Appunti sulla Computazione Quantistica

Victor Lopata

July 2024

Contents

1 Nozioni Matematiche

1.1 Strutture algebriche

Definition 1.1: Struttura Algebrica

Definiamo come **struttura algebrica** un insieme munito di una o più operazioni. Spesso viene indicato con la notazione (A, m), dove A è l'insieme ed m è l'operazione.

Definition 1.2: Principali strutture algebriche

Sia (A, m) una struttura algebrica, dove A è l'insieme ed m è un'operazione binaria chiusa sull'insieme. Tale struttura può essere definita come:

- **Semigruppo**: se m è associativa.
- **Monoide**: se m è associativa e munita dell'elemento neutro.
- **Gruppo**: se m è associativa, munita dell'elemento neutro e dell'elemento inverso.
- **Gruppo abeliano**: se m è associativa, munita dell'elemento neutro e dell'inverso ed è commutativa.

Definition 1.3: Anello

Sia $(A, +, \cdot)$ una struttura algebrica. Possiamo definirla come **anello** se:

- $(A, +)$ è un **gruppo abeliano**.
- $(A, \cdot)$ è un **semigruppo**.
- La moltiplicazione è distributiva rispetto alla somma:

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c) \end{aligned} \tag{1}$$

Possiamo definirlo anche come **anello commutativo** se $(A, \cdot)$ è munita della commutatività.

Fact 1.1

Sia $(A, +, \cdot)$ un anello. Allora:

$$\forall x, y \in A \quad (xy)^{-1} = y^{-1}x^{-1} \tag{2}$$

Definition 1.4: Campo

Sia $(K, +, \cdot)$ una struttura algebrica. Possiamo deifinirla come **campo** se:

- $(K, +, \cdot)$ è un **anello commutativo**.
- $(K \backslash 0, \cdot)$ è un **gruppo abeliano**.

1.2 Numeri complessi

1.3 Spazi Vettoriali

Definition 1.5: Norma Euclidiana

Sia v un vettore avente numeri complessi come entrate:

$$v = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \tag{3}$$

Definiamo la sua **norma Euclidiana** come:

$$\|v\| = \sqrt{\sum_{k=1}^{n} |{\alpha_k}^2|} \tag{4}$$

1.4 Matrici

Definition 1.6: Trasposta di una matrice

Sia A una matrice. Definiamo come **matrice trasposta** di A, rappresentata dal simbolo A^{T}, come la matrice avente il cui generico elemento con indici (i, j) è l'elemento con indice (j, i) della matrice originaria. In altre parole, la matrice trasposta di una matrice è la matrice ottenuta scambiandone le righe con le colonne.

Example 1.1

- $A = \begin{pmatrix} 2 & 1 & 4 \\ 0 & 0 & 3 \end{pmatrix} \quad A^{\mathrm{T}} = \begin{pmatrix} 2 & 0 \\ 1 & 0 \\ 4 & 3 \end{pmatrix}$
- $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \end{pmatrix} \quad A^{\mathrm{T}} = \begin{pmatrix} 1 & 6 & 11 & 16 \\ 2 & 7 & 12 & 17 \\ 3 & 8 & 13 & 18 \\ 4 & 9 & 14 & 19 \\ 5 & 10 & 15 & 20 \end{pmatrix}$

Definition 1.7: Matrice Trasposta Coniugata

Sia A una matrice avente come entrate valori complessi. Deifiniamo la sua **matrice trasposta coniugata**, rappresentata dal simbolo $A^{\dagger}$, come la matrice ottenuta effettuando la trasposta e scambiando ogni valore con il suo comlesso coniugato.

Example 1.2

$$A = \begin{pmatrix} 3+9i & 2+i \\ 7-6i & 1-3i \end{pmatrix} \quad A^{\dagger} = \begin{pmatrix} 3-9i & 7+6i \\ 2-i & 1+3i \end{pmatrix}$$

Definition 1.8: Matrici Unitarie

Sia U una matrice quadrata complessa. Definiamo U come una **matrice unitaria** se:

$$U^{\dagger}U = \mathbb{1} = UU^{\dagger}$$

dove $U^{\dagger}$ è la matrice trasposta coniugata di U e $\mathbb{1}$ è la matrice identità.

Fact 1.2

Sia U una matrice unitaria. Allora abbiamo che:

$$\|Uv\| = \|v\| \quad \forall v \text{ vettore}$$

1.5 Notazione Dirac

2 Introduzione all'informazione quantistica

2.1 Sistemi Singoli

Definition 2.1: Stato Quantistico

Definiamo come **stato quantistico** un **vettore colonna** tale che:

- Le entrate sono **numeri complessi**
- La somma dei valori assoluti elevati alla seconda deve essere uguale ad 1.

Le entrate dei vettori colonna, rappresentate dai numeri complessi, sono chiamati anche **ampiezza**.

Definition 2.2: Stato Quantistico (definizione alternativa)

Possiamo definire uno stato quantistico anche come un vettore colonna v che ha come entrate numeri complessi tale che $\|v\| = 1$.

Example 2.1: Stati Quantistici

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

Stati quantistici che non hanno una particolare denominazione vengono indicate con le lettere ψ o ϕ. Ad esempio

$$|\psi\rangle = \frac{1+2i}{3}|0\rangle - \frac{2}{3}|1\rangle$$

2.1.1 Misurazione di stati quantistici

2.1.2 Operazioni Unitarie

Le operazioni che si possono applicare sugli stati quantistici sono rappresentate dalle **matrici unitarie** (Definizione 1.4).

Observation 2.1

Se v è uno stato quantistico, allora anche Uv è uno stato quantistico.

Vediamo alcune delle più famose ed importanti operazione unitarie su un singolo Qubit:

- **Pauli Operations**:

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- **Hadamard Operation**:

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

- **Phase Operations**:

$$P_\Theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Theta} \end{pmatrix} \quad S = P_{\frac{\pi}{2}} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad T = P_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix}$$

Vediamo ora degli esempi sull'applicazione di queste operazioni sugli stati quantistici.

1. $H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle$
2. $H|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle$
3. $H|+\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$
4. $H|-\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$
5. $T|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$
6. $T|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{1+i}{\sqrt{2}} \end{pmatrix} = \frac{1+i}{\sqrt{2}}|1\rangle$
7. $T|+\rangle = T\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{\sqrt{2}}T|0\rangle + \frac{1}{\sqrt{2}}T|1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1+i}{2}|1\rangle$
8. $HSH = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$
9. $(HSH)^2 = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

2.2 Sistemi Multipli

I sistemi multipli possono esser visti come singoli sistemi composti tra di loro.

Definition 2.3: Stati quantistici nei Sistemi Multipli

Gli stati quantisitic nei sistemi multipli sono rappresentati sempre dai vettori colonna, le quali entrate hanno numeri complessi (come negli stati quantistici dei sistemi singoli) e gli indici dei vettori sono posizionati in corrispondenza del prodotto cartesiano tra gli insiemi degli stati di ciascun sistema.
Sia quindi v tale vettore, deve soddisfare sempre:

$$\|v\| = 1$$

Example 2.2

Ad esempio, siano X ed Y sistemi che rappresentano qubits e vogliamo rappresentare il sistema multiplo (X, Y). Allora il suo insieme degli stati classici è definito dal prodotto cartesiano:

$$\{0,1\} \times \{0,1\} = \{00, 01, 10, 11\}$$

Quindi un esempio di stato quantistico per il sistema multiplo (X, Y) può essere:

$$\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{6}}|01\rangle + \frac{i}{\sqrt{6}}|10\rangle + \frac{1}{\sqrt{6}}|11\rangle$$

Esistono molti modi su come rappresentare i vettori degli stati quantistici di sistemi multipli. Ecco alcuni di uso comune:

$$|0\rangle|1\rangle$$

$$|0\rangle \otimes |1\rangle$$

$$|0\rangle_X|1\rangle_Y$$

Oppure possiamo, ovviamente, scriverlo esplicitamente:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{6}} \\ \frac{i}{\sqrt{6}} \\ \frac{1}{\sqrt{6}} \end{pmatrix}$$

2.2.1 Prodotto Tensoriale di vettori di stati quantistici

Come per i vettori probabilistici, il prodotto tensoriale tra due vettori di stati quantistici produce un nuovo vettore di stato quantistico.

Theorem 2.1: Chiusura prodotto tensoriale

Siano $|\phi\rangle$ e $|\psi\rangle$ due stati quantistici rispettivamente di X e di Y. Il prodotto tensoriale tra i due stati quantistici produce uno stato quantistico.

Proof.

$$\||\phi\rangle \otimes |\psi\rangle\| = \sqrt{\sum_{(a,b)\in\Sigma\times\Gamma} |\langle ab|\phi\otimes\psi\rangle|^2} =$$

$$= \sqrt{\sum_{a\in\Sigma}\sum_{b\in\Gamma} |\langle a|\phi\rangle\langle b|\psi\rangle|^2} =$$

$$= \sqrt{\sum_{a\in\Sigma} |\langle a|\phi\rangle|^2 \sum_{b\in\Gamma}\langle b|\psi\rangle|^2} =$$

$$= \||\phi\rangle\|\||\psi\rangle\|$$

Sappiamo che $\|\phi\rangle\| = 1$ e $\|\psi\rangle\| = 1$. Di conseguenza $\||\phi\rangle\|\||\psi\rangle\| = 1$, dimostrando che $|\phi\rangle \otimes |\psi\rangle$ è uno vettore di uno stato quantistico. □

Tale teorema viene generalizzato in per **più di due sistemi**; siano $|\phi_1\rangle, \ldots, |\phi_n\rangle$ vettori di stati quantistici dei sistemi $X_1, \ldots, X_n$. Allora il prodotto tensoriale $|\phi_1\rangle \otimes \ldots \otimes |\phi_n\rangle$ produce un vettore di uno stato quantistico del sistema $(X_1, \ldots, X_n)$. È facilmente dimostrabile considerando la dimostrazione del precedente teorema.

Sia $|\phi\rangle$ uno stato quantistico del sistema X e sia $|\psi\rangle$ uno stato quanistico del sistema Y; allora, il vettore $|\phi\rangle \otimes |\psi\rangle$ rappresenta uno stato quantistico per il sistema multiplo (X, Y). Ricordiamo che il prodotto tensoriale rappresenta **l'indipendenza** tra i due sistemi, di conseguenza gli stati dei due sistemi non hanno niente a che vedere l'uno con l'altro.

2.2.2 Sistemi Entangled

Esistono vettori di sistemi quantistici che non sono il prodotto tensoriale tra due vettori di sistemi quantistici. Prendiamo come esempio il seguente stato quantistico:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \tag{5}$$

Non esistono stati tali che il loro prodotto tensoriale sia equivalente allo stato di sopra.

Proof. Siano, per assurdo, $|\phi\rangle$ e $|\psi\rangle$ i due stati tali che:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = |\phi\rangle \otimes |\psi\rangle$$

Deve essere necessariamente

$$\langle 0|\phi\rangle\langle 1|\phi\rangle = \langle 01|\phi \otimes \psi\rangle$$

implicando che:

$$\langle 0|\phi\rangle = 0 \vee \langle 1|\phi\rangle = 0$$

ma questo porta ad una contraddizione; infatti

$$\langle 0|\phi\rangle\langle 0|\psi\rangle = \langle 00|\phi \otimes \psi\rangle = \frac{1}{\sqrt{2}} \wedge \langle 1|\phi\rangle\langle 1|\psi\rangle = \langle 11|\phi \otimes \psi\rangle = \frac{1}{\sqrt{2}}$$

nessuna delle due equazioni produce 0. □

Lo stato rappresentato dal vettore dell'equazione 5, rappresenta una **correllazione** tra i due sistemi. Diciamo che questi sono **entangled (impigliati)**.

2.2.3 Bell States

Definition 2.4: Stati di Bell

Definiamo gli **stati di Bell** i seguenti stati quantistici:

1. $|\phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
2. $|\phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$
3. $|\psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$
4. $|\phi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$

La collezione dei quattro stati $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ forma la **base di Bell**: qualsiasi vettore di uno stato quantistico a due qubit può essere espresso come una combinazione lineare dei quattro stati di Bell.

2.2.4 Stati GHZ e W

Vediamo ora alcuni stati quantistici importanti di 3 quibt:

- **Stato GHZ**:
$$\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle \tag{6}$$
- **Stato Z**:
$$\frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|010\rangle + \frac{1}{\sqrt{3}}|100\rangle \tag{7}$$

Nessuno di questi due stati possono essere prodotti da stati quantistici attraverso il prodotto tensore.

2.2.5 Misurazione

Sia $(X_1, \ldots, X_n)$ un sistema multiplo avente come insieme degli stati $\Sigma = \Sigma_1 \times \ldots \times \Sigma_n$. Sia il sistema nello stato $|\phi\rangle$; allora, la probabilità di ottenere lo stato generico $(a_1, \ldots, a_n) \in \Sigma$ dopo la misurazione è data dalla formula:

$$|\langle a_1, \ldots, a_n | \psi \rangle|^2 \tag{8}$$

Vogliamo ora **misurare parzialmente** il sistema, quindi ottenere il nuovo stato quantistico dopo una misurazione parziale del sistema. Iniziamo a vedere come funziona per due sistemi, per poi generalizzare a più sistemi.

Sia quindi X e Y due sistemi aventi rispettivamente Σ e Γ come insieme degli stati classici. Supponiamo che stia in uno stato generico $|\psi\rangle$. Rappresentiamolo con la Dirac-notation:

$$|\psi\rangle = \sum_{(a,b) \in \Sigma \times \Gamma} \alpha_{ab} |ab\rangle$$

Supponiamo di voler misurare solo il sistema X, allora la probabilità che X sia in uno stato $a \in \Sigma$ è uguale ad:

$$\sum_{b \in \Gamma} |\langle ab | \psi \rangle|^2 = \sum_{b \in \Gamma} |\alpha_{ab}|^2$$

Dopo la misurazione di X, il suo stato cambia in $|a\rangle$. Cosa succede allo stato di Y? Per rispondere a questa domanda bisogna descrivere il nuovo stato di (X, Y) sotto l'assunzione che X è stata misurata ottenendo lo stato a.

Come primo passo, rappresentiamo lo stato $|\psi\rangle$ in questa maniera:

$$|\psi\rangle = \sum_{a \in \Sigma} |a\rangle \otimes |\phi_a\rangle$$

dove

$$|\phi_a\rangle = \sum_{b \in \Gamma} \alpha_{ab} |b\rangle$$

Possiamo osservare che:

$$\sum_{b \in \Gamma} |\alpha|^2 = \| |\phi\rangle \|^2$$

Abbiamo quindi che, il nuovo stato del sistema (X, Y) dopo la misurazione di X (con risultato a), è pari a

$$|a\rangle \otimes \frac{|\phi\rangle}{\| |\phi\rangle \|}$$

$|a\rangle \otimes |\phi\rangle$ rappresenta la parte di $|\psi\rangle$ consistente con la misurazione di X. Andiamo poi a *normalizzare* il vettore, dividendo per la sua norma Euclidiana ,

corrispondente a $|\phi\rangle$; quest'ultimo passaggio serve per portare lo stato ad avere la norma Euclidiana valida per gli stati quantistici, ovvero uguale ad 1.

Example 2.3

Consideriamo lo stato di due qubit (X, Y)

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{6}}|01\rangle + \frac{i}{\sqrt{6}}|10\rangle + \frac{1}{\sqrt{6}}|11\rangle$$

Inizialmente scriviamo lo stato nella seguente forma:

$$|\psi\rangle = |0\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{6}}|1\rangle\right) + |1\rangle \otimes \left(\frac{i}{\sqrt{6}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle\right)$$

La probabilità che, dopo la misurazione, X stia nello stato 0 è pari a

$$\|\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{6}}|1\rangle\|^2 = \frac{1}{2} + \frac{1}{6} = \frac{2}{3}$$

implicando che lo stato di (X, Y) diventa:

$$|0\rangle \otimes \frac{\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{6}}|1\rangle}{\sqrt{\frac{2}{3}}} = |0\rangle \otimes \left(\sqrt{\frac{3}{4}}|0\rangle - \frac{1}{2}|1\rangle\right)$$

I passaggi sono identici nel caso in cui la misurazione di X sia 1.
Vediamo ora cosa succede allo stato se misuriamo Y. Iniziamo rappresentando (analogamente) lo stato $|\psi\rangle$ nel modo che ci fa più comodo:

$$|\psi\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{6}}|1\rangle\right) \otimes |0\rangle + \left(-\frac{1}{\sqrt{6}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle\right) \otimes |1\rangle$$

Ipotizziamo quindi che, dopo la misurazione, Y stia nello stato di 0; la sua probabilità è pari a:

$$\| - \frac{1}{\sqrt{6}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle\|^2 = \frac{1}{6} + \frac{1}{6} = \frac{1}{3}$$

Allora il nuovo stato di (X, Y) diventa:

$$\frac{-\frac{1}{\sqrt{6}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle}{\sqrt{\frac{1}{3}}} \otimes |1\rangle = \left(-\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes |1\rangle$$

Tali passaggi possono essere effettuati per n sistemi congiunti: il passaggio chiave è ordinare e rappresentare lo stato $|\psi\rangle$ nel modo che ci fa più comodo.

2.2.6 Operazioni Unitarie

Come per lo stato singolo, usiamo le **matrici unitarie** per rappresentare operazioni quantistiche su sistemi composti. Gli indici dellerighe e delle colonne di tale matrice sono posizionati in corrispondenza del prodotto cartesiano tra gli insiemi degli stati di ciascun sistema.

Example 2.4

Siano X e Y due sistemi aventi rispettivamente $\Sigma = \{1, 2, 3\}$ e $\Gamma = \{0, 1\}$ come insieme degli stati. L'insieme dello stato multiplo (X, Y) corrisponde a $\Sigma \times \Gamma = \{(1,0), (1,1), (2,0), (2,1), (3,0), (3,1)\}$. Ecco un esempio di una matrice unitaria rappresentante un'operazione sul sistema (X, Y):

$$U = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{i}{2} & -\frac{1}{2} & 0 & 0 & -\frac{i}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{2} & -\frac{i}{2} & -\frac{1}{2} & 0 & 0 & \frac{i}{2} \\ 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{pmatrix}$$

Per dimostrare che sia **unitaria** basta verificare che $U^\dagger U = \mathbb{1} = UU^\dagger$. Applichiamo tale operazione allo stato $|11\rangle$:

$$U|11\rangle = \frac{1}{2}|10\rangle + \frac{i}{2}|11\rangle - \frac{1}{2}|20\rangle - \frac{i}{2}|30\rangle$$

Notiamo che le ampiezze di $U|11\rangle$ corrispondono alla seconda colonna della matrice unitaria.

Immaginiamo ora di avere le operazioni $U_1, \ldots, U_n$ applicabili rispettivamente sui sistemi $X_1, \ldots, X_n$. Se le operazioni vengono operate **indipendentemente** sui sistemi, allora l'operazione combinata sul sistema $(X_1, \ldots, X_n)$ è rappresentata dalla matrice unitaria $U_1 \otimes \ldots \otimes U_n$.

Una situazione comune è l'applicare operazioni solo su un sottoinsieme dei sistemi multipli. Ad esempio, sia (X, Y) un sistema e vogliamo applicare l'operazione U_Y sul sistema X; questo implica la non applicazione di alcuna operazione su Y, ovvero applicare la funzione identità su di esso. Ricapitolando, applicare un'operazione su X e non fare niente su Y equivale applicare l'operazione rappresentata dalla matrice unitaria $U_X \otimes \mathbb{1}_Y$. Lo stesso procedimento può essere applicato se non si vuole fare niente sul sistema X ed applicare U_Y ad Y: $\mathbb{1}_X \otimes U_Y$.

Observation 2.2

Non tutte le matrici unitarie possono essere espresse come prodotto tensoriale di matrici unitarie; questo fatto dipende dalla **dipendenza** che i sistemi hanno.

Vediamo qualche esempio di operazioni comuni che non possono esser rappresentate dal prodotto tensoirale di altre operazioni.

- **Operazione SWAP**: Siano X ed Y due sistemi che condividono lo stesso insieme di stati Σ. L'operazione di **SWAP** sul sistema (X, Y) è l'operazione che scambia le informazioni tra i due sistemi. Tale operazione è rappresentata dalla seguente matrice unitaria:

$$\textbf{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

  Sia, ad esempio, $\Sigma = \{0, 1\}$. Allora:

$$\textbf{SWAP}|01\rangle = |10\rangle$$

  Più in generale, tale operazione soddisfa:

$$\textbf{SWAP}|a\rangle|b\rangle \ = |b\rangle|a\rangle \qquad \forall a, b \in \Sigma$$

  Vediamo come si comporta con gli stati di Bell:

$$\textbf{SWAP}|\phi^+\rangle = |\phi^+\rangle$$

$$\textbf{SWAP}|\phi^-\rangle = |\phi^-\rangle$$

$$\textbf{SWAP}|\psi^+\rangle = |\psi^+\rangle$$

$$\textbf{SWAP}|\psi^-\rangle = -|\psi^-\rangle$$

- **Operazione Controlled-U** Sia Q un sistema rappresentante un qubit ed R un qualsiasi altro sistema arbitrario. Sia U un'operazione applicabile su R. Definiamo l'operazione **Controlled-U**, applicabile sul sistema multiplo (Q, R), come segue:

$$CU = |0\rangle\langle 0| \otimes \mathbb{1}_R + |1\rangle\langle 1| \otimes U$$

  In parole semplici, se $X = 0$ applica $\mathbb{1}$ ad R. Altrimenti, se $X = 1$, applica U ad R.

  Ad esempio, il **Controlled-NOT** è rappresentabile come:

$$CX = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \phi_X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Vediamo ora **CSWAP**:

$$\textbf{CSWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Questa operazione è meglio conosciuta come **operazione di Fredkin** (più comunemente Fredkin gate), e funziona nel seguente modo:

$$\textbf{CSWAP}|0bc\rangle = |0bc\rangle$$

$$\textbf{CSWAP}|1bc\rangle = |1cb\rangle$$

Infine, vediamo l'operazione **controlled-controlled-NOT**, o anche **CCX**. È comunemente conosciuta come l'operazione di **Toffoli** (Toffoli gate), e la sua matrice è rappresentata come:

$$\textbf{CCX} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

2.3 Circuiti Quantistici

Figure 1

Definition 2.5: Circuito

Definiamo come **circuito** un modello di computazione nella quale l'informazione è trasportata dai 'fili' (wires) attraverso una rete di 'porte' (gates), le quali rappresentano l'operazione applicata all'informazione trasportata.

Nel modello quantistico, i fili e le porte rappresentano rispettivamente i qubits e le operazioni applicabili su di essi. Ad esempio, la figura 1 rappresenta l'applicazione delle operazioni H, S, H e T su un singolo qubit. I circuiti quantistici hanno spesso i qubits inizializzati a $|0\rangle$. Se preferiamo, è possibile rappresentare alla fine del circuito il nuovo stato a seguito delle trasformazioni, come mostrato nella figura 2.

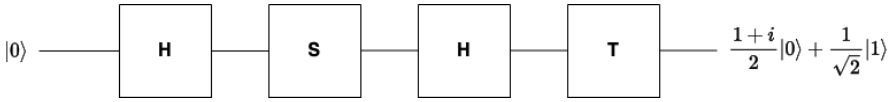

Figure 2

La figura 3, invece, mostra un'operazione su un sistema multiplo, a due qubit. La prima, intuitivamente, rappresenta l'operazione di Hadamard; la seconda, invece, è il controlled-NOT, dove il cerchio riempito rappresente il qubit di controllo, mentre il $\otimes$ rappresenta il qubit target.

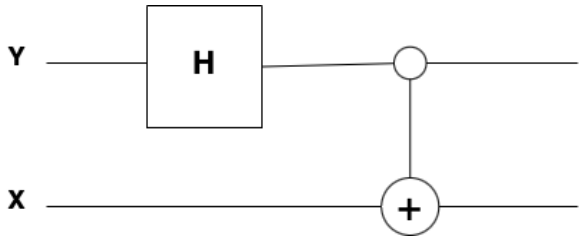

Figure 3

Notiamo anche che nel modello è implicito l'applicazione dell'operazione identità sul qubit X. Sia quindi U la matrice unitaria rappresentante le due

operazioni. U è definita come:

$$U = (\mathbb{1} \otimes H)\left(|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \phi_X\right) = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \end{pmatrix}$$

Abbiamo che:

$$\begin{aligned} U|00\rangle &= |\phi^+\rangle \\ U|01\rangle &= |\phi^-\rangle \\ U|10\rangle &= |\psi^+\rangle \\ U|11\rangle &= -|\psi^-\rangle \end{aligned}$$

I fili con due linee rappresentano i classici bit. Vengono utilizzati dopo aver eseguito una misurazione come mostrato nella figura 4.

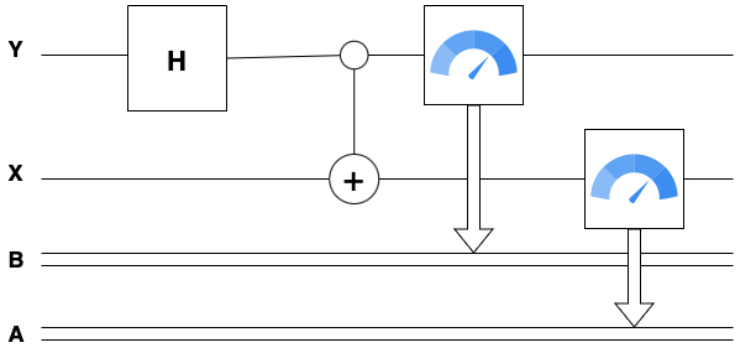

Figure 4

È spesso conveniente rappresentare i fili dei bit dopo la misurazione sullo stesso livello dei fili dei qubit, come mostrato nella figura 5

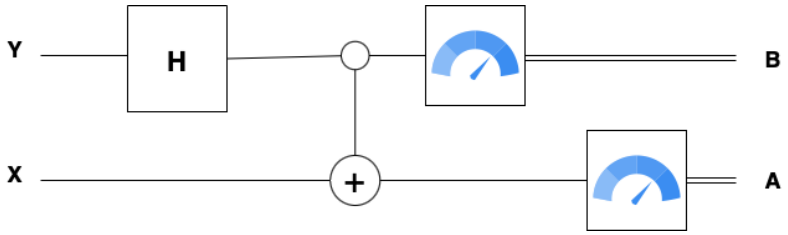

Figure 5

Ecco alcune porte comunemente usate per 1 o più qubit:

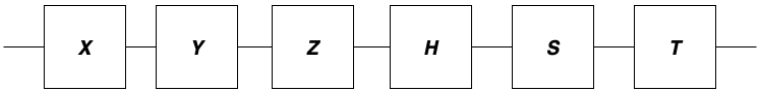

Figure 6

La figura 6 rappresenta le operazioni che si fanno su un singolo qubit, abbiamo in ordine: σ_x, σ_y, σ_z, Hadamard e le due Phase Operations.

La porta Not possiamo rappresentarla anche come nella figura 7.

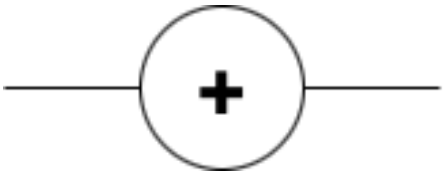

Figure 7: Not gate

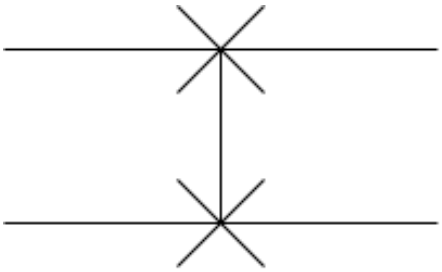

Figure 8: SWAP gate

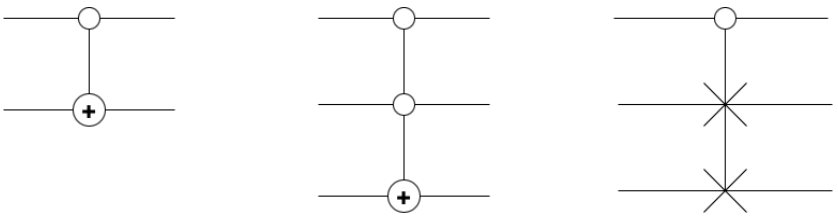

Figure 9

La figura 8 rappresenta la porta SWAP. Infine la figura 9 rappresentano le porte di controllo, rispettivamente **controlled-NOT**, **controlled-controlled-NOT** e **controlled-SWAP**.

Operazioni arbitrarie sono rappresentate da rettangoli nominati con il nome dell'operazione unitaria. La figura 10 mostra un esempio. La figura a destra è la versione controllata.

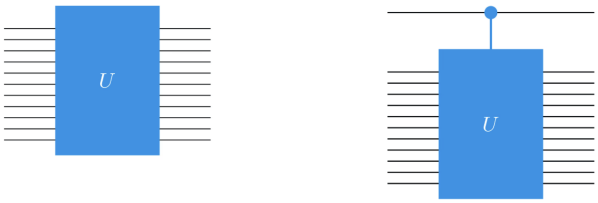

Figure 10

2.4 Limitazioni nell'informazione quantistica

2.4.1 Irrillevanza della fase globale

Siano $|\psi\rangle$ e $\phi\rangle$ due vettori unitari che rappresentano due stati quantistici. Assumiamo che esista un numero complesso α, con $|\alpha| = 1$, tale che:

$$|\phi\rangle = \alpha|\psi\rangle$$

Allora diciamo che i vettori $|\phi\rangle$ e $|\psi\rangle$ **differiscono di una fase globale**. Diciamo anche che α è la fase globale.

Consideriamo, quindi, un sistema che sta in uno dei due stati, $|\phi\rangle$ o $|\psi\rangle$ e che differiscono di una fase globale. Analizziamo cosa succede durante la misurazione. Nel caso in cui il sistema si trovi nello stato $|\psi\rangle$, abbiamo che la probabilità di misurare uno stato classico $a \in \Sigma$ è:

$$|\langle a|\psi\rangle|^2$$

Nel secondo caso, in cui lo stato sia $|\phi\rangle$, la probabilità che la misurazione dia come risultato lo stato $a \in \Sigma$ è:

$$|\langle a|\phi\rangle|^2 = |\alpha\langle a|\psi\rangle|^2 = |\alpha|^2|\langle a|\psi\rangle|^2 = |\langle a|\psi\rangle|^2$$

perchè $|\alpha|^2 = 1$. Notiamo che la probabilità di misurare uno stato classico a è esattamente lo stesso per i due stati.

Consideriamo ora l'applicazione di un'operazione unitaria U su entrambi gli stati. Nel caso in cui lo stato iniziale è $|\psi\rangle$, allora dopo l'applicazione il nuovo stato diventa:

$$U|\psi\rangle$$

Nel caso, invece, in cui lo stato iniziale è $|\phi\rangle$, dopo l'applicazione lo stato diventa:

$$U|\phi\rangle = \alpha U|\psi\rangle$$

Notiamo che i due stati risultanti differiscono dalla stessa fase globale α.

Concludiamo che, i due stati che differiscono da una fase globale sono completamente indistinguibili. Per questo, $|\phi\rangle$ e $|\psi\rangle$ sono considerati **equivalenti**, e sono visti effettivamente come lo stesso stato.

Example 2.5

Ad esempio $|-\rangle$ e $-|-\rangle$ differiscono per la fase globale -1, quindi possono essere considerati lo stesso stato.

2.4.2 Teorema no-cloning

Theorem 2.2: No-cloning

Siano X ed Y due sistemi che condividono lo stesso insieme di stati classici Σ (avente almeno 2 elementi). Allora, possiamo affermare che **non** esiste uno stato quanistico $|\phi\rangle$ di Y e un'operazione unitaria U sul sistema composto (X, Y) tale che

$$U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle \quad \forall |\psi\rangle \in X$$

Proof. Σ deve contenere almeno due elementi. Scegliamo, quindi, $a, b \in \Sigma$, con $a \neq b$. Supponiamo **per assurdo** che esista uno stato quantistico $|\phi\rangle$ e un'operazione unitaria U sul sistema composto (X, Y) tale che

$$U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle \quad \forall |\psi\rangle \in X$$

Nel nostro caso:

$$U(|a\rangle \otimes |\phi\rangle) = |a\rangle \otimes |a\rangle \wedge U(|b\rangle \otimes |\phi\rangle) = |b\rangle \otimes |b\rangle$$

Consideriamo il caso in cui $|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$. Sfruttando la caratteristica della linearità del prodotto tensoriale nel primo argomento ed la linearità del prodotto matrice-vettore nel secondo argomento, abbiamo che:

$$U\left(\left(\tfrac{1}{\sqrt{2}}|a\rangle + \tfrac{1}{\sqrt{2}}|b\rangle\right) \otimes |\phi\rangle\right)$$

$$= U\left(\tfrac{1}{\sqrt{2}}|a\rangle \otimes |\phi\rangle + \tfrac{1}{\sqrt{2}}|b\rangle \otimes |\phi\rangle\right)$$

$$= \tfrac{1}{\sqrt{2}}|a\rangle \otimes |a\rangle + \tfrac{1}{\sqrt{2}}|b\rangle \otimes |b\rangle$$

Svolgendo i conti senza sfruttare la linearità degli argomenti, notiamo che:

$$U\left(\left(\tfrac{1}{\sqrt{2}}|a\rangle + \tfrac{1}{\sqrt{2}}|b\rangle\right) \otimes |\phi\rangle\right)$$

$$= \left(\tfrac{1}{\sqrt{2}}|a\rangle + \tfrac{1}{\sqrt{2}}|b\rangle\right) \otimes \left(\tfrac{1}{\sqrt{2}}|a\rangle + \tfrac{1}{\sqrt{2}}|b\rangle\right) \neq \tfrac{1}{\sqrt{2}}|a\rangle \otimes |a\rangle + \tfrac{1}{\sqrt{2}}|b\rangle \otimes |b\rangle$$

□

Observation 2.3

La **clonazione perfetta** non esiste, ma è possibile clonare con una percentuale di accuratezza limitata.

Observation 2.4

È possibile clonare perfettamente stati appartenenti a una base standard, come gli stati classici dei qubits.

Costruiamo un circuito in grado di clonare uno stato classico del qubit, utilizzando l'operazione del **control-not**:

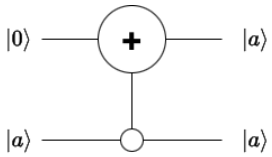

Figure 11

2.5 Teletrasporto Quantistico

Definition 2.6: Teletrasporto Quantistico

Definiamo come **teletrasporto quantistico** il protocollo tale che la sua funzione è il trasporto di informazione sfruttando gli e-bit (stati quantistici entangled).

Siano, quindi, Alice (mittente) e Bob (destinatario) due entità che vogliono scambiarsi un qubit. Assumiamo che entrambe le entità condividano un e-bit: Alice conserva il qubit **A** e Bob il qubit **B** e la loro unione formano lo stato **entangled** $|\phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Alice vuole 'spedire' il qubit **Q**, ovvero far in modo che Bob abbia un qubit avente lo stesso stato. Bob ed Alice non conoscono alcuna informazione riguardo allo stato Q. Non vi sono assunzioni riguardo a quest'ultimo, quindi potrebbe essere anche uno stato entangled con un altro stato.

La figura 12 mostra il circuito che descrive il funzionamento del protocollo.

Observation 2.5

Notiamo che il qubit Q che Alice vuole trasmettere a Bob viene distrutto, richiamando quindi il teorema no-cloning. Questo è il costo del teletrasporto quantistico.

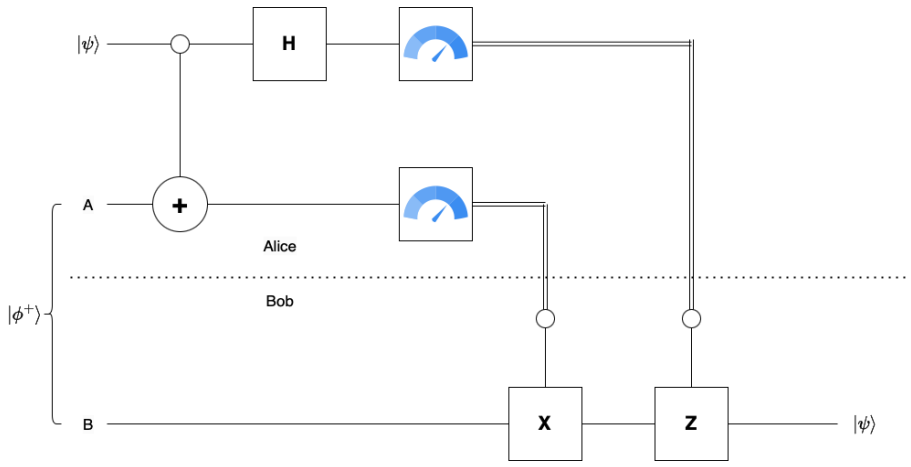

Figure 12

Andiamo ora ad analizzare il funzionamento del circuito. Sia Q nello stato generico

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

Sia (B,A,Q) il sistema che dello stato del circuito. Lo stato iniziale di tale sistema è:

$$|\phi^+\rangle \otimes \left(\alpha|0\rangle + \beta|1\rangle\right) = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|110\rangle + \beta|001\rangle + \beta|111\rangle\right)$$

Lo stato dopo aver applicato l'operazione controlled-not diventa:

$$\frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|110\rangle + \beta|011\rangle + \beta|101\rangle\right)$$

Applichiamo ora l'operazione di Hadamard, trasformando lo stato in:

$$\tfrac{1}{\sqrt{2}}\left(\alpha|00\rangle|+\rangle + \alpha|11\rangle|+\rangle + \beta|01\rangle|-\rangle + \beta|10\rangle|-\rangle\right)$$

$$= \tfrac{1}{2}\left(\alpha|000\rangle + \alpha|001\rangle + \alpha|110\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|011\rangle + \beta|100\rangle - \beta|101\rangle\right)$$

$$= \tfrac{1}{2}\left(\alpha|0\rangle + \beta|1\rangle\right)|00\rangle + \tfrac{1}{2}\left(\alpha|0\rangle - \beta|1\rangle\right)|01\rangle + \tfrac{1}{2}\left(\alpha|1\rangle + \beta|0\rangle\right)|10\rangle + \tfrac{1}{2}\left(\alpha|1\rangle - \beta|0\rangle\right)|11\rangle$$

Analizziamo i possibili casi di misurazione:

- La probabilità di misurare $A = 0$ e $Q = 0$ è di

  $$\|\frac{1}{2}\left(\alpha|0\rangle + \beta|1\rangle\right)|00\rangle\|^2 = \frac{1}{4}\left(|\alpha|^2 + |\beta|^2\right) = \frac{1}{4}$$

  e lo stato (B, A, Q) diventa:

  $$\left(\alpha|0\rangle + \beta|1\rangle\right)|00\rangle$$

  In questo caso, Bob non deve applicare alcuna operazione.

- La probabilità di misurare $A = 0$ e $Q = 1$ è di

$$\|\frac{1}{2}\left(\alpha|0\rangle - \beta|1\rangle\right)|01\rangle\|^2 = \frac{1}{4}\left(|\alpha|^2 - |\beta|^2\right) = \frac{1}{4}$$

e lo stato (B, A, Q) diventa:

$$\left(\alpha|0\rangle - \beta|1\rangle\right)|01\rangle$$

In questo caso, Bob deve applicare l'operazione Z al suo qubit B, ovvero:

$$\left(\alpha|0\rangle + \beta|1\rangle\right)|01\rangle$$

- La probabilità di misurare $A = 1$ e $Q = 0$ è di

$$\|\frac{1}{2}\left(\alpha|1\rangle + \beta|0\rangle\right)|10\rangle\|^2 = \frac{1}{4}\left(|\alpha|^2 + |\beta|^2\right) = \frac{1}{4}$$

e lo stato (B, A, Q) diventa:

$$\left(\alpha|1\rangle + \beta|0\rangle\right)|10\rangle$$

In questo caso, Bob deve applicare l'operazione X al suo qubit B, ovvero:

$$\left(\alpha|0\rangle + \beta|1\rangle\right)|10\rangle$$

- La probabilità di misurare $A = 1$ e $Q = 1$ è di

$$\|\frac{1}{2}\left(\alpha|1\rangle - \beta|0\rangle\right)|11\rangle\|^2 = \frac{1}{4}\left(|\alpha|^2 + |\beta|^2\right) = \frac{1}{4}$$

e lo stato (B, A, Q) diventa:

$$\left(\alpha|1\rangle - \beta|0\rangle\right)|11\rangle$$

In questo caso, Bob deve applicare l'operazione X e Z al suo qubit B, ovvero:

$$\left(\alpha|0\rangle + \beta|1\rangle\right)|11\rangle$$

Osserviamo che in tutti i casi, lo stato di B è uguale a $\alpha|0\rangle + \beta|1\rangle$, ovvero lo stato iniziale di Q; abbiamo, quindi, teletrasportato l'informazione del qubit Q da Alice a Bob.

3 Fondamenta degli Algoritmi Quantistici

In questa sezione viene descritto quali sono e come vengono eseguite le computazioni su un computer quantistico. Inizialmente vengono analizzate le differenze che si hanno quando ci si confronta con un modello di computazione classico e, nello specifico, verranno elencati algoritmi quantistici che offrono vantaggi rispetto ad una computazione classica.

3.1 Computazione classica vs Computazione quantistica

Uno dei primi vantaggi che una computazione quantistica può offrire è sicuramente quello del **tempo**; infatti, per alcuni problemi, sono state proposte nuove soluzione che hanno dimostrato un incremento esponenziale del tempo di esecuzione.

Mediante l'utilizzo di porta logica di **Toffoli**, è possibile simulare circuiti logici classici su circuiti quantistici. La porta di **Toffoli** riesce ad implementare un qualsiasi circuto Booleano; inoltre, la reversibilità di tale porta, contribuisce alla simulazione dei circuiti classici su circuiti quantistici.

Ad esempio, riusciamo a simulare la porta NAND (irreversibile) con la porta di Toffoli. La figura 13 mostra il NAND implementato con il Toffoli gate.

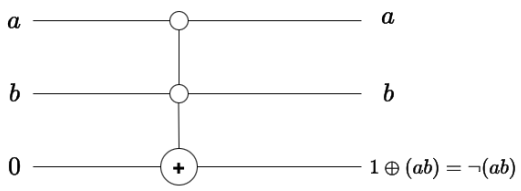

Figure 13

Fact 3.1

È possibile implementare qualsiasi circuito booleano classico attraverso la porta di Toffoli.

3.2 Parallelismo Quantistico

Data una funzione $f(x)$, definiamo (a parole semplici) il **parallelismo quantistico** come una caratteristica del mondo quantistico che permette la valutazione di $f(x)$ per diversi valori di x simultaneamente.

Supponiamo che $f(x) : \{0,1\} \to \{0,1\}$. Calcolare tale funzione in un'ambiente quantistico necessita la definizione di un'operazione unitaria, solitamente chiamata U_f, rappresentata nella figura 14. Quindi dobbiamo considerare un computer quantistico a due qubit, che inizializza lo stato a $|x, y\rangle$.

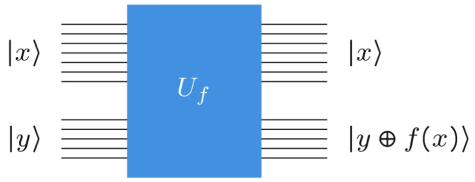

Figure 14

Dopo l'applicazione di U_f, riusciamo a trasformare lo stato in $|x, y \oplus f(x)\rangle$, dove $\oplus$ indica l'operazione *bitwise* dello XOR. Denominiamo il primo registro come *data* e il secondo come *target*.

Observation 3.1

Se $y = 0$, allora lo stato finale del secondo qubit è equivalente ad $f(x)$.

Supponiamo ora che inizializziamo il registro *data* nella superposizione

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

la quale può essere ottenuta, ad esempio, applicando la porta di Hadamard sullo stato base $|0\rangle$. Supponiamo anche di inizializzare il ragistro *target* con $|0\rangle$. Quindi:

$$U_f\left(\left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right) \otimes |0\rangle\right) = \tfrac{1}{\sqrt{2}}\left(U_f\left(|0\rangle \otimes |0\rangle\right) + U_f\left(|1\rangle \otimes |0\rangle\right)\right)$$

$$= \tfrac{1}{\sqrt{2}}\left(|0\rangle \otimes |f(0)\rangle + (|1\rangle \otimes |f(1)\rangle)\right)$$

Osserviamo, incredibilmente, di come ci sia bastata una singola valutazione per computare la funzione su tutto il dominio della funzione ($\{0, 1\}$). Abbiamo semplicemente sfruttato l'abilità di un qubit di stare in una superposizione tra stati differenti.

Questa procedura è generalizzabile per tutte le funzioni aventi un numero arbitrario di bits, utilizzando un'operazione generale conosciuta come **trasformazione di Hadamard**, o anche **trasformazione di Walsh-Hadamard**. È semplicemente l'applicazione di n porte di Hadamard in parallelo su n qubits.

Example 3.1

Ad esempio, per 2 qubit inizializzati allo stato base $|0\rangle$, la trasformazione ci da come output:

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{2}\right) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{\sqrt{2}}$$

Nel esempio, denotiamo con $H^{\otimes 2}$ l'operazione parallela delle porte di Hadamard. Più in generale, la computazione di tale trasformazione su n qubit con stato di partenza a $|0\rangle$ è equivalente a

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \Sigma} |x\rangle$$

ed indichiamo con $H^{\otimes n}$ tale operazione. Otteniamo una superposizione di 2^n stati usando solo n porte.

La misurazione dello stato $\frac{1}{\sqrt{2^n}} \sum_{x \in \Sigma} |x\rangle$ ci restituisce solo $f(x)$, per un singolo valore x. Non ci è tanto utile, quindi è necessaria l'abilità di estrazione di informazioni su più di un valore di $f(x)$ dalla superposizione per poter sfruttare questo parallelismo.

3.3 Algoritmo di Deutsch

L'algoritmo di Deutsch, proposto da David Deutsch, è il primo algoritmo quantistico che dimostra quanto i circuiti quantistici performino meglio dei circuiti classici.

Sia $f : \{0,1\} \to \{0,1\}$. Come abbiamo visto in precedenza, esistono 4 tipi di funzioni di questo tipo:

a	$f_1(a)$
0	0
0	0

a	$f_2(a)$
0	0
0	1

a	$f_3(a)$
0	1
0	0

a	$f_4(a)$
0	1
0	1

che rappresentano rispettivamente la costante 0, la funzione identità, la funzione di negazione e la costante 1. Definiamo la prima e l'ultima funzione come **costanti**, e la seconda e terza funzione come **bilanciate**.

Definition 3.1: Problema di Deutsch

Data in input una funzione $f : \{0,1\} \to \{0,1\}$, definiamo come **problema di Deutsch** il determinare se tale funzione è **costante** o **bilanciata**.

L'output di tale algoritmo ci darà 0 se f è costante, 1 se f è bilanciata. Associamo, per ogni funzione, la stringa $f(0)f(1)$:

funzione	**stringa**
f_1	00
f_2	01
f_3	10
f_4	11

Osserviamo che tale associazione funzione-stringa formi uno **XOR** nel nostro algoritmo.

Un qualsiasi algoritmo classico, richiede la valutazione di f almeno per 2 volte, una per $f(0)$ e l'altra per $f(1)$. Nel mondo quantistico, riusciamo ad ottenere il risultato corretto con una sola valutazione di f.

3.3.1 Implementazione

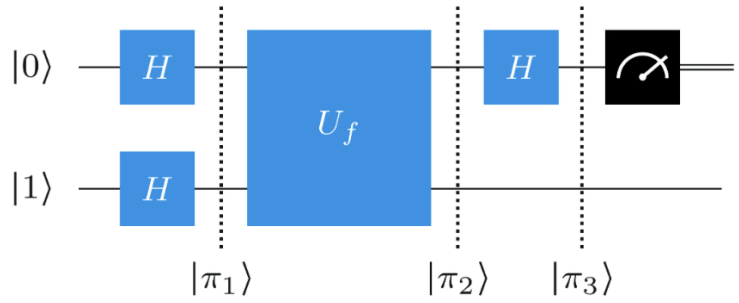

Figure 15

La Figura 15 mostra l'implementazione del circuito dell'algoritmo. Come prima, utilizziamo la porta di Hadamard per preparare il primo qubit nella superposizione $|+\rangle$; questa volta prepariamo anche il secondo qubit nella superposizione $|-\rangle$. Quindi avremo che:

$$|\pi_1\rangle = |+\rangle|-\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] = \frac{1}{2}\left(|0\rangle - |1\rangle\right)|0\rangle + \frac{1}{2}\left(|0\rangle - |1\rangle\right)|1\rangle$$

Il prossimo passo è l'esecuzione di U_f, che trasforma lo stato in

$$|\pi_2\rangle = \frac{1}{2}\left(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle\right)|0\rangle + \frac{1}{2}\left(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle\right)|1\rangle$$

Sapendo che:

$$|0 \oplus a\rangle - |1 \oplus a\rangle = (-1)^a(|0\rangle - |1\rangle)$$

quindi che:

$$|0 \oplus 0\rangle - |1 \oplus 0\rangle = (-1)^0(|0\rangle - |1\rangle)$$

$$|0 \oplus 1\rangle - |1 \oplus 1\rangle = (-1)^1(|0\rangle - |1\rangle)$$

allora possiamo scrivere lo stato $\pi_2\rangle$ come:

$$|\pi_2\rangle = \tfrac{1}{2}(-1)^{f(0)}(|0\rangle - |1\rangle)|0\rangle + \tfrac{1}{2}(-1)^{f(1)}(|0\rangle - |1\rangle)|1\rangle$$

$$= |-\rangle\left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right)$$

Osserviamo che il qubit più a sinistra è rimasto lo stesso ($|-\rangle$), mentre il qubit a sinistra è cambiato dopo l'esecuzione di U_f. Questo fenomeno è chiamato **kickback**.

Un'ultima semplificazione ci porta ad:

$$|\pi_2\rangle = (-1)^{f(0)}|-\rangle \left(\frac{|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}} \right) =$$

$$= \begin{cases} (-1)^{f(0)}|-\rangle|+\rangle & \text{se} \quad f(0) \oplus f(1) = 0 \\ (-1)^{f(0)}|-\rangle|-\rangle & \text{se} \quad f(0) \oplus f(1) = 1 \end{cases}$$

L'ultimo passaggio è quello di applicare la porta di Hadamard sul qubit di destra, trasformando lo stato in:

$$|\pi_3\rangle = \begin{cases} (-1)^{f(0)}|-\rangle|0\rangle & \text{se} \quad f(0) \oplus f(1) = 0 \\ (-1)^{f(0)}|-\rangle|1\rangle & \text{se} \quad f(0) \oplus f(1) = 1 \end{cases}$$

quindi avendo la certezza con probabilità 1 che la misurazione del qubit a destra ci dia il risultato corrispondente a 0 se f è costante, altrimenti 0 se f è bilanciata. Tutto questo è stato fatto con una sola valutazione di f, dimostrando il grande vantaggio della computazione quantistica rispetto a quella classica.

3.4 Algoritmo di Deutsch-Jozsa

L'algoritmo di Deutsch-Jozsa, proposto da David Deutsch e Richard Jozsa, è uno dei primi esempi di algoritmi quantistici ad essere esponenzialmente più veloce di un qualsiasi algoritmo deterministico classico. Questo algoritmo è un caso più generale del problema di Deutsch.

Sia $f : \{0,1\}^n \to \{0,1\}$ per una $n \in \mathbb{N}$. Diciamo che f è:

- **Costante** se $\forall x \in \{0,1\}^n \quad f(x) = 0 \bigvee f(x) = 1$,
- **Bilanciata** se $\sum_{x\in\{0,1\}^n} f(x) = \frac{2^n}{2} = 2^{n-1}$

Definition 3.2: Problema di Deutsch-Jozsa

Data in input una funzione $f : \{0,1\}^n \to \{0,1\}$, definiamo come **problema di Deutsch-Jozsa** il determinare se tale funzione è costante o bilanciata.

Observation 3.2

La maggior parte delle funzioni booleane non sono ne costanti e ne bilanciate. Tali funzioni vengono ignorate, considerate come *don't care* input.

In parole povere, possiamo descrivere l'algoritmo nella seguente maniera: attraverso una singola query, se ognuna delle n misurazioni produce 0, allora la funzione è costante; altrimenti, se almeno una misurazione produce 1, allora la funzione è bilanciata. In altre parole, stiamo eseguendo un OR sulle n misurazioni.

Nel caso classico, per scoprire il tipo di funzione, dovremmo valutare la funzione per almeno $\frac{2^n}{2} + 1$ volte; nel caso quantistico, invece, riusciamo a determinare il tipo di funzione con una sola valutazione di f.

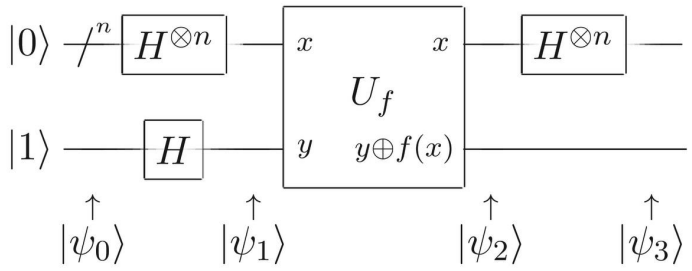

Figure 16

La figura 16 mostra il circuito quantistico che implementa l'algoritmo di Deutsch-Jozsa.

Analizziamo, inizialmente, il comportamento della porta di Hadamard:

$$H|a\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}(-1)^a|1\rangle = \frac{1}{\sqrt{2}} \sum_{b\in\{0,1\}} (-1)^{ab}|b\rangle$$

Supponiamo ora do avere n qubits eseguendo la trasformazione di Hadamard su ognuna di esse:

$$H^{\otimes n}|x_{n-1} \dots x_2 x_1\rangle =$$

$$= \big(H|x_{n-1}\rangle\big) \otimes \dots \otimes \big(H|x_0\rangle\big) =$$

$$= \Big(\tfrac{1}{\sqrt{2}} \textstyle\sum_{b_{n-1}\in\{0,1\}} (-1)^{x_{n-1}b_{n-1}}|b_{n-1}\rangle\Big) \otimes \dots \otimes \Big(\tfrac{1}{\sqrt{2}} \textstyle\sum_{0\in\{0,1\}} (-1)^{x_0 b_0}|b_0\rangle\Big) =$$

$$= \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{b_{n-1}\dots b_0\in\{0,1\}^n} (-1)^{x_{n-1}b_{n-1}+\dots+x_0 b_0}|b_{n-1} \dots b_2 b_1\rangle$$

Di conseguenza, abbiamo che:

$$|\psi_1\rangle = (H|1\rangle)(H^{\otimes n}|0 \dots 0\rangle) = |-\rangle \otimes \frac{1}{\sqrt{2^n}} \sum_{b_{n-1}\dots b_0\in\{0,1\}^n} |b_{n-1} \dots b_0\rangle$$

Eseguendo U_f sullo stato, otteniamo il seguente nuovo stato:

$$|\psi_2\rangle = |-\rangle \otimes \frac{1}{\sqrt{2^n}} \sum_{b_{n-1}\dots b_0\in\{0,1\}^n} (-1)^{f(b_{n-1}\dots b_0)}|b_{n-1} \dots b_0\rangle.$$

Abbiamo utilizzato lo stesso fenomeno di *kick-back* visto nell'algoritmo di Deutsch.

Infine applichiamo un secondo strato di porte di Hadamard, trasformando lo stato in:

$$|\psi_3\rangle = |-\rangle \otimes \frac{1}{2^n} \sum_{b_{n-1}\dots b_0 \in \{0,1\}^n} \sum_{c_{n-1}\dots c_0 \in \{0,1\}^n} (-1)^{f(b_{n-1}\dots b_0)+b_{n-1}c_{n-1}+\dots+b_0c_0} |c_{n-1}\dots c_0\rangle$$

A questo punto, dobbiamo semplicemente calcolare la probabilità che lo stato più a destra sia esattamente uguale a $|0\dots0\rangle$; infatti:

$$p(0^n) = |\frac{1}{2^n} \sum_{b_{n-1}\dots b_0 \in \{0,1\}^n} (-1)^{f(b_{n-1}\dots b_0)}| = \begin{cases} 1 & \text{se f è } \textbf{costante} \\ 0 & \text{se f è } \textbf{bilanciata} \end{cases}$$

Observation 3.3

Osserviamo che:

- Se f è **costante**, allora:
  - Se $f(b_{n-1}\dots b_0) = 0$ per una qualsiasi stringa $b_{n-1}\dots b_0 \in \{0,1\}^n$, abbiamo che la somma è 2^n, quindi $p(0^n) = 1$.
  - Altrimenti, se $f(b_{n-1}\dots b_0) = 1$, la somma è -2^n, quindi $p(0^n) = 1$.
- Se f è **bilanciata**, allora metà delle valutazioni di f sono uguali ad 1, l'altra metà sono uguali a 0. Avremo quindi una sommatoria con numero uguali di $+1$ e -1, annullandosi a vicenda, facendo risultare $p(0^n) = 0$.