$

The parameter ϕ remains the **relative phase** from the previous slide.
Why $\theta/2$? Its geometric meaning will be introduced later.

Why Do We Use the Half-Angle $\theta/2$?

From normalization, we obtained

$$|\psi\rangle = \cos\gamma\,|0\rangle + e^{i\phi}\sin\gamma\,|1\rangle.$$

We have already encountered the term **Bloch sphere**. For a point on the unit sphere with polar angle θ, $z = \cos\theta$. For a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, its corresponding z-coordinate [3] is

$$\boxed{z = |\alpha|^2 - |\beta|^2.}$$

For our state, $|\alpha| = \cos\gamma, \quad |\beta| = \sin\gamma$, so

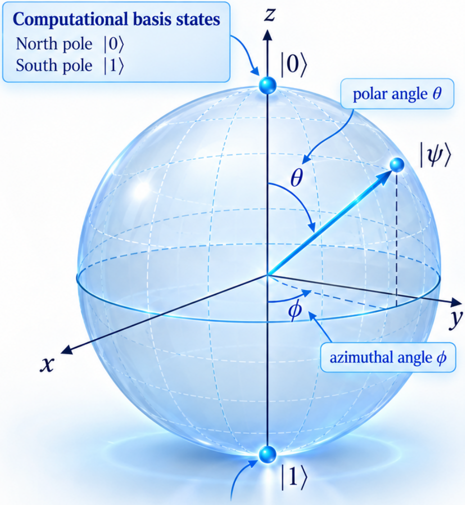
$$\begin{aligned} z &= \cos^2\gamma - \sin^2\gamma \\ &= \cos(2\gamma). \end{aligned}$$

To match the spherical-coordinate form $z = \cos\theta$, we choose

$$\boxed{\theta = 2\gamma} \quad \Longrightarrow \quad \boxed{\gamma = \frac{\theta}{2}}.$$

Therefore,

$$\boxed{|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle.}$$



Qubit state

Any pure state of a qubit can be represented as a point on the surface of the Bloch sphere (parameterized by θ and ϕ).

Qubit state (in computational basis)

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

Bloch-sphere coordinates

$$(x, y, z) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$$

Pauli Gates

The four **Pauli gates** are single-qubit gates represented by the matrices

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

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Since each gate acts on one qubit,

$$I, X, Y, Z \in \mathbb{C}^{2\times 2},$$

and each matrix is **unitary**.

Action of the Pauli Gates

The action of the Pauli gates on the single-qubit basis states $|0\rangle$ and $|1\rangle$ is

Gate	**On** $|0\rangle$	**On** $|1\rangle$	**Effect**
I	$I|0\rangle = |0\rangle$	$I|1\rangle = |1\rangle$	No change
X	$X|0\rangle = |1\rangle$	$X|1\rangle = |0\rangle$	Bit flip
Y	$Y|0\rangle = i|1\rangle$	$Y|1\rangle = -i|0\rangle$	Bit flip with phase
Z	$Z|0\rangle = |0\rangle$	$Z|1\rangle = -|1\rangle$	Phase flip

Circuit Diagrams of the Pauli Gates

The Pauli gates are represented in circuit diagrams as single-qubit gates:

Identity Gate I

$$|\psi\rangle \; —\boxed{I}— \; |\psi\rangle$$

Leaves the state unchanged.

Pauli-X Gate

$$|\psi\rangle \; —\boxed{X}— \; X|\psi\rangle$$

Acts as a bit flip.

Pauli-Y Gate

$$|\psi\rangle \; —\boxed{Y}— \; Y|\psi\rangle$$

Bit flip with a phase factor.

Pauli-Z Gate

$$|\psi\rangle \; —\boxed{Z}— \; Z|\psi\rangle$$

Acts as a phase flip.

Hadamard Gate

The **Hadamard gate** is a single-qubit unitary gate defined by

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

Its action on the computational basis states is

$$H|0\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right),$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right).$$

Thus, the Hadamard gate transforms a basis state into an **equal superposition** of $|0\rangle$ and $|1\rangle$.

Circuit representation

$$|\psi\rangle \;—\boxed{H}—\; H|\psi\rangle$$

Bitwise XOR and Bitwise Dot Product

Let $\vec{j}, \vec{k} \in \{0,1\}^n$.

Definition 10 (Bitwise XOR)

The **bitwise XOR** of $\vec{j}$ and $\vec{k}$ is

$$\boxed{\vec{j} \oplus \vec{k} = \vec{h}, \qquad \vec{h} \in \{0,1\}^n,}$$

where, for each position $p = 1, \ldots, n$,

$$\vec{h}_p = \begin{cases} 0, & \vec{j}_p = \vec{k}_p, \\ 1, & \vec{j}_p \neq \vec{k}_p. \end{cases}$$

Definition 11 (Bitwise Dot Product)

The **bitwise dot product** of $\vec{j}$ and $\vec{k}$ is

$$\boxed{\vec{j} \bullet \vec{k} = \sum_{h=1}^{n} \vec{j}_h \vec{k}_h.}$$

It counts the number of positions where both strings contain a 1.

Two-Qubit Gates: The CX (CNOT) Gate

A **two-qubit gate** acts jointly on two qubits and is represented by a unitary matrix in

$$\mathbb{C}^{4\times 4}.$$

A fundamental example is the **controlled-X gate**, also called the **CNOT gate**.
The first qubit is the **control** and the second qubit is the **target**.

$$\boxed{\begin{array}{lcl} \text{control} = 0 & \Longrightarrow & \text{target unchanged,} \\ \text{control} = 1 & \Longrightarrow & \text{target is flipped.} \end{array}}$$

Using the basis ordering

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

the matrix is

$$CX_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Its action is

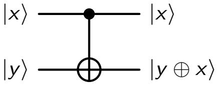
$$\begin{array}{lcllcl} CX_{12}|00\rangle & = & |00\rangle, & CX_{12}|01\rangle & = & |01\rangle, \\ CX_{12}|10\rangle & = & |11\rangle, & CX_{12}|11\rangle & = & |10\rangle. \end{array}$$

CX Gate: Formula and Circuit Diagram

The action of the controlled-X gate is

$$\boxed{CX_{12}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle, \qquad x, y \in \{0, 1\}.}$$

Here, $\oplus$ is the bitwise XOR operation from Definition 10.



The SWAP Gate

The **SWAP gate** is a two-qubit gate that exchanges the two qubits.
If two qubits are in a product state, then

$$\boxed{\mathsf{SWAP}\big(|\psi\rangle_1 \otimes |\phi\rangle_1\big) = |\phi\rangle_1 \otimes |\psi\rangle_1.}$$

Using the computational basis ordering

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

its action is

$$\mathsf{SWAP}|00\rangle = |00\rangle, \qquad \mathsf{SWAP}|01\rangle = |10\rangle,$$

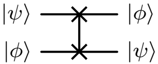
$$\mathsf{SWAP}|10\rangle = |01\rangle, \qquad \mathsf{SWAP}|11\rangle = |11\rangle.$$

Hence, the matrix representation is

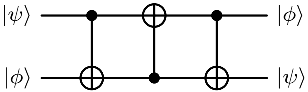
$$\mathsf{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

SWAP Gate: Circuit Diagram and Implementation

The circuit symbol for the SWAP gate is



It can be implemented using three controlled-X gates:



Thus,

$$\boxed{\text{SWAP} = CX_{12}\, CX_{21}\, CX_{12}.}$$

SWAP from Three CX Gates

The circuit constructed from three CX gates swaps qubits 1 and 2.
Proof. By linearity, it is enough to verify the action on the standard basis states [1]:

$$
\begin{aligned}
CX_{12}CX_{21}CX_{12}|00\rangle &= CX_{12}CX_{21}|00\rangle = CX_{12}|00\rangle = |00\rangle, \\
CX_{12}CX_{21}CX_{12}|01\rangle &= CX_{12}CX_{21}|01\rangle = CX_{12}|11\rangle = |10\rangle, \\
CX_{12}CX_{21}CX_{12}|10\rangle &= CX_{12}CX_{21}|11\rangle = CX_{12}|01\rangle = |01\rangle, \\
CX_{12}CX_{21}CX_{12}|11\rangle &= CX_{12}CX_{21}|10\rangle = CX_{12}|10\rangle = |11\rangle.
\end{aligned}
$$

Therefore,

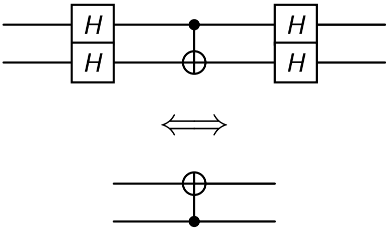
$$
\begin{aligned}
&\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \\
&\quad\longmapsto \quad \alpha_{00}|00\rangle + \alpha_{01}|10\rangle + \alpha_{10}|01\rangle + \alpha_{11}|11\rangle.
\end{aligned}
$$

Phase Kickback: A Guiding Question

Do CX (CNOT) gates always change the target qubit?

Phase Kickback: CNOT Under a Basis Change

Consider applying Hadamard gates to both qubits before and after CX_{12}.



$$\boxed{H^{\otimes 2}\, CX_{12}\, H^{\otimes 2} = CX_{21}}$$

Thus, changing both qubits to the Hadamard basis interchanges the roles of the control and target qubits.

Uncomputation

Definition 12 (Uncomputation)

Uncomputation reverses a quantum computation so that temporary auxiliary and working registers return to their initial all-zero states, while the useful output is preserved.

Suppose

$$f : \{0,1\}^m \longrightarrow \{0,1\}^n.$$

A unitary U_f implements the computation of f using an additional working register.

The basic idea is

$$\boxed{\text{compute} \longrightarrow \text{save the useful output} \longrightarrow \text{reverse the computation.}}$$

Since U_f is unitary,

$$\boxed{U_f^{-1} = U_f^{\dagger}.}$$

Uncomputation: Quantum Registers

The construction uses four quantum registers:

$$\boxed{|\vec{x}\rangle_m, \qquad |\vec{0}\rangle_n, \qquad |\vec{0}\rangle_q, \qquad |\vec{y}\rangle_n.}$$

$$\begin{array}{lcl} |\vec{x}\rangle_m & : & \text{input register with } m \text{ qubits,} \\ |\vec{0}\rangle_n & : & \text{auxiliary register with } n \text{ qubits,} \\ |\vec{0}\rangle_q & : & \text{working register with } q \text{ qubits,} \\ |\vec{y}\rangle_n & : & \text{output register with } n \text{ qubits.} \end{array}$$

The auxiliary and working registers begin in their **all-zero basis states**:

$$|\vec{0}\rangle_n, \qquad |\vec{0}\rangle_q.$$

Uncomputation: Computing $f(\vec{x})$

Initially, the four registers are

$$|\vec{x}\rangle_m|\vec{0}\rangle_n|\vec{0}\rangle_q|\vec{y}\rangle_n.$$

The unitary U_f acts on the first three registers:

$$|\vec{x}\rangle_m|\vec{0}\rangle_n|\vec{0}\rangle_q \xrightarrow{U_f} |\vec{x}\rangle_m|f(\vec{x})\rangle_n|w(\vec{x})\rangle_q.$$

Here,

$$|f(\vec{x})\rangle_n$$

is stored in the n-qubit auxiliary register.

$$|w(\vec{x})\rangle_q$$

denotes temporary information in the q-qubit working register.

Uncomputation: State After Computing $f(\vec{x})$

Including the output register, the state after applying U_f is

$$\boxed{|\vec{x}\rangle_m |f(\vec{x})\rangle_n |w(\vec{x})\rangle_q |\vec{y}\rangle_n.}$$

At this point,

- the input register still contains $|\vec{x}\rangle_m$,
- the auxiliary register contains $|f(\vec{x})\rangle_n$,
- the working register contains temporary information $|w(\vec{x})\rangle_q$,
- the output register is still $|\vec{y}\rangle_n$.

The next step is to save $f(\vec{x})$ in the output register before applying $U_f^\dagger$.

Uncomputation: Saving the Useful Output

After applying U_f, the state is

$$|\vec{x}\rangle_m|f(\vec{x})\rangle_n|w(\vec{x})\rangle_q|\vec{y}\rangle_n.$$

We now copy $f(\vec{x})$ into the output register using bitwise controlled-X operations:

$$|\vec{y}\rangle_n \longmapsto |\vec{y} \oplus f(\vec{x})\rangle_n.$$

Therefore,

$$\boxed{|\vec{x}\rangle_m|f(\vec{x})\rangle_n|w(\vec{x})\rangle_q|\vec{y}\rangle_n \;\longmapsto\; |\vec{x}\rangle_m|f(\vec{x})\rangle_n|w(\vec{x})\rangle_q|\vec{y} \oplus f(\vec{x})\rangle_n}$$

The useful value $f(\vec{x})$ is now preserved in the **output register**.

The next step is to apply

$$U_f^\dagger$$

to reset the auxiliary and working registers.

Uncomputation: Resetting the Temporary Registers

After saving the useful output, the state is

$$|\vec{x}\rangle_m |f(\vec{x})\rangle_n |w(\vec{x})\rangle_q |\vec{y} \oplus f(\vec{x})\rangle_n.$$

Now apply $U_f^\dagger$ to the first three registers:

$$|\vec{x}\rangle_m |f(\vec{x})\rangle_n |w(\vec{x})\rangle_q \xrightarrow{U_f^\dagger} |\vec{x}\rangle_m |\vec{0}\rangle_n |\vec{0}\rangle_q.$$

The output register is not affected by $U_f^\dagger$, so the final state is

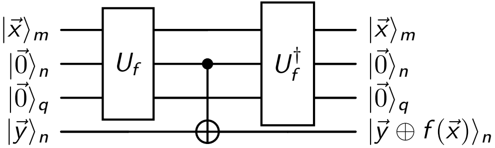
$$\boxed{|\vec{x}\rangle_m |\vec{0}\rangle_n |\vec{0}\rangle_q |\vec{y} \oplus f(\vec{x})\rangle_n.}$$

Thus,

$$\boxed{\text{temporary registers reset while the useful output is preserved}.}$$

Uncomputation: Circuit Summary

Combining the previous steps, uncomputation is implemented by the following **compute–copy–uncompute** circuit:



$$|\vec{x}\rangle_m|\vec{0}\rangle_n|\vec{0}\rangle_q|\vec{y}\rangle_n \longmapsto |\vec{x}\rangle_m|\vec{0}\rangle_n|\vec{0}\rangle_q|\vec{y} \oplus f(\vec{x})\rangle_n.$$

The middle controlled-X operation applies **CNOT gates** from the auxiliary register to the output register, producing

$$|\vec{y}\rangle_n \longmapsto |\vec{y} \oplus f(\vec{x})\rangle_n.$$

References

- Giacomo Nannicini.
  Quantum Algorithms for Optimizers.
  Society for Industrial and Applied Mathematics (SIAM), 2025.
  https://doi.org/10.1137/1.9781611978766

- IBM Quantum, *Limitations on Quantum Information: Irrelevance of Global Phases*, https://quantum.cloud.ibm.com/learning/en/courses/basics-of-quantum-information/quantum-circuits/limitations-on-quantum-information.

- V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, *Quantum Cloning*, Reviews of Modern Physics, Vol. 77, No. 4, pp. 1225–1256, 2005.
  https://doi.org/10.1103/RevModPhys.77.1225