Quantum Tools

Reversibility, Entanglement, Dense coding, Teleportation, Encoding.

F. Schillirò – INAF Osservatorio Astrofisico di Catania

Di Vincenzo Critieria

Implementation of Quantum Computers

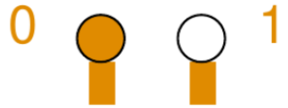
1. Well-defined qubits

2. Initialization to a pure state

$|00 \ldots 0\rangle$

3. Universal set of quantum gates

4. Qubit-specific measurement



5. Long coherence times

$|0\ldots 0\rangle + |1\ldots 1\rangle$

Reversibility in Quantum Computing

Quantum computations are fundamentally reversible.

Unlike classical logic gates, quantum gates correspond to **unitary operations**, which preserve information and can always be inverted.

Key principles

Unitary evolution

Quantum states evolve according to **unitary operators** U that satisfy

$$U^\dagger U = I$$

This guarantees that the transformation is **invertible**.

Information is preserved

No information about the quantum state is lost during computation.

The original state can always be recovered by applying the **inverse operation** $U^\dagger$.

Measurement breaks reversibility

The only non-reversible step in a quantum algorithm is the **measurement**, which collapses the quantum state.

Key idea

$$|\psi_{out}\rangle = U|\psi_{in}\rangle$$

and

$$|\psi_{in}\rangle = U^\dagger|\psi_{out}\rangle$$

Irreversible vs Reversible AND Operation

Classical AND gate (irreversible)

A	B	A AND B
0	0	0
0	1	0
1	0	0
1	1	1

Problem: different inputs produce the same output.

Example:

$$(0,1) \rightarrow 0$$

$$(1,0) \rightarrow 0$$

From the output **0**, it is impossible to reconstruct the original inputs.

➡️ **Information is lost → irreversible computation**

Quantum reversible implementation (Toffoli gate)

Quantum computing implements logical AND using a **reversible three-qubit gate** called the **Toffoli gate (CCNOT)**.

$$|a, b, c\rangle \rightarrow |a, b, c \oplus (a \cdot b)\rangle$$

If the third qubit starts in $c = 0$:

$$|a, b, 0\rangle \rightarrow |a, b, a \cdot b\rangle$$

Example:

$$|1, 1, 0\rangle \rightarrow |1, 1, 1\rangle$$

The inputs **a and b are preserved**, so the operation is **reversible**.

When information is lost, energy must be paid.

(Landauer, 1961)

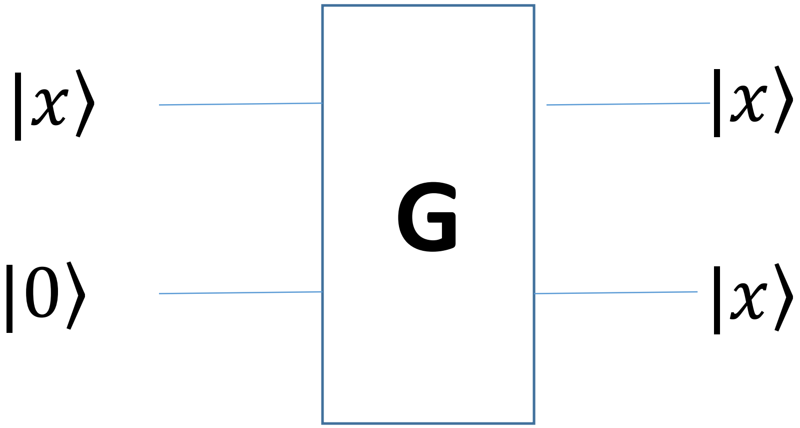
The No-Cloning Theorem

Statement

The **no-cloning theorem** states that it is **impossible to create an identical copy of an arbitrary unknown quantum state**.

$$|\psi\rangle \not\to |\psi\rangle|\psi\rangle$$

No physical operation can perfectly duplicate an unknown quantum state.



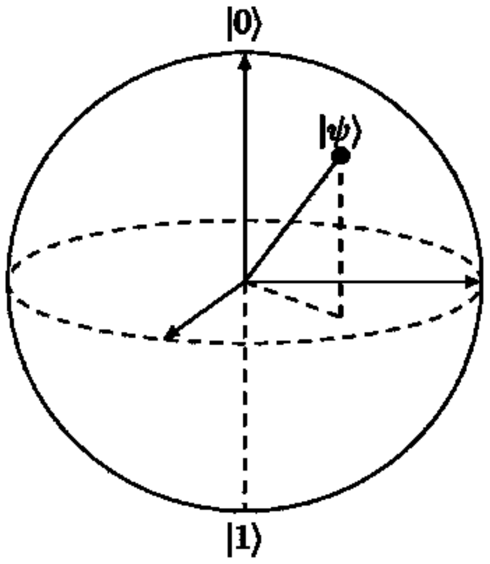
No fan out possible

No unitary, reversible and linear gate

Dim. (try with |x>=|0> , |x>=|1> and |x> a superposition of both

Quantum information is fragile: measurement is destructive and unknown states cannot be cloned.

BIT



QUBIT – Sfera di Bloch

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

We CAN calculate by simulation,
We CAN measure by projection
We CAN teleport
We CANNOT know without destroy the state.

Quantum Entanglement

An entangled state cannot be written as a tensor product of the states of its subsystems; it cannot be factorized into independent single-qubit states.

Consider two qubits:

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

$$|\phi\rangle = \gamma|0\rangle + \delta|1\rangle$$

The **tensor product** between the two states is

$$|\psi\rangle \otimes |\phi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$$

Expanding the product gives

$$|\psi\rangle \otimes |\phi\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

Result

$$|\psi\rangle \otimes |\phi\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

This represents a **separable two-qubit state**, because it can be written as the **tensor product of two individual qubit states**, meaning the qubits are **not entangled**.

Quantum Entanglement

Entanglement is a uniquely quantum correlation between particles in which the state of one qubit cannot be described independently of the other.

For an entangled pair, the system is described by a **single joint quantum state** rather than by two separate states.

Example of a Bell state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Measuring one qubit immediately determines the state of the other, regardless of the distance between them.

Creating Entanglement: H + CNOT

Entangled states can be generated using two fundamental quantum gates:

1. Hadamard gate (H)

The Hadamard gate creates a **superposition**:

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

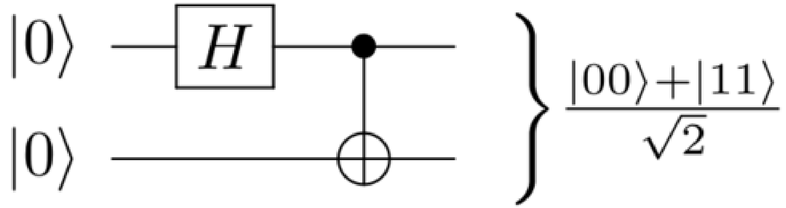
Circuit to create an entangled state

Start from:

$$|00\rangle$$

Apply **Hadamard on the first qubit**:

$$\frac{|00\rangle + |10\rangle}{\sqrt{2}}$$



Apply **CNOT**:

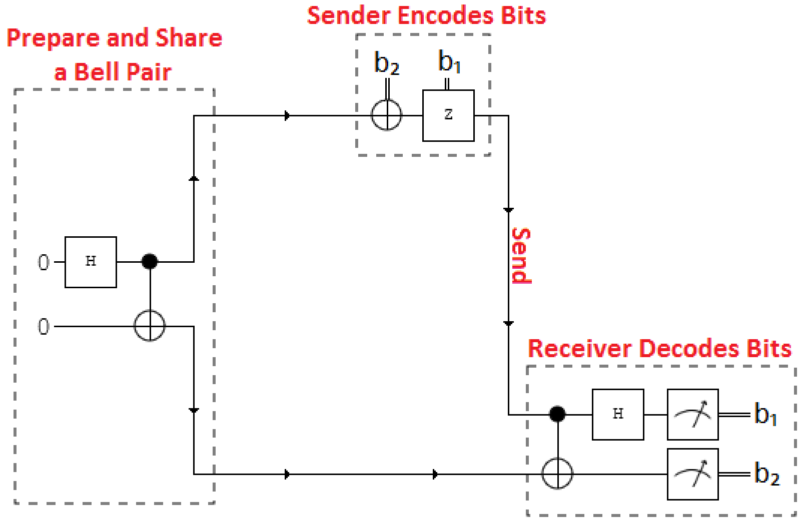
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

This produces the **Bell state**, a maximally entangled pair of qubits.

CODIFICA SUPERDENSA

Il **dense coding** è un protocollo della comunicazione quantistica che permette di **trasmettere due bit classici utilizzando un solo qubit**.

Questo è possibile grazie a una proprietà tipica della meccanica quantistica chiamata **entanglement**.



Nel protocollo ci sono due persone:

•**Alice** → vuole inviare il messaggio

•**Bob** → deve riceverlo

All'inizio condividono una coppia di qubit **entangled**.

Alice vuole inviare **due bit classici**.
Può farlo applicando una delle seguenti operazioni al suo qubit:

Alice invia il suo qbit processato;

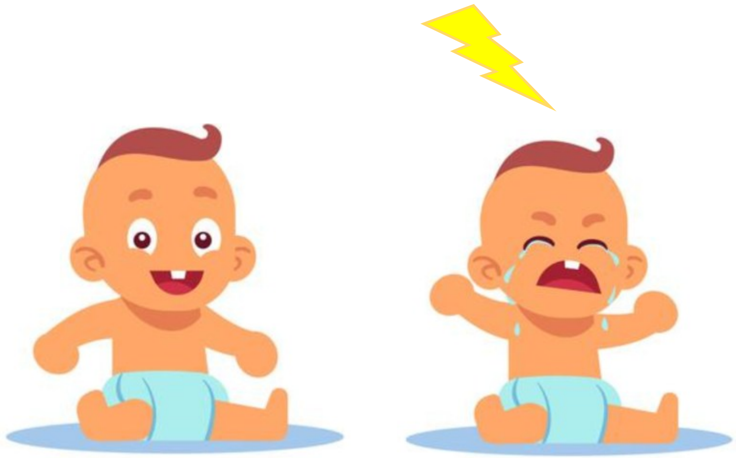
messaggio	operazione
00	nessuna operazione
01	porta X
10	porta Z
11	porta XZ

1) Bob adesso possiede la coppia : stati di bell

2) Bob disentangla lo stato di Bell

3) Bob ricostruisce la coppia

Teletrasporto Quantistico : idea naive



NomeA
Cog(nome) ??

NomeB
Cog(nome)??

Per la loro sicurezza, i gemelli :

- conoscono il proprio nome
- Non conoscono il nome del fratello
- Non conoscono il proprio cog(nome)

Giovanni	00
Pietro	01
Bruno	10

Codifica con 2 bit classici

Entanglement
nome-cog(nome)
(sono fratelli)

Teletrasporto Quantistico : idea naive

All’arrivo di B, al sicuro,
il mago svela ad A di chiamarsi
Giovanni Bruno

Lo stato cog(nome) collassa
ISTANTANEAMENTE in Bruno

Il collasso dello stato è
istantaneo anche per Pietro ,
ma lui non lo sa, perché non
può misurare il suo stato
(No cloning Theorem)

Giovanni	00
Pietro	01
Bruno	10

Teletrasporto Quantistico : idea naive

10

Canale di comunicazione classico

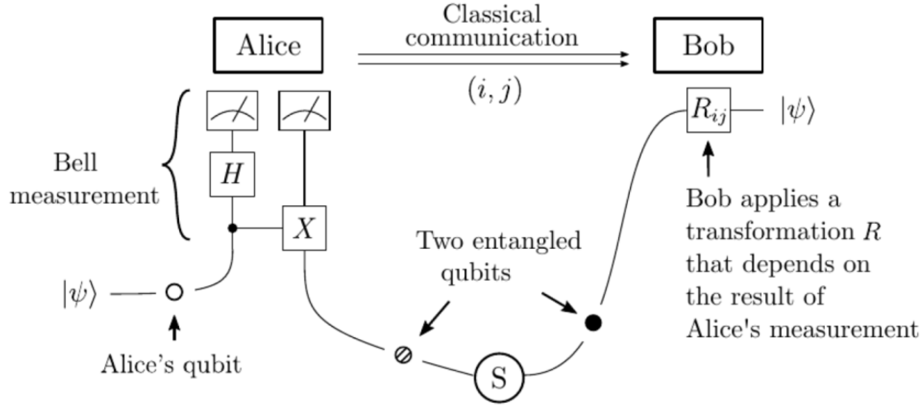
Giovanni invia la stringa di codifica di cog(nome) e Pietro conosce l'informazione solo confrontando il suo cifrario con la stringa.
L'informazione non è superluminale , la Teori della Relatività è salva.

Pietro riceve la stringa con canale classico e confronta con il cifrario, adesso conosce anche il suo cog(nome)

Giovanni	00
Pietro	01
Bruno	10

Se il diavoletto intercetta la stringa ed il cifrario, comunque non conoscerà tutte le informazioni poiché esse stanno nello stato quantistico [nome] dato al momento della partenza

TELETRASPORTO QUANTISTICO



$$|\psi\rangle|\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle)\,\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$= \frac{\alpha}{\sqrt{2}}|0\rangle\,(|00\rangle + |11\rangle) + \frac{\beta}{\sqrt{2}}|1\rangle(|00\rangle + |11\rangle). \tag{9.9}$$

Alice receives the incoming particle and makes it interact with her qubit. This interaction consists of a CNOT followed by a Hadamard. The first CNOT transforms (9.9) into

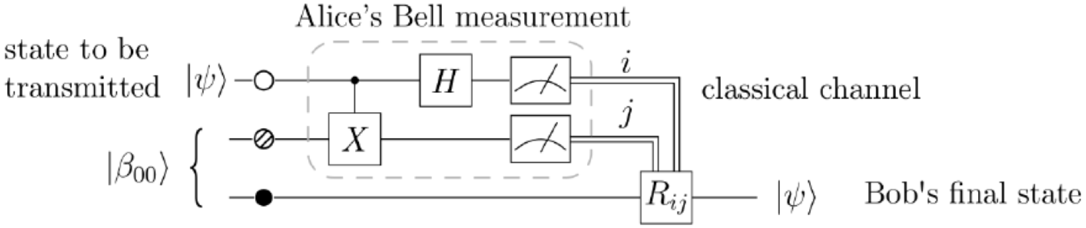
$$\frac{\alpha}{\sqrt{2}}|0\rangle\,(|00\rangle + |11\rangle) + \frac{\beta}{\sqrt{2}}|1\rangle(|10\rangle + |01\rangle),$$

and the additional Hadamard yields

$$\frac{\alpha}{\sqrt{2}}|+\rangle\,(|00\rangle + |11\rangle) + \frac{\beta}{\sqrt{2}}|-\rangle(|10\rangle + |01\rangle) =$$

$$= \frac{1}{2}\Big[\,|00\rangle\,(\alpha|0\rangle + \beta|1\rangle) + |01\rangle\,(\alpha|1\rangle + \beta|0\rangle)$$

$$+\,|10\rangle\,(\alpha|0\rangle - \beta|1\rangle) + |11\rangle\,(\alpha|1\rangle - \beta|0\rangle)\Big]. \tag{9.10}$$



Bob receives over the phone		Bob applies		Bob obtains
00	$\rightarrow$	$\hat{R}_{00} = \mathbb{1}$	$\rightarrow$	$\mathbb{1}\,(\alpha\|0\rangle + \beta\|1\rangle) = \|\psi\rangle$
01	$\rightarrow$	$\hat{R}_{01} = \hat{X}$	$\rightarrow$	$\hat{X}\,(\alpha\|1\rangle + \beta\|0\rangle) = \|\psi\rangle$
10	$\rightarrow$	$\hat{R}_{10} = \hat{Z}$	$\rightarrow$	$\hat{Z}\,(\alpha\|0\rangle - \beta\|1\rangle) = \|\psi\rangle$
11	$\rightarrow$	$\hat{R}_{11} = \hat{Z}\hat{X}$	$\rightarrow$	$\hat{Z}\hat{X}\,(\alpha\|1\rangle - \beta\|0\rangle) = \|\psi\rangle.$

Entangled Qubits are the vector of teleportation

Quantum ENCODING

1) BASIS ENCODING:
nessun guadagno di compressione in codifica

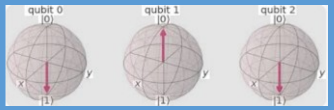
Inserire l'informazione nel mondo QUANTISTICO

1) BASIS ENCODING:

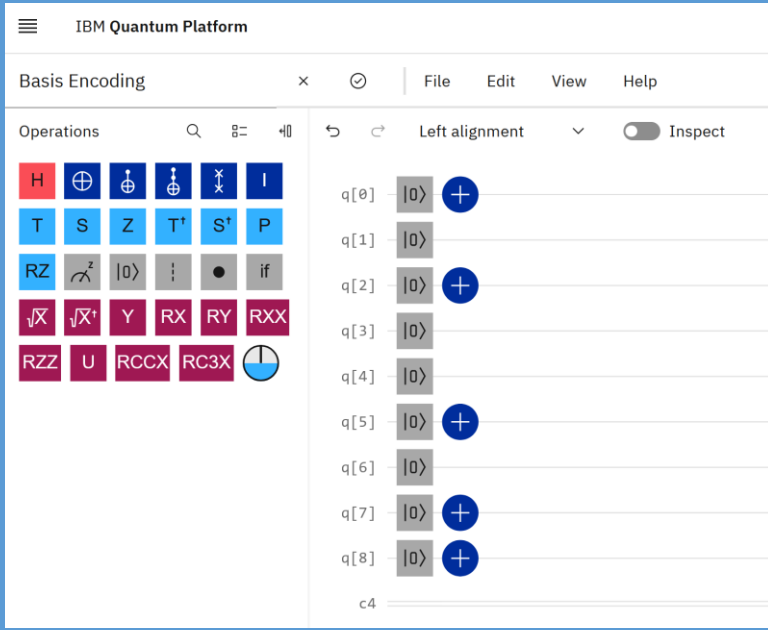
2) AMPLITUDE ENCODING

3) PHASE ENCODING

…..



X=(5,1,3)=
(101,001,011)



AMPLITUDE ENCODING

N valori –> $\log_2(N)$ qbit

$$|\psi_x^{(j)}\rangle = \frac{1}{\alpha}\sum_{i=1}^{N} x_i^{(j)} |i\rangle$$

Compresssione da N a log2(N)

$$|\psi\rangle = \quad + \quad$$

$$\mathrm{norm}_0^2 + \mathrm{norm}_1^2 = 1$$

AMPLITUDE ENCODING

1) Dati da codificare (4 numeri)

Scegliamo il vettore classico:

$$x = [1,\ 2,\ 3,\ 4]$$

L'**amplitude encoding** mette questi valori nelle **ampiezze** di uno stato quantistico a 2 qubit (perché $2^2 = 4$ ampiezze).

Normalizzazione (obbligatoria)

In un sistema quantistico la somma dei quadrati delle ampiezze deve fare 1.

Norma:

$$\|x\| = \sqrt{1^2 + 2^2 + 3^2 + 4^2} = \sqrt{30} \approx 5.4772$$

Ampiezze normalizzate:

$$\alpha_0 = \frac{1}{\sqrt{30}} \approx 0.1826, \quad \alpha_1 = \frac{2}{\sqrt{30}} \approx 0.3651, \quad \alpha_2 = \frac{3}{\sqrt{30}} \approx 0.5477, \quad \alpha_3 = \frac{4}{\sqrt{30}} \approx 0.7303$$

2) Stato quantistico risultante

Associamo i 4 numeri ai 4 stati base di 2 qubit:

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

Allora lo stato che vogliamo preparare è:

$$|\psi\rangle = 0.1826|00\rangle + 0.3651|01\rangle + 0.5477|10\rangle + 0.7303|11\rangle$$

Applichiamo $R_y(\theta)$ al primo qubit perché fa esattamente questo:

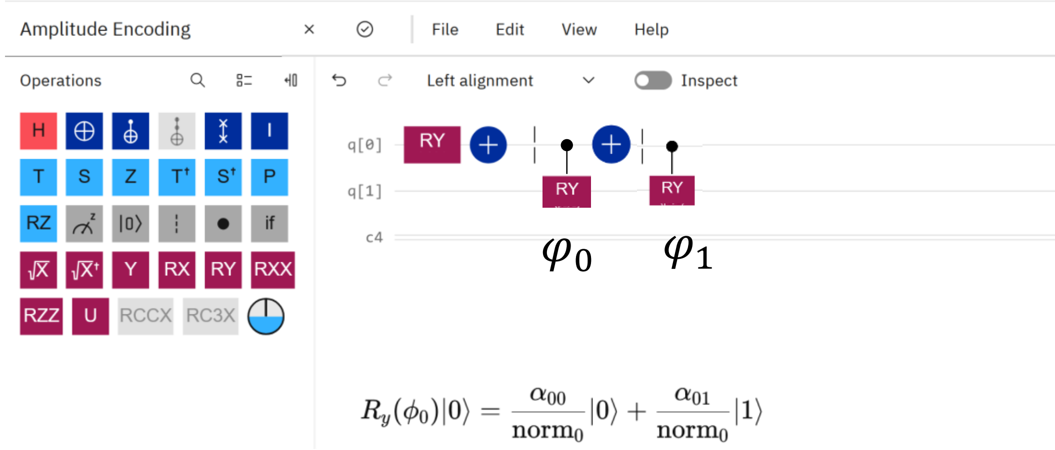
$$R_y(\theta)|0\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)|1\rangle$$

Quindi, partendo da $|00\rangle$:

$$|00\rangle \xrightarrow{R_y(\theta)\text{ su } q0} \cos(\theta/2)|00\rangle + \sin(\theta/2)|10\rangle$$

Nota cosa è successo:

- se il primo qubit è 0, siamo nel blocco $|00\rangle$
- se il primo qubit è 1, siamo nel blocco $|10\rangle$



$$R_y(\phi_0)|0\rangle = \frac{\alpha_{00}}{\text{norm}_0}|0\rangle + \frac{\alpha_{01}}{\text{norm}_0}|1\rangle$$

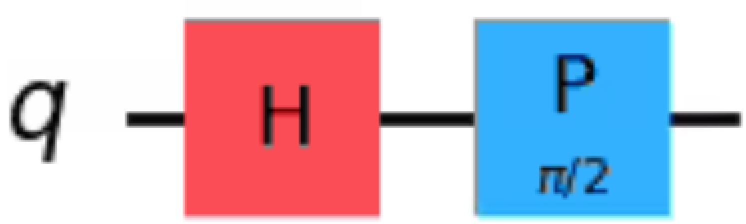
$$R_y(\phi_1)|0\rangle = \frac{\alpha_{10}}{\text{norm}_1}|0\rangle + \frac{\alpha_{11}}{\text{norm}_1}|1\rangle$$

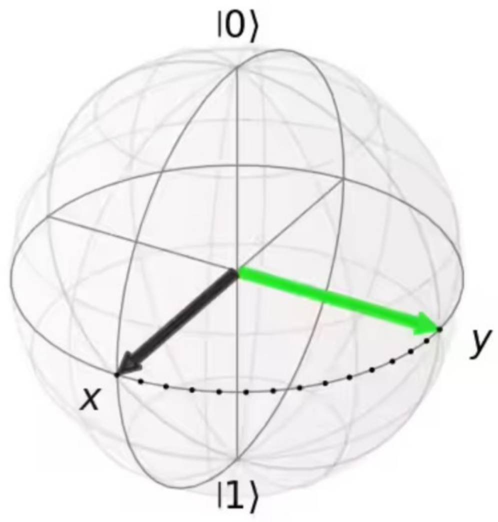
PHASE ENCODING

$$|\vec{x}_k^{(j)}\rangle = P(\phi = \vec{x}_k^{(j)})|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\vec{x}_k^{(j)}}|1\rangle\right)$$

E' la codifica più usata e più immediata da utilizzare.

Nella phase encoding i dati classici vengono inseriti nella fase delle ampiezze quantistiche. Questo significa che l'informazione non modifica direttamente le probabilità di misura, ma il modo in cui gli stati quantistici interferiscono tra loro.





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

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

$$|\alpha|^2 + |\beta|^2 = 1$$