



UNIVERSITÀ DEGLI STUDI  
DI GENOVA

UNIVERSITÀ DEGLI STUDI DI GENOVA

# Fondamenti di Computazione Quantistica

*Lorenzo Vaccarecci*

Anno Accademico 2024/2025

# Indice

<b>1</b>	<b>Introduzione</b>	<b>2</b>
1.1	Porte logiche universali . . . . .	2
1.2	Operazioni Bit-a-Bit . . . . .	2
1.2.1	Prodotto interno bit-per-bit . . . . .	3
1.2.2	Somma bit-per-bit: bitwise XOR . . . . .	3
1.3	Prerequisiti matematici . . . . .	3
1.3.1	Numeri complessi . . . . .	3
1.3.2	Spazi vettoriali in 2D . . . . .	3
1.3.3	Prodotto scalare e componenti . . . . .	4
1.3.4	Vettori ket e bra . . . . .	4
1.3.5	Prodotto tensore . . . . .	5
1.3.6	Operatori lineari . . . . .	5
1.3.7	Autovalori e Autovettori . . . . .	6

# Capitolo 1

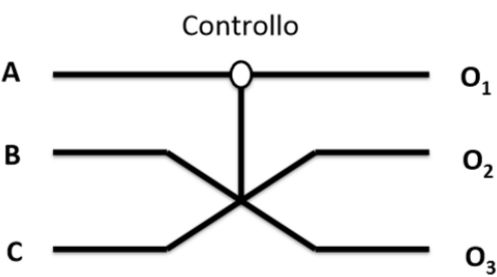
## Introduzione

### 1.1 Porte logiche universali

- $\text{NOT}(A) \equiv \bar{A}$
- $\text{AND}(A,B) \equiv A \cdot B$  oppure  $A \wedge B$
- $\text{OR}(A,B) \equiv A + B$  oppure  $A \vee B$
- $\text{XOR}(A,B) \equiv A \oplus B = (A + B) \bmod 2$
- $\text{NAND}(A,B) \equiv A \cdot \bar{B}$  oppure  $A \bar{\vee} B$
- $\text{NOR}(A,B) \equiv A \bar{+} B$  oppure  $A \bar{\wedge} B$

L'insieme di AND e NOT oppure di OR e NOT sono insiemi universali. Questo significa che, ad esempio, usando solo combinazioni di porte AND e NOT è possibile implementare una qualsiasi funzione booleana. Pur formando set universali, le porte AND, OR, NAND e NOR sono però **irreversibili**. A livello concettuale è interessante introdurre delle porte logiche che siano **reversibili**. Questo vuol dire che se combiniamo in sequenza una porta logica reversibile con la sua inversa, riotteniamo l'informazione originale. La porta di Fredkin può essere interpretata come uno *switch* controllato di bit. Il bit di controllo è A; se questo è acceso i bit B e C vengono scambiati, altrimenti vengono lasciati identici.

Controllo					
A	B	C	Out1	Out2	Out3
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1



### 1.2 Operazioni Bit-a-Bit

A una stringa di  $n$  bit possiamo associare un intero compreso fra 0 e  $N - 1$  con  $N = 2^n$ . All'intero  $x$  associamo la stringa di bit  $x_0x_1x_2 \dots x_n$  con  $x_i = 0, 1$  e  $i = 0, 1, \dots, n$  tale che  $x = \sum_{i=0}^n x_i 2^{n-i}$ . Possiamo codificare  $N = 2^n$  interi ma questi saranno compresi fra 0 e  $N - 1 = 2^n - 1$ .

### 1.2.1 Prodotto interno bit-per-bit

$$x \cdot z \equiv (x_1 z_1 + x_2 z_2 + \cdots + x_n z_n) \pmod{2}$$

E' anche chiamato prodotto AND bitwise perchè si ottiene prendendo le operazioni AND fra i singoli bit.

### 1.2.2 Somma bit-per-bit: bitwise XOR

Indichiamo con  $x \oplus z$  la somma bit-per bit, modulo 2. Il risultato questa volta è una stringa il cui  $i$ -esimo bit ha il valore  $x_i + z_i \pmod{2} = x_i \text{ XOR } z_i$ .

## 1.3 Prerequisiti matematici

### 1.3.1 Numeri complessi

Ogni numero complesso  $z \in \mathbb{C}$  può essere scritto come  $z = a + ib$ , con  $a \in \mathbb{R}$  **parte reale** e  $b \in \mathbb{R}$  **parte immaginaria**. Se  $z = a + ib$  e  $w = c + id$ , abbiamo

$$z + w = (a + c) + i(b + d)$$

$$z \cdot w = (ac - bd) + i(ad + bc)$$

Per ogni  $z \in \mathbb{C}$ ,  $z \cdot z^* = a^2 + b^2$  è reale e non negativo dove  $z^*$  è il **complesso coniugato** di  $z$  (la parte complessa è negata). Inoltre,  $\sqrt{a^2 + b^2} = |z|$  è detto **modulo** di  $z$ .

$$|z|^2 = z \cdot z^*$$

Possiamo rappresentare un numero complesso  $z = a + ib$  come una coppia (a,b) sul piano complesso. L'asse delle ascisse è utilizzato per la parte reale e l'asse delle ordinate per la parte immaginaria. Si ha  $a = |z| \cos \theta$  e  $b = |z| \sin \theta$  dove  $\theta$  è la **fase**. Se  $z = 0$  allora  $\theta$  non è definita. Per  $|z| = 1$ ,  $z = \cos \theta + i \sin \theta$ . Più in generale possiamo scrivere  $z = pe^{i\theta}$  con  $p = |z|$  e  $e^{i\theta} = \cos \theta + i \sin \theta$ .

### 1.3.2 Spazi vettoriali in 2D

- **Direzione:** rappresentata dalla retta su cui giace il vettore
- **Verso:** specifica in che direzione punta il vettore

Se abbiamo due vettori  $u$  e  $v$  possiamo definire la somma che sarà un vettore  $w = u + v$  ottenuto mediante la **regola del parallelogramma**.

Dato un numero  $\alpha \in \mathbb{R}$ , per ogni vettore  $v$ , possiamo definire il vettore  $\alpha v$  è la freccia ottenuta moltiplicando  $v$  per  $\alpha$  in modulo e lasciando invariata la direzione se  $\alpha > 0$  e invertendo il verso se  $\alpha < 0$ . Questa operazione è detta **moltiplicazione per scalare**. Se  $\alpha = -1$ , otteniamo il vettore  $-v$  che ha stesso modulo, stessa direzione ma verso opposto a  $v$ .

L'insieme di tutti i vettori del piano è allora uno spazio vettoriale reale  $V$  chiuso rispetto all'operazione di combinazione lineare:

$$u = \alpha v + \beta w$$

Per ogni vettore  $u$  e  $v \in V$  e per ogni  $\alpha, \beta \in \mathbb{R}$ .

### 1.3.3 Prodotto scalare e componenti

$$\langle \cdot, \cdot \rangle: V \times V \rightarrow \mathbb{C}$$

Che soddisfa le seguenti proprietà:

1.  $\forall u \in V, \langle u, u \rangle$  è un numero reale non negativo, con  $\langle u, u \rangle = 0 \iff u = 0$
2.  $\forall u, v \in V, \langle u, v \rangle = \langle v, u \rangle^*$
3.  $\forall u, v, w \in V, \forall \alpha, \beta \in \mathbb{C}, \langle w, \alpha u + \beta v \rangle = \alpha \langle w, u \rangle + \beta \langle w, v \rangle$

Due vettori per i quali il prodotto scalare è nullo sono *ortogonali*, sono base ortogonali se sono ortogonali e a norma unitaria ( $\|\langle \cdot, \cdot \rangle\|_2 = 1$ ).

Inoltre riscrivendo  $u = u_0 v_0 + u_1 v_1$  si ha:

$$\langle u, u \rangle = \langle u_0 v_0 + u_1 v_1, u_0 v_0 + u_1 v_1 \rangle = u_0^2 + u_1^2$$

Dove  $u_0 = \langle u, v_0 \rangle$  e  $u_1 = \langle u, v_1 \rangle$

### 1.3.4 Vettori ket e bra

- **Ket:** vettore  $u \rightarrow |u\rangle$
- **Bra:** vettore  $u \rightarrow \langle u|$

Usando questa notazione il prodotto scalare si forma con *braket*:

$$\langle u, v \rangle = \langle u|v\rangle$$

Usando la scomposizione di  $v$  in componenti:

- $|v\rangle = u_0|v_0\rangle + u_1|v_1\rangle$
- $\langle v| = u_0^*\langle v_0| + u_1^*\langle v_1|$

**Delta di Kronecker**

$$\langle v_i, v_j \rangle = \delta_{ij} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

Usando queste notazioni possiamo scrivere il prodotto scalare come:

$$\begin{aligned} \langle v|v\rangle &= (u_0^*\langle v_0| + u_1^*\langle v_1|) \cdot (u_0|v_0\rangle + u_1|v_1\rangle) \\ &= |u_0|^2 \langle v_0|v_0\rangle + u_0^* u_1 \langle v_0|v_1\rangle + u_1^* u_0 \langle v_1|v_0\rangle + |u_1|^2 \langle v_1|v_1\rangle \\ &= |u_0|^2 \cdot 1 + u_0^* u_1 \cdot 0 + u_1^* u_0 \cdot 0 + |u_1|^2 \cdot 1 \\ &= |u_0|^2 + |u_1|^2 \\ &= ||v\rangle|^2 \end{aligned}$$

### 1.3.5 Prodotto tensore

Consideriamo ora due spazi vettoriali  $V$  e  $W$  con basi, rispettivamente,  $A = \{|\alpha_1\rangle_V, \dots, |\alpha_n\rangle_V\}$  e  $B = \{|\beta_1\rangle_W, \dots, |\beta_m\rangle_W\}$ . Da questa scrittura deduciamo che  $V$  è uno spazio vettoriale di dimensione  $n$  e  $W$  di dimensione  $m$ .

Il prodotto tendore di  $V$  e  $W$  viene indicato con  $V \otimes W$  ha dimensione  $\dim(V \otimes W) = n m$  con la base costituita da  $n m$  elementi della forma  $|\alpha_i\rangle_V \otimes |\beta_j\rangle_W$ .

**La notazione  $|\alpha_i\rangle_V \otimes |\beta_j\rangle_W$  può essere scritta come  $|\alpha_i\beta_j\rangle$ .**

Proprietà:

1.  $\forall |v\rangle, |v'\rangle \in V, |w\rangle \in W \quad (|v\rangle + |v'\rangle) \otimes |w\rangle = |v\rangle \otimes |w\rangle + |v'\rangle \otimes |w\rangle$
2.  $\forall |v\rangle \in V, |w\rangle, |w'\rangle \in W \quad |v\rangle \otimes (|w\rangle + |w'\rangle) = |v\rangle \otimes |w\rangle + |v\rangle \otimes |w'\rangle$
3.  $\forall |v\rangle \in V, |w\rangle \in W, \alpha \in \mathbb{C} \quad (\alpha|v\rangle) \otimes |w\rangle = |v\rangle \otimes (\alpha|w\rangle) = \alpha(|v\rangle \otimes |w\rangle)$

Se  $V$  e  $W$  ammettono prodotto scalare, allora  $V \otimes W$  ammette un prodotto scalare definito come:

$$\langle u|u'\rangle = (\langle v| \otimes \langle w|) \cdot (|v'\rangle \otimes |w'\rangle) = \langle v|v'\rangle \cdot \langle w|w'\rangle \in \mathbb{C}$$

Alcune "proprietà":

1.  $(\langle \alpha_1| \otimes \langle \beta_2|) \cdot (|\alpha_1\rangle \otimes |\beta_2\rangle) = \langle \alpha_1|\alpha_1\rangle \cdot \langle \beta_2|\beta_2\rangle = 1$
2.  $\{|\alpha_i\rangle \otimes |\beta_j\rangle\}$  è una base ortonormale  $V \otimes W$ 
  - Se  $\langle \alpha_i|\alpha_k\rangle \cdot \langle \beta_j|\beta_l\rangle = 1 \rightarrow$  normalizzati
  - Se  $\langle \alpha_i|\alpha_k\rangle \cdot \langle \beta_j|\beta_l\rangle = 0 \rightarrow$  ortogonali

#### Esempio

$$|v\rangle = a|\alpha_1\rangle_V + b|\alpha_2\rangle_V \in V$$

$$|w\rangle = c|\beta_1\rangle_W + d|\beta_2\rangle_W \in W$$

$$|v\rangle \otimes |w\rangle = (a|\alpha_1\rangle_V + b|\alpha_2\rangle_V) \otimes (c|\beta_1\rangle_W + d|\beta_2\rangle_W)$$

$$= ac(|\alpha_1\rangle_V \otimes |\beta_1\rangle_W) + ad(|\alpha_1\rangle_V \otimes |\beta_2\rangle_W) + bc(|\alpha_2\rangle_V \otimes |\beta_1\rangle_W) + bd(|\alpha_2\rangle_V \otimes |\beta_2\rangle_W)$$

$$\langle v| \otimes \langle w| = (a\langle \alpha_1|_V + b\langle \alpha_2|_V) \otimes (c\langle \beta_1|_W + d\langle \beta_2|_W)$$

$$= ac(\langle \alpha_1|_V \otimes \langle \beta_1|_W) + ad(\langle \alpha_1|_V \otimes \langle \beta_2|_W) + bc(\langle \alpha_2|_V \otimes \langle \beta_1|_W) + bd(\langle \alpha_2|_V \otimes \langle \beta_2|_W)$$

$$(\langle v| \otimes \langle w|) \cdot (|v\rangle \otimes |w\rangle) = [(a\langle \alpha_1|_V + b\langle \alpha_2|_V) \otimes (c\langle \beta_1|_W + d\langle \beta_2|_W)] \cdot [(a|\alpha_1\rangle_V + b|\alpha_2\rangle_V) \otimes (c|\beta_1\rangle_W + d|\beta_2\rangle_W)]$$

$$=$$

$$= (|a|^2 + |b|^2) \cdot (|c|^2 + |d|^2)$$

### 1.3.6 Operatori lineari

Gli operatori lineari in generale sono tali che agendo su un vettore dello spazio lineare danno un altro vettore dello stesso spazio:  $O : V \rightarrow V$ . Usando la notazione braket possiamo scrivere

$$O|v\rangle = |w\rangle$$

Scegliamo una base (ortonormale) dello spazio vettoriale  $\{|\alpha_1\rangle, \dots, |\alpha_n\rangle\}$ , l'elemento della matrice  $O$  in posizione  $(i, j)$  sarà  $O_{ij} = \langle \alpha_i| \cdot (O|\alpha_j\rangle)$

### Esempio

Voglio calcolare  $O_{12}$ :

$$\begin{aligned} O_{12} &= \langle \alpha_1 | \left( \sum_{ij}^n O_{ij} |\alpha_i\rangle \langle \alpha_j| \right) | \alpha_2 \rangle \\ &= \sum_{ij}^n O_{ij} \langle \alpha_1 | \alpha_i \rangle \langle \alpha_j | \alpha_2 \rangle \\ &= O_{12} \end{aligned}$$

Grazie al delta di Kronecker.

### 1.3.7 Autovalori e Autovettori

Diremo che se  $O|v\rangle = \lambda|v\rangle$  per un vettore non nullo  $|v\rangle$ , diremo che  $v$  è un **autovettore** di  $O$  e  $\lambda$  è l'**autovalore** corrispondente.