



UNIVERSITÀ DEGLI STUDI
DI GENOVA

UNIVERSITÀ DEGLI STUDI DI GENOVA

Fondamenti di Computazione Quantistica

Lorenzo Vaccarecci

Anno Accademico 2024/2025

Indice

1	Fisica della computazione	2
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
2	Apparato matematico	4
2.1	Prerequisiti matematici	4
2.1.1	Numeri complessi	4
2.1.2	Spazi vettoriali in 2D	4
2.1.3	Prodotto scalare e componenti	5
2.1.4	Vettori ket e bra	5
2.1.5	Prodotto tensore	6
2.1.6	Operatori lineari	6
2.1.7	Autovalori e Autovettori	7
3	Introduzione ai fenomeni quantistici	8
3.1	Regole dal postulato della misura	8
3.2	Fase globale e relativa	8
3.2.1	Fase globale	8
3.3	Stati a molti qubit	9
3.3.1	Stati a due qubit separabili	9
3.3.2	Stati a due qubit entangled	9
3.4	Trasformazioni unitarie	10
3.4.1	Porte quantistiche	10
3.5	Sfera di Bloch	11
4	Informazione Quantistica	13
4.1	Parallelismo quantistico	13
4.2	Teorema no-cloning	13
4.3	Superdense coding	14
4.4	Teletrasporto quantistico	15
4.5	Algoritmi quantistici	16
4.5.1	Algoritmo di Deutch	16
4.5.2	Algoritmo di Deutch-Josza	17
4.5.3	Algoritmo di Bernstein-Vazirani	18
4.5.4	Algoritmo di Simon	18

Capitolo 1

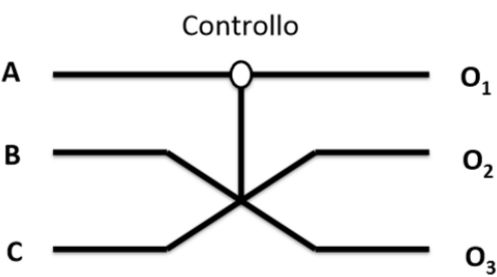
Fisica della computazione

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 $x_i + z_i \pmod{2} = x_i \text{ XOR } z_i$.

Capitolo 2

Apparato matematico

2.1 Prerequisiti matematici

2.1.1 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 θ è la **fase**. Se $z = 0$ allora θ 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 $e^{i\theta} = \cos \theta + i \sin \theta$.

$$i * (-i) = -1$$

2.1.2 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 αv è la freccia ottenuta moltiplicando v per α 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 $\alpha, \beta \in \mathbb{R}$.

2.1.3 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 $u_1 = \langle u, v_1 \rangle$

2.1.4 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:

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

2.1.5 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

$$\begin{aligned} |v\rangle &= a|\alpha_1\rangle_V + b|\alpha_2\rangle_V \in V \\ |w\rangle &= c|\beta_1\rangle_W + d|\beta_2\rangle_W \in W \end{aligned}$$

$$\begin{aligned} |v\rangle \otimes |w\rangle &= (a|\alpha_1\rangle_V + b|\alpha_2\rangle_V) \otimes (c|\beta_1\rangle_W + d|\beta_2\rangle_W) \\ &= ac(|\alpha_1\rangle_V \otimes |\beta_1\rangle_W) + ad(|\alpha_1\rangle_V \otimes |\beta_2\rangle_W) + bc(|\alpha_2\rangle_V \otimes |\beta_1\rangle_W) + bd(|\alpha_2\rangle_V \otimes |\beta_2\rangle_W) \\ \langle v| \otimes \langle w| &= (a\langle \alpha_1|_V + b\langle \alpha_2|_V) \otimes (c\langle \beta_1|_W + d\langle \beta_2|_W) \\ &= ac(\langle \alpha_1|_V \otimes \langle \beta_1|_W) + ad(\langle \alpha_1|_V \otimes \langle \beta_2|_W) + bc(\langle \alpha_2|_V \otimes \langle \beta_1|_W) + bd(\langle \alpha_2|_V \otimes \langle \beta_2|_W) \\ (\langle v| \otimes \langle w|) \cdot (|v\rangle \otimes |w\rangle) &= [(a\langle \alpha_1|_V + b\langle \alpha_2|_V) \otimes (c\langle \beta_1|_W + d\langle \beta_2|_W)] \cdot [(a|\alpha_1\rangle_V + b|\alpha_2\rangle_V) \otimes (c|\beta_1\rangle_W + d|\beta_2\rangle_W)] \\ &= \\ &= (|a|^2 + |b|^2) \cdot (|c|^2 + |d|^2) \end{aligned}$$

2.1.6 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.

2.1.7 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 λ è l'**autovalore** corrispondente.

Capitolo 3

Introduzione ai fenomeni quantistici

Un osservabile fisico può essere associato ad un operatore Hermitiano ϕ da cui possiamo ottenere i loro autovalori e autovettori. Il punto fondamentale di questa discussione è che la base, gli autovalori e il risultato dipende dall'osservabile che vogliamo misurare.

3.1 Regole dal postulato della misura

1. Se vogliamo misurare un osservabile ϕ , dobbiamo conoscere i suoi autovalori $\{\phi_i\}$ e autovettori $\{|\phi_i\rangle\}$; cioè gli stati tali che $\phi|\phi_i\rangle = \phi_i|\phi_i\rangle$. Gli autovettori saranno la base su cui decomporre lo stato del nostro sistema. Ovvero dobbiamo scrivere $|a\rangle = \sum_i a_i|\phi_i\rangle$ con $a_i = \langle\phi_i|a\rangle$.
2. La misura avrà come risultato l'autovalore ϕ_i con probabilità $|a_i|^2$.
3. Dopo la misura, il sistema si troverà nello stato $|\phi_i\rangle$ associato all'autovalore misurato.

Stati quantistici sono normalizzati:

$$\sum_{i=1}^N |a_i|^2 = 1$$

3.2 Fase globale e relativa

3.2.1 Fase globale

Consideriamo i vettori $|u\rangle$ e $e^{i\phi}|u\rangle$ che hanno lo stesso modulo ma differiscono per una fase globale ϕ . Il calcolo delle probabilità dei risultati di una qualunque misura fornisce sempre gli stessi valori.

Sia $|u\rangle = \sum_i \alpha_i |\phi_i\rangle$ dove $\{|\phi_i\rangle\}$ formano una base ortonormale dello spazio vettoriale. Lo stato con una fase globale si scriverà $e^{i\phi}|u\rangle = \sum_i e^{i\phi} \alpha_i |\phi_i\rangle$

Esempio di fase globale/relativa Fase relativa

$$\begin{array}{c} \uparrow \text{ Fase globale} \\ e^{i\phi} \frac{(|0\rangle + e^{i(\gamma-\phi)}|1\rangle)}{\sqrt{2}} \end{array}$$

3.3 Stati a molti qubit

- **Base del qubit:** $\{|0\rangle, |1\rangle\}$
- **Stato:** $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Consideriamo:

$$\begin{aligned} \text{A: } |\psi\rangle &= \alpha|0\rangle + \beta|1\rangle \\ \text{B: } |\phi\rangle &= \gamma|0\rangle + \delta|1\rangle \end{aligned} \tag{3.1}$$

La base B la otteniamo con:

$$\begin{aligned} |\psi\rangle \oplus |\phi\rangle &= (\alpha|0\rangle + \beta|1\rangle) \oplus (\gamma|0\rangle + \delta|1\rangle) \\ &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \end{aligned}$$

Per ricavare la base ci fermiamo al secondo passaggio, quindi avremo $B : \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

3.3.1 Stati a due qubit separabili

Usando $|\psi\rangle$ e $|\phi\rangle$ (3.1), a volte conviene scrivere lo stato come:

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

Perchè in questo modo si possono determinare le probabilità di collasso in modo più semplice:

$$\begin{cases} \text{Se collassa } \alpha: |\alpha|^2, \phi_0 \rightarrow |0\rangle \oplus (\gamma|0\rangle + \delta|1\rangle) = \begin{cases} \text{Se collassa } \gamma: |\gamma|^2, \phi_0 \rightarrow |00\rangle \\ \text{Se collassa } \delta: |\delta|^2, \phi_1 \rightarrow |01\rangle \end{cases} \\ \text{Se collassa } \beta: |\beta|^2, \phi_1 \rightarrow |1\rangle \oplus (\gamma|0\rangle + \delta|1\rangle) = \begin{cases} \text{Se collassa } \gamma: |\gamma|^2, \phi_0 \rightarrow |10\rangle \\ \text{Se collassa } \delta: |\delta|^2, \phi_1 \rightarrow |11\rangle \end{cases} \end{cases}$$

Esempio

$$\begin{aligned} |\varepsilon\rangle &= \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) = |\psi\rangle \oplus |\phi\rangle \\ &= \frac{1}{\sqrt{2}} (|01\rangle) + \frac{1}{\sqrt{2}} (|10\rangle) = \begin{cases} \text{Se collassa } |01\rangle: \frac{1}{2}, \phi_0 \rightarrow |01\rangle \rightarrow 1, \phi_0 \rightarrow |01\rangle \\ \text{Se collassa } |10\rangle: \frac{1}{2}, \phi_1 \rightarrow |10\rangle \rightarrow 1, \phi_1 \rightarrow |10\rangle \end{cases} \end{aligned}$$

Possiamo dedurre che se A misura 0, B misura 1 e viceversa.

3.3.2 Stati a due qubit entangled

Gli elementi dello spazio vettoriale $A \oplus B$ non sono tutti ottenibili come prodotto tensoriale di due elementi di A e B .

Un esempio di stati entangled sono gli stati di Bell:

$$\begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A \oplus |0\rangle_B + |1\rangle_A \oplus |1\rangle_B) \\ |\phi^-\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A \oplus |0\rangle_B - |1\rangle_A \oplus |1\rangle_B) \\ |\psi^+\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A \oplus |1\rangle_B + |1\rangle_A \oplus |0\rangle_B) \\ |\psi^-\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A \oplus |1\rangle_B - |1\rangle_A \oplus |0\rangle_B) \end{aligned}$$

Per descrivere lo stato di un sistema a due qubit possiamo alternativamente usare la base canonica $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ o la base di Bell $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$.

$$O = \lambda_0 |\phi^+\rangle\langle\phi^+| + \lambda_1 |\phi^-\rangle\langle\phi^-| + \lambda_2 |\psi^+\rangle\langle\psi^+| + \lambda_3 |\psi^-\rangle\langle\psi^-|$$

Quindi se il sistema si trova in uno stato di Bell, una misura dell'operatore O darà con certezza l'autovalore corrispondente.

3.4 Trasformazioni unitarie

Sia $|a\rangle = \alpha|x_0\rangle + \beta|x_1\rangle$, una trasformazione unitaria U è

- **Lineare:** $U|a\rangle = U(\alpha|x_0\rangle + \beta|x_1\rangle) = \alpha U|x_0\rangle + \beta U|x_1\rangle$
- **Invertibile con l'inversa uguale alla trasposta coniugata:** $U^{-1}|a\rangle = U^\dagger|a\rangle$

Quest'ultima proprietà garantisce che le trasformazioni unitarie lasciano invariati i prodotti scalari, e quindi anche la norma dei vettori su cui agiscono e le probabilità associate alle misure. Infatti, prendiamo due stati $|a\rangle$ e $|b\rangle$ con prodotto scalare $\langle b|a\rangle$. Se questi evolvono secondo un operatore unitario U avremo $|a'\rangle = U|a\rangle$ e $|b'\rangle = U|b\rangle$ ($\langle b'| = \langle b|U^\dagger$), il prodotto scalare degli stati evoluti sarà $\langle b'|a'\rangle = \langle b|U^\dagger U|a\rangle = \langle b|a\rangle$ perchè $U^\dagger U = \text{Identità}$.

3.4.1 Porte quantistiche

Trasformazioni di Pauli

Nel nostro caso scegliamo la base canonica $\{|0\rangle, |1\rangle\}$ e definiamo, oltre all'identità Id , le tre trasformazioni di Pauli X, Y, Z :

$$\begin{aligned} Id|0\rangle &:= |0\rangle & Id|1\rangle &:= |1\rangle \\ X|0\rangle &:= |1\rangle & X|1\rangle &:= |0\rangle \\ Y|0\rangle &:= -i|1\rangle & Y|1\rangle &:= i|0\rangle \\ Z|0\rangle &:= -|0\rangle & Z|1\rangle &:= |1\rangle \end{aligned}$$

Analizzando l'effetto degli operatori, si nota che nella base canonica, X corrisponde al NOT tra bit classici. L'operatore Z genera un cambio della fase relativa e, infine, l'operatore Y può essere visto come una combinazione dei due precedenti dato che $Y = -iXZ$.

Esempio

$$\begin{aligned} Z(\alpha|0\rangle + \beta|1\rangle) &= \alpha Z|0\rangle + \beta Z|1\rangle \\ &= -\alpha|0\rangle + \beta|1\rangle \end{aligned}$$

Trasformazioni di Hadarmard

$$\begin{aligned} H|0\rangle &= |+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \\ H|1\rangle &= |-\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \end{aligned}$$

In forma matriciale (nella base canonica $\{|0\rangle, |1\rangle\}$) l'operatore di Hadarmard si scrive come:

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

Controlled-NOT

Consideriamo ora, il controlled-NOT, **CNOT**, una trasformazione che agisce su 2 qubit, A e B . Nella base canonica l'azione del **CNOT** é:

$$\begin{aligned}CNOT|0\rangle_A \oplus |0\rangle_B &= |0\rangle_A \oplus |0\rangle_B \\CNOT|0\rangle_A \oplus |1\rangle_B &= |0\rangle_A \oplus |1\rangle_B \\CNOT|1\rangle_A \oplus |0\rangle_B &= |1\rangle_A \oplus |1\rangle_B \\CNOT|1\rangle_A \oplus |1\rangle_B &= |1\rangle_A \oplus |0\rangle_B\end{aligned}$$

In linea generale possiamo scrivere il **CNOT** come:

$$C_iNOT_j$$

Dove i è il qubit di controllo e j il qubit target. Se il qubit di controllo è acceso allora applica un NOT al qubit target.

L'importanza dell'operatore **CNOT** risiede nel fatto che può generare entanglement fra due qubit.

Esempio

$$|00\rangle \xrightarrow{H_1} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \oplus |0\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |10\rangle) \xrightarrow{C_1NOT_2} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = \text{Stato di Bell}$$

Se eseguo l'operatore **CNOT** due volte ottengo lo stato iniziale:

$$CNOT^2 = Id$$

3.5 Sfera di Bloch

Come detto un generico stato quantistico a due livelli o qubit è scritto come $|v\rangle = \alpha|0\rangle + \beta|1\rangle$ con il vincolo ulteriore di normalizzazione dello stato: $|\alpha|^2 + |\beta|^2 = 1$. Quindi in generale possiamo scrivere $|\alpha|^2 = \cos^2(\theta) \rightarrow |\alpha| = \cos(\frac{\theta}{2})$ e $|\beta|^2 = \sin^2(\theta) \rightarrow |\beta| = \sin(\frac{\theta}{2})$. Possiamo rappresentare gli stati dei qubit in modo geometrico. Consideriamo lo stato generico

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

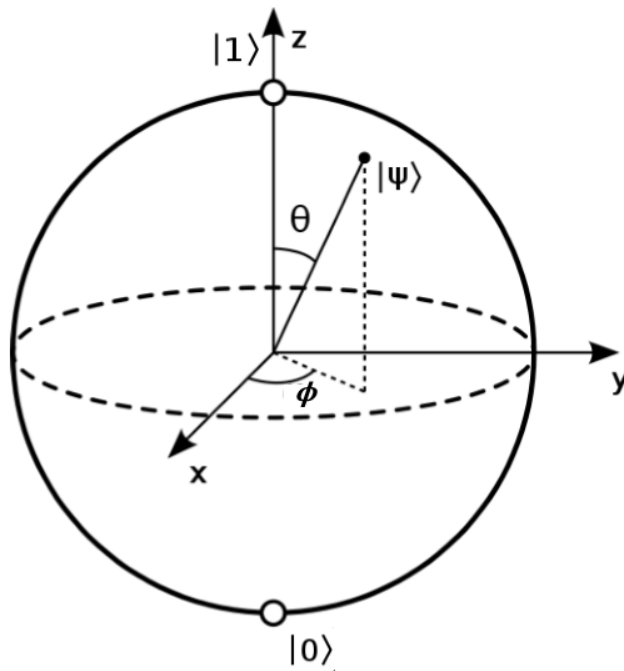
e il relativo stato bra

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

Calcoliamo i valori medi degli operatori di Pauli X, Y, Z con lo stato $|\psi\rangle$

$$\begin{aligned}x &= \langle\psi|X|\psi\rangle = \cos\phi \sin\theta \\y &= \langle\psi|Y|\psi\rangle = \sin\phi \sin\theta \\z &= \langle\psi|Z|\psi\rangle = \cos\theta \text{ (oppure } -\cos\theta)\end{aligned}$$

Queste non sono altro che le coordinate in uno spazio tridimensionale di un punto che si muove su una sfera. Se consideriamo il vettore che congiunge l'origine degli assi con il punto di coordinate $\{x, y, z\}$, l'angolo θ è quello formato dal vettore e dall'asse z mentre l'angolo ϕ è quello formato dal vettore sul piano $y - z$



Concludiamo che ogni operatore unitario può essere visto come una rotazione sulla sfera di Bloch che unisce lo stato iniziale con lo stato finale.

L'operatore U possiamo scriverlo più generalmente come:

$$U = \cos\left(\frac{\alpha}{2}\right) Id - i \sin\left(\frac{\alpha}{2}\right) Y$$

Esempio

$$\begin{aligned} |\psi\rangle &= |1\rangle \\ |\psi_f\rangle &= U|\psi\rangle \\ &= \cos\left(\frac{\alpha}{2}\right) Id|1\rangle - i \sin\left(\frac{\alpha}{2}\right) Y|1\rangle \\ &= \cos\left(\frac{\alpha}{2}\right) |1\rangle - i \sin\left(\frac{\alpha}{2}\right) i|0\rangle \\ &= \cos\left(\frac{\alpha}{2}\right) |1\rangle + \sin\left(\frac{\alpha}{2}\right) |0\rangle \end{aligned}$$

Capitolo 4

Informazione Quantistica

4.1 Parallelismo quantistico

Supponiamo di partire dai due qubit inizializzati nello stato $|00\rangle \equiv |0\rangle \otimes |0\rangle$ e di applicare due porte di Hadarmard ai singoli qubit. Le due porte applicate contemporaneamente si denotano come $H \otimes H \equiv H^{\otimes 2}$ dove la notazione \otimes indica che la prima porta è applicata al primo qubit e la seconda al secondo qubit

$$\begin{aligned} |0\rangle \otimes |0\rangle &\xrightarrow{H^{\otimes 2}} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|00\rangle}{2} + \frac{|01\rangle}{2} + \frac{|10\rangle}{2} + \frac{|11\rangle}{2} \\ &= \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \end{aligned}$$

Se applichiamo un operatore unitario U

$$\frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \xrightarrow{U} \frac{1}{2} (U|00\rangle + U|01\rangle + U|10\rangle + U|11\rangle)$$

Ovvero agirà contemporaneamente su tutti gli stati logici. Questo ragionamento si estende in maniera semplice al caso di n qubit. In questo caso lo stato iniziale sarà $|00 \dots 0\rangle$ e applicheremo n porte di Hadarmard $H^{\otimes n}$

$$\begin{aligned} |00 \dots 0\rangle &\xrightarrow{H^{\otimes n}} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \dots \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{2^{\frac{n}{2}}} (|00 \dots 0\rangle + |10 \dots 0\rangle + \dots + |11 \dots 1\rangle) \\ &= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \end{aligned}$$

Dove $N = 2^n$ e anche in questo caso, applicando successivamente un operatore unitario U avremo

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} U|x\rangle$$

Possiamo manipolare parallelamente tutte le N stringhe logiche.

4.2 Teorema no-cloning

Supponiamo di avere un singolo qubit di informazione e che si trovi nello stato $|\psi\rangle = a|0\rangle + b|1\rangle$ (con $|a|^2 + |b|^2 = 1$). Per copiarlo, prendiamo un secondo qubit inizializzato nello stato $|0\rangle$. Avremo $|\psi 0\rangle = a|00\rangle + b|10\rangle$ e applichiamo la porta **CNOT**

$$|\psi 0\rangle = a|00\rangle + b|10\rangle \xrightarrow{C_1NOT_2} a|00\rangle + b|11\rangle$$

Se consideriamo lo stato più generale $|\psi\rangle = a|00\rangle + b|10\rangle$ per copiarlo dovremmo avere un operatore il cui risultato sia

$$|\psi\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$$

Se lo stato da copiare è sconosciuto, non è possibile copiarlo.

L'operazione di copiatura sarà descritta da un'evoluzione unitaria U_{COPY} tale che

$$|\psi\rangle|s\rangle \xrightarrow{U_{COPY}} |\psi\rangle|s\rangle = |\psi\psi\rangle$$

Supponiamo di voler copiare anche uno stato $|\varphi\rangle$

$$|\varphi\rangle|s\rangle \xrightarrow{U_{COPY}} |\varphi\rangle|s\rangle = |\varphi\varphi\rangle$$

Se prendendo il prodotto scalare degli stati finali abbiamo

$$\langle\varphi s|U_{COPY}^\dagger U_{COPY}|\psi s\rangle = \langle\varphi s|\psi s\rangle = \langle\varphi|\psi\rangle\langle s|s\rangle = \langle\varphi|\psi\rangle$$

Esempio

$s = 0$

$$\begin{aligned} \langle\varphi|\langle 0|U_{COPY}^\dagger (U_{COPY}|\psi\rangle|0\rangle) &= \langle\varphi|\langle 0|I|\psi\rangle|0\rangle \\ &= (\langle\varphi|\langle 0|)(|\psi\rangle|0\rangle) \\ &= \langle\varphi|\psi\rangle\langle 0|0\rangle \\ &= \langle\varphi|\psi\rangle \end{aligned}$$

Dalle equazioni di sopra, questo deve essere uguale a $\langle\psi\psi|\varphi\varphi\rangle = \langle\varphi|\psi\rangle\langle\varphi|\psi\rangle$

$$\langle\varphi|\psi\rangle = (\langle\varphi|\psi\rangle)^2$$

Quindi può esistere un operatore unitario di copia U_{COPY} solo se gli stati $|\psi\rangle$ e $|\varphi\rangle$ sono ortogonali ($\langle\varphi|\psi\rangle = 0$) oppure identici ($\langle\varphi|\psi\rangle = 1$).

Concludiamo che se gli stati da copiare sono noti e ortogonali è possibile costruire un operatore unitario U_{COPY} che li copi. In genere, però non è possibile copiare stati quantistici qualsiasi; ovvero non esiste nessun operatore U_{COPY} capace di copiare tutti gli stati quantistici.

4.3 Superdense coding

Supponiamo che Alice voglia mandare due bit di informazione classica. Alice e Bob devono condividere uno stato entangled (di Bell)

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$$

Dove gli stati $|\dots\rangle_A$ e $|\dots\rangle_B$ sono rispettivamente di Alice e Bob.

Bit di Alice	Porta logica applicata	Stato di Bob
00	I	$\frac{(00\rangle_B + 11\rangle_B)}{\sqrt{2}} \xrightarrow{C_1 NOT_2} \frac{(00\rangle_B + 10\rangle_B)}{\sqrt{2}} \xrightarrow{H} 00\rangle_B$
01	X	$\frac{(10\rangle_B + 01\rangle_B)}{\sqrt{2}} \xrightarrow{C_1 NOT_2} \frac{(11\rangle_B + 01\rangle_B)}{\sqrt{2}} \xrightarrow{H} 01\rangle_B$
10	Z	$\frac{(00\rangle_B - 11\rangle_B)}{\sqrt{2}} \xrightarrow{C_1 NOT_2} \frac{(00\rangle_B - 10\rangle_B)}{\sqrt{2}} \xrightarrow{H} 10\rangle_B$
11	iY	$\frac{(01\rangle_B - 10\rangle_B)}{\sqrt{2}} \xrightarrow{C_1 NOT_2} \frac{(01\rangle_B - 11\rangle_B)}{\sqrt{2}} \xrightarrow{H} 11\rangle_B$

4.4 Teletrasporto quantistico

Supponiamo che Alice (A) e Bob (B) condividano uno stato entangled $|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$. Questa notazione sta per la più precisa

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

Supponiamo che Alice abbia un qubit di informazione $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (con $|\alpha|^2 + |\beta|^2 = 1$) che vuole mandare a Bob. Per far questo, lo accoppia allo stato entangled $|\beta_{00}\rangle$

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}} [\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)]$$

Dove si intende, ad esempio, $|0\rangle|00\rangle = |0\rangle_A|0\rangle_A|0\rangle_B$.

Poi viene applicata una porta **CNOT** usando il primo qubit A come bit di controllo e il secondo qubit B come bit target (se vediamo i qubit come $|000\rangle$ sarebbe C_1NOT_3)

$$|\psi_0\rangle \xrightarrow{C_1NOT_2} |\psi_1\rangle = \frac{1}{\sqrt{2}} [\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|01\rangle + |10\rangle)]$$

Successivamente Alice applica una porta di Hadarmard al primo qubit

$$\begin{aligned} |\psi_1\rangle \xrightarrow{H_1} |\psi_2\rangle &= \frac{1}{2} [\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|01\rangle + |10\rangle)] \\ &= \frac{1}{2} [|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)] \end{aligned}$$

l'ultimo passo è quindi quello di rendere tale informazione accessibile a Bob. Per fare questo, Alice misura i suoi due qubit e dato che i qubit di Alice e Bob sono entangled, la misura di Alice induce un collasso dello stato di Bob. I possibili risultati della misura di Alice e i corrispondenti stati di Bob sono

Misura	Stato di Bob	Probabilità di misurare 0	Probabilità di misurare 1
00	$\alpha 0\rangle + \beta 1\rangle$	$\mathcal{P}_{00}(0) = \alpha ^2$	$\mathcal{P}_{00}(1) = \beta ^2$
01	$\alpha 1\rangle + \beta 0\rangle$	$\mathcal{P}_{01}(0) = \beta ^2$	$\mathcal{P}_{01}(1) = \alpha ^2$
10	$\alpha 0\rangle - \beta 1\rangle$	$\mathcal{P}_{10}(0) = \alpha ^2$	$\mathcal{P}_{10}(1) = \beta ^2$
11	$\alpha 1\rangle - \beta 0\rangle$	$\mathcal{P}_{11}(0) = \beta ^2$	$\mathcal{P}_{11}(1) = \alpha ^2$

Ognuno di queste misure capita con probabilità di $\frac{1}{4}$. Affinchè Bob posseda sempre lo stato $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, Alice chiama attraverso un canale classico Bob e gli dice quale è stato il risultato della sua misura. A questo punto Bob applica un'operatore correttivo

Misura	Operatore correttivo
00	I
01	X
10	Z
11	Y

La probabilità totale di misurare 0 per Bob è

$$\begin{aligned} \mathcal{P}_{Bob}(0) &= \frac{1}{4} (\mathcal{P}_{00}(0) + \mathcal{P}_{01}(0) + \mathcal{P}_{10}(0) + \mathcal{P}_{11}(0)) \\ &= \frac{1}{4} (|\alpha|^2 + |\beta|^2 + |\alpha|^2 + |\beta|^2) \\ &= \frac{1}{4} (1 + 1) = \frac{1}{2} \end{aligned}$$

Stessa cosa per $\mathcal{P}_{Bob}(1) = \frac{1}{2}$.

La conclusione è che sebbene Alice abbia modificato lo stato (o gli stati) di Bob, quest'ultimo non è in grado di estrarre nessuna informazione.

4.5 Algoritmi quantistici

4.5.1 Algoritmo di Deutch

Data una funzione f ad un bit, l'algoritmo di Deutch permette di capire se sia costante o no; nel caso in cui f non sia costante viene spesso chiamata **bilanciata**. Si consideri una funzione ad un bit $f(x) : \{0, 1\} \rightarrow \{0, 1\}$, la funzione f sarà costante se $f(0) = f(1)$ e sarà bilanciata se $f(0) \neq f(1)$.

Lo stato iniziale dell'algoritmo di Deutch è costituito da due qubit: $|\psi_0\rangle = |01\rangle$. Ad entrambi viene applicata una porta di Hadarmard per ottenere

$$|\psi_0\rangle \rightarrow |\psi_1\rangle = \frac{1}{2} (|0\rangle + |1\rangle) (|0\rangle - |1\rangle)$$

L'operatore U_f

L'effetto di questo operatore è quello di calcolare $f(x)$, l'addizione modulo 2 di $y \oplus f(x)$ e lo possa immagazzinare nel secondo qubit ($|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$). L'addizione modulo 2 è equivalente ad una porta XOR.

Per capire come agisce l'operatore U_f , nell'algoritmo di Deutch, lo applichiamo ad uno stato generico $|x\rangle|-\rangle$:

$$\begin{aligned} |x\rangle|-\rangle &= |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{U_f} |0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} (|00\rangle - |01\rangle) \\ &\xrightarrow{U_f} \frac{1}{\sqrt{2}} (|0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle) = \begin{cases} \frac{1}{\sqrt{2}} (|00\rangle - |01\rangle) = |0\rangle|-\rangle & \text{se } f(0) = 0 \\ \frac{1}{\sqrt{2}} (|01\rangle - |00\rangle) = -|0\rangle|-\rangle & \text{se } f(0) = 1 \end{cases} \end{aligned}$$

In sostanza, l'applicazione dell'operatore U_f lascia invariato sia il primo qubit che il secondo ma lo stato acquista una fase $(-1)^{f(x)}$ che dipende dal valore della funzione f calcolata per x :

$$|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \rightarrow (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Possiamo dire che lo stato $|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ è un autovettore dell'operatore U_f con autovalore $(-1)^{f(x)}$. Tornando allo stato iniziale $|\psi_1\rangle$, applichiamo l'operatore U_f e una porta di Hadarmard sul primo qubit per ottenere

$$\begin{aligned} |\psi_2\rangle &= U_f |\psi_1\rangle = \frac{1}{\sqrt{2}} ((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle) \\ &\xrightarrow{H_1} \frac{1}{2} [|0\rangle ((-1)^{f(0)} + (-1)^{f(1)}) + |1\rangle ((-1)^{f(0)} - (-1)^{f(1)})] \end{aligned}$$

Se la funzione è costante avremo che $(-1)^{f(0)} + (-1)^{f(1)} = 2$ e $(-1)^{f(0)} - (-1)^{f(1)} = 0$ quindi $|\psi_2\rangle = |0\rangle$. Al contrario se la funzione è bilanciata avremo che $(-1)^{f(0)} + (-1)^{f(1)} = 0$ e $(-1)^{f(0)} - (-1)^{f(1)} = \pm 2$ quindi $|\psi_2\rangle = \pm |1\rangle$ e visto che il segno \pm può essere visto come fase globale, possiamo dire che lo stato finale è $|1\rangle$.

L'algoritmo di Deutch permette di migliorare le performance dell'algoritmo classico perchè usa il parallelismo quantistico.

4.5.2 Algoritmo di Deutch-Josza

L'algoritmo di Deutch-Josza segue i passaggi dell'algoritmo di Deutch. Lo stato iniziale è

$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$$

Vengono applicate $n + 1$ porte di Hadarmard ai primi $n + 1$ qubit. In questo modo otteniamo la sovrapposizione di tutte le stringhe di bit con gli interi da 0 a $N - 1 = 2^n - 1$. Lo stato diviene

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |-\rangle$$

A questo punto a questo stato viene applicato l'operatore U_f (da Bob) che si comporta così $U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ e quindi

$$|\psi_2\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{f(x)} |x\rangle |-\rangle$$

Successivamente Alice applica n porte di Hadarmard ai primi n qubit. Per capire come queste agiscono, è utile considerare il singolo qubit $|k\rangle$ con $k = \{0, 1\}$. Conosciamo il risultato dal calcolo diretto ma è utile scriverlo in maniera compatta come

$$H|k\rangle = \frac{1}{\sqrt{2}} \sum_{z=0}^1 (-1)^{kz} |z\rangle$$

Estendendo questo ragionamento a tutti gli n qubit, otteniamo

$$H^{\otimes n} |x_1, x_2, \dots, x_n\rangle = \sum_{x_1, x_2, \dots, x_n} \frac{(-1)^{x_1 z_1 + x_2 z_2 + \dots + x_n z_n}}{\sqrt{N}} |z_1, z_2, \dots, z_n\rangle$$

Che può essere riscritta in maniera compatta come:

$$H^{\otimes n} |x\rangle = \sum_{z=0}^{N-1} \frac{(-1)^{x \cdot z}}{\sqrt{N}} |z\rangle$$

Ora riscriviamo lo stato $|\psi\rangle$

$$|\psi_2\rangle = \sum_{x=0}^{N-1} \sum_{z=0}^{N-1} \frac{(-1)^{x \cdot z + f(x)}}{N} |z\rangle |-\rangle$$

Se $z = 0$ sappiamo che $x \cdot z = 0$ e se f costante ($f(x) \rightarrow \bar{f}$) per tutti i valori di x allora il termine $(-1)^{f(x)}$ non dipende più da x

$$\sum_{x=0}^{N-1} \frac{(-1)^{\bar{f}}}{N} = (-1)^{\bar{f}} \sum_{x=0}^{N-1} \frac{1}{N} = (-1)^{\bar{f}}$$

Quindi se la funzione è costante

$$|\psi_2\rangle = |0\rangle |-\rangle$$

e una misura dei primi n qubit restituirà sempre 0.

Se la funzione è bilanciata non possiamo portare fuori il fattore $(-1)^{f(x)}$ però sappiamo che per $\frac{N}{2}$ stringhe varrà $+1$ ($f(x) = 0$) e per le altre $\frac{N}{2}$ varrà -1 ($f(x) = 1$). Quindi il coefficiente dello stato $|0\rangle$ sarà

$$\sum_{x=0}^{N-1} \frac{(-1)^{f(x)}}{N} = \left(\sum_{f(x)=0} \frac{1}{N} \right) - \left(\sum_{f(x)=1} \frac{1}{N} \right) = \frac{1}{N} \left(\frac{N}{2} - \frac{N}{2} \right) = 0$$

4.5.3 Algoritmo di Bernstein-Vazirani

Supponiamo di avere uno spazio logico a n bit e di avere una funzione che per ogni input x calcola $f_a(x) = x \cdot a = x_1a_1 + x_2a_2 + \dots + x_na_n$ dove la stringa a n bit a è ignota. L'obiettivo è quello di determinare la stringa a .

L'azione dell'oracolo non sarà quello di aggiungere una fase $(-1)^{f(x)}$ ma una fase $(-1)^{x \cdot a}$ ($f_a(x) = x \cdot a$).

$$\begin{aligned} |\psi_2\rangle &= \sum_{x=0}^{N-1} \sum_{z=0}^{N-1} \frac{(-1)^{x \cdot z + x \cdot a}}{N} |z\rangle |-\rangle \\ &= \sum_{x=0}^{N-1} \sum_{z=0}^{N-1} \frac{(-1)^{(z \oplus a) \cdot x}}{N} |z\rangle |-\rangle \\ &= \sum_{z=0}^{N-1} \left(\sum_{x=0}^{N-1} \frac{(-1)^{(z \oplus a) \cdot x}}{N} \right) |z\rangle |-\rangle \\ &= \sum_{z=0}^{N-1} X_z |z\rangle |-\rangle \end{aligned}$$

Se $z = a$ vuol dire che le due stringhe hanno tutti gli n bit uguali ($z_i = a_i$). Per l' i -esimo bit dovremmo calcolare $z_i \text{ XOR } a_i$.

Il passo successivo è calcolare $(z+a) \cdot x$ che darà 0 visto che per i singoli bit avremo $(z_i + a_i) \cdot x_i = 0$ di conseguenza abbiamo che

$$X_{z=a} = \sum_{x=0}^{N-1} \frac{1}{N} = 1$$

e quindi tutti gli altri coefficienti devono essere annullati $X_{z \neq a} = 0$

4.5.4 Algoritmo di Simon

$$f : \{0, 1\}^n \rightarrow \{0, 1\}^n$$

La funzione f ha la caratteristica che per ogni x esiste un solo y tale che $f(x) = f(y)$. Tale y non è casuale ma sappiamo che è calcolato secondo la regola $y = x \oplus a$ dove a è una stringa di n bit. L'obiettivo è quello di determinare la stringa a , ovvero, la periodicità della funzione f . L'unica possibilità che abbiamo è di dare all'oracolo una serie di stringhe fino a che non troviamo una coppia x e y tale che $f(x) = f(y)$. Una volta trovate tali stringhe, il periodo può essere calcolato come $a = x \oplus y$.

In media sono necessari $2^{\frac{n}{2}}$ tentativi e chiamate dell'oracolo. Supponiamo come nell'algoritmo di Deutsch-Josza di partire da n bit logici più n qubit addizionali $|\psi_0\rangle = |0\rangle^{\otimes n} |0\rangle^{\otimes n}$ e di applicare N porte di Hadarmard ai primi n qubit:

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |0\rangle^{\otimes n}$$

Dato che $|0 \oplus f(x)\rangle = |f(x)\rangle$

$$|\psi_1\rangle \xrightarrow{O} |\psi_2\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle$$

Dato che per ogni x esiste un $x \oplus a$ tale che $f(x) = f(x \oplus a)$, possiamo scrivere

$$|\psi_2\rangle = \frac{1}{\sqrt{\frac{N}{2}}} \sum_{x=0}^{N-1} \frac{|x\rangle + |x \oplus a\rangle}{\sqrt{2}} |f(x)\rangle$$

$f(x)$ collassa a $f(x_0)$ con probabilità $\frac{1}{2^{n-1}} = \frac{2}{N}$ e il valore di questa stringa non è importante quindi possiamo scrivere lo stato come

$$|\psi_3\rangle = \frac{|x_0\rangle + |x_0 \oplus a_0\rangle}{\sqrt{2}}$$

Applichiamo n porte di Hadarmard

$$\begin{aligned} \frac{|x_0\rangle + |x_0 \oplus a\rangle}{\sqrt{2}} &\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} (-1)^{x_0 \cdot z} |z\rangle + \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} (-1)^{(x_0 \oplus a) \cdot z} |z\rangle \right) \\ &= \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} (-1)^{x_0 \cdot z} |z\rangle + \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} (-1)^{x_0 \cdot z + a \cdot z} |z\rangle \right) \\ &= \frac{1}{\sqrt{2N}} \left(\sum_{z=0}^{N-1} (-1)^{x_0 \cdot z} (1 + (-1)^{a \cdot z}) |z\rangle \right) \end{aligned}$$

Il prodotto interno bit-per-bit $a \cdot z = \{0, 1\}$ per le stringhe z per cui $a \cdot z = 1$, il coefficiente dello stato $|z\rangle$ è 0. Al contrario se $a \cdot z = 0$ il coefficiente è 1. La possiamo riscrivere come:

$$|\psi_4\rangle = \frac{1}{\sqrt{2N}} \sum_{a \cdot z = 0} (-1)^{x_0 \cdot z} [1 + (-1)^{a \cdot z}] |z\rangle$$

Dobbiamo iterare la procedura per ottenere diversi valori z_2, z_3, \dots, z_n tali che $a \cdot z_i = 0$ per $i = 1, \dots, n$. Con questi z_i possiamo risolvere il sistema di equazioni

$$\begin{cases} a \cdot z_1 = 0 \\ a \cdot z_2 = 0 \\ \vdots \\ a \cdot z_n = 0 \end{cases}$$

Se le equazioni sono linearmente indipendenti esiste una sola stringa a che le soddisfa tutte e può essere facilmente determinata.