Quantum Computing

Alessandra Di Pierro

Introduzione

1 Fisica e Computazione

Un processo di calcolo è essenzialmente un processo fisico che viene eseguito su una macchina il cui funzionamento obbedisce a certe leggi fisiche. La teoria classica della computazione si basa su un modello astratto di macchina universale (la Macchina di Turing Universale) che funziona secondo un insieme di regole e di principi enunciati nel 1936 da Alan Turing ed elaborati successivamente da John von Neumann negli anni '40. Questi principi sono rimasti essenzialmente immutati da allora, nonostante gli enormi progressi tecnologici che permettono oggi di produrre dispositivi di gran lunga piú potenti rispetto a quelli che si potevano realizzare nella prima metá del ventesimo secolo. La tacita assunzione alla base di questi principi è che una macchina di Turing idealizza un dispositivo meccanico di computazione (con una memoria potenzialmente infinita) che obbedisce alle leggi della fisica classica.

La computazione quantistica nasce come un paradigma alternativo basato sui principi della *meccanica quantistica*. Questi sono gli unici in grado di giustificare i fenomeni fisici che avvengono a livello microscopico, come per esempio all'interno di un atomo. Questi fenomeni saranno imprescindibili nella costruzione di computers elettronici in un futuro ormai prossimo se la legge di Moore continuerà a valere, come ci si aspetta. Questa legge formulata già negli anni Sessanta prevedeva che la potenza di un computer sarebbe raddoppiata una volta ogni due anni. In pratica questa legge ha dimostrato fino ad oggi la sua validità, e attualmente effetti quantistici incominciano ad interferire nel funzionamento dei dispositivi elettronici man mano che le loro dimensioni diventano più piccole.

L'idea di realizzare un modello di computazione come un sistema quantistico isolato cominció ad affacciarsi agli inizi degli anni Ottanta, quando P.

Benioff, partendo da considerazioni precedentemente elaborate da C. Bennet, definí la Macchina di Turing reversibile: una computazione puó sempre essere eseguita in modo da ritornare allo stato inziale ripercorrendo all'indietro i vari passi di computazione.

Successivamente R. Feynman domostró che nessuna Macchina di Turing classica poteva simulare certi fenomeni fisici senza incorrere in un rallentamento esponenziale delle sue prestazioni. Al contario, un "simulatore quantistico universale" avrebbe potuto effettuare la simulazione in maniera piú efficiente.

Nel 1985 D. Deutsch formalizzó queste idee nella sua Macchina di Turing Quantistica Universale, che rappresenta in teoria della calcolabitá quantistica esattamente quello che la Macchina di Turing Universale rappresenta per la calcolabitá classica e ha portato alla concezione moderna di *computazione quantistica.*

Naturalmente gli effetti dell'introduzione del nuovo modello di calcolo si sono fatti sentire anche nel campo della complessitá computazionale, (come previsto da Feynman), provocando il cambiamento della nozione di "trattabilitá". Ad esempio, nel 1994 P. Shor dimostra che il problema della fattorizzazione dei numeri primi (classicamente considerato intrattabile) si puó risolvere efficientemente (cioé in tempo polinomiale) con un algoritmo quantistico.

Queste considerazioni unite a quelle di tipo tecnologico accennate precedentemente, hanno portato all'affermarsi di un campo di ricerca oggi noto come teoria dell'informazione e della computazione quantistica. Concentrandoci su quest'ultima, ne studieremo le differenze fondamentali con il paradigma classico. Queste derivano essenzialmente dai principi della teoria quantistica che regolano il mondo dell'infinitamente piccolo. In particolare, avremo a che fare con i tre fenomeni, tanto fondamentali quanto poco intuitivi, della teoria quantistica su cui la computazione quantistica si basa in maniera essenziale e che determinano la sua enorme potenzialiá di calcolo: il *principio di sovrapposizione degli stati*, il *principio di misurazione* e il fenomeno dell'*entanglement.*

2 Quantum bits

Il concetto fondamentale della computazione classica è il *bit.* La computazione quantistica si basa su un concetto analogo, il *quantum bit*, o in breve *qubit*, di cui descriviamo nel seguito le proprietà fondamentali sottolineandone le differenze con il bit classico.

2.1 Interpretazione matematica

Descriveremo un qubit come un oggetto matematico astratto che gode di certe particolari proprietà. La natura fisica di tale oggetto verrà chiarita successivamente osservando la corrispondenza tra le proprietà di un qubit con quelle di un qualsiasi sistema quantistico a due stati. Richiamiamo innanzitutto alcune definizioni e notazioni alla base del modello matematico del qubit.

2.1.1 Spazi vettoriali

Lo spazio vettoriale reale a due dimensioni $\mathbb{R}^2$ è l'insieme dei vettori colonna della forma

$$v = \begin{pmatrix} a \\ b \end{pmatrix}$$

dove $a, b \in \mathbb{R}$ sono numeri reali. La norma di v è data da $\|v\| = \sqrt{a^2 + b^2}$. Il trasposto di v è il vettore riga $v^T = (a, b)$. Il prodotto scalare di due vettori

$$v_1 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \text{ e } v_2 = \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}$$

è dato da $v_1 \cdot v_2 \stackrel{\text{def}}{=} v_1^T v_2 = (a_1, b_1) \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = a_1 a_2 + b_1 b_2 = \|v_1\| \|v_2\| \cos\theta$, dove θ è l'angolo tra v_1 e v_2. Se $v_1 \cdot v_2 = 0$, allora i due vettori sono detti ortogonali.

I vettori $\{v_i \in \mathbb{R}^2 \mid i = 1, 2, \ldots, k\}$ sono detti linearmente indipendenti se

$$a_1 v_1 + a_2 v_2 + \ldots + a_k v_k = 0, \;\; a_i \in \mathbb{R},$$

implica che $a_i = 0$ per ogni $i = 1, 2, \ldots, k$. Altrimenti sono detti linearmente dipendenti.

Una base di $\mathbb{R}^2$ è un qualsiasi insieme di vettori linearmente indipendenti tali che ogni altro vettore in $\mathbb{R}^2$ si può esprimere come combinazione lineare dei vettori nell'insieme. Ogni coppia di vettori v_1 e v_2 linearmente indipendenti forma una base per $\mathbb{R}^2$. Si dice che v_1 e v_2 formano una base ortonormale per $\mathbb{R}^2$ se $\|v_1\| = \|v_2\| = 1$ e $v_1 \cdot v_2 = 0$. I due vettori

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

formano una base ortonormale per $\mathbb{R}^2$ detta la base standard di $\mathbb{R}^2$.

Esercizio 2.1 *Estendere le definizioni e proprietà date per* $\mathbb{R}^2$ *a* $\mathbb{R}^d, d \in \mathbb{N}$.

Analogamente, lo spazio vettoriale complesso a due dimensioni $\mathbb{C}^2$ è l'insieme dei vettori colonna della forma

$$w = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

con $\alpha, \beta \in \mathbb{C}$. La norma di w è data da $\|w\| = \sqrt{|\alpha|^2 + |\beta|^2}$, dove $|z|$ è il modulo del numero complesso z. Il coniugato complesso di w è il vettore riga $w^\dagger = (\alpha^*, \beta^*)$. In analogia con il prodotto scalare di due vettori reali, si definisce il prodotto scalare (o inner product) di due vettori complessi

$$w_1 = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \; w_2 = \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}$$

come

$$(w_1, w_2) \stackrel{\text{def}}{=} w_1^\dagger w_2 = (\alpha_1^*, \beta_1^*) \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \alpha_1^* \alpha_2 + \beta_1^* \beta_2.$$

Lo spazio vettoriale $\mathbb{C}^2$ con il suo prodotto scalare è detto spazio di Hilbert a due dimensioni.

Le definizioni di indipendenza lineare, base e base ortonormale sono analoghe a quelle per $\mathbb{R}^2$. I due vettori

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \; \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

formano una base ortonormale per $\mathbb{C}^2$ (detta base canonica).

2.2 Notazione di Dirac

Per rappresentare gli elementi di uno spazio vettoriale complesso é conveniente usare una notazione detta *notazione di Dirac* dal nome del famoso fisico inglese, pioniere della teoria quantistica, che la introdusse. Essa rappresenta la notazione standard in meccanica quantistica. Secondo questa notazione $|v\rangle$ (o *ket*) indica un generico elemento dello spazio vettoriale e $|i\rangle$ indica l'i-esimo elemento della base ortonormale canonica.

Se $|v\rangle = \sum_i \alpha_i |i\rangle$ e $|w\rangle = \sum_i \beta_i |i\rangle$, allora il loro prodotto scalare

$$(v, w) = (\alpha_1^*, \ldots, \alpha_d^*) \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_d \end{pmatrix},$$

si indica con $\langle v|w\rangle$, e in generale il vettore riga $(\alpha_1^*, \dots, \alpha_d^*)$ si denota con $\langle v|$ o *bra* (cosí che $\langle v|w\rangle$ formano un *braket*.

L'utilitá di questa notazione sará particolarmente evidente quando studieremo la misurazione quantistica e in particolare gli operatori di proiezione.

2.2.1 Qubit come vettore unitario complesso

Lo stato di un bit classico viene descritto mediante i valori 0 e 1. Il modo piu' diretto per rappresentare lo stato di un qubit è mediante un vettore unitario in uno spazio vettoriale complesso a due dimensioni. I vettori $|0\rangle$ e $|1\rangle$ formano una base ortonormale per questo spazio vettoriale, nota come *base computazionale standard*. Usando la notazione classica dell'algebra lineare, possiamo rappresentare $|0\rangle$ con il vettore colonna $(1,0)^T$ e $|1\rangle$ con il vettore $(0,1)^T$, dove T indica il trasposto. Gli stati $|0\rangle$ e $|1\rangle$ di un qubit si possono vedere come i corrispondenti degli stati 0 e 1 di un bit classico. La differenza tra bits e qubits sta nel fatto che un qubit si può trovare anche in altri stati diversi da $|0\rangle$ e $|1\rangle$. Infatti, ogni combinazione lineare

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

dove α e β sono numeri complessi tali che $|\alpha|^2 + |\beta|^2 = 1$, è un possibile stato per un qubit. In notazione algebrica, il vettore $|\psi\rangle$ corrisponde a

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Tali stati sono spesso chiamati *sovrapposizioni* (superpositions).

2.2.2 Principio di misurazione

Mentre per un bit classico possiamo sempre determinarne lo stato e stabilire con precisione se è 0 o 1, per un qubit non possiamo determinare con altrettanta precisione il suo stato quantistico, cioè i valori di α e β. La meccanica quantistica ci dice che quando misuriamo un qubit possiamo solo ottenere lo stato $|0\rangle$ con una probabilità pari a $|\alpha|^2$ oppure lo stato $|1\rangle$ con una probabilità pari a $|\beta|^2$. Per questo motivo i valori α e β sono chiamati *ampiezze di probabilità* e la somma $|\alpha|^2 + |\beta|^2$ deve essere 1. Geometricamente questo significa che gli stati di un qubit sono vettori normalizzati di lunghezza 1 (o vettori unitari).

Abbiamo quindi stabilito che un qubit si può trovare in un numero di stati che è infinitamente maggiore di quello dei possibili stati di un bit classico. Si vedrà successivamente che la realizzazione fisica di un qubit non permette di osservare direttamente questi stati: la "misurazione" di un qubit darà sempre come risultato o lo stato $|0\rangle$ oppure lo stato $|1\rangle$. Si noti tuttavia che i risultati delle misurazioni dipendono strettamente dalle proprietà specifiche dello stato su cui si sono effettuate operazioni di trasformazioni. In questo risiede essenzialmente la potenza del calcolo quantistico.

Esempio 2.2 *Un qubit si può trovare nello stato*

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

fino al momento in cui viene osservato. Nel momento in cui lo misuriamo, il risultato sarà 0 nel 50% dei casi e 1 nel rimanente 50% dei casi. Cioè otterremo il risultato 0 con probabilità $(1/\sqrt{2})^2 = 1/2$ *e il risultato 1 con probabilità* $(1/\sqrt{2})^2 = 1/2$.

2.2.3 Cambio di base

Una qualsiasi base di $\mathbb{C}^2$ puó essere vista come una base computazionale.

Per esempio i due qubits $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ formano anch'essi una base computazionale. Si calcola facilmente che:

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \text{ e}$$

$$|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle).$$

Quindi un qubit arbitrario $\alpha|0\rangle + \beta|1\rangle$ puó essere espresso nella nuova base come:

$$\begin{aligned} \alpha|0\rangle + \beta|1\rangle &= \tfrac{\alpha}{\sqrt{2}}(|+\rangle + |-\rangle) + \tfrac{\beta}{\sqrt{2}}(|+\rangle - |-\rangle) \\ &= \tfrac{\alpha+\beta}{\sqrt{2}}|+\rangle + \tfrac{\alpha-\beta}{\sqrt{2}}|-\rangle. \end{aligned}$$

Si possono anche fare misurazioni rispetto ad una base diversa dalla base standard $\{|0\rangle, |1\rangle\}$. In questo caso il qubit misurato collasserá a uno degli stati della base computazionale considerata. Nell'esempio visto prima, questi corrispondono a $|+\rangle$ e $|-\rangle$.

2.3 Interpretazione geometrica

Una visualizzazione utile di un qubit si puó ottenere mediante un'interpretazione geometrica che associa gli stati di un qubit ai punti sulla superficie di una sfera di raggio unitario. Il polo sud della sfera corrisponde a 1 e il polo nord a 0. Le altre locazioni sono le sovrapposizioni quantistiche di 0 e 1. Questa

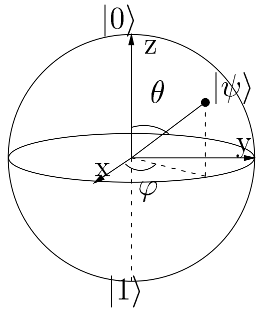

Figure 1: La sfera di Bloch

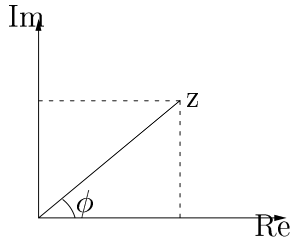

Figure 2: Il piano complesso: $z = a + ib$

sfera è nota come la *sfera di Bloch* ed é rappresentata in Figura 1. Molte delle operazioni su un singolo qubit che studieremo possono essere descritte all'interno di questa sfera, che ci aiuta cosi' a coglierne il significato intuitivo.

Esiste una corrispondenza biunivoca tra un generico stato di un qubit

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

e un punto sulla sfera unitaria in $\mathbb{R}^3$ rappresentato come

$$\cos(\theta/2) |0\rangle + e^{i\varphi} \sin(\theta/2) |1\rangle ,$$

dove θ e φ sono numeri reali (le coordinate sferiche del punto).
Per vedere questa corrispondenza ricordiamo prima la definizione di numero complesso.
Un numero complesso ha la forma $z = a + ib$, dove $i = \sqrt{-1}$, $a = Re(z)$ è la parte reale di z, $b = Im(z)$ è la parte immaginaria di z e $a, b \in \mathbb{R}$ sono numeri reali. La *norma* o *modulo* di z è $|z| = \sqrt{a^2 + b^2}$. Il *coniugato* di z è $z^* = a - ib$. Si denota con $\mathbb{C}$ l'insieme dei numeri complessi.
Un numero complesso $z \in \mathbb{C}$ si può vedere come un punto nel piano complesso in Figura 2.

Due rappresentazioni equivalenti di z come punto in questo piano sono:

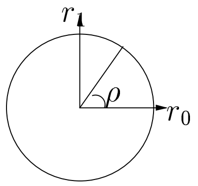

Figure 3: Il cerchio unitario di equazione $r_0^2 + r_1^2 = 1$

Coordinate cartesiane: z è il punto di coordinate a (sull'asse reale Re) e b (sull'asse immaginario Im), cioè $z = a + ib$, con $a, b \in \mathbb{R}$.

Coordinate polari: se ϕ è l'angolo che il vettore z forma con l'asse Re e $r = \sqrt{a^2 + b^2}$ è il modulo di z, allora $a = r\cos(\phi)$ e $b = r\sin(\phi)$. Quindi z è individuato dalle coordinate (r, ϕ), cioè $z = r(\cos(\phi) + i\sin(\phi))$. Dalla formula di Eulero

$$e^{i\phi} = \cos(\phi) + i\sin(\phi),$$

si ottiene quindi la rappresentazione di z come $re^{i\phi}$.

In un qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, i valori α e β sono numeri complessi tali che $|\alpha|^2 + |\beta|^2 = 1$. Usando la descrizione di α e β in coordinate polari possiamo scrivere $|\psi\rangle$ come

$$|\psi\rangle = r_0 e^{i\phi_0}|0\rangle + r_1 e^{i\phi_1}|1\rangle,$$

con

$$r_0^2 + r_1^2 = 1. \tag{1}$$

Notiamo che l'equazione (1) descrive i punti del cerchio unitario in $\mathbb{R}^2$ (cf. Figura 3). Possiamo quindi rappresentare i moduli di α e β mediante l'angolo ρ, ponendo

$$r_0 = \cos(\rho) \text{ e } r_1 = \sin(\rho).$$

Ponendo $\rho = \theta/2$, otteniamo l'espressione

$$|\psi\rangle = \cos(\theta/2)e^{i\phi_0}|0\rangle + \sin(\theta/2)e^{i\phi_1}|1\rangle,$$

con $0 \leq \theta \leq \pi$, o equivalentemente

$$|\psi\rangle = e^{i\gamma}(\cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle),$$

con $\varphi = \phi_1 - \phi_0$ e $\gamma = \phi_0$, $0 \leq \varphi \leq 2\pi$.

Vedremo che da un punto di vista fisico il fattore $e^{i\gamma}$ (detto fase globale) si può ignorare in quanto non ha *effetti osservabili*, cioé dal punto di vista osservazionale i due stati $e^{i\gamma}|\psi\rangle$ e $|\psi\rangle$ sono identici (dal principio di misurazione quantistica). Notiamo infine che l'angolo sferico θ che un punto sulla sfera unitaria in $\mathbb{R}^3$ forma con l'asse z soddisfa esattamente la stessa condizione $0 \leq \theta \leq \pi$ dell'angolo θ nella rappresentazione del qubit $\cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle$. Anche l'angolo φ in questa rappresentazione varia nello stesso intervallo $0 \leq \varphi \leq 2\pi$ dell'angolo che la proiezione di un vettore unitario nella sfera di Bloch sul piano (x, y) forma con l'asse x.

Quindi esiste effettivamente una corrispondenza biunivoca tra i qubits rappresentati come

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle ,$$

e i punti sulla sfera di Bloch.

Poiché possiamo codificare nel numero θ stringhe di bits di lunghezza arbitraria, l'informazione classica che puó contenere un qubit sembrerebbe infinita. Tuttavia l'unico modo per estrarre l'informazione contenuta in un qubit é attraverso una misurazione. Secondo le leggi della meccanica quantistica il risultato di tale misurazione é sempre un singolo bit classico – 0 oppure 1 – con probabilitá che dipende dalla "latitudine" del qubit.

2.4 Interpretazione fisica

La descrizione astratta di un qubit come un vettore in uno spazio bi- dimensionale complesso ha un corrispondente nel mondo reale. In particolare, un qualsiasi sistema fisico con almeno due livelli di energia discreti e sufficientemente separati è un candidato appropriato per rappresentare un qubit. Per realizzare fisicamente un qubit i tre approcci piú comuni sono quelli basati su:

- le due diverse polarizzazione di un fotone;
- l'allineamento di uno spin nucleare in un campo magnetico uniforme;
- i due stati di un elettrone che orbita in un singolo atomo.

Ad esempio possiamo considerare il sistema costituito dall'atomo di idrogeno H. In questo sistema, lo stato $|0\rangle$ del qubit può essere rappresentato dal primo livello di energia ($n = 0$), corrispondente allo stato base dell'elettrone, e lo stato $|1\rangle$ dal secondo livello di energia ($n = 1$) corrispondente allo stato eccitato dell'elettrone, come in Figura 4. Il passaggio dell'elettrone da uno stato all'altro può essere realizzato sottoponendo

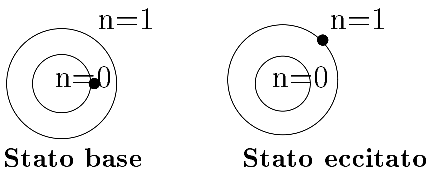

Figure 4: Qubit rappresentato da un elettrone in un atomo di idrogeno

l'elettrone ad un impulso laser di appropriata intensità, durata e lunghezza d'onda. Riducendo opportunamente la durata, si può realizzare il passaggio di un elettrone inizialmente nello stato $|0\rangle$ ad uno stato che si trova "a metà" tra $|0\rangle$ e $|1\rangle$, corrispondente allo stato $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ dell'esempio 2.2.

Come illustrato nell'Esempio 2.2, quando osserviamo un qubit, il risultato può solo essere 0 oppure 1. Inoltre, la misurazione che abbiamo fatto *cambia* lo stato del qubit facendolo collassare dalla sua sovrapposizione di $|0\rangle$ e $|1\rangle$ allo stato specifico consistente con il risultato della misurazione. Queste proprietà si spiegano mediante i principi della meccanica quantistica che illustriamo brevemente nel seguente esempio.

3 Registri quantistici

Con due bits classici possiamo formare quattro possibili stati: 00, 01, 10, 11. In generale, con n bits è possibile costruire 2^n stati distinti. Quanti stati si possono ottenere con n qubits? Lo spazio degli stati generato da un sistema di n qubits ha dimensione 2^n: ogni vettore normalizzato in questo spazio rappresenta un possibile stato computazionale, che chiameremo *registro quantistico a n qubits*. Questa crescita esponenziale nel numero dei qubits delle dimensioni dello spazio degli stati suggerisce la potenziale capacità di un computer quantistico di elaborare informazioni ad una velocità esponenzialmente superiore a quella di un computer classico. Si noti che per $n = 200$ si ottiene un numero che è più grande del numero di atomi nell'universo.

Formalmente un registro quantistico di n qubits è un elemento dello spazio di Hilbert 2^n-dimensionale, $\mathbb{C}^{2^n}$, con base computazionale formata da 2^n registri a n qubits

$$|i_1\rangle \otimes |i_2\rangle \otimes \ldots \otimes |i_n\rangle$$

con $i_j \in \{0,1\}$, $1 \leq j \leq n$. Per convenienza, questo vettore della base si scrive $|i_1\rangle |i_2\rangle \ldots |i_n\rangle$ oppure semplicemente $|i_1 i_2 \ldots i_n\rangle$.

Consideriamo il caso di due qubits. In analogia con il singolo qubit, possiamo costruire la base computazionale dello spazio degli stati come formata dai vettori $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Come osservato precedentemente, $|x, y\rangle$ è un'abbreviazione di $|x\rangle \otimes |y\rangle$, il prodotto tensore di x e y. In notazione algebrica questi vettori corrispondono quindi a

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Un registro quantistico a due qubits è una sovrapposizione della forma:

$$|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle ,$$

con la condizione di normalizzazione $\sum_{i \in \{0,1\}^2} |\alpha_i|^2 = 1$.

Analogamente al caso di un singolo qubit, il risultato di una misurazione sarà uno degli stati $i \in \{0,1\}^2$ con probabilità $|\alpha_i|^2$.

In un sistema di n qubits possiamo anche misurare solo un sottoinsieme degli n qubits. Per esempio, nel caso di un registro a due qubit possiamo misurare il primo qubit ottenendo come risultato 0 con probabilità $|\alpha_{00}|^2 + |\alpha_{01}|^2$. Dopo aver effettuato la misurazione lo stato collasserà a

$$\frac{\alpha_{00} |00\rangle + \alpha_{01} |01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}.$$

Nota che lo stato viene rinormalizzato per avere lunghezza 1.

Esercizio 3.1 *Scrivere le basi computazionali per un registro quantistico a 3 qubits e a 4 qubits.*

3.1 Prodotto tensore

Il prodotto tensore è un'operazione che combina spazi vettoriali per formare spazi vettoriali più grandi. La costruzione generale per spazi vettoriali complessi di dimensione finita è definita come segue.

Nota che per ogni intero positivo m, lo spazio vettoriale complesso m-dimensionale $\mathbb{C}^m$ ha come base standard

$$b_1^m, b_2^m, \ldots, b_m^m,$$

dove il vettore colonna di dimensione m, b_j^m, ha componenti tutte nulle tranne la j-sima che è 1. Quindi, ogni vettore $u \in \mathbb{C}^m$ si può scrivere come $\sum_{j=1}^m u_j b_j^m$, per qualche $u_j \in \mathbb{C}$:

$$u = \begin{pmatrix} u_1 \\ \vdots \\ u_j \\ \vdots \\ u_m \end{pmatrix}$$

Dati due spazi vettoriali $\mathbb{C}^k$ e $\mathbb{C}^l$, si definisce il prodotto tensore come la funzione

$$\otimes : \mathbb{C}^k \times \mathbb{C}^l \to \mathbb{C}^{kl},$$

con

$$v \otimes w = \begin{pmatrix} v_1 w \\ \vdots \\ v_j w \\ \vdots \\ v_k w \end{pmatrix}$$

dove per ogni $1 \leq j \leq k$, $v_j w$ è la moltiplicazione del vettore colonna $w \in \mathbb{C}^l$ per lo scalare $v_j \in \mathbb{C}^l$.

Per definizione, il prodotto tensore soddisfa le seguenti proprietà. Indichiamo con z un arbitrario scalare in $\mathbb{C}$ e con V e W due generici spazi di Hilbert di dimensione k e l rispettivamente.

1. Per ogni $|v\rangle \in V$ e $|w\rangle \in W$,

$$z(|v\rangle \otimes |w\rangle) = (z\,|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z\,|w\rangle).$$

2. Per ogni $|v_1\rangle, |v_2\rangle \in V$ e $|w\rangle \in W$,

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle.$$

3. Per ogni $|v\rangle \in V$ e $|w_1\rangle, |w_2\rangle \in W$,

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle.$$

Esercizio 3.2 *Dimostra la proprietà di bilinearità:*

$$\begin{aligned}&(\alpha v + \alpha' v') \otimes (\beta w + \beta' w') = \\ &\alpha\beta v \otimes w + \alpha\beta' v \otimes w' + \alpha'\beta v' \otimes w + \alpha'\beta' v' \otimes w',\end{aligned}$$

dove $\alpha, \beta, \alpha', \beta' \in \mathbb{C}$, $v, v' \in \mathbb{C}^k$ *e* $w, w' \in \mathbb{C}^l$.

Esercizio 3.3 *Dimostra che:*

$$b_i^k \otimes b_j^l = b_{(i-1)l+j}^{kl}.$$

Esercizio 3.4 *Dimostra che per ogni* $v, v' \in \mathbb{C}^k$ *e* $w, w' \in \mathbb{C}^l$,

$$\langle v \otimes w | v' \otimes w' \rangle = \langle v | v' \rangle \langle w | w' \rangle.$$

3.1.1 Prodotto tensore di matrici

Dati due operatori lineari con matrici di rappresentazione

$$M : \mathbb{C}^k \mapsto \mathbb{C}^k \text{ e } N : \mathbb{C}^l \mapsto \mathbb{C}^l,$$

rispetto alle basi standard di $\mathbb{C}^k$ e $\mathbb{C}^l$, il prodotto tensore di M ed N è l'operatore lineare su $\mathbb{C}^{kl}$ con matrice di rappresentazione

$$M \otimes N : \mathbb{C}^{kl} \mapsto \mathbb{C}^{kl}$$

definita da

$$M \otimes N = \begin{bmatrix} M_{11}N & M_{12}N & \dots & M_{1k}N \\ M_{21}N & M_{22}N & \dots & M_{2k}N \\ \vdots & \vdots & \vdots & \vdots \\ M_{k1}N & M_{k2}N & \dots & M_{kk}N \end{bmatrix},$$

dove M_{ij} è l'elemento di indici i, j della matrice M e $M_{ij}N$ è la matrice $l \times l$ ottenuta moltiplicando N per il numero complesso M_{ij}.

Esempio 3.5 *Il prodotto tensore delle matrici*

$$M = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \text{ e } N = \begin{bmatrix} 0 & 1 \\ -1 & 2 \end{bmatrix}$$

è la matrice

$$M \otimes N = \begin{bmatrix} 0 & 1 & 0 & 3 \\ -1 & 2 & -3 & 6 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 2 \end{bmatrix}.$$

Esercizio 3.6 *Dimostrare le seguenti proprietà:*

1. $(M \otimes N)(v \otimes w) = (Mv) \otimes (Nw)$.

2. $(\alpha M + \alpha' M') \otimes (\beta N + \beta' N') =$
$\alpha\beta M \otimes N + \alpha\beta' M \otimes N' + \alpha'\beta M' \otimes N + \alpha'\beta' M' \otimes N'$.

3. $(M \otimes N)(M' \otimes N') = (MM') \otimes (NN')$.

4. $$\begin{aligned} (M \otimes N)^* &= M^* \otimes N^*, \\ (M \otimes N)^T &= M^T \otimes N^T, \\ (M \otimes N)^\dagger &= M^\dagger \otimes N^\dagger. \end{aligned}$$

5. *Se M ed N sono unitarie (invertibili), allora anche $M \otimes N$ è unitaria (invertibile).*

Esercizio 3.7 *Verifica che*

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle .$$

Esercizio 3.8 *Verifica che*

$$\begin{aligned} H |x\rangle &= \frac{1}{\sqrt{2}} \sum_{y \in \{0,1\}} (-1)^{xy} |y\rangle \\ H^{\otimes n} |x\rangle &= \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle , \end{aligned}$$

dove $x \in \{0,1\}^n$ e $x \cdot y$ è $\sum_{j=1}^n x_i y_i$ modulo 2.

3.2 Stati “entangled”

Una proprietà importante dei registri quantistici a n qubits è che non è sempre possibile decomporli negli stati dei qubit componenti. Gli stati di questo tipo sono detti *entangled* e godono di proprietá che non si possono ritrovare in nessun oggetto della fisica classica. I membri di una collezione entangled non hanno un proprio stato individuale, solo l'intera collezione corrisponde a uno stato ben definito. Gli stati entangled si comportano come se fossero strettamente connessi l'uno all'altro indipendentemente dalla distanza che li separa. Ad esempio, una misurazione di uno dei due stati di una coppia entangled fornisce simultaneamente informazioni riguardo al secondo stato. Questa proprietá é alla base di soluzioni di problemi in information-processing che non possono essere riprodotte classicamente. Un esempio che vedremo nel seguito é la realizzazione di circuiti quantistici per il teletrasporto di uno stato quantistico da una locazione all'altra.

Esempio 3.9 (Entanglement) *Lo stato* $|00\rangle + |11\rangle$ *non può essere fattorizzato nel prodotto tensore di due qubits indipendenti, cioè non esistono* a_1, a_2, b_1, b_2 *tali che*

$$|00\rangle + |11\rangle = (a_1\,|0\rangle + b_1\,|1\rangle) \otimes (a_2\,|0\rangle + b_2\,|1\rangle).$$

Esercizio 3.10 *Dimostrare l'affermazione dell'Esempio 3.9.*