UNIVERSITÀ DI PISA

DIPARTIMENTO DI INGEGNERIA
DELL'INFORMAZIONE

Tesi di Laurea Triennale in Ingegneria Informatica

Fondamenti della computazione quantistica e una sua applicazione nel campo della crittografia

Candidato:
Ilaria Salvetti

Relatori:
Prof. Giuseppe Anastasi
Prof. Enzo Mingozzi
Corelatore:
Prof. Luciano Lenzini

Anno Accademico 2023/2024

INDICE

1. Introduzione

Cos'è un computer quantistico? La risposta a questa domanda coinvolge varie discipline scientifiche: la meccanica quantistica, la teoria dell'informazione quantistica e l'informatica. Nell'ambito di questa tesi, ci concentreremo sugli aspetti che rendono un computer quantistico distinto dai computer classici. Con questa prospettiva, un computer quantistico lo possiamo definire come un dispositivo che si avvale della meccanica quantistica per eseguire computazione utilizzando i qubit (*quantum bit*) invece dei bit classici.
Mentre Richard Feynman è spesso accreditato come l'inventore del computer quantistico, ci sono stati diversi ricercatori che hanno anticipato questa idea. Nel 1979, Paul Benioff, un giovane fisico presso i laboratori nazionali di Argonne, ha presentato un articolo intitolato: *The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines [1]*. Da notare che Benioff completò e presentò l'articolo nel 1979 e fu pubblicato l'anno successivo, nel 1980. In questo articolo, Benioff ha dimostrato le basi teoriche per il calcolo quantistico e ha poi suggerito che un tale computer potrebbe essere costruito:

> *That is, the whole computation process is described by a pure state evolving under the action of a given Hamiltonian. Thus all the component parts of the Turing machine are described by states which have a definite phase relation to one another as the calculation progresses...The existence of such models at least suggests that the possibility of actually constructing such coherent machines should be examined.*

Anche Yuri Manin ha esposto l'idea centrale del calcolo quantistico nel suo libro del 1980 *Computable and Non-Computable [2]*. Tuttavia, il libro è stato scritto in russo e tradotto solo anni dopo.

Nel 1981, Feynman tenne una conferenza intitolata *Simulating Physics with Computers [3]*. In questo intervento, sostenne che un sistema classico non poteva rappresentare adeguatamente un sistema meccanico quantistico:

> *...nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy...*

Feynman delineò inoltre le caratteristiche che un computer quantistico dovrebbe avere per essere utile. Al momento di questa conferenza, tuttavia, non era chiaro né a Feynman né alla comunità dei fisici come si potesse costruire una tale macchina.

Una volta che Benioff, Manin e Feynman aprirono le porte di questo filone rivoluzionario di ricerca, i ricercatori iniziarono a investigare la natura degli algoritmi che potevano essere eseguiti sui computer quantistici. David Deutsch, un fisico di Oxford, sviluppò un esempio di algoritmo che sarebbe stato eseguito più velocemente su un computer quantistico. Successivamente generalizzò ulteriormente questo algoritmo in collaborazione con Richard Jozsa *[4]*.

Nel 1994, Shor era un ricercatore nella divisione matematica dei Bell Labs nel New Jersey. Shor si rese conto che poteva costruire un algoritmo per fattorizzare grandi numeri in due fattori primi; la fattorizzazione di grandi numeri è considerata intrattabile su un computer classico, ma l'algoritmo di fattorizzazione di Shor funziona rapidamente su un computer quantistico *[5]*. La fattorizzazione di grandi numeri è, naturalmente, il problema intenzionalmente difficile al centro della crittografia a chiave pubblica (PKC) come implementato nell'algoritmo RSA, il tipo di crittografia che è alla base di quasi tutte le comunicazioni odierne su internet. Questo include l'invio sicuro di numeri di carte di credito, pagamenti bancari e la garanzia della sicurezza dei sistemi di messaggistica online.

La crittografia basata su RSA trae vantaggio dalla difficoltà unidirezionale derivante dalla fattorizzazione di grandi numeri in due fattori primi. Produrre un numero grande è facile, basta moltiplicare i due fattori. Dato un numero arbitrariamente grande, tuttavia, è esponenzialmente difficile trovare i suoi due fattori primi.

Dopo Shor, nel 1999 Lov Grover dimostrò che si può ottenere un certo miglioramento in un algoritmo di ricerca non strutturata su un computer quantistico. L'algoritmo di Grover *[6]* ottiene un miglioramento quadratico, non esponenziale (come fa quello di Shor), ma è comunque un risultato estremamente significativo.

Mentre un gruppo di ricercatori stava facendo progressi nell'identificazione degli algoritmi che avrebbero funzionato su un computer quantistico con un'accelerazione rispetto ai computer classici, altri stavano facendo progressi nella realizzazione fisica di un computer quantistico.
Nel 1998, Isaac Chuang del Los Alamos National Laboratory, Neil Gershenfeld del Massachusetts Institute of Technology (MIT) e Mark Kubinec dell'Università della California a Berkeley crearono il primo computer quantistico (a 2 qubit) che poteva essere caricato con dati e fornire una soluzione. Anche se il loro sistema era coerente solo per pochi nanosecondi e banale dal punto di vista della risoluzione di problemi significativi, dimostrò in modo concreto i principi del calcolo quantistico.

Da quel momento in poi i grandi players dell'informatica, come ad esempio IBM e Google, si sono posti l'obiettivo di realizzare computer quantistici commerciali (ovvero disponibili a livello di mercato), in grado di eseguire algoritmi che su un computer classico impiegherebbero tempi "geologici".

La grande sfida che il *Quantum Computing* sta affrontando sin dall'inizio, riguarda la qualità dei qubit: sono molto delicati e perdono facilmente le loro

proprietà quantistiche se si presentano fattori come vibrazioni o fluttuazioni della temperatura. Proprio a causa di queste difficoltà pratiche, dovute all'effetto della *decoerenza quantistica*, lo sviluppo teorico di questo settore è sempre stato molto più avanti di quello sperimentale. Il Quantum Computing ci darà la possibilità di risolvere alcune classi di problemi in maniera più efficiente: il vantaggio nell'usare un computer quantistico, non sarà nella velocità di compilazione, ma nel modo in cui questa velocità scala al crescere delle dimensioni dell'input dato.

Una delle principali applicazioni sarà nella Cyber Security, in cui il Quantum Computing permetterà di sviluppare una crittografia più sofisticata basata sulla distribuzione di chiavi quantistiche, algoritmi di sicurezza quantistica e generatori di numeri casuali quantici. In seguito ne vedremo una prima applicazione con il Protocollo BB84, un protocollo quantistico per la distribuzione di chiavi per un sistema di crittografia sviluppato da Charles H. Bennet e Gilles Brassard nel 1984. L'altra applicazione che verrà descritta con qualche dettaglio è il Teleporting che sta alla base del futuro Quantum Internet.

Di seguito vengono elencati i capitoli in cui si snoda l'argomentazione della tesi. Per ognuno vengono elencati i temi trattati:

- Capitolo 2: vengono affrontati i postulati della meccanica quantistica;
- Capitolo 3: viene definito il concetto di qubit e la sua rappresentazione sulla sfera di Bloch;
- Capitolo 4: annovera le principali porte quantistiche a un qubit con cenni alla nomenclatura e a strumenti per mettere in relazione 2 stati, come il prodotto interno e il prodotto esterno;
- Capitolo 5: viene definito il prodotto tensore e alcune porte quantistiche a qubit multipli, con un piccolo accenno ai circuiti quantistici;
- Capitolo 6: in questo capitolo viene trattato il fenomeno dell'entanglement e degli stati entangled con l'esempio degli Stati di Bell;
- Capitolo 7: viene presa in esame la tecnica del Quantum Teleportation, affrontando anche il teorema della non-clonazione;

- Capitolo 8: tratta il protocollo BB84, primo metodo di crittografia quantistica;
- Capitolo 9: nella parte finale vengono espresse le conclusioni e gli obiettivi futuri in questo ambito.

2. Qubit

Il bit è il concetto fondamentale della computazione classica e dell'informazione classica. La computazione quantistica e l'informazione quantistica si basano su un concetto analogo, il bit quantistico, o *qubit* in breve. In questo capitolo introduciamo le proprietà del singolo qubit, confrontandole e mettendole in contrasto con le proprietà dei bit classici.

Sebbene i qubit siano oggetti fisici, nella tesi li descriveremo come oggetti matematici con determinate proprietà specifiche. La bellezza di trattare i qubit come entità astratte è che ci dà la libertà di costruire una teoria generale della computazione quantistica e dell'informazione quantistica che non dipende da un sistema specifico per la sua realizzazione. Proprio come un bit classico ha uno stato – o 0 o 1 – anche un qubit ha uno stato. Due stati possibili per un qubit sono gli stati $|0\rangle$ e $|1\rangle$, che come si può immaginare, corrispondono agli stati 0 e 1 per un bit classico. La notazione come '$|\rangle$' è chiamata *notazione di Dirac*, e la vedremo spesso, poiché è la notazione standard per gli stati nella meccanica quantistica. La differenza tra bit e qubit è che un qubit può essere in uno stato diverso da $|0\rangle$ o $|1\rangle$. È anche possibile formare combinazioni lineari di stati, spesso chiamate sovrapposizioni (*superpositions*):

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

dove i numeri α e β, denominati *ampiezze*, sono numeri complessi, che per motivi spiegati nel capitolo successivo, soddisfano il seguente vincolo: $|\alpha|^2 + |\beta|^2 = 1$.

In altre parole, lo stato di un qubit è un vettore in uno spazio vettoriale complesso bidimensionale. Gli stati speciali $|0\rangle$ e $|1\rangle$ sono conosciuti come stati di *base computazionale* e formano una base ortonormale per questo spazio vettoriale. Essi sono rappresentati dai vettori con componenti 0 ed 1:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Possiamo esaminare un bit classico per determinare se si trova nello stato 0 o 1. Viceversa, non possiamo esaminare un qubit per determinare il suo stato quantistico, cioè i valori di α e β. Invece, la meccanica quantistica ci dice che possiamo ottenere solo informazioni molto più limitate sullo stato quantistico. Quando misuriamo un qubit, otteniamo il risultato 0, con probabilità $|\alpha|^2$, o il risultato 1, con probabilità $|\beta|^2$. Naturalmente, $|\alpha|^2 + |\beta|^2 = 1$, poiché le probabilità devono sommare a uno. Geometricamente, possiamo interpretare questo come la condizione che lo stato del qubit sia normalizzato a lunghezza 1. Quindi, in generale lo stato di un qubit è un vettore unitario in uno spazio vettoriale complesso bidimensionale.

Questa dicotomia tra lo stato non osservabile di un qubit e le osservazioni che possiamo fare è al cuore della computazione quantistica e dell'informazione quantistica. Nella maggior parte dei nostri modelli astratti del mondo, c'è una corrispondenza diretta tra gli elementi dell'astrazione e il mondo reale. La mancanza di questa corrispondenza diretta nella meccanica quantistica rende difficile intuire il comportamento dei sistemi quantistici, tuttavia, c'è una corrispondenza indiretta, poiché gli stati dei qubit possono essere manipolati e trasformati in modi che portino a risultati di misurazione che dipendono distintamente dalle diverse proprietà dello stato. Quindi, questi stati quantistici hanno conseguenze reali, sperimentalmente verificabili, che vedremo essere essenziali per la potenza della computazione quantistica e dell'informazione quantistica.

2.1. Fase

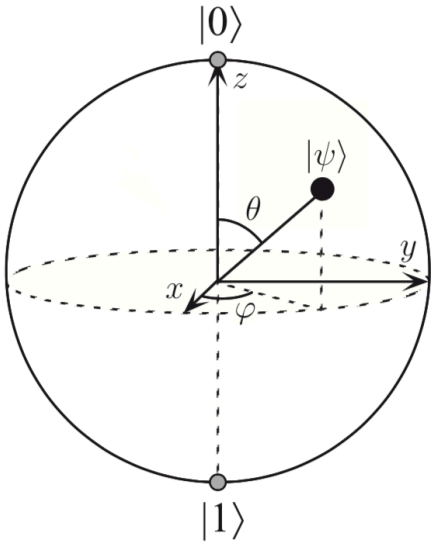
Il termine "fase" è comunemente usato in meccanica quantistica, con diversi significati dipendenti dal contesto. A questo punto è utile esaminare un paio di questi significati. Consideriamo, ad esempio, lo stato $e^{i\theta}|\psi\rangle$, dove $|\psi\rangle$ è un vettore di stato e θ è un numero reale. Diciamo che lo stato $e^{i\theta}|\psi\rangle$ è uguale a $|\psi\rangle$, a meno del fattore di *fase globale* $e^{i\theta}$. È interessante notare che le statistiche della misurazione previste per questi due stati sono le stesse. Pertanto, da un punto di vista osservativo questi due stati sono identici. Per questo motivo possiamo ignorare i fattori di fase globali come irrilevanti per le proprietà osservate del sistema fisico.

C'è un altro tipo di fase nota come *fase relativa*, che ha un significato piuttosto diverso. Consideriamo gli stati $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$ e $\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$. Nel primo stato l'ampiezza di $|1\rangle$ è $\frac{1}{\sqrt{2}}$. Per il secondo stato l'ampiezza è $-\frac{1}{\sqrt{2}}$. In entrambi i casi il valore assoluto delle ampiezze è lo stesso, ma differiscono nel segno. Più in generale, diciamo che due ampiezze, α e β, differiscono per una fase relativa se esiste un θ reale tale che $\alpha = e^{i\theta}\beta$. Più in generale ancora, due stati si dicono differire per una fase relativa in una certa base se ciascuna delle ampiezze in quella base è correlata da tale fattore di fase. Ad esempio, i due stati mostrati sopra sono gli stessi fino a uno spostamento di fase relativa perché le ampiezze di $|0\rangle$ sono identiche (un fattore di fase relativa di 1), e le ampiezze di $|1\rangle$ differiscono solo per un fattore di fase relativa di -1. La differenza tra fattori di fase relativa e globale è che per la fase relativa i fattori di fase possono variare da ampiezza ad ampiezza. Questo rende la fase relativa un concetto dipendente dalla base, a differenza della fase globale. Di conseguenza, gli stati che differiscono solo per fasi relative in una certa base danno luogo a differenze fisicamente osservabili nelle statistiche di misurazione, e non è possibile considerare questi stati come equivalenti

fisicamente, come facciamo con gli stati che differiscono per un fattore di fase globale.
Una rappresentazione utile per i qubit è la seguente rappresentazione geometrica di Bloch.

2.2. Sfera di Bloch

Lo stato di un singolo qubit può essere visualizzato geometricamente come un punto nella *sfera di Bloch*. Quest'ultima è una sfera di raggio unitario che ci fornisce un'interpretazione geometrica dello stato di un qubit, permettendoci di visualizzare e analizzare facilmente le sue proprietà.



Per poter determinare la posizione di un generico qubit all'interno della sfera di Bloch dobbiamo riscrivere lo stato del qubit come:

$$|\psi\rangle = cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi} sen\left(\frac{\theta}{2}\right)|1\rangle \qquad \text{dove } 0 \leq \theta \leq \pi \text{ e } 0 \leq \varphi \leq 2\pi$$

con le ampiezze, α reale e positiva e β complessa, scritte in funzione di θ:

$$\alpha = cos\left(\frac{\theta}{2}\right) \qquad \beta = e^{i\varphi} sen\left(\frac{\theta}{2}\right)$$

Sfruttando la condizione di normalizzazione:

$$sin^2 x + cos^2 x = 1$$

Vediamo perché nelle ampiezze α e β consideriamo metà dell'angolo θ.
Consideriamo:

$$|\psi\rangle = cos\theta' |0\rangle + e^{i\varphi} sen\theta' |1\rangle$$

Possiamo notare che $\theta' = 0 \Rightarrow |\psi\rangle = |0\rangle$ e $\theta' = \frac{\pi}{2} \Rightarrow |\psi\rangle = e^{i\varphi}|1\rangle$, il che ci suggerisce che $0 \leq \theta \leq \frac{\pi}{2}$ può generare tutti i punti della sfera di Bloch.
Consideriamo il punto $|\psi'\rangle$, corrispondente al punto opposto della sfera, con coordinate polari $(1, \pi - \theta', \varphi - \pi)$

$$|\psi'\rangle = cos(\pi - \theta')|0\rangle + e^{i(\varphi - \pi)} sin(\pi - \theta')|1\rangle$$

$$= -cos(\theta')|0\rangle + e^{i\varphi} e^{i\pi} sin(\theta')|1\rangle$$

$$= -cos(\theta')|0\rangle - e^{i\varphi} sin(\theta')|1\rangle$$

$$|\psi'\rangle = -|\psi\rangle = e^{i\pi}|\Psi\rangle \text{ con } e^{i\pi} = cos\,\pi + isin\,\pi = -1$$

Quindi è necessario considerare solo l'emisfero superiore $0 \leq \theta' \leq \frac{\pi}{2}$, poiché i punti opposti nell'emisfero inferiore differiscono solo per un fattore di fase -1 e quindi sono equivalenti nella rappresentazione della sfera di Bloch.
Possiamo mappare punti dell'emisfero superiore in punti sulla sfera definendo:

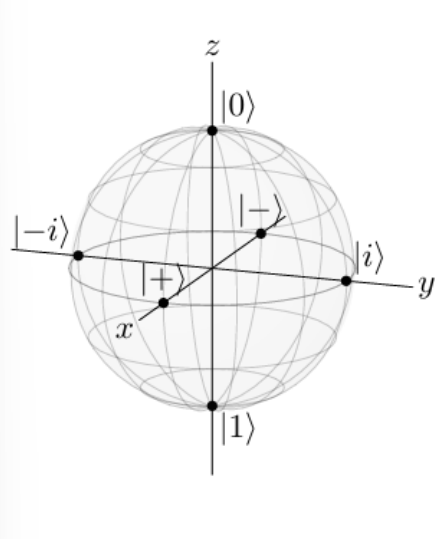
$$\theta = 2\theta' \Rightarrow \theta' = \frac{\theta}{2}$$

e così otteniamo:

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

Quindi, un generico vettore di stato $|\psi\rangle$ è immerso nella sfera di Bloch ed è caratterizzato da un vettore unitario, individuato dai due angoli θ *e* φ.

Alcuni stati noti sono:



"plus" $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

"minus" $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

"i" $|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$

"-i" $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

2.3. Basi quantistiche

Ogni coppia di punti opposti sulla sfera di Bloch sono ortogonali e di norma uno per cui tale coppia può essere considerata una *base* dello spazio di Hilbert associato al qubit in esame. Riportiamo di seguito alcune basi molto usate nella computazione quantistica e la loro relazione con la base computazionale.

- *base* Z: asse *z* della sfera di Bloch

$$\{|0\rangle, |1\rangle\}$$

- *base* X: asse *x* della sfera di Bloch

$$\{|+\rangle, |-\rangle\}$$

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

- *base* Y: asse y della sfera di Bloch

$$\{|i\rangle, |-i\rangle\}$$

$$|0\rangle = \frac{1}{\sqrt{2}}\left(|i\rangle + |-i\rangle\right), \; |1\rangle = \frac{-i}{\sqrt{2}}\left(|i\rangle - |-i\rangle\right)$$

3. Note di Algebra Lineare

Nella tesi tralasciamo la descrizione dello spazio di Hilbert. Viceversa, riportiamo di seguito alcune proprietà dello spazio di Hilbert che vengono utilizzate frequentemente nello sviluppo della tesi.

3.1. Il vettore “bra” associato a un vettore “ket”

Un generico qubit viene scritto con la notazione “*ket*”

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha\\0\end{pmatrix} + \begin{pmatrix}0\\\beta\end{pmatrix} = \begin{pmatrix}\alpha\\\beta\end{pmatrix}$$

Se vogliamo scrivere la *trasposta coniugata*, usiamo la notazione “*bra*”:

$$\langle\Psi| = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix} = \begin{pmatrix}\alpha^* & 0\end{pmatrix} + \begin{pmatrix}0 & \beta^*\end{pmatrix} = \alpha^*\begin{pmatrix}1 & 0\end{pmatrix} + \beta^*\begin{pmatrix}0 & 1\end{pmatrix} = \\ = \alpha^*\langle 0| + \beta^*\langle 1|$$

In $\langle\Psi|$ le ampiezze sono α^* e β^*, che sono le ampiezze di $|\Psi\rangle$ complesse coniugate. Il passaggio da *ket* a *bra* prende il nome di “*taking the dual*” (“prendendo il duale”)

3.2. Prodotto interno

Supponiamo di avere 2 stati:

$$|\Psi\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix} \qquad\qquad |\Phi\rangle = \begin{pmatrix}\gamma\\\delta\end{pmatrix}$$

Un modo per moltiplicare $|\Psi\rangle$ e $|\Phi\rangle$ è prendere il loro *prodotto interno*, definito come $\langle\Psi|\Phi\rangle$, chiamato "*bra-ket*".

$$\langle \Psi \,|\, \Phi \rangle \;=\; \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \;=\; \alpha^*\gamma + \beta^*\delta$$

Il risultato è un numero scalare che corrisponde al complesso coniugato del prodotto interno di $|\Phi\rangle$ e $|\Psi\rangle$.

$$\langle \Psi \,|\, \Phi \rangle \;=\; \langle \Phi \,|\, \Psi \rangle^*$$

Alcune proprietà possono essere espresse usando il prodotto interno:

- dato uno stato $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, questo è *normalizzato* se il suo prodotto interno con se stesso è uguale a 1, ovvero se la sua probabilità totale, $\langle\Psi|\Psi\rangle$è 1:

  $$\langle \Psi \,|\, \Psi \rangle \;=\; \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \;=\; |\alpha|^2 \,+\, |\beta|^2 \;=\; 1$$

- data una coppia di stati ai lati opposti della sfera di Bloch il loro prodotto interno è 0 e i due stati si dicono *ortogonali.*

  Es.

  $$\langle 0 \,|\, 1 \rangle \;=\; \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \;=\; 1 \cdot 0 + 0 \cdot 1 \;=\; 0 + 0 \;=\; 0$$

  $$\langle + \,|\, - \rangle \;=\; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \;=\; \frac{1}{2}(1 - 1) = 0$$

  $$\langle i \,|\, -i \rangle \;=\; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \;=\; \frac{1}{2}\left(1 + i^2\right) \;=\; 0$$

- le due proprietà precedenti, *normalità* e *ortogonalità*, possono essere combinate in una singola proprietà chiamata *ortonormalità.* Ad esempio, gli stati delle basi Z, X e Y, rispettivamente, $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$ e $\{|i\rangle, |-i\rangle\}$, sono ortonormali perché tra loro ortogonali e individualmente normalizzati.

I prodotti interni possono essere utilizzati per trovare le ampiezze degli stati quantistici, la cui norma quadratica ci da la probabilità. Le ampiezze possono essere usate per cambiare la base, infatti, per una base ortonormale $\{|\alpha\rangle, |\beta\rangle\}$, lo stato di un qubit può essere scritto come:

$$|\Psi\rangle = a|\alpha\rangle + b|\beta\rangle \quad \text{con } a = \langle\alpha|\Psi\rangle \text{ e } b = \langle\beta|\Psi\rangle$$

$\langle\alpha|\Psi\rangle$ è l'ampiezza di $|\Psi\rangle$ in $|\alpha\rangle$ ma anche la quantità di $|\Psi\rangle$ che è in $|\alpha\rangle$ o la quantità di sovrapposizione di $|\Psi\rangle$ e $|\alpha\rangle$.

3.3. Prodotto esterno

Considerando sempre due stati generici, $|\Psi\rangle$ e $|\Phi\rangle$, un altro modo per moltiplicarli è fare il loro *prodotto esterno*:

$$|\Psi\rangle\langle\Phi| = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}(\gamma^* \quad \delta^*)$$

Il risultato è una matrice 2x2. È possibile sommare più prodotti esterni per costruire diverse porte quantistiche.
Il prodotto esterno di $|\Phi\rangle$ e $|\Psi\rangle$ è la coniugata trasposta del prodotto esterno di $|\Psi\rangle$ e $|\Phi\rangle$:

$$|\Phi\rangle\langle\Psi| = |\Psi\rangle\langle\Phi|^\dagger$$

Abbiamo detto che per ogni base ortonormale $\{|\alpha\rangle, |\beta\rangle\}$, lo stato di un qubit può essere scritto come:

$$|\Psi\rangle = \langle\alpha|\Psi\rangle\ |\alpha\rangle + \langle\beta|\Psi\rangle\ |\beta\rangle$$

ed essendo i prodotti interni degli scalari, possiamo spostare il loro prodotto da sinistra a destra, in questo modo:

$$|\Psi\rangle = |\alpha\rangle\langle\alpha|\Psi\rangle + |\beta\rangle\langle\beta|\Psi\rangle$$

Perciò possiamo scrivere:

$$|\psi\rangle = |\alpha\rangle\langle\alpha|\,|\psi\rangle + |\beta\rangle\langle\beta|\,|\psi\rangle$$

$$|\psi\rangle = \left(|\alpha\rangle\langle\alpha| + |\beta\rangle\langle\beta|\right)|\psi\rangle$$

$$|\alpha\rangle\langle\alpha| + |\beta\rangle\langle\beta| = I$$

Questa è chiamata *relazione di completezza* e indica lo stato di qualsiasi qubit che può essere espresso in termini $|\alpha\rangle$ e $|\beta\rangle$, e questa proprietà prende il nome di *completezza*. Ciascuna coppia di stati ai lati opposti della sfera di Bloch è completa.

Base $\{|\alpha\rangle, |\beta\rangle\}$ ortonormale e completa, soddisfa la relazione:

$$|\alpha\rangle\langle\alpha| + |\beta\rangle\langle\beta| = I$$

4. Postulati della meccanica quantistica

La meccanica quantistica fornisce uno schema (*framework*) matematico per lo sviluppo delle teorie fisiche. Da sola, la meccanica quantistica non ci dice quali leggi un sistema fisico deve seguire, ma fornisce un quadro matematico e concettuale per lo sviluppo di tali leggi. Nei prossimi capitoli daremo una descrizione completa dei postulati di base della meccanica quantistica. Questi postulati forniscono una connessione tra il mondo fisico (nel nostro caso il computer quantistico) e il formalismo matematico della meccanica quantistica.

4.1. Lo Spazio degli Stati

Il primo postulato della meccanica quantistica stabilisce l'arena in cui si svolge la meccanica quantistica. L'arena è il nostro amico familiare dell'algebra lineare, lo spazio di Hilbert.

<u>*Postulato I*</u>**:**

> *Associato a qualsiasi sistema fisico isolato vi è uno spazio vettoriale complesso con prodotto interno (cioè, uno spazio di Hilbert) noto come lo spazio degli stati del sistema. Il sistema è completamente descritto dal suo vettore di stato, che è un vettore unitario nello spazio degli stati del sistema.*

La meccanica quantistica non ci dice, per un dato sistema fisico, quale sia lo spazio degli stati di quel sistema, né ci dice quale sia il vettore di stato del sistema. Il sistema di cui ci occuperemo maggiormente è il qubit. Un qubit ha uno spazio degli stati bidimensionale. Supponiamo che $|0\rangle$ e $|1\rangle$ formino una base ortonormale per quello spazio degli stati. Allora un vettore di stato arbitrario nello spazio degli stati può essere scritto come $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ dove

α e β sono numeri complessi. La condizione che $|\psi\rangle$ sia un vettore unitario è equivalente a $|\alpha|^2 + |\beta|^2 = 1$, spesso conosciuta come la *condizione di normalizzazione* per i vettori di stato. Prenderemo il qubit come nostro sistema fondamentale di meccanica quantistica. Nella realtà esistono sistemi fisici che possono implementare i qubit. Per noi, tuttavia, è sufficiente pensare ai qubit in termini astratti, senza riferimento a una realizzazione specifica. Le nostre discussioni sui qubit si riferiranno sempre a un insieme ortonormale di vettori base, $|0\rangle$ e $|1\rangle$, che dovrebbero essere considerati fissati in anticipo. Intuitivamente, gli stati $|0\rangle$ e $|1\rangle$ sono analoghi ai due valori 0 e 1 che un bit classico può assumere. La differenza tra un qubit e un bit è che possono esistere sovrapposizioni di questi due stati, della forma $\alpha|0\rangle + \beta|1\rangle$, in cui non è possibile dire che il qubit sia definitivamente nello stato $|0\rangle$ o definitivamente nello stato $|1\rangle$. Concludiamo con una terminologia utile spesso utilizzata in connessione con la descrizione degli stati quantistici. Diciamo che qualsiasi combinazione lineare $\sum_i \alpha_i |\psi_i\rangle$ è una sovrapposizione degli stati $|\psi_i\rangle$ con ampiezza α_i per lo stato $|\psi_i\rangle$.

Quindi, per esempio, lo stato $\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$ è una sovrapposizione degli stati $|0\rangle$ e $|1\rangle$ con ampiezza $\frac{1}{\sqrt{2}}$ per lo stato $|0\rangle$, e ampiezza $-\frac{1}{\sqrt{2}}$ per lo stato $|1\rangle$.

4.2. Evoluzione

Come cambia nel tempo lo stato $|\psi\rangle$ di un sistema meccanico quantistico? Il seguente postulato fornisce una prescrizione per la descrizione di tali cambiamenti di stato.

<u>*Postulato II*</u>:

> *L'evoluzione di un sistema quantistico chiuso è descritta da una trasformazione unitaria. Cioè, lo stato $|\psi\rangle$ del sistema al tempo t_1 è correlato allo stato $|\psi'\rangle$ del sistema al tempo t_2 tramite un operatore unitario U che dipende solo dai tempi t_1 e t_2,*

$$|\psi'\rangle = U(t_1 , t_2) \ |\psi\rangle.$$

Così come la meccanica quantistica non ci dice quale sia lo spazio degli stati o lo stato quantistico di un particolare sistema quantistico, non ci dice nemmeno quali operatori unitari U descrivano la dinamica quantistica del mondo reale. La meccanica quantistica ci assicura semplicemente che l'evoluzione di qualsiasi sistema quantistico chiuso può essere descritta in questo modo. Una domanda ovvia da porsi è: quali operatori unitari sono naturali da considerare? Nel caso dei singoli qubit, risulta che qualsiasi operatore unitario può essere realizzato in sistemi realistici.

Vedremo più avanti gli operatori unitari su un singolo qubit che sono importanti nella computazione quantistica e nell'informazione quantistica (per esempio gli operatori di Pauli X, Y, Z).

Il Postulato II richiede che il sistema descritto sia chiuso. Esistono comunque strumenti che ci permettono di descrivere sistemi che non sono chiusi, ma che noi non analizzeremo in questa tesi.
Il Postulato descrive come gli stati quantistici di un sistema quantistico chiuso, in due momenti diversi siano correlati. Una versione più raffinata di questo postulato può essere data per descrivere l'evoluzione di un sistema quantistico nel tempo continuo.

<u>*Postulato II'*</u>:

> *L'evoluzione temporale dello stato di un sistema quantistico chiuso è descritta dall'equazione di Schrödinger*,
>
> $$i\hbar d|\psi\rangle dt = H|\psi\rangle.$$

In questa equazione, $\hbar$ è una costante fisica nota come costante di Planck il cui valore deve essere determinato sperimentalmente. Il valore esatto non è

importante per noi. In pratica, è comune assorbire il fattore $\hbar$ in H, effettivamente ponendo $\hbar$=1. H è un operatore hermitiano fisso noto come l'Hamiltoniana del sistema chiuso.

Se conosciamo l'Hamiltoniano di un sistema, allora (insieme alla conoscenza di $\hbar$) comprendiamo completamente la sua dinamica, almeno in linea di principio. In generale, determinare l'Hamiltoniana necessaria per descrivere un particolare sistema fisico è un problema molto difficile - gran parte della fisica del ventesimo secolo si è occupata di questo problema - che richiede un sostanziale contributo dagli esperimenti per essere risolto. Nei casi relativi alla nostra discussione sulla computazione quantistica non avremo bisogno di discutere le Hamiltoniane.

Qual è il collegamento tra l'approccio hamiltoniano alla dinamica, il Postulato II', e l'approccio degli operatori unitari, il Postulato II? La risposta è fornita scrivendo la soluzione dell'equazione di Schrödinger, che è facilmente verificabile essere:

$$|\psi(t_2)\rangle = e^{(-iH(t_2 - t_1))}|\psi(t_1)\rangle = U(t_1,t_2)|\psi(t_1)\rangle,$$

dove definiamo

$$U(t_1,t_2) \equiv e^{(-iH(t_2 - t_1)}.$$

Si può dimostrare che questo operatore è unitario, e inoltre, che qualsiasi operatore unitario U può essere realizzato nella forma $U = e^{iK}$ per qualche operatore hermitiano K. C'è quindi una corrispondenza biunivoca tra la descrizione della dinamica nel tempo discreto usando operatori unitari e la descrizione nel tempo continuo usando operatori Hamiltoniani.

4.3. Misura quantistica

Abbiamo postulato che i sistemi quantistici chiusi evolvono secondo un'evoluzione unitaria. L'evoluzione dei sistemi che non interagiscono con il resto del mondo va bene, ma ci devono anche essere momenti in cui lo sperimentatore, con una apparecchiatura di misura - ovvero un sistema fisico esterno - osserva il sistema per capire cosa stia accadendo all'interno del sistema. Tale apparato di misura provoca un'interazione che rende il sistema non più chiuso e quindi non necessariamente soggetto a un'evoluzione unitaria. Per spiegare cosa accade quando ciò viene fatto, introduciamo il Postulato III, che fornisce un mezzo per descrivere gli effetti delle misurazioni sui sistemi quantistici, e quindi, in particolare sui nostri qubit.

<u>*Postulato III*</u>:

> *Le misurazioni quantistiche sono descritte da una collezione* $\{M_m\}$ *di operatori di misura. Questi sono operatori che agiscono sullo spazio degli stati del sistema in fase di misurazione. L'indice m si riferisce agli esiti della misurazione che possono verificarsi nell'esperimento. Se lo stato del sistema quantistico è* $|\psi\rangle$ *immediatamente prima della misurazione, allora la probabilità che si verifichi il risultato m è data da:*
>
> $$p(m) = \langle \psi | \, M_m^\dagger M_m \, | \, \phi \rangle,$$
>
> *e lo stato del sistema dopo la misurazione è*
>
> $$\frac{M_m|\psi\rangle}{(\langle\psi| M_m^\dagger M_m |\psi\rangle)^{\frac{1}{2}}}$$
>
> *Gli operatori di misurazione soddisfano l'equazione di completezza,*
>
> $$\sum_m M_m^\dagger M_m = I.$$

L'equazione di completezza esprime il fatto che le probabilità si sommano a uno:

$$1 = \sum_{mp}(m) = \sum_{m} \langle\psi| \, \mathrm{M}_m^{\dagger} \mathrm{M}_m \, |\psi\rangle.$$

Il fatto che questa equazione sia soddisfatta per tutti $|\psi\rangle$ è equivalente all'equazione di completezza. Tuttavia, l'equazione di completezza è molto più facile da verificare direttamente, ecco perché compare nella formulazione del postulato.

Un esempio semplice ma importante di misurazione è la misurazione di un qubit nella base computazionale. Questa è una misurazione su un singolo qubit con due esiti definiti dagli operatori di misurazione $\mathrm{M}_0 = |0\rangle\langle 0|$ e $\mathrm{M}_1 = |1\rangle\langle 1|$. Osserva che ogni operatore di misurazione è Hermitiano, e che $M_0^2 = M_0$, $M_1^2 = M_1$. Pertanto la relazione di completezza è rispettata, $I = \mathrm{M}_0^{\dagger}\mathrm{M}_0 + \mathrm{M}_1^{\dagger}\mathrm{M}_1 = \mathrm{M}_0 + \mathrm{M}_1$. Supponiamo che lo stato in fase di misurazione sia $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Allora la probabilità di ottenere l'esito di misura 0 è:

$$p(0) = \langle\psi| \, \mathrm{M}_0^{\dagger}\mathrm{M}_0 \, |\psi\rangle = \langle\psi| \, \mathrm{M}_0 \, |\psi\rangle = |a|^2.$$

Analogamente, la probabilità di ottenere l'esito di misura 1 è $p(1) = |b|^2$.

Lo stato dopo la misurazione nei due casi è quindi:

$$\frac{M0|\psi\rangle}{|\alpha|} = \frac{\alpha}{|\alpha|}|0\rangle$$

$$\frac{M0|\psi\rangle}{|\beta|} = \frac{\beta}{|\beta|}|1\rangle$$

4.4. Sistemi composti

Supponiamo di essere interessati a un sistema quantistico composto da due (o più) sistemi fisici distinti, qubit nel caso nostro. Come dovremmo descrivere gli stati del sistema composto? Il seguente postulato descrive come lo spazio degli stati di un sistema composto è costruito dagli spazi degli stati dei sistemi componenti.

Postulato IV:

> *Lo spazio degli stati di un sistema fisico composto è il prodotto tensore degli spazi degli stati dei sistemi fisici componenti. Inoltre, se abbiamo sistemi numerati da 1 a n, e il sistema numero i è preparato nello stato* $|\psi_i\rangle$*, allora lo stato congiunto del sistema totale è*
>
> $$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle.$$

Il postulato IV ci consente anche di definire una delle idee più interessanti e sconcertanti associate ai sistemi quantistici compositi: *l'entanglement*. Consideriamo lo stato a due qubit $|\psi\rangle = \frac{(|00\rangle + |11\rangle)}{\sqrt{2}}$. Questo stato ha la notevole proprietà che non esistono stati a singolo qubit $|\alpha\rangle$ e $|\beta\rangle$ tali che $|\psi\rangle = |\alpha\rangle\ |\beta\rangle$. Diciamo che uno stato di un sistema composito che possiede questa proprietà (ovvero che non può essere scritto come un prodotto degli stati dei suoi sistemi componenti) è uno stato *entangled*. Per ragioni che nessuno comprende appieno, gli stati entangled svolgono un ruolo cruciale nella computazione quantistica e nell'informazione quantistica. In questa tesi vedremo, in particolare, che l'entanglement svolge un ruolo cruciale nel teletrasporto quantistico, come descritto nel Capitolo 7.

4.5. Meccanica quantistica: una visione globale

Ora abbiamo spiegato tutti i postulati fondamentali della meccanica quantistica. La maggior parte del resto della tesi è dedicata a derivare le conseguenze di questi postulati.
Rivediamo rapidamente i postulati e cerchiamo di collocarli in una sorta di prospettiva globale:

- il *postulato I* stabilisce l'arena per la meccanica quantistica, specificando come deve essere descritto lo stato di un sistema quantistico isolato;
- il *postulato II* ci dice che la dinamica dei sistemi quantistici chiusi è descritta dall'equazione di Schrödinger, e quindi dall'evoluzione unitaria;
- il *postulato III* ci dice come estrarre informazioni dai nostri sistemi quantistici fornendo una prescrizione per la descrizione della misurazione;
- il *postulato IV* ci dice come gli spazi degli stati di diversi sistemi quantistici possono essere combinati per fornire una descrizione del sistema composito.

Ciò che è strano della meccanica quantistica, almeno secondo la nostra visione classica, è che non possiamo osservare direttamente il vettore di stato. La fisica classica – e la nostra intuizione – ci dice che le proprietà fondamentali di un oggetto, come energia, posizione e velocità, sono direttamente accessibili all'osservazione. Nella meccanica quantistica queste quantità non appaiono più come fondamentali, essendo sostituite dal vettore di stato, che non può essere osservato direttamente. È come se ci fosse un mondo nascosto nella meccanica quantistica, che possiamo accedere solo indirettamente e in modo imperfetto.

Inoltre, osservare un sistema classico non cambia necessariamente lo stato del sistema. Immagina quanto sarebbe difficile giocare a tennis se ogni volta che guardi la palla la sua posizione cambiasse! Ma secondo il postulato III, l'osservazione nella meccanica quantistica è una procedura invasiva che tipicamente cambia lo stato del sistema.

5. Porte quantistiche

Le porte quantistiche sono delle mappe lineari che trasformano lo stato di un qubit andando a modificare le probabilità degli output della superposition, ma mantenendo la probabilità totale uguale a 1.
Vediamo alcune porte quantistiche a singolo qubit:

- *Identità*: non fa niente e lascia lo stato inalterato

$$I|0\rangle = |0\rangle \qquad I|1\rangle = |1\rangle \qquad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- *Pauli* X-*Gate*: possiamo paragonarla alla classica porta NOT, sulla sfera di Bloch corrisponde a una rotazione di 180° dell'asse x ($X^2 = I$)

$$X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- *Pauli* Y-*Gate*: corrisponde a una rotazione di 180° dell'asse y sulla sfera di Bloch ($Y^2 = I$)

$$Y|0\rangle = i|1\rangle \qquad Y|1\rangle = -i|0\rangle \qquad Y = \begin{pmatrix} o & -i \\ i & 0 \end{pmatrix}$$

- *Pauli* Z-*Gate*: corrisponde a una rotazione di 180° dell'asse z sulla sfera di Bloch ($Z^2 = I$)

$$Z|0\rangle = |0\rangle \qquad Z|1\rangle = -|1\rangle \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- S-*Gate*: "Phase Gate", è la radice quadrata del Z-Gate ($S^2 = Z \rightarrow S^4 = I$); corrisponde a una rotazione di 90° dell'asse z sulla sfera di Bloch

$$S|0\rangle = |0\rangle \qquad S|1\rangle = i|1\rangle \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

- *T-Gate*: è la radice quadrata del S-Gate ($T^2 = S \rightarrow T^4 = Z$); corrisponde a una rotazione di 45° dell'asse z sulla sfera di Bloch

$$T|0\rangle = |0\rangle \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$
$$T|1\rangle = e^{i\frac{\pi}{4}}|1\rangle$$

- *H-Gate*: "Hadamard Gate", corrisponde a una rotazione di 180° dell'asse $x+z$ sulla sfera di Bloch ($H^2 = I$)

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

Dunque, le porte quantistiche a un qubit sono rotazioni sulla sfera di Bloch: il qubit è un punto sulla sfera e ruotando rimane un punto.
Dal punto di vista più matematico: ruotiamo di un angolo θ intorno agli assi x, y, z con direzione dell'asse, rispettivamente, $\hat{x}, \hat{y}, \hat{z}$.
L'asse di rotazione sarà:

$$\hat{n} = n_x\hat{x} + n_y\hat{y} + n_z\hat{z}$$

$\hat{n}$ è un vettore unitario: $n_x^2 + n_y^2 + n_z^2 = 1$.

Possiamo scrivere una rotazione di angolo θ attorno all'asse $\hat{n}$ in termini di porte quantistiche I, X, Y e Z, come un operatore unitario arbitrario a singolo qubit:

$$U = e^{i\gamma}\left[\cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)\left(n_xX + n_yY + n_zZ\right)\right]$$

con γ la fase globale, a cui possiamo assegnare qualsiasi valore, o addirittura eliminare, in quanto non ha nessuna rilevanza fisica.
Consideriamo una porta quantistica U in forma di matrice che agisce su uno stato $|\Psi\rangle \rightarrow U|\Psi\rangle = |U\Psi\rangle$ (in notazione contratta). Perché U sia una porta

quantistica valida deve essere normalizzata, ovvero il prodotto intero di $|U\Psi\rangle$ con ste stesso deve essere uguale a 1:

$$\langle U\Psi|U\Psi\rangle = 1$$

$$\langle\Psi|U^{\dagger}U|\Psi\rangle = \langle\Psi|\Psi\rangle$$

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

Una matrice che soddisfa la proprietà $U^{\dagger}U = 1$ è detta *unitaria*.

Inoltre, una porta quantistica è sempre una matrice *reversibile*, e la sua inversa è proprio $U^{\dagger}$:

$$U^{\dagger}U|\Psi\rangle = I|\Psi\rangle = |\Psi\rangle$$

6. Stati a qubit multipli

6.1. Prodotto tensoriale

Fino ad ora abbiamo visto stati a un singolo qubit, il sistema fisico quanto meccanico più semplice, il cui stato è rappresentato da un vettore di norma uno appartenente ad uno spazio di Hilbert bidimensionale. Nella realtà esistono anche sistemi fisici composti da un numero $n > 1$ di qubit. In tal caso, lo spazio di Hilbert che rappresenta gli stati del sistema fisico ha dimensione 2^n.
Quando abbiamo un sistema ad n > 1 qubits, ciascuno dei quali inizializzato, per esempio a $|0\rangle$, il *postulato IV* della meccanica quantistica ci consente di scrivere lo stato del sistema a due qubit nel modo seguente:

$$|0\rangle \otimes |0\rangle \qquad \text{(zero tensore zero)}$$

$$\text{notazione compressa: } |0\rangle|0\rangle \rightarrow |00\rangle$$

In un sistema di due qubits il numero totale di ampiezze è quattro, e lo è anche il numero di stati. Nella base Z, uno stato generico a 2 qubit può essere scritto come:

$$\Psi = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

La probabilità totale è:

$$|c_0|^2 + |c_1|^2 + |c_2|^2 + |c_3|^2 = 1$$

Preso il vettore di stato, la probabilità che un measurement restituisca come output, ad esempio, lo stato $|01\rangle$ è uguale $|c_1|^2$. Usando il prodotto interno:

$$P(|01\rangle) = |\langle\Psi|01\rangle|^2$$

Anche la notazione *bra* può essere espressa con il prodotto tensoriale:
Es.

$$\langle 0| \otimes \langle 0| = \langle 0|\langle 0| = \langle 00|$$

6.2. Prodotto di Kronecker

Per la rappresentazione dello stato come matrice, si usa un caso particolare di prodotto tensoriale, ovvero il *prodotto di Kronecker*:

$$|a\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \quad |b\rangle = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}$$

$$|\Psi\rangle = |b\rangle \otimes |a\rangle = \begin{pmatrix} b_0 \times \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \\ b_1 \times \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} b_0 \times a_0 \\ b_0 \times a_1 \\ b_1 \times a_0 \\ b_1 \times a_1 \end{pmatrix}$$

Possiamo generalizzare il problema e considerare n qubits, dove avremo $N = 2^n$ stati, e quindi ampiezze. Questa è la maggiore differenza con gli elaboratori classici, per i quali è difficile simulare il comportamento di un elaboratore quantistico, proprio a causa dell' elevato numero di ampiezze da considerare.

6.3. Porte quantistiche a un qubit

È possibile applicare porte quantistiche a un qubit a sistemi con qubit multipli, semplicemente gestendo i qubit singolarmente:
Es.

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

In questo modo sto applicando una porta H al primo qubit lasciando inalterato il secondo, usando una porta Identità.

6.4. Porte quantistiche a qubit multipli

Ovviamente esistono anche porte quantistiche che mettono in relazione più qubits tra loro, mantenendo le proprietà di un gate valido. Vediamo alcune porte quantistiche a 2 qubits:

6.4.1. Porta CNOT

CNOT-Gate o *Controlled-NOT Gate* (può essere chiamato anche *CX-Gate* dal momento che *X-Gate* è di fatto un *NOT-Gate*)

→ inverte il qubit destro se quello sinistro è uguale a 1

$$CNOT\ |00\rangle = |00\rangle$$

$$CNOT\ |\ 01\rangle = |\ 01\rangle$$

$$CNOT\ |\ 10\rangle = |\ 11\ \rangle$$

$$CNOT\ |\ 11\ \rangle = |\ 10\rangle$$

Il qubit sinistro è chiamato *control qubit* ed è quello che non viene modificato dalla porta CNOT, mentre il qubit di destra è chiamato *target qubit* ed è il risultato di uno XOR tra gli input:

$$CNOT\ |a\rangle|b\rangle = |a\rangle\ |a \oplus b\rangle$$

Da ciò possiamo dedurre come la porta CNOT sia la porta quantistica che corrisponde alla porta classica XOR.

Quando agisce su una superposition di fatto si limita a scambiare le ampiezze degli stati $|10\rangle$ e $|11\rangle$:

$$CNOT\ (c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle) =$$

$$= c_0 CNOT\ |00\rangle + c_1 CNOT\ |01\rangle + c_2 CNOT\ |10\rangle + c_3 CNOT\ |11\rangle =$$

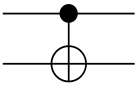
$$= c_0|00\rangle + c_1|01\rangle + c_2|11\rangle + c_3|10\rangle =$$

$$= c_0|00\rangle + c_1|01\rangle + c_3|10\rangle + c_2|11\rangle$$

La matrice corrispondente al CNOT è la seguente:

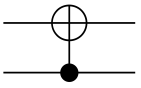
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

La rappresentazione grafica di tale porta in un circuito è mostrata nella seguente figura, dove il secondo qubit è il target.

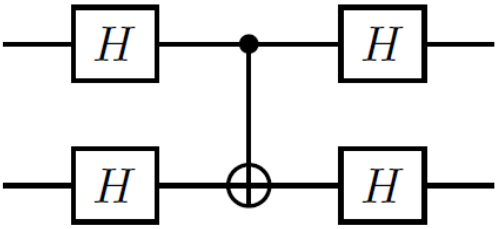


Se volessimo scambiare i qubit control e target avremmo una porta $CNOT_{01}$ (la porta CNOT corrisponde a $CNOT_{10}$). Di fatto la porta $CNOT_{01}$ scambia le ampiezze degli stati $|01\rangle$ e $|11\rangle$.

$$CNOT_{01}\,(c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle) =$$
$$= c_0|00\rangle + c_3|01\rangle + c_2|10\rangle + c_1|11\rangle$$



Un altro modo per scambiare control e target è quello di applicare H-Gate ad entrambi i lati di una porta CNOT, nel seguente modo:



$$(H \otimes H)\ CNOT\ (H \otimes H) = CNOT_{01}$$

Questo è l'esempio più semplice di un fenomeno chiamato *phase kickback*: l'effetto del CNOT compreso tra gli operatori H viene trasferito dal secondo al primo qubit. Parliamo un attimo di questo fenomeno:
phase kickback è un artificio quantistico che viene applicato su un registro di qubits tramite l'implementazione di uno specifico design circuitale e consente di trasportare informazioni da un qubit ad un insieme di qubits tramite una serie di operazioni di controllo. In altre parole, la fase di un qubit viene di fatto trasferita a un altro qubit durante un'operazione di controllo, creando entanglement e

vantaggi computazionali che permettono di implementare alcuni famosi algoritmi computazionali e protocolli.
Tornando all'esempio del $CNOT_{01}$, possiamo dire che la fase generata dal gate CNOT viene trasferita da uno dei due fili del registro all'altro.

Porta CNOT applicata alla base X:

$$CNOT\ |+\ +\rangle = |+\ +\rangle$$

$$CNOT\ |+\ -\rangle = |-\ -\rangle$$

$$CNOT\ |-\ +\rangle = |-\ +\rangle$$

$$CNOT\ |-\ -\rangle = |+\ -\rangle$$

6.4.2. Porta Controlled-U

Controlled-U Gate
→ applica una porta quantistica U al qubit destro se quello sinistro è uguale a 1

$$cU\ |00\rangle = |00\rangle$$

$$cU\ |01\rangle = |01\rangle$$

$$cU\ |10\rangle = |1\rangle \otimes U|0\rangle$$

$$cU\ |\ 11\ \rangle = |1\rangle \otimes U|1\rangle$$

$$\rightarrow cU|10\rangle = |1\rangle \otimes (a|0\rangle + b|1\rangle) = a|10\rangle + b|\ 11\ \rangle$$

$$\rightarrow cU|\ 11\ \rangle = |1\rangle \otimes (c|0\rangle + d|1\rangle) = c|10\rangle + d|\ 11\ \rangle$$

Come matrice, la porta quantistica risulta:

$$cU = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}$$

6.4.3. Porta SWAP

SWAP-Gate

→ scambia i due qubit

$$\text{SWAP} \mid 00\rangle = \mid 00\rangle$$

$$\text{SWAP} \mid 01\rangle = \mid 10\rangle$$

$$\text{SWAP} \mid 10\rangle = \mid 01\rangle$$

$$\text{SWAP} \mid 11\rangle = \mid 11\rangle$$

$$\Rightarrow \text{SWAP} \mid a\rangle \mid b\rangle = \mid b\rangle \mid a\rangle$$

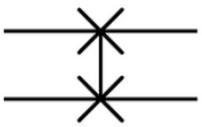
Su una superposition:

$$\text{SWAP}\,(c_0 \mid 00\rangle + c_1 \mid 01\rangle + c_2 \mid 10\rangle + c_3 \mid 11\rangle) =$$

$$= c_0 \mid 00\rangle + c_2 \mid 01\rangle + c_1 \mid 10\rangle + c_3 \mid 11\rangle$$

scampia le ampiezze di $\mid 01\rangle$ e $\mid 10\rangle$.

Questa porta viene indicata con il simbolo:



e corrisponde alla matrice:

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

Uno SWAP-Gate può essere creato usando tre CNOT-Gate:

$$\text{SWAP} = (\text{CNOT})(\text{CNOT}_{01})(\text{CNOT})$$

$$|a\rangle\,|b\rangle \rightarrow_{\text{CNOT}} |a\rangle\,|a \oplus b\rangle \rightarrow_{\text{CNOT01}} |a \oplus a \oplus b\rangle\,|a \oplus b\rangle = |b\rangle\,|a \oplus b\rangle$$

$$\rightarrow_{\text{CNOT}} |b, a \oplus b \oplus b\rangle = |b\rangle\,|a\rangle$$

6.4.4. Porta MS

Mølmer - Sørensen (MS) Gate

→ porta a due qubit che può essere naturalmente implementata sui computer quantistici con ioni intrappolati, trasforma gli stati della base Z

$$|00\rangle \rightarrow (|00\rangle + i|11\rangle)$$

$$|01\rangle \rightarrow (|01\rangle - i|10\rangle)$$

$$|10\rangle \rightarrow (|10\rangle - i|01\rangle)$$

$$|11\rangle \rightarrow (|11\rangle + i|00\rangle)$$

6.4.5. Porta Toffoli

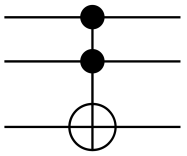
Una porta quantistica che opera su 3 qubits è il *Toffoli Gate*. Viene anche detto *CCNOT* in quanto agisce come il CNOT ma con un doppio controllo

→ inverte il qubit destro se quello sinistro e quello in mezzo sono a 1

$$\text{Toffoli}\ |a\rangle|b\rangle|c\rangle = |a\rangle|b\rangle|ab \oplus c\rangle$$

La matrice per questa porta risulta:

$$Toffoli = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

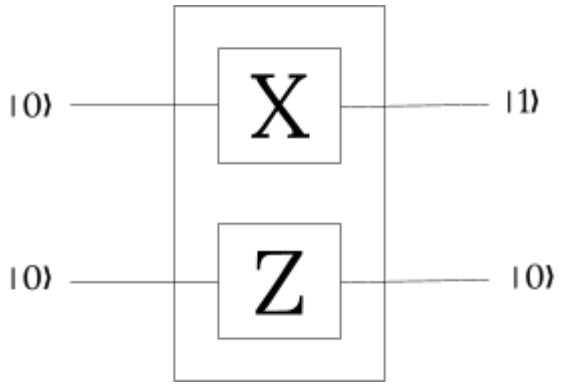


Applicato a una superposition si limita a scambiare le ampiezze degli stati $|110\rangle$ e $|111\rangle$.

6.5. Circuiti quantistici

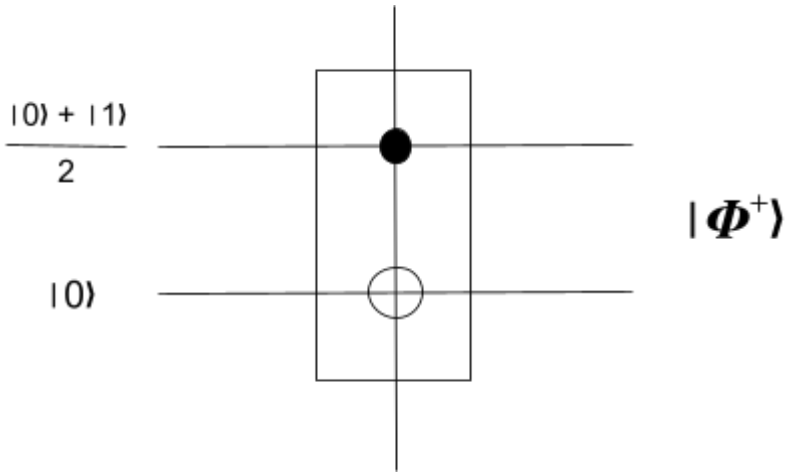
Un circuito quantistico è una serie di porte quantistiche applicate al qubit per eseguire calcoli. È un processo computazionale che riceve in input uno stato iniziale e fornisce in output il risultato di una misurazione. Esso è composto da un insieme di corde, che fanno riferimento ai qubits del sistema, e da una serie consecutiva di gates, attraverso cui è possibile compiere trasformazioni lineari del vettore di stato in superposition.
I circuiti quantistici sono gli elementi costitutivi degli algoritmi quantistici e svolgono un ruolo cruciale nell'informatica quantistica: consentono la manipolazione di stati quantistici e l'esecuzione di operazioni quantistiche.
Alcuni esempi:

Porte X e Z:



$|0\rangle \otimes |0\rangle$ $X \otimes Z$ $|1\rangle \otimes |0\rangle$

CNOT:



$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|0\rangle|0\rangle + |1\rangle|0\rangle}{\sqrt{2}} \longrightarrow \text{CNOT} \longrightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Phi^+\rangle$$

I concetti sviluppati precedentemente ci consentono adesso di approfondire alcuni argomenti che sono di fondamentale importanza per il quantum computing e per il quantum Internet.

7. Entanglement e Bell State

L'*entanglement* è una risorsa esclusivamente meccanico-quantistica che gioca un ruolo chiave in molte delle applicazioni più interessanti della computazione quantistica e dell'informazione quantistica. Negli ultimi anni c'è stato un enorme sforzo per comprendere meglio le proprietà dell'entanglement considerato come una risorsa fondamentale della Natura, di importanza paragonabile all'energia, all'informazione, all'entropia o a qualsiasi altra risorsa fondamentale. Sebbene non esista ancora una teoria completa dell'entanglement, sono stati fatti alcuni progressi nella comprensione di questa strana proprietà della meccanica quantistica. Molti ricercatori sperano che ulteriori studi sulle proprietà dell'entanglement possano offrire intuizioni che facilitino lo sviluppo di nuove applicazioni nella computazione quantistica e nell'informazione quantistica.

7.1. Stati entangled ed entanglement

Alcuni stati quantistici possono essere fattorizzati nel prodotto tensoriale di singoli stati di qubit. Dato uno stato a due qubit:

$$\alpha_1\alpha_0 |00\rangle + \alpha_1\beta_0 |01\rangle + \beta_1\alpha_0 |10\rangle + \beta_1\beta_0 |11\rangle$$

può essere scritto come:

$$(\alpha_1 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_0 |0\rangle + \beta_0 |1\rangle)$$

ovvero come prodotto tensore di due stati, ciascuno dei quali appartiene ai singoli qubit. Tali stati fattorizzabili prendono il nome di *stati prodotto* o *stati separabili*.

Esistono, però, degli stati quantistici che non possono essere fattorizzati in stati prodotto e che vengono chiamati *entangled states*.

Come descritto in wong [7], il seguente sistema non ha soluzione:

Es.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$\alpha_1\alpha_0 = \frac{1}{\sqrt{2}}\ ,\ \alpha_1\beta_0 = 0\ ,\ \beta_1\alpha_0 = 0\ ,\ \beta_1\beta_0 = \frac{1}{\sqrt{2}}$$

Questa proprietà per cui gli stati dei qubit sono intrecciati è chiamata *entanglement*.

L'entanglement descrive una correlazione tra diverse parti di un sistema quantistico che non ha riscontro nella fisica classica. Come abbiamo visto prima, tale proprietà si manifesta quando i sottosistemi interagiscono in modo tale che lo stato risultante dell'intero sistema non possa essere espresso come il prodotto diretto degli stati delle sue parti. Quando un sistema quantistico è in uno stato *entangled*, le azioni eseguite su un sottosistema avranno un effetto collaterale su un altro sottosistema, anche se quest'ultimo non viene direttamente manipolato. Inoltre, a condizione che i sottosistemi siano separati in modo tale che nessuno dei due sia misurato, tale entanglement persisterà indipendentemente dalla distanza tra i sottosistemi. Questo porta a fenomeni altamente controintuitivi, che Einstein definì come "*Spooky action at a distance*", di cui parleremo più dettagliatamente quando descriveremo il teleporting.

Tutti gli algoritmi quantistici noti che mostrano un'accelerazione esponenziale rispetto ai loro equivalenti classici sfruttano tali effetti collaterali indotti dall'entanglement, in un modo o nell'altro. Inoltre, alcuni meccanismi, che sono impossibili secondo gli standard classici, come il teletrasporto di uno stato quantistico, dipendono in modo essenziale dall'entanglement. Pertanto, l'entanglement merita di essere definito un fenomeno quantistico "essenziale" che gioca un ruolo importante nel rendere il calcolo quantistico più potente rispetto a quello classico e nel consentire operazioni di informazione quantistica che sono impossibili nel contesto classico. Sebbene i qubit di una coppia entangled possano influenzarsi a vicenda istantaneamente, e quindi a velocità infinita, questa proprietà non può essere usata per comunicare più velocemente della luce. Inoltre, l'entanglement è monogamo, ovvero, se 2 qubit sono *maximally entangled*, non possono essere entangled con un terzo qubit.

7.2. Circuito per la generazione di Stati di Bell

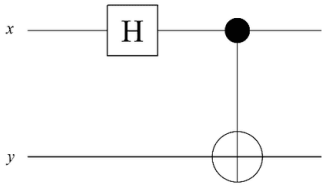
Le porte quantistiche a un qubit non sono in grado di creare stati entangled perché ogni qubit evolve indipendentemente dagli altri. Per creare entanglement dobbiamo usare porte che operano su più qubit alla volta. Per questo motivo è tanto importante il *CNOT-Gate* perché ci permette di ottenere 4 coppie entangled al massimo, conosciute come *Stati di Bell*, o *Coppie EPR*. Questi stati si ottengono dall'applicazione di un *H-Gate* al primo qubit e di un CNOT con target il secondo qubit:

$$\text{CNOT}|+\rangle|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$$

$$\text{CNOT}|-\rangle|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Phi^-\rangle$$

$$\text{CNOT}|+\rangle|1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\Psi^+\rangle$$

$$\text{CNOT}|-\rangle|1\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\Psi^-\rangle$$



Questi quattro stati formano una base ortonormale completa chiamata *Base di Bell*.

7.3. Parallelismo quantistico

Il parallelismo quantistico è una caratteristica fondamentale di molti algoritmi quantistici. Euristicamente, e con il rischio di semplificare eccessivamente, il parallelismo quantistico consente di valutare tutti i possibili valori della funzione $f(x)$ simultaneamente, anche se apparentemente abbiamo valutato f una sola

volta. Tuttavia, questo parallelismo non è immediatamente utile, infatti, il parallelismo quantistico produce in generale il seguente stato

$$\frac{1}{2^n}\sum_x |x\rangle|f(x)\rangle$$

a fronte di un input del tipo:

$$\frac{1}{2^n}\sum_x |x\rangle$$

dove n è il numero di qubits.

In questo caso, la misura dello stato $\sum_x |x\rangle|f(x)\rangle$ darebbe solo $f(x)$ per un singolo valore di x. Naturalmente, un computer classico può fare questo facilmente!

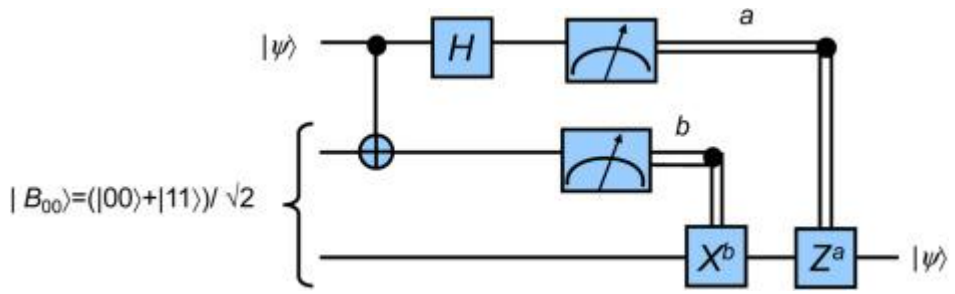
Fortunatamente, è possibile ottenere determinate proprietà congiunte di tutti gli output di $f(x)$. Infatti, quando gli algoritmi vengono descritti in termini di parallelismo quantistico, il cuore dell'algoritmo è il modo in cui l'algoritmo manipola lo stato generato dal parallelismo quantistico. Questo tipo di manipolazione non ha analoghi classici e richiede tecniche di programmazione non tradizionali. Elenchiamo di seguito un paio di tecniche generali:

- amplificare i valori di output di interesse: l'idea generale è di trasformare lo stato in modo tale che i valori di interesse abbiano un'ampiezza maggiore e quindi una probabilità più alta di essere misurati. L'algoritmo di Grover sfrutta questo approccio, così come molti algoritmi strettamente correlati;
- trovare le proprietà dell'insieme di tutti i valori di $f(x)$: questa idea è sfruttata nell'algoritmo di Shor, che utilizza una trasformazione di Fourier quantistica per ottenere il periodo di f. Gli algoritmi di Deutsch-Jozsa, Bernstein-Vazirani e Simon adottano tutti questo approccio.

8. Quantum Teleportation

È una tecnica per trasferire lo stato $|\Psi\rangle$ di un qubit da un sorgente (Alice) a una destinazione (Bob) facendo uso di uno stato entangled condiviso da Alice e Bob. Il teletrasporto è alla base del networking quantistico. Il sistema del quantum teleportation impiega tre qubits: un qubit è lo stato arbitrario che dovrà essere teleportato, mentre gli altri due, che si trovano (ad esempio) nello stato di Bell $|\Phi^+\rangle$, sono posseduti uno da Alice e l'altro da Bob.

Nello schema mostrato in figura, i risultati delle due misure effettuate da Alice, una sul qubit che deve essere teletrasportato e l'altra sul qubit entangled con quello in possesso di Bob, vengono trasmesse a Bob su una linea classica. Bob utilizza tali risultati per effettuare due operazioni di controllo sui gates X e Z.



Al termine di queste operazioni, lo stato del qubit che Alice ha teletrasportato a Bob si "materializza" nel qubit di Bob precedentemente entangled con quello di Alice.

Il teletrasporto quantistico non trasmette informazione, ma permette solo di trasferire uno stato generico da un mittente a un destinatario, senza che nessuno dei due conosca le ampiezze α e β. Inoltre non è istantaneo: per poter

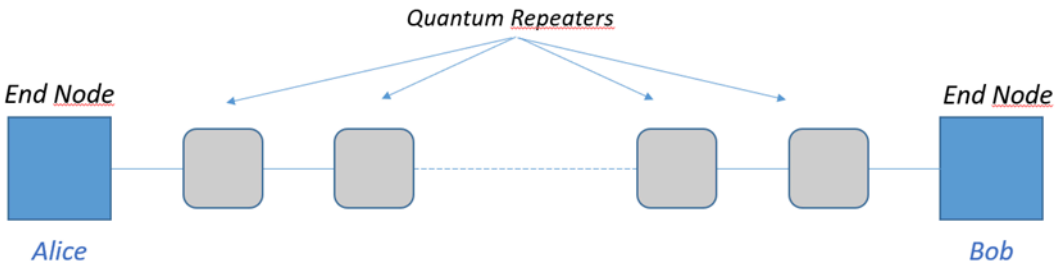
ricostruire lo stato iniziale, il destinatario deve conoscere il risultato della misura effettuata dal mittente, trasmesso su un canale "classico". Perciò il segnale non può viaggiare a velocità superiore alla velocità della luce. Inoltre, la misura fatta dal mittente sul qubit da teletrasportare porta al collasso del medesimo su uno stato diverso, perdendo quello iniziale. Quest'ultima considerazione è compatibile con il *no-cloning Theorem* nel senso che il qubit di Alice "evapora" per ripresentarsi sul qubit in possesso di Bob per cui alla fine esiste una sola copia di $|\Psi\rangle$.

8.1. Entanglement Swapping

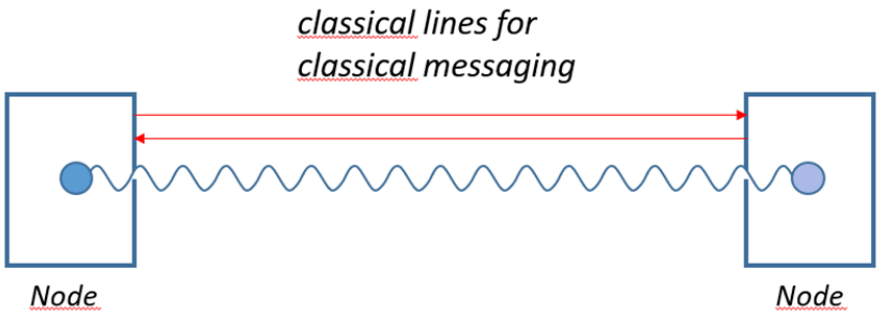
La luce si muove più lentamente attraverso la fibra ottica rispetto all'aria o al vuoto, tipicamente a circa 0.7c, dove c è la velocità della luce nel vuoto, ovvero 300.000 Km/sec. La latenza della fibra è di circa 5 μs per chilometro. Purtroppo, la trasmissione di fotoni è limitata dalle perdite nel canale, lo stesso problema che affligge la comunicazione classica. Per recuperare dalle perdite nella fibra, l'amplificazione classica del segnale fornisce una soluzione elegante per il mondo classico. Tuttavia, questo non è possibile nel mondo quantistico, poiché il *Teorema della non-clonazione* proibisce che i fotoni (qubits) vengano copiati o amplificati. Pertanto, un fattore chiave nella progettazione dei canali è il compromesso tra distanze più lunghe tra i nodi finali, che è desiderabile economicamente e logisticamente, e la maggiore perdita in un canale più lungo, che riduce drasticamente le prestazioni.

Poiché l'amplificazione del segnale è esclusa come mezzo per superare le perdite, è stato concepito un nuovo sviluppo tecnologico radicale – il ripetitore quantistico (*quantum repeater*) – per costruire l'Internet quantistico.

La tecnologia odierna è ancora lontana dall'avere un ripetitore quantistico completo, ma la ricerca sta avanzando rapidamente. I ripetitori quantistici permettono di creare uno stato massimamente entangled tra due nodi finali (spesso chiamati *Alice* e *Bob*) della rete, segmentando prima la fibra ottica in piccoli tronconi e posizionando un ripetitore quantistico tra due tronconi consecutivi. Alice e Bob sono intervallati da una serie di ripetitori posti a una distanza di alcune decine di chilometri l'uno dall'altro.



Per coordinare le loro operazioni quantistiche, è necessario che due nodi si scambino messaggi classici e questo può essere realizzato utilizzando linee classiche o connessioni di trasporto fornite dall'infrastruttura di Internet classica.

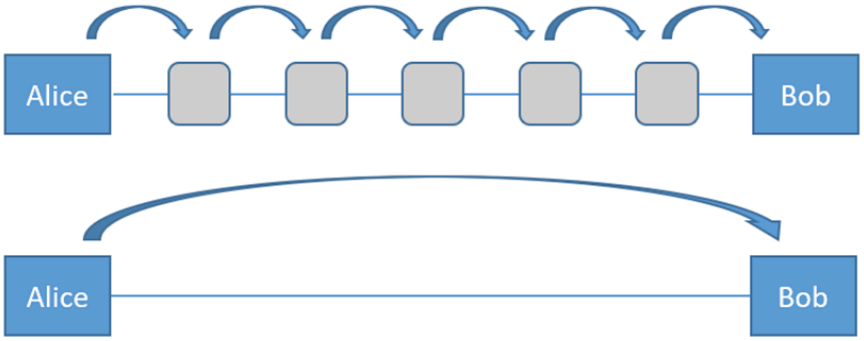


Per creare una coppia di qubit entangled a lunga distanza e ad alta fedeltà che possa essere utilizzata per effettuare comunicazione quantistica tramite il teletrasporto, un ripetitore quantistico deve eseguire diverse operazioni tra cui:

- *Entanglement Distribution*
- *Entanglement Swapping*

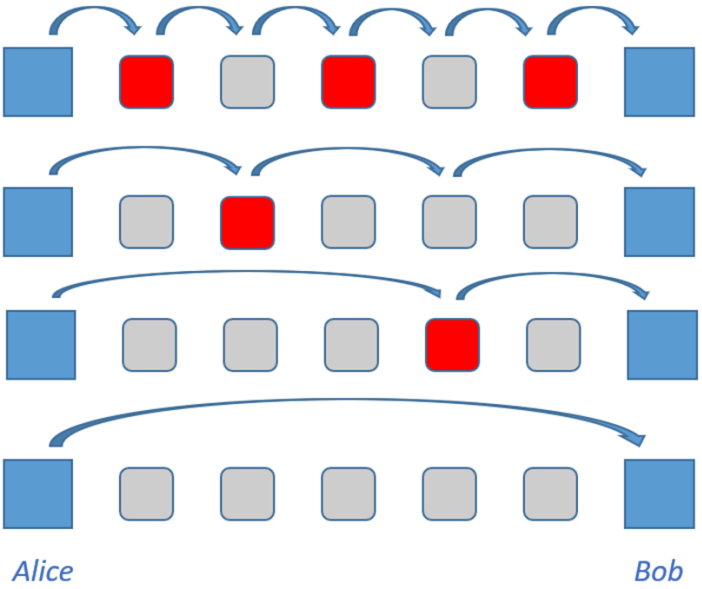
che descriveremo brevemente di seguito.

Entanglement Distribution: è il processo di creazione di coppie di qubit entangled a breve distanza (o collegamenti entangled) tra nodi adiacenti.

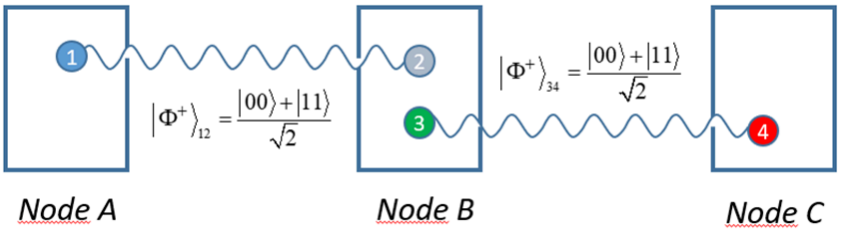


Ora l'entanglement è necessario solo tra nodi adiacenti e quindi la probabilità di successo per generare il collegamento entangled dipende dalla distanza dei nodi adiacenti, piuttosto che dalla distanza totale tra i nodi finali.

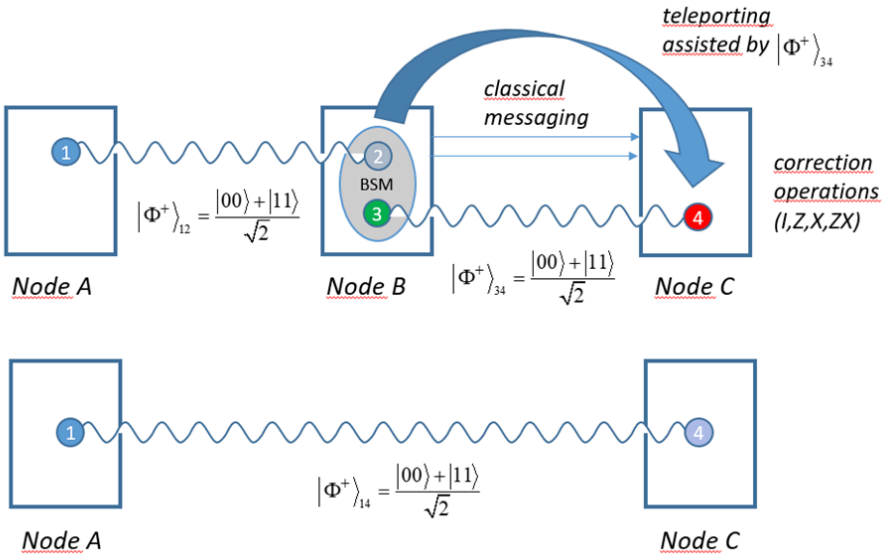
Entanglement Swapping: è il processo che permette di creare un collegamento entangled più lungo connettendo nodi adiacenti. I nodi rossi sono quelli che eseguono l'entanglement swapping.



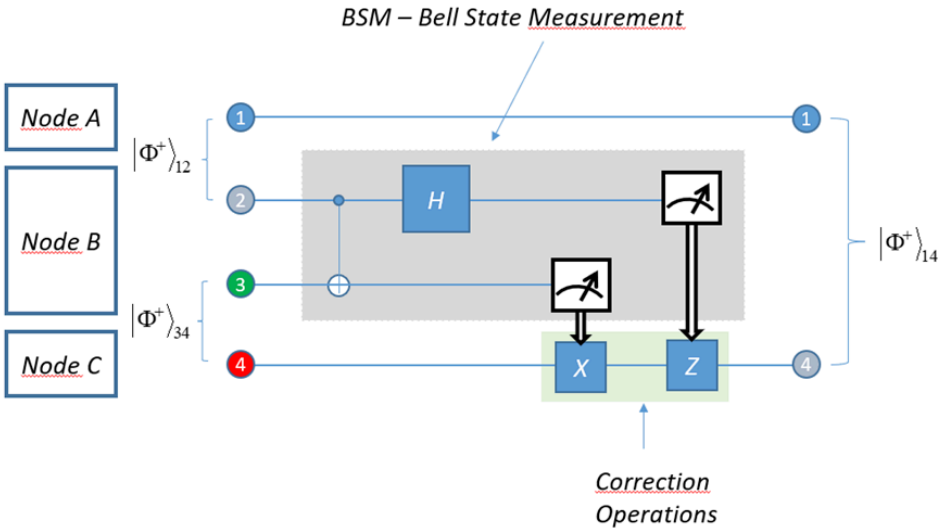
Di conseguenza, i ripetitori quantistici consentono di creare connessioni di entanglement a lunga distanza unendo insieme collegamenti di entanglement a breve distanza. L'entanglement swapping può essere considerato un'applicazione del teleporting.



I nodi A e B condividono una coppia di qubit massimamente entangled (qubit 1 e 2), e i nodi B e C condividono un'altra coppia di qubit massimamente entangled (qubit 3 e 4).



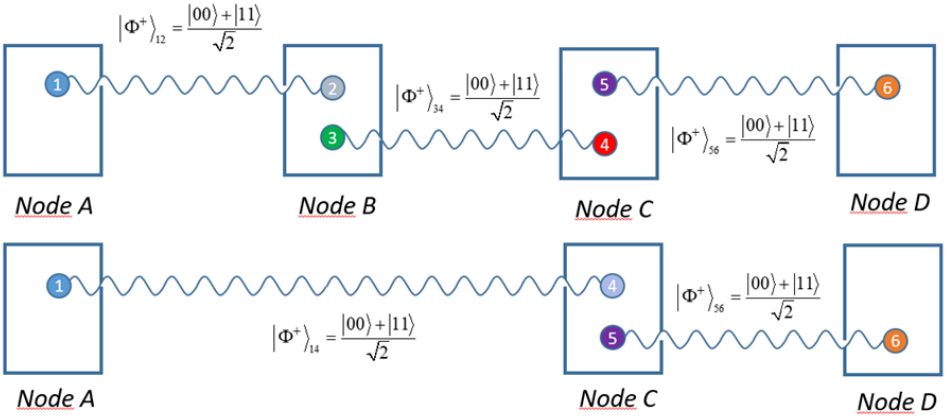
Il nodo B trasferisce (tramite teleporting) lo stato del qubit 2 al qubit 4 posseduto dal nodo C utilizzando la coppia di qubit entangled (qubit 3 e 4) tra i nodi B e C. Il qubit 1 al nodo A è ora entangled con il qubit 4 al nodo C, dando luogo ad un collegamento entanglement più lungo. Il circuito quantistico che consente l'entangled swapping è illustrato nella seguente figura:



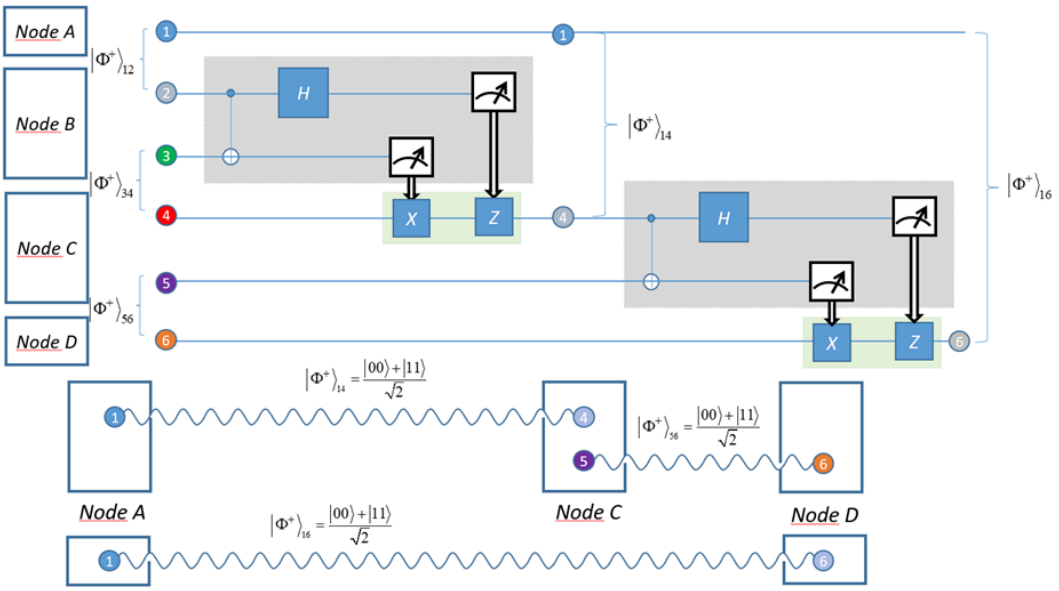
Aggiungiamo ora il nodo D che condivide con il nodo C una coppia di qubit massimamente entangled (qubit 5 e 6).

Ora la configurazione è la seguente:

- i nodi A e C condividono una coppia di qubit massimamente entangled (qubit 1 e 4);
- i nodi C e D condividono una coppia di qubit massimamente entangled (qubit 5 e 6).



Il processo di entanglement swapping può essere rappresentato dal seguente circuito quantistico:



Effettuando un certo numero di *entanglement swapping* in cascata o in parallelo si ottiene infine una connessione entangled tra Alice e Bob.

Questo processo è fondamentale per creare connessioni di entanglement a lunga distanza nel futuro quantum Internet.

8.2. Teorema di non-clonazione

Il *teorema della non-clonazione* quantistica afferma che non è possibile duplicare, clonare, a priori uno stato quantistico sconosciuto. Viceversa, è sempre possibile duplicare uno stato conosciuto a priori ed ogni stato ad esso ortogonale.
Supponiamo di avere un qubit in uno stato quantistico noto, ad esempio $|+\rangle$. Poiché conosciamo il suo stato, possiamo crearne ulteriori copie:

$$|+\rangle|0\rangle \rightarrow \mathrm{I} \otimes \mathrm{H} \rightarrow \ |+\rangle|+\rangle$$

Supponiamo, adesso, di avere uno stato quantistico sconosciuto:

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

e vorremmo farne una copia, in modo da ottenere $|\psi\rangle|\psi\rangle$. Se esistesse una porta quantistica U che permette di copiare un qualsiasi qubit sconosciuto dovrebbe soddisfare tale relazione:

$$\mathrm{U}|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$$

Espressa in algebra lineare:

$$\begin{pmatrix} U_{11} & U_{12} & U_{13} & U_{14} \\ U_{21} & U_{22} & U_{23} & U_{24} \\ U_{31} & U_{32} & U_{33} & U_{34} \\ U_{41} & U_{42} & U_{43} & U_{44} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\begin{pmatrix} U_{11} & U_{12} & U_{13} & U_{14} \\ U_{21} & U_{22} & U_{23} & U_{24} \\ U_{31} & U_{32} & U_{33} & U_{34} \\ U_{41} & U_{42} & U_{43} & U_{44} \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{pmatrix}$$

$$\begin{pmatrix} U_{11}\,\alpha + U_{13}\,\beta \\ U_{21}\,\alpha + U_{23}\,\beta \\ U_{31}\,\alpha + U_{33}\,\beta \\ U_{41}\,\alpha + U_{43}\,\beta \end{pmatrix} = \begin{pmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{pmatrix}$$

Possiamo avere varie soluzioni che richiedono tutte, però, la conoscenza di α e β, che non conosciamo.

Quindi, qualsiasi soluzione generale richiede la conoscenza di α e β, perciò non esiste alcun operatore U che ci permetta di copiare uno stato quantistico generale e sconosciuto.

9. Protocollo BB84

Un metodo quantistico per stabilire una chiave segreta condivisa. È stato introdotto da Charles H. Bennett e Gilles Brassard nel 1984 ed è il primo metodo di crittografia quantistica mai inventato.

- Alice sceglie una sequenza iniziale di 1 e 0 e per ognuno di essi sceglie casualmente la base, Z o X.
- Alice e Bob concordano la seguente strategia di codifica:
    - se il bit che Alice vuole inviare è uno 0:
        - se sceglie la base Z, allora invia a Bob $|0\rangle$.
        - se sceglie la base X, allora invia a Bob $|+\rangle$.
    - se invece il bit che Alice vuole inviare è uno 1:
        - se sceglie la base Z, allora invia a Bob $|1\rangle$.
        - se sceglie la base X, allora invia a Bob $|-\rangle$.
- Bob riceve i qubit e sceglie arbitrariamente la base in cui fare le misurazioni: se la base scelta è la stessa, allora Bob e Alice condivideranno lo stesso bit, altrimenti, il bit risultante concorda con il bit inviato solo metà delle volte. Adesso Alice e Bob utilizzeranno un canale di comunicazione pubblico per scambiarsi informazioni.
- Bob comunica ad Alice quali basi ha scelto per ciascuna misurazione ed eliminano tutti i bit corrispondenti alle basi diverse. A partire dai bit rimasti, Alice e Bob costruiscono la chiave segreta.
- Alice e Bob si scambiano e comparano una parte della chiave per stimare l'*errore percentuale*, che potrebbe esser stato causato da un eventuale intercettatore Eve. Se la percentuale è alta, i due interlocutori ricominciano il protocollo dall'inizio. Tale parte di chiave, essendo visibile sul canale classico, alla fine viene scartata.

Possiamo notare come gli stati delle basi utilizzate siano *non ortogonali* e ciò comporta che Eve non ha la possibilità di copiarli perfettamente o misurarsi senza alterarli (*no-cloning theorem*). Perciò risulterà impossibile rubare informazioni senza che gli utenti se ne accorgano.

La strategia di intercettazione più semplice è l'*Intercept and Resend*, in cui Eve intercetta e rileva i qubit inviati da Alice soltanto la metà delle volte.
Se indovina la base di codifica, Eve riesce a ottenere il corretto qubit senza alterarne lo stato e, in seguito, inviarlo a Bob, agendo del tutto inosservata. Altrimenti, se Eve sceglie una base diversa, lo stato da inviare a Bob risulterà alterato rispetto a quello inviato da Alice.
La probabilità che Eve scelga la base scorretta è di $\frac{1}{2}$ e se Bob misura con la stessa base scelta da Alice otterrà un risultato casuale e quindi il risultato sbagliato con una probabilità pari a $\frac{1}{2}$. Dunque la probabilità che un qubit intercettato generi un errore è pari a $\frac{1}{4}$.
Se Alice e Bob condividono n bit della chiave, la probabilità che Eve non venga rilevata per tutti gli n bits è $\left(\frac{3}{4}\right)^n$. La probabilità che Eve venga scoperta, per un numero di bit $n \to \infty$, è:

$$Pr = 1 - \left(\frac{3}{4}\right)^n \to 1$$

Per individuare Eve con una probabilità pari a 0.999999999, dovranno essere confrontati $n = 72$ bit della chiave, numero relativamente piccolo.

In conclusione Eve sarà sempre intercettabile e la sicurezza del protocollo viene garantita dalle leggi della fisica.

10. Conclusioni

Oggi, la comunità scientifica continua a fare ricerche sulla computazione quantistica e ad investigare le potenziali applicazioni quantistiche. Sebbene la meccanica quantistica possa prevedere la probabilità di una misurazione con incredibile precisione, molti ricercatori rimangono scettici sul fatto che fornisca una descrizione completa della realtà. L'idea è che i computer quantistici permettano di arrivare dove i computer tradizionali non riescono, realizzando la cosiddetta *supremazia quantistica*, concetto espresso dal fisico della Caltech, John Preskill: ottenere la supremazia quantistica vuol dire riuscire a risolvere, con un computer quantistico, un calcolo che un computer tradizionale non riuscirebbe a risolvere, quantomeno in un tempo ragionevole. Tuttavia, così come la tecnologia quantistica avanza nel tempo, lo stesso accade con la tecnologia classica. L'obiettivo finale non è allora la supremazia quantistica, ma bensì, il cosiddetto *vantaggio quantistico*, ossia l'effettiva capacità di un calcolatore quantistico di eseguire algoritmi in un tempo considerevolmente inferiore rispetto ai tempi impiegati dal più potente supercomputer. Come già accennato, la teoria è molto più avanti rispetto alla tecnologia, questo perché è ancora molto difficile ottenere una computazione quantistica senza errori per un tempo sufficientemente lungo: la più minuscola vibrazione o variazione della temperatura del sistema, o più in generale ogni interazione con l'ambiente esterno, causa il degrado dello stato dei qubit, vanificando qualsiasi risultato di calcolo. Al momento sono stati costruiti computer quantistici che mantengono lo stato di un migliaio di qubit per tempi dell'ordine di qualche centinaio di microsecondi: l'obiettivo della ricerca è quello di aumentare il più possibile questi tempi, in modo che i qubit possano svolgere calcoli più elaborati prima che il loro stato quantistico si perda definitivamente.

11. Bibliografia

[1] P. Benioff. *The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines*. Journal of Statistical Physics, 22(5):563–591, May 1980.

[2] Y. Manin. *Computable and Non-Computable* (in Russian). Sovetskoye Radio, Moscow, 1980.

[3] R. P. Feynman. *Simulating physics with computers*. International Journal of Theoretical Physics, 21(6):467–488, Jun 1982.

[4] D. Deutsch and R. Jozsa. *Rapid solution of problems by quantum computation*. Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, 439(1907):553–558, 1992.

[5] P. Shor. *Algorithms for quantum computation: discrete logarithms and factoring*. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pages 124–134. IEEE Computer Society, 1994.

[6] L. K. Grover. *Quantum mechanics helps in searching for a needle in a haystack*. Phys. Rev. Lett., 79:325– 328, Jul 1997. arXiv: quant-ph/9706033.

[7] Thomas G. Wong. *Introduction to Classical and Quantum Computing*. Page 143. January 5, 2022.