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:

$$\|Uv\| = \|v\|$$

1.5 Notazione Dirac

2 Informazione Classica

Per comprendere al meglio come funziona l'informazione e la computazone quantistica, è bene avere le idee chiare su come funziona quella classica.

2.1 Sistemi Singoli

Sia X un sistema fisico che memorizza l'informazione. X può stare in un numero **finito di stati**. Definiamo anche Σ come l'insieme finito degli stati che X può assumere.

Example 2.1

Ad esempio possiamo pensare ad X come un bit, quindi $\Sigma = \{0, 1\}$.

Definition 2.1: Stato Probabilistico

Sia X un sistema e Σ il suo insieme di stati. Definiamo gli **stati probabilistici** di X se associamo ad ogni stato una **probabilità** tale che:

- $0 \leq p(\sigma) \leq 1$ per ogni $\sigma \in \Sigma$
- $\sum_{\sigma \in \Sigma} p(\sigma) = 1$

Possiamo rappresentare gli **stati probabilistici** come vettori, chiamati anche **vettori probabilistici**.

Example 2.2

Sia X il sistema che rappresenta un bit. Con probabilità $\frac{3}{4}$ X assume lo stato di 0, con $\frac{1}{4}$ assume 1. Allora possiamo rappresentare questo stato attraverso il seguente vettore:

$$\begin{pmatrix} \frac{3}{4} \\ \\ \frac{1}{4} \end{pmatrix}$$

dove la prima entrata corrisponde la probabilità che X assuma lo stato 0, la seconda entrata corrisponde alla probabilità che X assuma lo stato 1.

È comodo utilizzare la Dirac Notation (Sezione 1.5) per esprimere uno stato probabilistico.

Definition 2.2: Standard Basis Vectors

Definiamo come **Standard Basis Vectors** i vettori che hanno tutte le entrate 0 eccetto una singola entrata avente 1. Sono utili per rappresentare gli stati classici.

In particolare, per il nostro sistema binario, gli standard basis vectors sono $|0\rangle$, corrispondente a $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e $|1\rangle$, corrispondente a $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Fact 2.1

Ogni vettore probabilistico può essere espresso unicamente come una **combinazione lineare** degli standard basis vectors.

Example 2.3

$$\begin{pmatrix} \frac{3}{4} \\ \\ \frac{1}{4} \end{pmatrix} = \frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle$$

2.1.1 Misurazione di stati probabilistici

2.1.2 Operazioni deterministiche

2.1.3 Operazioni probablistiche

2.1.4 Composizione di operazioni probabilistiche

2.2 Sistemi Multipli

2.2.1 Stati Classici

2.2.2 Stati Probabilistici

2.2.3 Misurazione di stati probabilistici

2.2.4 Operazioni sugli stati probabilistici

3 Informazione Quantistica

3.1 Sistemi Singoli

Definition 3.1: 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 3.2: 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 3.1: 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

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

3.1.1 Misurazione di stati quantistici

3.1.2 Operazioni Unitarie

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

Observation 3.1

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. $(HSH)^2 = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

3.2 Sistemi Multipli

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

Definition 3.3: 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 3.2

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:

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

3.2.1 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 3.1: 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.

3.2.2 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)**.

3.2.3 Bell States

Definition 3.4: 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.

3.2.4 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.

3.2.5 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 3.3

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.

3.2.6 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 3.4

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 3.2

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:

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

3.3 Circuiti Quantistici

Figure 1

Definition 3.5: 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.

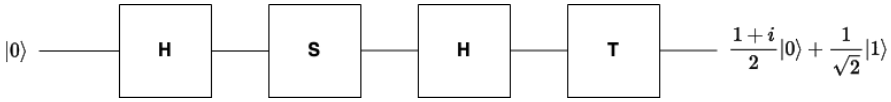

Figure 2

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.

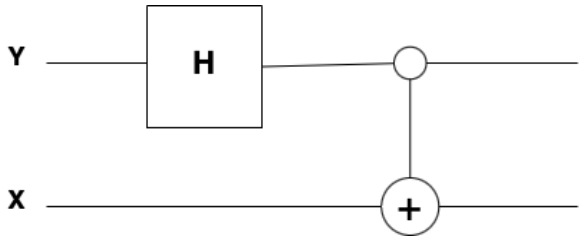

Figure 3

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.

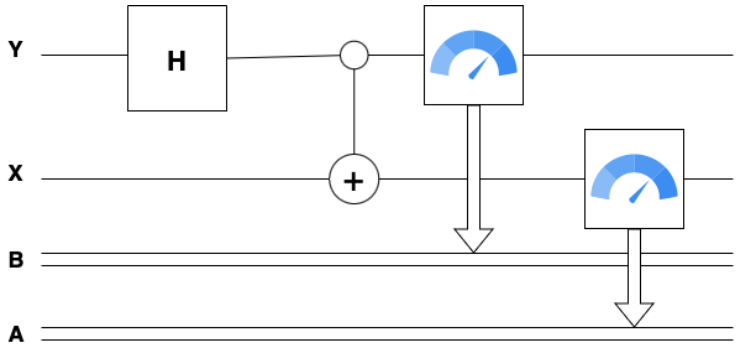

Figure 4

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

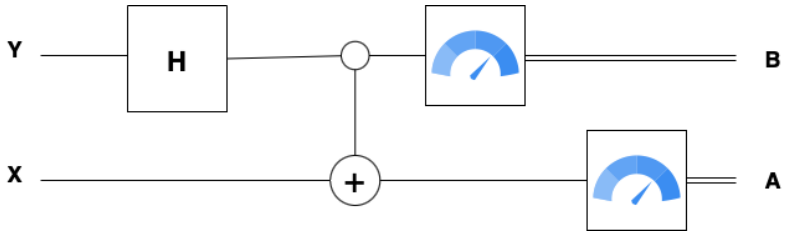

Figure 5

Ecco alcune porte comunemente usate per 1 o più qubit:

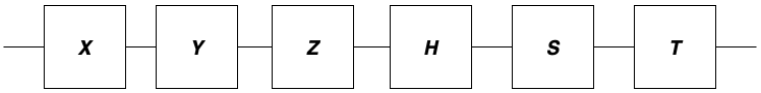

Figure 6

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.

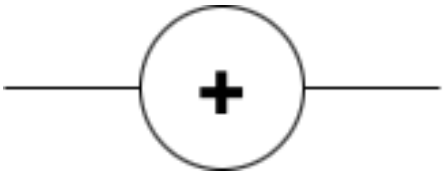

Figure 7: Not gate

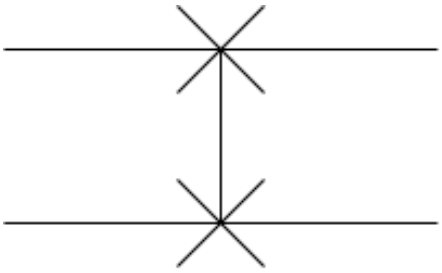

Figure 8: SWAP gate

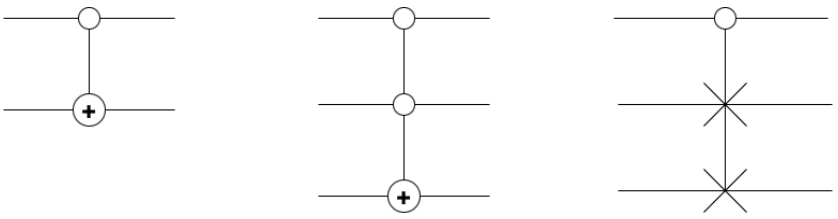

Figure 9

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.

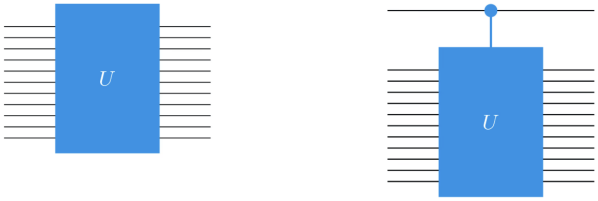

Figure 10

3.4 Misurazione Proiettiva