

UNIVERSITÀ DEGLI STUDI DI MILANO - BICOCCA

---

# **Teoria della Informazione e Computazione Quantistica**

---

Raccolta di appunti, dispense e libri

Anno accademico 2021/2022

**Marco Gobbo e Gabriele Morandi**

<https://github.com/marcogobbo/tecnologie-quantistiche>

9 gennaio 2022



# Indice

<b>1 Meccanica quantistica</b>	<b>5</b>
1.1 Stati e qubit . . . . .	5
1.1.1 Sfera di Bloch . . . . .	8
1.2 Osservabili . . . . .	9
1.3 Misurazioni . . . . .	11
1.4 Evoluzione temporale . . . . .	12
1.5 Gate . . . . .	13
1.6 Sistemi a più qubit . . . . .	15
1.7 Teorema di no-cloning . . . . .	19
<b>2 Entanglement</b>	<b>21</b>
2.1 Superdense coding . . . . .	23
2.2 Teleportation . . . . .	24
2.3 Disuguaglianze di Bell . . . . .	25
2.3.1 Disuguagliaza CHSH . . . . .	27
<b>3 Algoritmi quantistici</b>	<b>29</b>
3.1 Crittografia quantistica . . . . .	29
3.1.1 Esempio di crittografia classica . . . . .	29
3.1.2 Il protocollo BB84 . . . . .	30
3.1.3 Quantum nondemolition measurement . . . . .	32
3.2 Proprietà dei gate . . . . .	33
3.2.1 Gate classici: il Toffoli-gate . . . . .	33
3.2.2 Gate quantistici: reversibili e continui . . . . .	35
3.3 Quantum Parallelism . . . . .	37
3.4 Algoritmo di Deutsch . . . . .	39
3.5 Algoritmo di Deutsch-Jozsa . . . . .	42
3.6 Algoritmo di Bernstein-Vazirani . . . . .	44
3.7 Quantum Fourier Transform . . . . .	46
3.8 Algoritmo di Shor: period finding . . . . .	50
3.8.1 Violazione della crittografia RSA . . . . .	54
3.9 Algoritmo di Grover . . . . .	56
3.9.1 Interpretazione geometrica . . . . .	59
3.9.2 Interpretazione grafica: inversione rispetto alla media . . . . .	60
<b>4 Sistemi aperti</b>	<b>63</b>
4.1 Matrice densità . . . . .	63
4.2 Sottosistemi e traccia parziale . . . . .	68

4.3	Interazione con l'ambiente . . . . .	70
4.3.1	Amplitude damping . . . . .	77
4.3.2	Phase damping . . . . .	79
4.3.3	Combinazione di amplitude e phase damping . . . . .	83
<b>5</b>	<b>Quantum error correction</b>	<b>85</b>
5.1	Correzione classica degli errori . . . . .	85
5.2	Introduzione alla correzione quantistica degli errori . . . . .	86
5.3	Stabilizers . . . . .	88
5.4	Codice di correzione di Shor a 9 qubit . . . . .	93
5.5	Codice di correzione di Steane a 7 qubit . . . . .	97
5.6	Fault tolerance . . . . .	101
5.7	Toric code . . . . .	102
5.7.1	Correzione degli errori . . . . .	107
5.7.2	Interpretazione in meccanica statistica . . . . .	110
5.7.3	Topological quantum computing . . . . .	112
<b>6</b>	<b>Realizzazione fisica dei qubit</b>	<b>117</b>
6.1	Introduzione . . . . .	117
6.2	Oscillatore armonico quantistico . . . . .	119
6.3	Campo elettromagnetico quantizzato . . . . .	122
6.4	Accoppiamento qubit - campo e.m. classico . . . . .	126
6.5	Accoppiamento qubit - cavità QED . . . . .	134
6.5.1	Operazioni su 2 qubit . . . . .	142
6.6	Sistemi a trappola ionica . . . . .	143
6.6.1	Cirac-Zoller gate . . . . .	147
6.6.2	Mølmer-Sørensen gate . . . . .	149
6.7	Sistemi superconduttori . . . . .	151
6.7.1	Cenni di superconduttività . . . . .	151
6.7.2	cQED . . . . .	152
6.7.3	Interpretazione dell'effetto Josephson . . . . .	156
6.7.4	Transmon qubit . . . . .	159
<b>Bibliografia</b>		<b>172</b>

# Capitolo 1

## Meccanica quantistica

LEZIONE 1 - 04/10/2021

### 1.1 Stati e qubit

Il **bit** è il concetto fondamentale su cui si basa la teoria dell'informazione e computazione classica. Similmente, la teoria dell'informazione e computazione quantistica si basa sul concetto analogo di **quantum bit** o **qubit**. Che cos'è un qubit? Dal punto di vista della meccanica quantistica un qubit è un qualsiasi sistema a due stati (livelli). Ad esempio, lo si può creare utilizzando le due differenti polarizzazioni del fotone, utilizzando l'allineamento dello spin di un nucleo immerso in un campo magnetico uniforme oppure anche usando i due stati di un elettrone che orbita attorno ad un singolo atomo o molecola (si veda per esempio *ammonia-based quantum computer*<sup>i</sup>); in quest'ultimo caso solitamente si impiegano degli atomi i cui spettri presentano due livelli energetici molto vicini tra loro e al tempo stesso molto lontani da tutti gli altri livelli.

Così come il bit classico possiede uno **stato**, il quale è identificato da 0 o 1, anche un qubit è identificato da uno stato i cui livelli sono solitamente indicati con  $|0\rangle$  e  $|1\rangle$  (utilizzeremo durante tutto il corso la *notazione di Dirac*<sup>ii</sup>). L'idea è quella di considerare i qubit come portatori di informazioni esattamente come lo sono i bit nei computer classici. La differenza fondamentale tra bit e qubit è che gli stati quantistici possono esistere in configurazioni differenti dai singoli  $|0\rangle$  e  $|1\rangle$  poiché è possibile formare *combinazioni lineari* o *sovraposizioni* di stati:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \text{ dove } \alpha, \beta \in \mathbb{C}.$$

Vedremo più avanti che formalmente uno stato  $|\psi\rangle$  non è altro che un vettore di un opportuno spazio vettoriale: tale vettore può essere decomposto sugli elementi della base ortonormale  $\{|0\rangle, |1\rangle\}$ , chiamata anche **base computazionale**.

Per capire il significato di questa scrittura si ricordi che la QM (Quantum Mechanics) presenta una natura probabilistica e ci permette di estrarre solamente un'informazione ben precisa: quando si ha solamente lo stato  $|0\rangle$  (o  $|1\rangle$ ) si ha la certezza che il sistema si

<sup>i</sup>Ferguson, A., Cain, P., Williams, D., & Briggs, G. (2002). Ammonia-based quantum computer. *Phys. Rev. A*, 65, 034303.

<sup>ii</sup>Anche conosciuta come la notazione bra-ket, si tratta di un formalismo introdotto da Paul Dirac per indicare uno stato quantistico e tutte le operazioni ad esso collegate. Il nome deriva dal fatto che il prodotto scalare di uno stato  $|\psi\rangle$  (ket) con uno stato duale  $\langle\phi|$  (bra) viene indicato con una parentesi  $\langle\phi|\psi\rangle$  (bra-ket).

trovi in  $|0\rangle$  (o  $|1\rangle$ ) (la probabilità è 1), tuttavia quando si ha la sovrapposizione precedente, la frazione di volte che una misura dia come risultato  $|0\rangle$  o  $|1\rangle$  dipende direttamente dai coefficienti  $\alpha$  e  $\beta$ . In altre parole, un sistema che si trova in una sovrapposizione di stati ha una certa probabilità che la misura produca  $|0\rangle$  o  $|1\rangle$ . Dalle leggi della QM la suddetta probabilità è data da  $P(|0\rangle) = |\alpha|^2$  e  $P(|1\rangle) = |\beta|^2$ . La corretta normalizzazione di  $|\psi\rangle$  impone pertanto che

$$|\alpha|^2 + |\beta|^2 = 1.$$

Si noti che un'eventuale fase globale in  $|\psi\rangle$  è irrilevante perché scompare sempre in qualsiasi calcolo fisico (moduli quadri, valori di aspettazione, ecc.). Sono quindi due i numeri reali indipendenti che possono essere impiegati per la caratterizzazione univoca di un qubit: per tale ragione sembrerebbe che a differenza di un bit classico, un qubit possa memorizzare un'infinità di informazioni. Il problema è che tale conclusione non è del tutto vera per via del bizzarro comportamento della QM: l'unico modo di estrarre informazioni dagli stati è effettuare una **misura**, ma è impossibile estrarre da una singola misurazione sia  $\alpha$  che  $\beta$  a causa del collasso dello stato. Ad esempio, supponiamo che il sistema si trovi in  $\alpha|0\rangle + \beta|1\rangle$  e supponiamo che una misura sperimentale dia come risultato 0 (singolo bit di informazione): in seguito alla misura lo stato collassa in  $|0\rangle$  e d'ora in avanti qualsiasi misura effettuata su questo sistema produrrà sempre 0 con probabilità 1.

Per determinare univocamente  $\alpha$  e  $\beta$  si necessiterebbero un'infinità di esperimenti su un'infinità di stati tutti preparati nel medesimo qubit, ma, come vedremo, ciò non è auspicabile a causa delle leggi della QM. Nonostante ciò, questo non significa che non sia possibile impiegare i qubit per estrarre e contenere informazioni nei computer, perché questo strano comportamento fa sì che solamente particolari operazioni siano predittive: uno degli scopi del corso è proprio quello di cercare di studiare e comprendere come si possono ricavare informazioni, quali informazioni possono essere estratte e in che modo lo si può fare.

Per comprendere al meglio i concetti che introdurremo cominciamo con un riassunto dei principi generali della QM:

- **I Postulato (Stato):** Che cos'è uno stato? Utilizziamo la notazione di Dirac per rappresentare un vettore  $|\psi\rangle$  di uno spazio di Hilbert  $\mathcal{H}$  (molto spesso uno spazio vettoriale finito dimensionale) e diremo che  $|\psi\rangle \in \mathcal{H}$ . Uno stato è un **raggio** tale che  $\|\psi\| = 1$  (per la conservazione della probabilità) e  $|\psi\rangle \cong e^{i\alpha} |\psi\rangle$ <sup>iii</sup> con  $\alpha \in \mathbb{R}$ . Dato che la fase globale è irrilevante, quando due stati differiscono per una fase hanno il medesimo effetto fisico.

Consideriamo due stati  $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$ : la loro combinazione lineare  $|\psi\rangle \equiv \alpha_1 |\psi_1\rangle + \alpha_2 |\psi_2\rangle \in \mathcal{H}$ . Per mantenere la conservazione della probabilità, si può sempre normalizzare lo stato:  $|\psi\rangle \rightarrow \frac{|\psi\rangle}{\|\psi\|}$ .

**Definizione 1.1 (Prodotto scalare).** Sia  $|\psi\rangle$  uno stato ("vettore", "ket") e  $\langle\phi|$  uno stato duale ("vettore duale", "bra"). Definiamo **prodotto scalare** la seguente azione del bra sul ket:

$$\langle\phi| : |\psi\rangle \longrightarrow \langle\phi|\psi\rangle \in \mathbb{C}.$$

---

<sup>iii</sup>La notazione  $\cong$  significa "equivalente a".

Nel caso dei qubit consideriamo  $\mathcal{H} = \mathbb{C}^2$ , quindi un generico vettore viene indicato con  $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$  dove  $z_1, z_2 \in \mathbb{C}$ . Come detto in precedenza, possiamo considerare la base ortonormale

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}; \quad (1.1.1)$$

in questo modo il generico vettore di  $\mathbb{C}^2$  può essere scritto come combinazione lineare dei vettori di base:

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = z_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + z_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = z_1 |0\rangle + z_2 |1\rangle.$$

Usando questa notazione vettoriale possiamo anche riscrivere il prodotto scalare di due stati generici:

$$|\phi\rangle = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}, \quad |\psi\rangle = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}, \quad \Rightarrow \quad \langle\psi|\phi\rangle = w_1^* z_1 + w_2^* z_2;$$

chiaramente i vettori di base sono ortonormali:  $\langle 0|0\rangle = \langle 1|1\rangle = 1$  e  $\langle 0|1\rangle = \langle 1|0\rangle = 0$ . Dato un ket (vettore) come costruiamo il bra (vettore duale)? Prendendo l'aggiunto, ossia il trasposto complesso coniugato:

$$|\phi\rangle = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}, \quad \Rightarrow \quad \langle\phi| \equiv |\phi\rangle^\dagger = (z_1^* \ z_2^*) = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}^\dagger = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}^{t,*};$$

in questo modo il prodotto scalare è direttamente il prodotto matriciale riga  $\times$  colonna:

$$\langle\psi|\phi\rangle = (w_1^* \ w_2^*) \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = w_1^* z_1 + w_2^* z_2.$$

Riassumendo, come possiamo scrivere un generico qubit? Possiamo pensarlo come un vettore di  $\mathbb{C}^2$  decomposto sulla base computazionale

$$|\psi\rangle = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = z_1 |0\rangle + z_2 |1\rangle,$$

che soddisfa i seguenti due vincoli:

- **Conservazione della probabilità:**  $|z_1|^2 + |z_2|^2 = 1$ ;
- **Invarianza di fase:**  $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \cong e^{i\alpha} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \Rightarrow \frac{z_1}{z_2} \cong e^{i\alpha} \frac{z_1}{z_2}$ .

Per implementare il primo vincolo possiamo facilmente scrivere

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) e^{i\phi_1} |0\rangle + \sin\left(\frac{\theta}{2}\right) e^{i\phi_2} |1\rangle;$$

mentre per implementare l'invarianza di fase dobbiamo ricordarci che  $\phi_1$  e  $\phi_2$  sono fasi arbitrarie perciò abbiamo un grado di libertà e possiamo moltiplicare lo stato precedente per  $e^{i\alpha}$ :

$$e^{i\alpha} |\psi\rangle \cong |\psi\rangle = \left[ \cos\left(\frac{\theta}{2}\right) e^{i\phi_1} |0\rangle + \sin\left(\frac{\theta}{2}\right) e^{i\phi_2} |1\rangle \right] e^{i\alpha};$$

la scelta standard è quella di porre  $\alpha = -\phi_1$  in maniera tale che

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle, \quad (1.1.2)$$

con  $\phi = \phi_2 - \phi_1$ . La relazione in (1.1.2) rappresenta la parametrizzazione standard di un generico qubit mediante due numeri reali  $\theta$  e  $\phi$ . Si noti che come sottolineato in precedenza la fase globale scompare in qualsiasi conto fisico, tuttavia  $e^{i\phi}$  è fondamentale perché dà luogo a fenomeni di interferenza.

### 1.1.1 Sfera di Bloch

È possibile visualizzare lo stato generico di un qubit mediante un espediente grafico: si introduce il seguente versore unitario in 3 dimensioni  $\vec{n} = (\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta)$  e si disegna la sfera  $S^2 \in \mathbb{R}^3$ ; in questo modo il generico qubit in (1.1.2) può essere disegnato identificando il punto sulla sfera individuato dagli angoli  $\theta$  e  $\phi$ . Tale sfera prende il nome di **Sfera di Bloch**: esiste una corrispondenza biunivoca fra tutti i possibili qubit scrivibili mediante la (1.1.2) e i punti sulla superficie della sfera di Bloch.

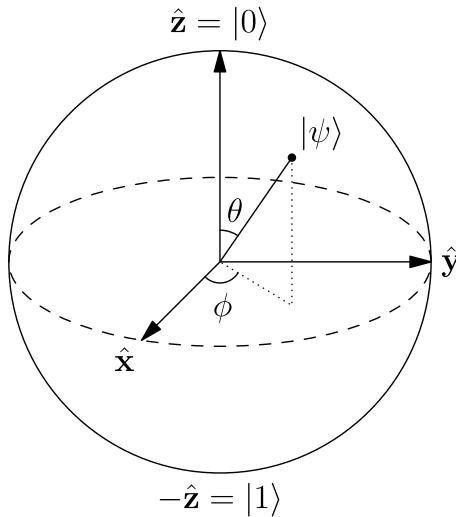


Figura 1.1: Rappresentazione generale di un qubit  $|\psi\rangle$  sulla sfera di Bloch. Si noti dalla relazione in (1.1.2) che per  $\theta = 0$  si ha  $|\psi\rangle = |0\rangle$  (polo nord) e invece per  $\theta = \pi$  risulta  $|\psi\rangle = |1\rangle$  (polo sud).

È fondamentale evidenziare che la rappresentazione dei qubit tramite sfera di Bloch è solo un espediente grafico poiché il prodotto scalare tra qubit è diverso dal classico prodotto scalare di  $\mathbb{R}^3$ . In  $\mathbb{C}^2$  gli stati  $|0\rangle$  e  $|1\rangle$  sono ovviamente ortogonali, mentre, come evidente dalla figura, su  $S^2$  si ha  $\langle 0|1 \rangle = -1$ . Questo fatto è dovuto ad una sorta di doppio conteggio in (1.1.2) per la presenza di  $\theta/2$ .

LEZIONE 2 - 08/10/2021

## 1.2 Osservabili

- **II Postulato (Osservabili):** Che cosa si può misurare in QM? Vengono misurate le **osservabili**, ossia **operatori autoaggiunti** (o **hermitiani**)  $\hat{A}$  tali che

$$\hat{A} : \mathcal{H} \rightarrow \mathcal{H} \text{ con } \hat{A}^\dagger = \hat{A},$$

dove più precisamente  $\hat{A}^\dagger \equiv (\hat{A}^t)^*$ . Dal punto di vista degli elementi di matrice, calcolare l'aggiunto di  $A_{ij}$  significa  $A_{ij}^\dagger = A_{ji}^*$ . Dunque le matrici autoaggiunte (hermitiane) sono tali che  $A^\dagger \equiv (A^t)^* = A$ .

In base a ciò che abbiamo visto sulla notazione braket ( $\langle \phi | = |\phi \rangle^\dagger$ ) abbiamo necessariamente che

$$|\psi\rangle = B|\phi\rangle, \Rightarrow \langle\psi| = \langle\phi|B^\dagger.$$

Focalizzando la nostra attenzione sugli operatori autoaggiunti, richiamiamo un importante teorema di algebra lineare:

**Teorema 1.1 (Teorema Spettrale).** *Sia  $\hat{A}$  un operatore autoaggiunto su uno spazio di Hilbert  $\mathcal{H}$ . Allora esiste una base ortonormale di  $\mathcal{H}$  composta da autovettori di  $\hat{A}$ , ossia  $\exists \{|n\rangle\} \in \mathcal{H}$  tale che  $\hat{A}|n\rangle = a_n|n\rangle$  dove gli autovalori  $a_n \in \mathbb{R}$ .*

Si noti dal teorema che  $\langle n|m \rangle = \delta_{nm}$  dove  $n, m = 1, \dots, N$  con  $N \equiv \dim \mathcal{H}$ . Trattandosi di una base, qualsiasi vettore dello spazio di Hilbert può essere scritto come combinazione lineare di tali vettori:

$$|\psi\rangle = \sum_{n=1}^N \alpha_n |n\rangle, \text{ dove } \alpha_n \equiv \langle n|\psi \rangle \in \mathbb{C}.$$

Ritornando al nostro caso del sistema a due livelli, lo spazio di Hilbert in esame è  $\mathbb{C}^2$ , dove consideriamo la **base canonica** (o **base computazionale**) data dagli stati  $|0\rangle$  e  $|1\rangle$  (si vedano le definizioni in (1.1.1)). In questo spazio vettoriale gli operatori sono rappresentati da matrici  $2 \times 2$ . La più generale matrice  $2 \times 2$  hermitiana contenente 4 parametri reali è

$$A = \begin{pmatrix} a+b & c-id \\ c+id & a-b \end{pmatrix},$$

dove  $a, b, c, d \in \mathbb{R}$ . Si noti che sulla diagonale le entrate sono puramente reali. Così come abbiamo decomposto uno stato generico  $|\psi\rangle$  mediante combinazione lineare di autovettori  $|n\rangle$ , possiamo decomporre il generico operatore hermitiano di  $\mathbb{C}^2$  come

$$A = a\mathbb{I} + c\sigma_1 + d\sigma_2 + b\sigma_3, \tag{1.2.1}$$

dove  $\mathbb{I}$  è la matrice **identità** e  $\sigma_1, \sigma_2, \sigma_3$  sono le **matrici Pauli**:

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.2.2}$$

Matrice di Pauli	Autovettori	Autovalori
$\sigma_1$	$ +\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad  -\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$	$\{1, -1\}$
$\sigma_2$	$ i\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \quad  -i\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$	$\{1, -1\}$
$\sigma_3$	$ 0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad  1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\{1, -1\}$

Tabella 1.1: Autovettori e autovalori delle matrici di Pauli.

Si ricordi che le matrici di Pauli sono i generatori del momento angolare in QM e sono infatti utilizzate per descrivere l'operatore di spin  $\hat{\vec{S}} = \frac{\hbar}{2}\hat{\vec{\sigma}}$ . I relativi autovalori e autovettori sono mostrati nella Tabella 1.1.

Dato che in futuro ci tornerà utile, osserviamo che gli autovettori di  $\sigma_1$  e  $\sigma_2$  possono essere espressi mediante base computazionale come

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \quad |i\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \quad |-i\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}, \quad (1.2.3)$$

Utilizzando la rappresentazione dei qubit tramite sfera di Bloch, questi autovettori sono mostrati in Figura 1.2.

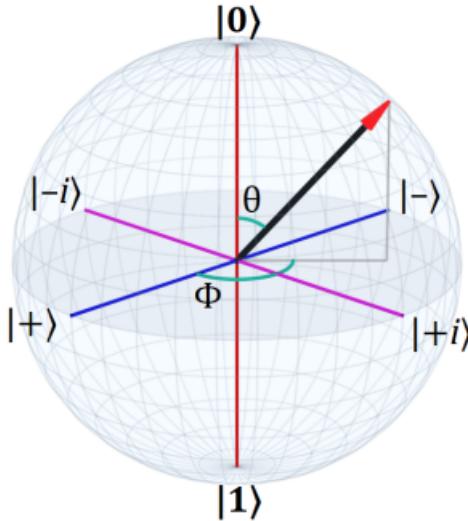


Figura 1.2: Rappresentazione degli autovettori delle matrici di Pauli sulla sfera di Bloch. Il punto indicato dalla freccia rossa indica un generico qubit.

Come detto in precedenza, le 3 matrici di Pauli parametrizzano lo spin e i 3 assi della sfera di Bloch possono essere associati allo spin. Considerando lo stato generico  $|\psi\rangle$  della (1.1.2), possiamo definire lo spin lungo una direzione generica  $\vec{\sigma} \cdot \vec{n}$  dove  $\vec{n} = (\cos \phi \sin \theta, \sin \phi \sin \theta, \cos \theta)$ :

$$\vec{\sigma} \cdot \vec{n} = \cos \phi \sin \theta \sigma_1 + \sin \phi \sin \theta \sigma_2 + \cos \theta \sigma_3;$$

così facendo è un semplice esercizio di QM dimostrare che  $|\psi\rangle$  è autostato di  $\vec{\sigma} \cdot \vec{n}$  con autovalore 1, ossia  $\vec{\sigma} \cdot \vec{n} |\psi\rangle = |\psi\rangle$ . Questo significa che dato uno stato sulla sfera di

Bloch, allora esso è anche autostato di spin nella direzione individuata da tale qubit: infatti l'idea fisica alla base della sfera di Bloch è che la direzione arbitraria scelta non è altro che la direzione della quantizzazione dello spin.

## 1.3 Misurazioni

- **III Postulato (Regola di Born):**

1. **Misurazione:** sia  $\hat{A}$  un osservabile con autostati  $|n\rangle$ , ossia  $\hat{A}|n\rangle = a_n|n\rangle$ . Prendiamo per semplicità  $a_n \neq a_m \forall n \neq m$  (osservabile con autovalori distinti). Consideriamo uno stato generico espanso sugli autostati precedenti:  $|\psi\rangle = \sum_n \alpha_n |n\rangle$ . Allora una misura dell'osservabile  $\hat{A}$  produce il valore  $a_n$  con probabilità data da  $|\alpha_n|^2$  (assumendo lo stato correttamente normalizzato).
2. **Collasso dello stato:** cosa succede allo stato del sistema dopo la misurazione? Instantaneamente lo stato  $|\psi\rangle$  collassa sull'autostato associato all'autovalore risultante dalla misura. Ad esempio se misurando otteniamo  $a_n$  allora  $|\psi\rangle \rightarrow |n\rangle$ . Effettuando delle misure successive sullo stato si ottiene sempre  $|n\rangle$  con probabilità esattamente uguale a 1.

**Esempio 1.1.** Consideriamo per esempio il generico qubit in (1.1.2) e immaginiamo di voler effettuare delle misurazioni in differenti basi. Supponiamo di voler misurare lo spin lungo  $z$  (base  $\{|0\rangle, |1\rangle\}$  di  $\sigma_3$ ) e lungo  $x$  (base  $\{|+\rangle, |-\rangle\}$  di  $\sigma_1$ ). Essendo il qubit già decomposto sulla base computazionale, una misurazione lungo  $z$  produrrà

$$P(|0\rangle) = \left| \cos\left(\frac{\theta}{2}\right) \right|^2, \quad P(|1\rangle) = \left| \sin\left(\frac{\theta}{2}\right) \right|^2.$$

Per capire il risultato della misurazione lungo  $x$ , invece, dobbiamo espandere  $|\psi\rangle$  sulla base  $\{|+\rangle, |-\rangle\}$ : usando le (1.2.3) per esprimere  $\{|0\rangle, |1\rangle\}$  in termini di  $\{|+\rangle, |-\rangle\}$  ricaviamo

$$P(|+\rangle) = \frac{1}{2} \left| \cos\left(\frac{\theta}{2}\right) + e^{i\phi} \sin\left(\frac{\theta}{2}\right) \right|^2, \quad P(|-\rangle) = \frac{1}{2} \left| \cos\left(\frac{\theta}{2}\right) - e^{i\phi} \sin\left(\frac{\theta}{2}\right) \right|^2.$$

Si noti come in entrambe le situazioni la probabilità risulta correttamente normalizzata:  $P(|0\rangle) + P(|1\rangle) = P(|+\rangle) + P(|-\rangle) = 1$ .

**Esempio 1.2.** Consideriamo lo stato  $|+\rangle$  delle (1.2.3). Qual è l'interpretazione fisica di tale stato? Supponiamo che rappresenti lo spin di una particella: quando lo spin si trova in  $|+\rangle$  allora sappiamo con certezza che punta lungo la direzione  $x$ , ossia  $P(|+\rangle) = 1$ . Al contrario, per una misurazione lungo  $z$  sappiamo che  $P(|0\rangle) = 1/2$  e  $P(|1\rangle) = 1/2$ : abbiamo la certezza del risultato lungo l'asse  $x$ , ma lungo l'asse  $z$  si ha totale incertezza. Questo fenomeno è dovuto alla non commutatività degli operatori di spin nelle 3 direzioni:

$$[\hat{S}_i, \hat{S}_j] = i\hbar\varepsilon_{ijk}\hat{S}_k.$$

Se consideriamo infatti il sistema preparato in  $|+\rangle$  e supponiamo di effettuare una misura lungo  $z$  ottenendo  $|0\rangle$  allora lo stato collasserà in  $|0\rangle$  e, d'ora in avanti, qualsiasi misurazione lungo  $z$  produrrà sempre  $|0\rangle$  con  $P(|0\rangle) = 1$ . Nonostante ciò, il fatto che  $\hat{S}_z$  non commuti con  $\hat{S}_x$  fa sì che una misura successiva lungo  $x$  "rigeneri" dell'incertezza:  $P(|+\rangle) = 1/2$  e  $P(|-\rangle) = 1/2$  (si veda  $|0\rangle$  espresso in termini di  $\{|+\rangle, |-\rangle\}$  dalle (1.2.3)).

Discutiamo la generalizzazione del III postulato nel caso in cui alcuni autovalori associati ad autostati differenti siano uguali, cioè siamo in presenza di **degenerazione**. Per esempio supponiamo il caso  $N = \dim \mathcal{H} = 6$ :

$$|\psi\rangle = \alpha_1 |1\rangle + \alpha_2 |2\rangle + \alpha_3 |3\rangle + \alpha_4 |4\rangle + \alpha_5 |5\rangle + \alpha_6 |6\rangle ,$$

dove supponiamo la degenerazione su  $a_1 = a_2$  e  $a_4 = a_5 = a_6$ . Introduciamo gli operatori  $\hat{P}_{a_i}$  che considerano solamente la parte di  $|\psi\rangle$  corrispondente all'autospazio associato ad  $a_i$ :

$$|\psi\rangle = \underbrace{\alpha_1 |1\rangle + \alpha_2 |2\rangle}_{\hat{P}_{a_1} |\psi\rangle} + \underbrace{\alpha_3 |3\rangle}_{\hat{P}_{a_3} |\psi\rangle} + \underbrace{\alpha_4 |4\rangle + \alpha_5 |5\rangle + \alpha_6 |6\rangle}_{\hat{P}_{a_4} |\psi\rangle} ;$$

tali operatori prendono il nome di **proiettori** e soddisfano le proprietà seguenti:

$$1. \hat{P}_{a_i}^\dagger = \hat{P}_{a_i};$$

$$2. \hat{P}_{a_i}^2 = \hat{P}_{a_i};$$

$$3. \sum_i \hat{P}_{a_i} = \mathbb{I}.$$

I proiettori sono utili per scrivere la **regola di Born** (III postulato) nel caso generale: dato uno stato  $|\psi\rangle$  con degenerazione sugli autovalori  $a_i$ , la probabilità di ottenere il risultato  $a_n$  è

$$P(a_n) = \left\| \hat{P}_{a_n} |\psi\rangle \right\|^2;$$

dopo la misura, la funzione d'onda collassa nel seguente stato normalizzato:

$$|\psi\rangle \rightarrow \frac{\hat{P}_{a_n} |\psi\rangle}{\left\| \hat{P}_{a_n} |\psi\rangle \right\|} .$$

Ad esempio, nel caso dello stato sopra scritto, la probabilità di ottenere  $a_1 = a_2$  non è altro che

$$P(a_1) = \left\| \hat{P}_{a_1} |\psi\rangle \right\|^2 = \|\alpha_1 |1\rangle + \alpha_2 |2\rangle\|^2 = |\alpha_1|^2 + |\alpha_2|^2 ,$$

e lo stato collassa in

$$|\psi\rangle \rightarrow \frac{\alpha_1 |1\rangle + \alpha_2 |2\rangle}{\sqrt{|\alpha_1|^2 + |\alpha_2|^2}} ;$$

si noti che si ha ancora incertezza su in quale stato si trovi  $|\psi\rangle$ , ma con un esperimento successivo **diverso** siamo in grado di risolvere la degenerazione e ottenere  $|1\rangle$  o  $|2\rangle$ .

## 1.4 Evoluzione temporale

Il postulato successivo riguarda l'evoluzione temporale degli stati:

- **IV Postulato (Evoluzione temporale):** L’evoluzione temporale di uno stato generico  $|\psi(0)\rangle$  è descritta dall’equazione di Schrödinger:

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle ,$$

dove  $\hat{H}$  è l’operatore (hermitiano) **hamiltoniana** del sistema. L’equazione di Schrödinger conserva le probabilità:  $\langle\psi(t)|\psi(t)\rangle = \langle\psi(0)|\psi(0)\rangle = 1$ .

Solitamente si risolve questa equazione introducendo l’**operatore di evoluzione temporale**  $\hat{U}(t)$ :

$$|\psi(t)\rangle = \hat{U}(t) |\psi(0)\rangle ;$$

quando l’hamiltoniana è indipendente dal tempo,  $\hat{U}(t)$  diventa semplicemente

$$\hat{U}(t) = e^{-\frac{i}{\hbar} \hat{H} t} ;$$

se invece  $\hat{H} = \hat{H}(t)$ , è necessario distinguere i casi di hamiltoniane commutanti o non commutanti a tempi differenti.

Come detto sopra, l’evoluzione temporale preserva le probabilità e ciò è una diretta conseguenza del fatto che  $\hat{U}(t)$  sia **unitario**:

- $\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \mathbb{I} \Rightarrow \hat{U}^\dagger = \hat{U}^{-1}$ .
- Il prodotto scalare è conservato:  $\langle \hat{U}\phi | \hat{U}\psi \rangle = \langle \phi | \hat{U}^\dagger \hat{U}\psi \rangle = \langle \phi | \psi \rangle$ .

Notiamo che  $\hat{U}(t)$  per hamiltoniane indipendenti da  $t$  è effettivamente unitario:

$$\hat{U}^\dagger \hat{U} = \left( e^{-\frac{i}{\hbar} \hat{H} t} \right)^\dagger e^{-\frac{i}{\hbar} \hat{H} t} = e^{\frac{i}{\hbar} \hat{H} t} e^{-\frac{i}{\hbar} \hat{H} t} = \mathbb{I} .$$

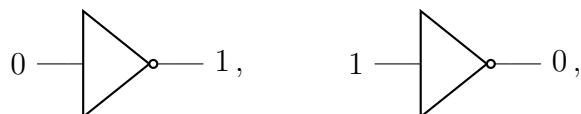
## 1.5 Gate

**Definizione 1.2 (Porte quantistiche).** *L’analogo quantistico delle porte (o gate) logiche classiche sono le **porte quantistiche** (o **gate quantistici**). Un gate quantistico è un operatore unitario che cambia lo stato del sistema.*

Notiamo che una delle principali differenze che rendono di difficile implementazione le porte quantistiche risiede nel fatto che non possiamo implementare direttamente le più semplici operazioni classiche come AND, OR o XOR.

**Definizione 1.3 (Circuito Quantistico).** *Un **circuito quantistico** è un modello di computazione quantistica in cui una sequenza ordinata di gate quantistici è applicata ai qubit.*

In un circuito classico l’uso dei gate logici è banale. Supponiamo di considerare un bit che si trova in 0 o 1: un gate costituisce l’implementazione di un agente esterno che cambia lo stato del bit. Si pensi ad esempio al gate NOT per il quale  $a \rightarrow \text{NOT } a$ :



Nel caso invece di un qubit, i circuiti funzionano diversamente perché le porte agiscono su sistemi a due livelli. Immaginiamo che a causa di un agente esterno il qubit  $|\psi\rangle$  subisca un'evoluzione temporale  $\hat{U}$ : rappresentiamo questo fatto mediante il circuito seguente

$$|\psi\rangle \xrightarrow{\quad} \boxed{\hat{U}} \xrightarrow{\quad} \hat{U} |\psi\rangle ,$$

Si ricordi che  $\hat{U}$  è sempre un operatore unitario: ad esempio per un'hamiltoniana indipendente dal tempo si ha semplicemente  $\hat{U}(t) = e^{-\frac{i}{\hbar}\hat{H}t}$ .

Consideriamo le matrici di Pauli: sappiamo che sono hermitiane ( $\sigma_i^\dagger = \sigma_i$ ) e che soddisfano la proprietà  $\sigma_i^2 = \mathbb{I}$ , ma questo significa che sono anche matrici unitarie. Questo fatto ci permette di costruire<sup>iv</sup> dei gate in cui  $\hat{U} = \hat{\sigma}_i$ . Ad esempio è possibile implementare dei gate come  $\mathbb{I}$ ,  $\sigma_1 \equiv X$ ,  $\sigma_2 \equiv Y$  e  $\sigma_3 \equiv Z$ . Ricordando che  $\sigma_i \sigma_j = 2i\varepsilon_{ijk}\sigma_k$ , notiamo che  $XZ = -iY$  e inoltre anche la matrice  $-iY$  è unitaria. Per tale ragione molto spesso, al posto di considerare i gate  $\{\mathbb{I}, X, Y, Z\}$  si sceglie la base  $\{\mathbb{I}, X, Z, XZ\}$ : questo significa che possiamo implementare i gate seguenti

$$\xrightarrow{\quad} \boxed{X} \xrightarrow{\quad} , \quad \xrightarrow{\quad} \boxed{Z} \xrightarrow{\quad} , \quad \xrightarrow{\quad} \boxed{XZ} \xrightarrow{\quad} ,$$

Consideriamo l'**X-gate**: dalle (1.2.2) è evidente che  $X$  rappresenta una sorta di "quantum" NOT perché inverte semplicemente lo stato della base computazionale:

$$\begin{aligned} |0\rangle &\xrightarrow{\quad} \boxed{X} \xrightarrow{\quad} |1\rangle , \\ |1\rangle &\xrightarrow{\quad} \boxed{X} \xrightarrow{\quad} |0\rangle , \end{aligned}$$

Consideriamo ora lo **Z-gate**: gli stati della base computazionale sono autovettori con autovalori 0 e 1 di  $\sigma_3$ , quindi questo gate inverte semplicemente il segno

$$\begin{aligned} |0\rangle &\xrightarrow{\quad} \boxed{Z} \xrightarrow{\quad} |0\rangle , \\ |1\rangle &\xrightarrow{\quad} \boxed{Z} \xrightarrow{\quad} -|1\rangle , \end{aligned}$$

L'azione dello **Z-gate** su un generico qubit risulterà quindi in

$$a|0\rangle + b|1\rangle \xrightarrow{\quad} \boxed{Z} \xrightarrow{\quad} a|0\rangle - b|1\rangle ,$$

e questo significa che  $Z$  aggiunge semplicemente una fase  $e^{i\pi} = -1$  allo stato. Ricapitolando: l'**X-gate** implementa un'interferenza dall'esterno che inverte lo stato (ad esempio cambia segno dello spin lungo  $z$ ) e lo **Z-gate** implementa l'introduzione di una fase.

Una matrice particolarmente importante per i nostri scopi è

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} , \quad (1.5.1)$$

chiamata **matrice di Hadamard**. Notiamo che è unitaria in quanto  $H^\dagger H = \mathbb{I}$ . Essa può essere implementata nel cosiddetto **H-gate** o **gate di Hadamard**: si tratta di un gate particolarmente importante (lo useremo largamente durante tutto il corso) in quanto permette di cambiare base  $\{|0\rangle, |1\rangle\} \leftrightarrow \{|+\rangle, |-\rangle\}$

$$\begin{aligned} |0\rangle &\xrightarrow{\quad} \boxed{H} \xrightarrow{\quad} |+\rangle , & |+\rangle &\xrightarrow{\quad} \boxed{H} \xrightarrow{\quad} |0\rangle , \\ |1\rangle &\xrightarrow{\quad} \boxed{H} \xrightarrow{\quad} |-\rangle , & |-\rangle &\xrightarrow{\quad} \boxed{H} \xrightarrow{\quad} |1\rangle , \end{aligned}$$

<sup>iv</sup>Un tale sistema in natura è abbastanza semplice da implementare poiché, essendo  $\hat{H} = \vec{\sigma} \cdot \vec{B}$  l'accoppiamento tra spin e campo magnetico, è facile costruire una tale evoluzione temporale.

Possiamo introdurre anche le matrici seguenti (ci serviranno più avanti)

$$S \equiv \sqrt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T \equiv \sqrt{S} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}, \quad (1.5.2)$$

Le matrici introdotte in precedenza costituiscono gli oggetti base con cui andremo a implementare diversi gate e circuiti durante tutto il corso. Per costruire il gate più generale possiamo esponenziare scrivendo  $U = e^{-\frac{i}{\hbar}Ht}$  dove  $H = a\mathbb{I} + b_i\sigma_i$  e  $a, b_i \in \mathbb{R}$  con  $i = 1, 2, 3$ . In particolare esiste una particolare classe di operatori che utilizzeremo molto

$$R_{\vec{n}} = e^{-i\frac{\lambda}{2}(\vec{n}\cdot\vec{\sigma})};$$

si tratta di un caso particolare dell'esponenziazione precedente in cui  $a = 0$  e i coefficienti  $b_i$  sono scelti lungo un particolare versore  $\vec{n}$ . Questo operatore unitario implementa una rotazione di angolo  $\lambda$  attorno ad una direzione individuata da  $\vec{n}$ :

$$R_{\vec{n}}(\lambda) = e^{-i\frac{\lambda}{2}(\vec{n}\cdot\vec{\sigma})} = \cos\left(\frac{\lambda}{2}\right)\mathbb{I} - i\sin\left(\frac{\lambda}{2}\right)\vec{\sigma}\cdot\vec{n}; \quad (1.5.3)$$

(si espanda il LHS con la serie di Taylor dell'esponenziale e si usi  $(\vec{\sigma}\cdot\vec{n})^2 = \mathbb{I}$  per dimostrare l'uguaglianza con il RHS). È possibile dimostrare, inoltre, che qualsiasi matrice unitaria  $2 \times 2$  può essere scritta nella forma seguente

$$U = e^{i\alpha} \begin{pmatrix} e^{-i\frac{\beta}{2}} & 0 \\ 0 & e^{i\frac{\beta}{2}} \end{pmatrix} \begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{pmatrix} = e^{i\alpha} R_z(\beta) R_x(\gamma) R_z(\delta); \quad (1.5.4)$$

perciò il più generale operatore unitario presenta 4 parametri reali  $\alpha, \beta, \gamma, \delta \in \mathbb{R}$  e può implementare un possibile gate in un computer quantistico. Appare subito evidente come la scelta di 4 possibili parametri reali (quindi continui) consenta di realizzare un numero nettamente maggiore di gate logici quantistici rispetto al caso dei gate logici classici.

LEZIONE 3 - 11/10/2021

## 1.6 Sistemi a più qubit

Enunciamo l'ultimo postulato della QM riguardante i sistemi composti da diversi sottosistemi:

- **V Postulato (Sistemi multi-partiti):** Consideriamo un sistema quantistico composto da 2 sottosistemi  $A$  e  $B$  con spazi di Hilbert  $\mathcal{H}_A$  e  $\mathcal{H}_B$  rispettivamente. Lo spazio di Hilbert del sistema totale è dato da<sup>v</sup>  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ .

**Esempio 1.3 (Sistema di 2 qubit).** *Immaginiamo un sistema quantistico costituito da 2 qubit tale che ogni qubit possa esistere in uno stato differente, ossia  $|0\rangle$  o  $|1\rangle$ . Ovviamente ci sono 4 possibili scelte per il sistema totale:  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  e  $|11\rangle$ , dove la notazione indica che la prima entrata si riferisce al primo qubit e la seconda al secondo qubit. Il generico stato del sistema è dato da una combinazione lineare di questi ultimi:*

---

<sup>v</sup>Il simbolo " $\otimes$ " indica il **prodotto tensoriale** tra spazi.

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

con la condizione di normalizzazione  $\sum_{i,j=0}^1 |\alpha_{ij}|^2 = 1$ . La probabilità che il primo qubit si trovi in  $|i\rangle$  e al contempo il secondo si trovi in  $|j\rangle$  è data da  $P(|ij\rangle) = |\alpha_{ij}|^2$ . Se introduciamo i proiettori  $\hat{P}_0$  e  $\hat{P}_1$  sul risultato del primo qubit, possiamo allora scrivere che

$$|\psi\rangle = \underbrace{\alpha_{00} |00\rangle + \alpha_{01} |01\rangle}_{\hat{P}_0|\psi\rangle} + \underbrace{\alpha_{10} |10\rangle + \alpha_{11} |11\rangle}_{\hat{P}_1|\psi\rangle} = \hat{P}_0|\psi\rangle + \hat{P}_1|\psi\rangle ;$$

dalla regola di Born generalizzata avremo che

$$\begin{aligned} P_1(|0\rangle) &= \left\| \hat{P}_0|\psi\rangle \right\|^2 = |\alpha_{00}|^2 + |\alpha_{01}|^2, \quad \Rightarrow \quad |\psi\rangle \rightarrow \frac{\hat{P}_0|\psi\rangle}{\left\| \hat{P}_0|\psi\rangle \right\|}, \\ P_1(|1\rangle) &= \left\| \hat{P}_1|\psi\rangle \right\|^2 = |\alpha_{10}|^2 + |\alpha_{11}|^2, \quad \Rightarrow \quad |\psi\rangle \rightarrow \frac{\hat{P}_1|\psi\rangle}{\left\| \hat{P}_1|\psi\rangle \right\|}. \end{aligned}$$

Più in generale, consideriamo il caso di due spazi di Hilbert generici  $\mathcal{H}_A$  e  $\mathcal{H}_B$  con basi  $|n\rangle_A$  e  $|n\rangle_B$  rispettivamente. Possiamo scrivere lo spazio di Hilbert totale come

$$\mathcal{H}_A \otimes \mathcal{H}_B = \left\{ \sum_{n,m} \alpha_{nm} |nm\rangle \right\},$$

dove  $\dim(\mathcal{H}_A \otimes \mathcal{H}_B) = (\dim \mathcal{H}_A) \times (\dim \mathcal{H}_B)$ . Questo spazio possiede la seguente operazione

**Definizione 1.4 (Prodotto Tensoriale).** Siano  $\{|n\rangle_A\}$  e  $\{|n\rangle_B\}$  i due set di basi di due spazi di Hilbert  $\mathcal{H}_A$  e  $\mathcal{H}_B$ . Definiamo **prodotto tensoriale** la funzione  $\otimes : \mathcal{H}_A \times \mathcal{H}_B \rightarrow \mathcal{H}_A \otimes \mathcal{H}_B$  con la regola

$$\{|n\rangle_A, |n\rangle_B\} \rightarrow |n\rangle_A \otimes |n\rangle_B \equiv |nm\rangle .$$

Questa operazione può essere estesa per linearità su tutto lo spazio di Hilbert: consideriamo due stati  $|\psi\rangle_A \in \mathcal{H}_A$  e  $|\phi\rangle_B \in \mathcal{H}_B$ , allora

$$|\psi\rangle_A \otimes |\phi\rangle_B = \left( \sum_n \alpha_n |n\rangle_A \right) \otimes \left( \sum_m \beta_m |m\rangle_B \right) = \sum_{n,m} \underbrace{\alpha_n \beta_m}_{\alpha_{nm}} |nm\rangle . \quad (1.6.1)$$

Vettori di  $\mathcal{H}_A \otimes \mathcal{H}_B$  che possono essere scritti come la decomposizione in (1.6.1) sono detti **separabili**. Solamente alcuni vettori di  $\mathcal{H}_A \otimes \mathcal{H}_B$  sono separabili perché  $\alpha_{nm}$  è una matrice particolare, risultante dal prodotto dei due vettori contenenti i coefficienti  $\alpha_n$  e  $\beta_m$ . È possibile dimostrare che tali matrici che si scrivono come  $A_{nm} = \alpha_n \beta_m$  hanno  $\det A_{nm} = 0$  (sono di rango 1). Gli stati particolarmente interessanti che tratteremo a lungo durante il corso sono quelli che non soddisfano la decomposizione in (1.6.1), detti stati **entangled**.

**Esempio 1.4.** Il seguente stato è separabile:

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \equiv \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |\psi\rangle_A \otimes |\phi\rangle_B .$$

Al contrario lo stato  $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  è entangled poiché non può essere decomposto come in (1.6.1).

Analizziamo ciò che abbiamo appena visto nel contesto di qubit e circuiti. In qualità di portatori di informazioni denoteremo due qubit con due linee in questo modo

$$\begin{array}{c} |0\rangle, |1\rangle \\ |0\rangle, |1\rangle \end{array}$$

mentre il risultato di tali qubit è la combinazione lineare  $\sum_{n,m} \alpha_{nm} |nm\rangle$ . Dato che sappiamo che  $\dim(\mathcal{H}_A \otimes \mathcal{H}_B) = 2 \times 2 = 4$  allora  $\mathcal{H}_A \otimes \mathcal{H}_B \simeq \mathbb{C}^4$  e su tale spazio di Hilbert gli operatori unitari corrispondenti ai gate quantistici sono le matrici unitarie  $4 \times 4$ . Alcune di queste matrici derivano dalle operazioni sui qubit singoli: ad esempio se

$$\begin{array}{ccc} |\psi\rangle & \xrightarrow{\quad A \quad} & A|\psi\rangle , \\ |\phi\rangle & \xrightarrow{\quad B \quad} & B|\phi\rangle , \end{array}$$

la matrice risultante agente se entrambi i qubit è  $U = A \otimes B$ , la quale agisce naturalmente come  $U(|\psi\rangle \otimes |\phi\rangle) = A|\psi\rangle \otimes B|\phi\rangle$ . Queste tipologie di matrici sono molto speciali e non sono sicuramente le più generali.

Come facciamo a passare dai vettori a 2 componenti di ciascun qubit ad un vettore a 4 componenti del sistema a 2 qubit? Supponiamo che ciascun qubit sia un vettore

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle \equiv \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \in \mathbb{C}^2 ,$$

e consideriamo il vettore risultante dal sistema di due qubit

$$\alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle \equiv \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \in \mathbb{C}^4 .$$

Per passare dall'uno all'altro possiamo utilizzare il prodotto seguente:

**Definizione 1.5 (Prodotto di Kronecker).** Siano  $A$  e  $B$  due matrici. Assumendo che  $A$  sia una matrice  $q \times p$  allora definiamo il prodotto di Kronecker  $A \otimes B$  come

$$A \otimes B = \begin{pmatrix} A_{11}B & A_{12}B & \cdots & A_{1p}B \\ \vdots & & \ddots & \\ A_{q1}B & A_{q2}B & \cdots & A_{qp}B \end{pmatrix}$$

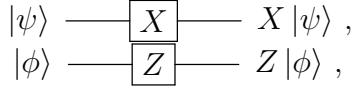
**Esempio 1.5** (Vettore sistema di due qubit). Utilizzando il prodotto di Kronecker il vettore risultante di un sistema di due qubit può essere scritto come

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix} ;$$

notiamo infatti che questo vettore di coefficienti è lo stesso risultante dal prodotto tensoriale dei due qubit

$$(\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) = \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle .$$

**Esempio 1.6.** Chiaramente il prodotto di Kronecker funziona anche per un sistema di due qubit in cui agiscono un *X-gate* e un *Z-gate*



la matrice  $4 \times 4$  risultante sarà

$$X \otimes Z = \sigma_1 \otimes \sigma_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

Così come sottolineato in precedenza per gli stati separabili, queste matrici non costituiscono il caso generale perché, essendo frutto di un prodotto tensoriale, in realtà agiscono separatamente su un singolo qubit alla volta: quello di cui abbiamo bisogno in QC ("quantum computing") è di utilizzare matrici generiche che rendono i qubit entangled.

Cominciamo a vedere qualche esempio nel caso del CC ("classical computing"). Oltre al gate logico NOT, vediamo l'azione di altri gate

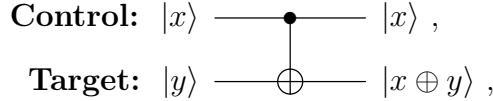
$$\begin{aligned} x \text{ AND } y &= \begin{cases} 1, & \text{se entrambi } x = y = 1 \\ 0, & \text{altrimenti} \end{cases}, \\ x \text{ OR } y &= \begin{cases} 1, & \text{se } x = 1 \text{ oppure } y = 1 \\ 0, & \text{altrimenti} \end{cases}, \\ x \text{ XOR } y &= (x + y) \bmod 2 \equiv x \oplus y = \begin{cases} 0 \oplus 0 = 0 \\ 0 \oplus 1 = 1 \\ 1 \oplus 0 = 1 \\ 1 \oplus 1 = 0 \end{cases}, \end{aligned}$$

dove l'operazione  $(x + y)\bmod 2$  indica il resto della divisione per 2 della somma  $x + y$ . Tutte queste operazioni non possono essere fattorizzate perché non sono il prodotto di operazioni sui singoli bit.

Consideriamo ora il caso quantistico. Una delle operazioni più importanti è il **controlled NOT** o **CNOT-gate**, il quale è una sorta di generalizzazione al caso quantistico del classico XOR. Si tratta di un gate  $U_{CN}$  (unitario) che agisce su un sistema di 2 qubit (sistema di dimensione 4) come segue:

$$U_{CN} : \begin{array}{ll} |00\rangle \rightarrow |00\rangle, & |01\rangle \rightarrow |01\rangle, \\ |10\rangle \rightarrow |11\rangle, & |11\rangle \rightarrow |10\rangle, \end{array}$$

Come evidente, il primo qubit è utilizzato come qubit di **controllo**, mentre il secondo funge da **target**: a seconda del valore del primo qubit si svolge o meno un'azione sul secondo. In particolare quando il primo qubit è in  $|0\rangle$ , il secondo non viene toccato; quando invece il primo si trova in  $|1\rangle$ , il secondo viene scambiato. Dal punto di vista grafico indicheremo il CNOT-gate come



È chiaro che per  $x = 0$  si ha  $y \rightarrow 0 \oplus y = y$  mentre per  $x = 1$  si ha  $y \rightarrow 1 \oplus y$ , il quale risulta 1 per  $y = 0$  e 0 per  $y = 1$ . In forma matriciale questo gate non è altro che

$$U_{\text{CN}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

Si tratta di un esempio di gate (matrice  $4 \times 4$ ) che agisce in maniera non banale sui qubit e che non può essere fattorizzato come azione sui singoli qubit.

Un punto fondamentale che differenzia i gate quantistici da quelli classici è che, essendo unitari, sono sempre **reversibili**. Infatti

$$|\psi\rangle \xrightarrow{[U]} \xrightarrow{[U^\dagger]} UU^\dagger |\psi\rangle = |\psi\rangle,$$

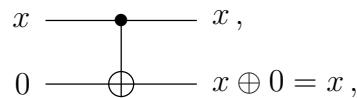
Si noti al contrario che in generale il CC non è reversibile<sup>vi</sup>: ad esempio se si ha che  $x \text{ AND } y = 0$  non possiamo dire nulla su  $x$  e  $y$  separatamente.

## 1.7 Teorema di no-cloning

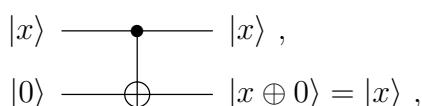
Il teorema di no-cloning è un risultato molto importante in QM perché stabilisce che cosa è permesso fare o meno in un computer quantistico. Discutiamolo in dettaglio. Supponiamo di considerare lo stato  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ : anche se, a differenza del caso classico, i coefficienti  $\alpha$  e  $\beta$  sono arbitrari, il problema risiede nell'estrarrre informazioni. Per trovare in quale stato preciso si trova il sistema bisogna considerare un numero infinito di qubit tutti preparati nel medesimo stato iniziale, ma in un computer quantistico tipicamente si ha solamente 1 singolo qubit! Il punto è che c'è moltissima informazione in  $|\psi\rangle$  ma non sappiamo come estrarla: infatti l'arte del quantum computing consiste nell'estrarrre *particolari* informazioni riguardanti  $\alpha$  e  $\beta$  usando solamente una sola misurazione.

Un problema come questo potrebbe essere risolto se potessimo duplicare gli stati: il teorema di no-cloning stabilisce proprio il fatto che ciò non è possibile. Nonostante ciò la questione è sottile quindi vediamo di analizzarla in dettaglio.

Nel CC è possibile clonare un bit utilizzando un **CNOT-gate** classico: per  $y = 0$  infatti (indichiamo nel circuito seguente i singoli bit e non gli stati perché è un circuito classico)



siamo quindi riusciti ad ottenere due copie esatte del bit  $x$ . Nell'analogo caso quantistico abbiamo



<sup>vi</sup>In realtà esiste un modo per calcolare solamente operazioni reversibili mediante gate reversibili in un computer classico. Si tratta di convertire le operazioni base dell'aritmetica in calcoli step by step reversibili.

perciò sembrerebbe che siamo riusciti a clonare anche lo stato quantistico. Ad esempio per  $x = 0$  si ha  $|00\rangle \xrightarrow{\text{CNOT}} |00\rangle$  e per  $x = 1$  si ha  $|10\rangle \xrightarrow{\text{CNOT}} |11\rangle$ . Da questi esempi si potrebbe ingenuamente concludere che sia possibile clonare uno stato anche nel mondo quantistico. In realtà la questione è più sottile perché è possibile clonare uno stato che appartiene ad una base, come  $\{|0\rangle, |1\rangle\}$ , ma è molto semplice vedere che non si può clonare uno stato generico. Ad esempio, prendiamo il caso in cui vogliamo clonare il generico qubit  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ . Applichiamo un CNOT-gate con un target dato da  $|0\rangle$ :

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle = \alpha|00\rangle + \beta|10\rangle \xrightarrow{\text{CNOT}} \alpha|00\rangle + \beta|11\rangle ,$$

questo risultato è chiaramente differente da

$$|\psi\rangle \otimes |\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle ,$$

nel caso generale in cui  $\alpha \neq 0$  e  $\beta \neq 0$ . In generale è possibile clonare solamente stati ortogonali tra loro. Enunciamo il teorema:

**Teorema 1.2 (Teorema di no-cloning).** *Dato uno stato generico  $|\phi\rangle$  normalizzato, non esiste alcun operatore unitario  $U$  tale che*

$$|\psi\rangle \otimes |\phi\rangle \rightarrow U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle , \quad \forall |\psi\rangle \text{ normalizzato.} \quad (1.7.1)$$

*Dimostrazione.* Supponiamo per assurdo che esista un operatore unitario  $U$  che realizza la trasformazione in (1.7.1). Supponiamo di aver clonato due generici stati  $|\psi_1\rangle$  e  $|\psi_2\rangle$ :

$$\begin{aligned} |\psi_1\rangle \otimes |\phi\rangle &\xrightarrow{U} |\psi_1\rangle \otimes |\psi_1\rangle , \\ |\psi_2\rangle \otimes |\phi\rangle &\xrightarrow{U} |\psi_2\rangle \otimes |\psi_2\rangle , \end{aligned}$$

ma dato che l'operatore è unitario deve preservare il prodotto scalare:

$$\begin{aligned} (\langle\psi_2| \otimes \langle\phi|)(|\psi_1\rangle \otimes |\phi\rangle) &\stackrel{?}{=} (\langle\psi_2| \otimes \langle\psi_2|)(|\psi_1\rangle \otimes |\psi_1\rangle) , \\ \Rightarrow \quad \langle\psi_2|\psi_1\rangle &= \langle\psi_2|\psi_1\rangle^2 , \end{aligned}$$

dove abbiamo assunto  $\langle\phi|\phi\rangle = 1$ . Questo significa che  $\langle\psi_2|\psi_1\rangle(1 - \langle\psi_2|\psi_1\rangle) = 0$ , quindi  $\langle\psi_2|\psi_1\rangle = 0$  (i due stati sono ortogonali) oppure  $\langle\psi_2|\psi_1\rangle = 1$ , il che significa che  $|\psi_1\rangle = e^{i\alpha}|\psi_2\rangle$ , quindi i due stati sono proporzionali per una fase e quindi di fatto si tratta dello stesso stato. In definitiva non è possibile clonare stati generici, ma solamente stati particolari.  $\square$

Dobbiamo capire come superare queste limitazioni in un computer quantistico. In realtà vedremo che per la maggior parte delle situazioni fisicamente rilevanti è già abbastanza clonare solamente degli stati che appartengono ad una base, quindi non sarà necessario duplicare stati generici.

# Capitolo 2

## Entanglement

In questo capitolo affronteremo molti argomenti riguardanti il concetto di *teletrasporto*, *crittografia quantistica* e *disuguaglianze di Bell*. Tutti questi temi sono legati dal fenomeno dell'**entanglement**. Innanzitutto ricordiamo che uno stato è definito **entangled** se **non** può essere scritto come stato separabile  $|\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B$ , ovvero non è frutto del prodotto tensoriale di stati appartenenti a differenti spazi di Hilbert.

**Esempio 2.1.** Per un sistema in cui è presente una particella dotata di spin, lo stato di singoletto<sup>i</sup>  $|00\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$  (momento angolare totale nullo) è uno stato entangled.

Gli stati entangled danno origine a numerosi paradossi che sono stati studiati a partire dall'inizio del '900. Il paradosso più famoso è probabilmente il **paradosso EPR** (dai nomi Einstein-Podolski-Rosen).

**Esempio 2.2 (Paradosso EPR).** Consideriamo un sistema costituito da 2 qubit (o due particelle dotate di spin) che si trova nello stato entangled  $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$  e immaginiamo di voler effettuare una misurazione sul primo qubit (spin). Secondo le regole della QM, semplicemente avremo che

$$\begin{aligned} P(|0\rangle_1) &= \frac{1}{2}, & P(|1\rangle_1) &= \frac{1}{2}, \\ P(|0\rangle_2) &= \frac{1}{2}, & P(|1\rangle_2) &= \frac{1}{2}, \end{aligned}$$

dove il pedice numerico sui ket indica il qubit (spin) che è stato misurato. Dalla forma dello stato  $|\psi\rangle$  notiamo che le misure sono correlate perché una misura sul sistema causa il collasso dello stato in  $|01\rangle$  o  $|10\rangle$  e quindi il risultato della misura sull'altro qubit viene direttamente influenzato. La correlazione è sottile perché se supponiamo di separare le due particelle (due qubit) in due città differenti mantenendo lo stato totale entangled allora è possibile determinare il risultato di entrambe le misure effettuando una singola misurazione! Ad esempio, se una misura sul primo qubit produce  $|0\rangle_1$  allora  $|\psi\rangle$  collassa istantaneamente in  $|01\rangle$  (ora lo stato non è più entangled): d'ora in avanti il secondo sperimentatore che si trova nell'altra città trova sempre  $P(|1\rangle_2) = 1$ , sebbene prima del collasso vedeva le probabilità equiprobabili.

Chiaramente ciò che accade nel paradosso EPR è molto strano: il fatto che lo stato sia entangled suggerisce una sorta di azione istantanea a distanza. È importante evidenziare

---

<sup>i</sup>In generale non è difficile realizzare un tale stato in natura. Si vedano ad esempio l'ortoelio e il paraelio.

che questo paradosso non ha nulla a che fare con la violazione della relatività speciale perché nessuno dei due sperimentatori ha inviato informazioni istantanee. Uno dei due aspetti che il paradosso vuole sottolineare è la violazione del **principio di località**: secondo tale assunto una misura effettuata in una regione non può influenzare istantaneamente una misura che viene effettuata in un'altra regione casualmente disconnessa dalla precedente. Ma come l'evidenza sperimentale mostra, il risultato è l'esatto contrario.

LEZIONE 4 - 15/10/2021

Continuiamo la discussione riguardante il concetto di entanglement. Dato che questo fenomeno si manifesta in sistemi con almeno due qubit, possiamo utilizzare due differenti basi:

- **Base computazionale (o standard)**: formata dagli stati  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$  (la due entrate indicano gli stati del primo e secondo qubit rispettivamente).
- **Base di Bell (o EPR)**: costituita dagli stati

$$\begin{aligned} |\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), & |\beta_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |\beta_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), & |\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle); \end{aligned}$$

notiamo che si trattano di stati entangled costruiti a partire da combinazioni lineari indipendenti degli stati della base computazionale.

Chiaramente, trattandosi di una base, possiamo espandere qualsiasi stato  $|\psi\rangle$  nella base EPR, scrivendo

$$|\psi\rangle = \sum_{n,m=0}^1 \alpha_{nm} |\beta_{nm}\rangle .$$

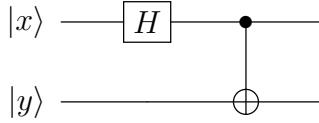
Conseguentemente, se si cerca la probabilità di trovarsi in  $|\beta_{nm}\rangle$  si può effettuare una misurazione nella base di Bell e ottenere  $P(|\beta_{nm}\rangle) = |\alpha_{nm}|^2$ .

Gli stati della base di Bell non sono difficili da costruire utilizzando i gate che abbiamo visto precedentemente. Supponiamo di poter utilizzare un computer quantistico i cui qubit si trovano nella base standard  $\{|0\rangle, |1\rangle\}$ . Utilizziamo l'**H-gate** e il **CNOT-gate**:

- Ricordiamo che  $H|0\rangle = |+\rangle$  e  $H|1\rangle = |-\rangle$ , quindi il gate di Hadamard permette di passare da un qubit nella base computazionale ad un qubit in una combinazione lineare di elementi di questa base (si ricordi la matrice in (1.5.1) e le definizioni in (1.2.3)).
- Il **CNOT-gate**, invece, scambia il secondo qubit solamente se il primo si trova in  $|1\rangle$ :

$$\begin{aligned} |00\rangle &\xrightarrow{\text{CNOT}} |00\rangle , & |01\rangle &\xrightarrow{\text{CNOT}} |01\rangle , \\ |10\rangle &\xrightarrow{\text{CNOT}} |11\rangle , & |11\rangle &\xrightarrow{\text{CNOT}} |10\rangle . \end{aligned}$$

Utilizzando questi due gate possiamo facilmente implementare il circuito seguente



i cui output sono esattamente gli stati  $|\beta_{xy}\rangle$  della base di Bell. Verifichiamolo:

$$\begin{aligned}
 |00\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \equiv |\beta_{00}\rangle , \\
 |01\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \equiv |\beta_{01}\rangle , \\
 |10\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \equiv |\beta_{10}\rangle , \\
 |11\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |1\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \equiv |\beta_{11}\rangle ;
 \end{aligned}$$

si noti come l'azione di un gate (in questo caso l'**H-gate**) su un singolo qubit non basti per produrre uno stato entangled. Al contrario il **CNOT-gate**, invece, crea stati entangled poiché agisce su coppie di qubit.

Vediamo ora due esplicite applicazioni dell'entanglement.

## 2.1 Superdense coding

Si tratta del primo esempio esplicito delle potenzialità dei metodi quantistici contro i metodi classici. Il problema riguarda il come inviare informazioni di due bit classici (00, 01, 10, 11) ad un generico sperimentatore. Consideriamo la sperimentatrice Alice e supponiamo che abbia due bit di informazione (due numeri  $xy$ ) e che voglia inviarli allo sperimentatore Bob. Dal punto di vista classico, Alice semplicemente utilizza un canale classico (un telefono ad esempio) per comunicare direttamente a Bob quale coppia di numeri possiede. Nel caso in cui Alice possieda due qubit, invece, può inviare solamente uno dei due sfruttando il fatto che siano entangled. Supponiamo che Alice e Bob condividano due qubit entangled, ad esempio

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\beta_{00}\rangle ,$$

dove Alice possiede il primo qubit (prima entrata del ket) e Bob il secondo. Cosa deve fare Alice per inviare solamente un singolo "pezzo" di informazione? Ad esempio Alice può effettuare una qualche operazione sul suo qubit e, sfruttando l'entanglement, Bob sarà in grado di leggere l'informazione desiderata (la coppia di numeri  $xy$  che Alice vuole inviare) facendo una singola misurazione. Più precisamente, supponiamo che Alice voglia inviare delle informazioni effettuando le seguenti operazioni sul proprio qubit di  $|\psi\rangle$ :

$$\text{Alice invia: } \begin{cases} 00, & \text{non fa niente} \\ 10, & \text{applica } Z \\ 01, & \text{applica } X \\ 11, & \text{applica } ZX \end{cases} .$$

Cosa succede allo stato condiviso quando applica queste operazioni?

- Quando vuole inviare 00 non effettua alcuna operazione quindi  $|\psi\rangle \rightarrow |\psi\rangle = |\beta_{00}\rangle$ .
- Nel caso in cui decide di inviare 10 applica  $Z$ :

$$|\psi\rangle \rightarrow Z \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) = |\beta_{10}\rangle .$$

- Quando invece vuole inviare 01 applica  $X$ :

$$|\psi\rangle \rightarrow X \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} (|10\rangle + |01\rangle) = |\beta_{01}\rangle .$$

- Infine se vuole inviare 11 applica  $ZX$ :

$$|\psi\rangle \rightarrow ZX \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = Z \frac{1}{\sqrt{2}} (|10\rangle + |01\rangle) = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) = |\beta_{11}\rangle .$$

Effettuando queste operazioni, Alice è in grado di spedire ciò che vuole:  $xy \rightarrow |\beta_{xy}\rangle$ . Bob può effettuare una (singola) misura nella base di Bell, stabilire quale dei 4 stati possiede, e leggere quindi i bit corrispondenti  $xy$ . L'informazione classica corrispondente a due bit è stata inviata attraverso un solo qubit.

Questo esempio, nonostante sia un po' accademico, risulta particolarmente interessante perché mette in risalto come, grazie all'entanglement, sia possibile ridurre il numero di operazioni necessarie per inviare un'informazione rispetto al caso classico.

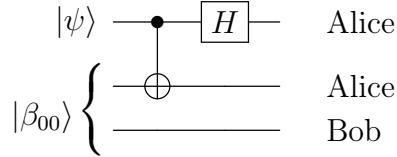
## 2.2 Teleportation

Innanzitutto che cosa intendiamo con il termine *teletrasporto*? In questo contesto viene inteso con il significato di ricostruire un qubit molto lontano da dove si trovava in origine: il qubit originale sparisce e una sua nuova copia viene creata altrove. L'idea è quella di effettuare questa particolare ricostruzione usando solamente operazioni classiche sui qubit.

Supponiamo che Alice (d'ora in avanti chiameremo sempre in questo modo i nostri due sperimentatori) abbia un generico qubit  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  e che voglia inviarlo a Bob senza utilizzare alcun canale quantistico. Dalle leggi della QM sappiamo che non possiamo estrarre sia  $\alpha$  che  $\beta$  con una singola misura e inoltre non è possibile clonare questo stato generico. Inoltre, se volesse inviare direttamente questo stato con assoluta precisione (assumiamo  $\alpha, \beta \in \mathbb{R}$ ) mediante un canale classico, allora necessiterebbe due stringhe infinite di bit e quindi del tempo infinito per inviarle. Come nel caso precedente, assumiamo che Alice e Bob condividano lo stato entangled  $|\beta_{00}\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$ , dove il primo qubit è di Alice e il secondo di Bob. Notiamo che Alice possiede due qubit: il qubit generico  $|\psi\rangle$  che vuole teletrasportare e il qubit entangled con quello di Bob. Lo stato iniziale non è quindi altro che

$$(\alpha|0\rangle + \beta|1\rangle) |\beta_{00}\rangle = \frac{\alpha}{\sqrt{2}} |0\rangle (|00\rangle + |11\rangle) + \frac{\beta}{\sqrt{2}} |1\rangle (|00\rangle + |11\rangle) . \quad (2.2.1)$$

Alice sottopone gli stati in suo possesso al seguente circuito:



dove si è indicato in output a chi appartiene quel determinato qubit. Esplicitamente, si applica **CNOT-gate** ai due qubit di Alice in (2.2.1):

$$\frac{\alpha}{\sqrt{2}} |0\rangle (|00\rangle + |11\rangle) + \frac{\beta}{\sqrt{2}} |1\rangle (|10\rangle + |01\rangle) ;$$

dopodiché viene applicato H-gate al primo qubit di Alice:

$$\frac{\alpha}{2} (|0\rangle + |1\rangle) (|00\rangle + |11\rangle) + \frac{\beta}{2} (|0\rangle - |1\rangle) (|10\rangle + |01\rangle) ;$$

infine possiamo riscrivere l'espressione nel modo seguente

$$\frac{1}{2} \left[ |00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle) \right] ,$$

dove in questo ultimo passaggio abbiamo svolto i conti e riordinato l'espressione focalizzandoci su ciò che è posseduto da Alice (i due qubit di fronte alle 4 parentesi tonde) e da Bob (stato nella parentesi tonda). Consideriamo ora la Tabella 2.1: Alice può effettuare una misura nella base computazionale e dire a Bob (mediante un canale classico) ciò che ha ottenuto; dopo la misura lo stato collassa e Bob, a seconda del risultato, può effettuare o meno un'opportuna operazione sul proprio stato per ricostruire precisamente ciò che si voleva teletrasportare.

Alice misura	Bob trova	Bob applica
$ 00\rangle$	$\alpha  0\rangle + \beta  1\rangle$	Nulla
$ 01\rangle$	$\alpha  1\rangle + \beta  0\rangle$	$X$
$ 10\rangle$	$\alpha  0\rangle - \beta  1\rangle$	$Z$
$ 11\rangle$	$\alpha  1\rangle - \beta  0\rangle$	$ZX$

Tabella 2.1: Una volta che Alice effettua la propria misura nella base computazionale e dice a Bob ciò che ha ottenuto, quest'ultimo può applicare una precisa operazione per ricostruire lo stato  $|\psi\rangle$  che Alice voleva teletrasportare. Si noti che, in tutti e quattro i casi, lo stato finale che ha Bob è sempre  $|\psi\rangle$  indipendentemente dal risultato di Alice.

Un fatto fondamentale da evidenziare è che solamente informazioni classiche sono state trasferite tra Bob e Alice poiché tutto il resto (misurazioni e operazioni sugli stati) viene svolto localmente nel laboratorio: non c'è né violazione della relatività speciale in quanto non avviene alcun trasferimento di informazioni più veloce della luce, né violazione del teorema di no-cloning perché, una volta che Bob ottiene  $|\psi\rangle$ , Alice non possiede più lo stato che voleva teletrasportare. Si tratta solamente di un modo ingegnoso per sfruttare l'entanglement.

## 2.3 Disuguaglianze di Bell

L'argomento delle disuguaglianze di Bell è un tema molto vasto che comprende moltissime disuguaglianze testabili sperimentalmente: ciò che accomuna tutte le misurazioni è

la profonda differenza tra il concetto di probabilità *classica* e *quantistica*. Nella prima metà del '900, dopo la nascita della QM e i conseguenti trionfi che tale teoria era in grado di riportare, molti fisici, tra cui lo stesso Einstein, erano profondamente insoddisfatti del concetto intrinseco ed inevitabile di probabilità che permea tale teoria. In particolare, coloro che non accettavano la QM come teoria completa, credevano che il suo comportamento fosse in realtà dovuto alla nostra ignoranza su teorie ancora più fondamentali. Questo gruppo di persone credevano che le **osservabili**, in fisica, dovessero sempre soddisfare 2 requisiti base:

- **Realismo:** un'osservabile deve avere un valore definito anche prima che la misura sia effettuata.
- **Località:** un esperimento effettuato in un ben preciso luogo ha solamente un effetto locale perché non può in alcun modo modificare risultati e comportamenti di altri esperimenti effettuati in regioni causalmente disconnesse. L'entanglement, ad esempio, è in profondo contrasto con il concetto di località.

Nel corso di quegli anni furono svolti numerosi tentativi di riscrivere la QM in maniera tale che soddisfacesse i requisiti precedenti. Ad esempio, furono utilizzate le cosiddette **teorie delle variabili nascoste**. Tali teorie si basano sull'assunto secondo cui quando si misura un valore  $a$  di un'osservabile  $A$ , in realtà il risultato della misurazione è incompleto perché l'intera teoria prevede l'esistenza di un'altra variabile  $\lambda$  *nascosta* ed inaccessibile. Se si potesse conoscere  $\lambda$  allora si potrebbe predire qualsiasi cosa in maniera del tutto deterministica. Nonostante ciò, il concetto di probabilità in QM viola queste regole e, come vedremo tra poco, utilizzando le disuguaglianze di Bell è possibile rilevare sperimentalmente tale violazione.

**Esempio 2.3** (Singolo qubit). *Consideriamo nuovamente il caso di un qubit e immaginiamo di trovarci nello stato  $|0\rangle$ . Nella Sezione 1.2 abbiamo visto che il più generale operatore hermitiano che agisce su un singolo qubit è dato da una combinazione lineare di matrici di Pauli (non consideriamo l'identità), ossia  $\vec{\sigma} \cdot \vec{n}$  dove  $|\vec{n}| = 1$ . Supponiamo che a seguito di una misurazione possiamo ottenere  $\vec{\sigma} \cdot \vec{n} |\vec{n}\rangle = |\vec{n}\rangle$  e  $\vec{\sigma} \cdot \vec{n} |-\vec{n}\rangle = -|-\vec{n}\rangle$ , quindi il risultato è  $\pm 1$ . Perciò, ricordando la decomposizione  $|0\rangle = c_1 |\vec{n}\rangle + c_2 |-\vec{n}\rangle$ , la probabilità di misurare 1 è  $P(\vec{\sigma} \cdot \vec{n} = 1) = |c_1|^2 = |\langle 0 | \vec{n} \rangle|^2$ . Al tempo stesso sappiamo anche che il generico qubit si scrive come in (1.1.2), quindi  $\vec{n}$  può essere specificato scegliendo gli angoli  $\theta$  e  $\phi$ : dato che avevamo sottolineato che  $\vec{\sigma} \cdot \vec{n} |\psi\rangle = |\psi\rangle$  allora la soluzione che cerchiamo è  $|\vec{n}\rangle = |\psi\rangle$ , quindi*

$$P(\vec{\sigma} \cdot \vec{n} = 1) = |\langle 0 | \vec{n} \rangle|^2 = |\langle 0 | \psi \rangle|^2 = \cos^2\left(\frac{\theta}{2}\right).$$

*Vediamo se riusciamo a riprodurre la medesima distribuzione di probabilità utilizzando una teoria classica basata sulle variabili nascoste. Supponiamo che, oltre allo spin, la particella sia in realtà descritta da un'extra variabile  $\lambda$ : tutte le particelle sono specificate dalla coppia fissata ( $a = \pm 1, \lambda$ ), ossia hanno spin  $a = \pm 1$  e un preciso valore di  $\lambda$  persino prima di effettuare la misurazione. Per semplicità assumiamo  $\lambda \in [0, 1]$ . Supponiamo di voler effettuare una misurazione dello spin in una particolare direzione  $|n\rangle$ : la misurazione, in questa teoria, corrisponde a particolari valori di spin e  $\lambda$  con l'idea che una misura effettuata con angolo  $\theta$  abbia risultato dipendente dal valore assunto da  $\lambda$  nell'intervallo  $[0, 1]$ . Più precisamente, consideriamo una teoria con variabili nascoste in*

cui il risultato delle misure sia quello indicato nella formula seguente. Assumendo di non poter rilevare il valore  $\lambda$  e richiedendo che le particelle abbiano dei valori di tale variabile uniformemente distribuiti, un esperimento di questo tipo produce

$$\begin{cases} \text{spin } |\uparrow\rangle, & \text{per } 0 \leq \lambda \leq \cos^2 \theta/2 \\ \text{spin } |\downarrow\rangle, & \text{per } \cos^2 \theta/2 \leq \lambda \leq 1 \end{cases}, \Rightarrow P(a=1) = \cos^2\left(\frac{\theta}{2}\right).$$

Nell'esempio precedente è stato analizzato il caso di un singolo qubit, che è riproducibile da una teoria con variabili nascoste. Prendiamo ora in esame il sistema di 2 qubit, dove sappiamo che l'entanglement gioca un ruolo centrale e dove ci sarà differenza tra probabilità *classica* e *quantistica*. Esistono diversi modi per scrivere delle disuguaglianze che testino sperimentalmente questa profonda differenza. Uno dei più famosi è il seguente

### 2.3.1 Disuguagliaza CHSH

Si tratta di una semplice generalizzazione delle disuguaglianze scritte originariamente da Bell e utilizzata per le verifiche sperimentali. Ancora una volta, consideriamo i due sperimentatori Alice e Bob situati in città differenti. Supponiamo che entrambi abbiano a disposizione un apparato identico su cui possano effettuare misure e che vengano riforniti (ad esempio da un terzo sperimentatore) di infinite copie di particelle correlate sulle quali possono compiere dei test, e ciascuno possiede una particella della coppia. Alice misura le osservabili  $a, a'$  per la sua particella, mentre Bob misura  $b, b'$  per la sua, dove  $a, a', b, b' = \pm 1$ . Entrambi scelgono di fare misurazioni simultanee di una sola delle due osservabili scelta ogni volta in maniera casuale.

In un'ipotetica teoria basata sulle variabili nascoste, dato questo sistema è impossibile stabilire immediatamente quale sia il risultato di una misura poiché ci sarà necessariamente una distribuzione di probabilità classica, che chiamiamo  $P(a, a', b, b')$ , associata alla nostra ignoranza. Consideriamo ora l'osservabile  $C = (a + a')b + (a - a')b'$ ; per costruzione sappiamo che

$$\begin{cases} a + a' = 0, a - a' = \pm 2, & \text{se } a \neq a' \\ a + a' = \pm 2, a - a' = 0, & \text{se } a = a' \end{cases},$$

ma questo significa allora che per qualsiasi valore delle 4 osservabili in gioco si ha sempre  $C = \pm 2$ . Dalla teoria della probabilità classica sappiamo che  $|\langle C \rangle| \leq \langle |C| \rangle$  dato che  $|\sum_c c p(c)| \leq \sum_c |c| p(c)$ . Siccome assumiamo che  $a, a', b, b', C$  esistano indipendentemente dalla nostra misura, possiamo applicare questa disuguaglianza: in tutte le possibili configurazioni  $|C| = 2$  quindi  $\langle |C| \rangle = 2$  e allora

$$|\langle C \rangle| \leq 2. \quad (2.3.1)$$

La disuguaglianza precedente prende il nome di **disuguaglianza CHSH**<sup>ii</sup>. Notiamo che si tratta di un risultato classico derivante dalla teoria della probabilità.

In QM è facile trovare un esempio nel quale questa disuguaglianza è violata. Supponiamo che Alice e Bob condividano lo stato entangled  $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$  e che entrambi decidano di misurare qualcosa che in QM abbia 2 possibili valori. In particolare misurano

$$\begin{array}{ll} a = \vec{\sigma} \cdot \hat{a} = \pm 1, & a' = \vec{\sigma} \cdot \hat{a}' = \pm 1, \\ b = \vec{\sigma} \cdot \hat{b} = \pm 1, & b' = \vec{\sigma} \cdot \hat{b}' = \pm 1, \end{array}$$

---

<sup>ii</sup> Clauser, J., Horne, M., Shimony, A., & Holt, R. (1969). Proposed Experiment to Test Local Hidden-Variable Theories. *Phys. Rev. Lett.*, 23, 880–884.

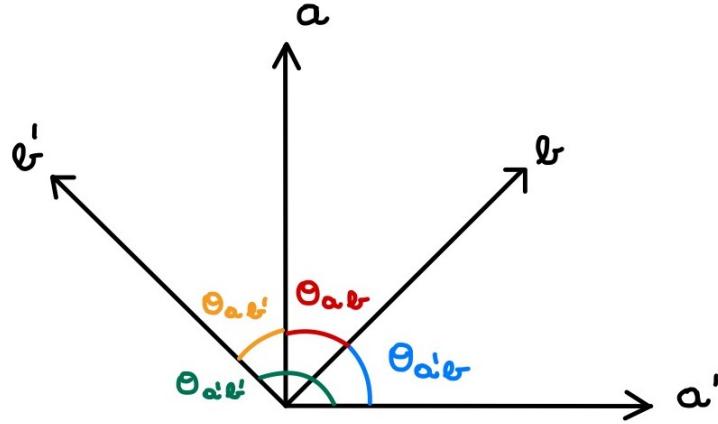


Figura 2.1: Direzioni spaziali delle 4 osservabili misurate da Alice e Bob. Si noti che l'apparato di uno è ruotato di  $45^\circ$  rispetto a quello dell'altro perciò  $\theta_{a'b} = \theta_{ab} = \theta_{ab'} = 45^\circ$  e  $\theta_{a'b'} = 135^\circ$ .

dove il simbolo " $\hat{\cdot}$ " indica un vettore di modulo unitario. È possibile dimostrare in QM che

$$\langle \psi | (\vec{\sigma} \cdot \hat{c}) \otimes (\vec{\sigma} \cdot \hat{d}) | \psi \rangle = -\hat{c} \cdot \hat{d} = -\cos \theta, \quad (2.3.2)$$

dove  $\theta$  è l'angolo tra  $\hat{c}$  e  $\hat{d}$ . Supponiamo che Alice e Bob decidano di misurare nelle direzioni indicate dagli angoli di Figura 2.1. Utilizzando la (2.3.2) possiamo calcolare il valore di aspettazione di  $C$ :

$$\langle C \rangle = \langle \psi | ab + a'b + ab' - a'b' | \psi \rangle = - \left[ \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} - \left( -\frac{1}{\sqrt{2}} \right) \right] = -2\sqrt{2}.$$

Abbiamo quindi ricavato che, secondo la QM,  $|\langle C \rangle| = 2\sqrt{2}$ , in disaccordo<sup>iii</sup> con il risultato classico in (2.3.1): la probabilità *quantistica* è intrinsecamente differente dalla probabilità *classica*!

Altri esperimenti degni di nota sono quelli condotti da Freedman e Clauser nel 1972, la serie di esperimenti condotti da Aspect negli anni 1981 e 1982, da Tittel e il gruppo Geneva nel 1988 e da Weihs sotto condizioni di località "strettamente einsteniane" nel 1998. La serie di esperimenti sulle disuguaglianze di Bell, di crescente sofisticazione, ha ridotto i critici, che mettono in discussione i risultati, a indicare falle in tale esperimenti, alcune delle quali distorcerebbero i risultati sperimentali in favore della meccanica quantistica. Nel 2015 è stato pubblicato il primo esperimento dichiarato totalmente privo di falle (loopholes), che ha confermato i risultati degli esperimenti precedenti.

---

<sup>iii</sup>In realtà esiste un teorema che stabilisce che  $2\sqrt{2}$  è il più grande valore che può essere ottenuto.

# Capitolo 3

## Algoritmi quantistici

LEZIONE 5 - 18/10/2021

Prima di cominciare la vera discussione riguardante gli algoritmi più importanti e conosciuti della computazione quantistica, affrontiamo l'analisi della crittografia quantistica, la quale mostra ancora una volta le potenzialità dei metodi quantistici rispetto a quelli classici.

### 3.1 Crittografia quantistica

Molti anni prima che fu introdotta la crittografia RSA<sup>i</sup> che utilizziamo oggigiorno, molte persone pensavano che gli stati quantistici e il *bizzarro* comportamento della QM potessero essere utilizzati per scopi crittografici. Il protocollo quantistico che fu pensato per trasmettere dati criptati è il **protocollo BB84**. Consideriamo, come al solito, Alice e Bob in differenti città e supponiamo che vogliano comunicare tra loro tramite una linea criptata. Vediamo come viene affrontato questo problema sia dal punto di vista classico che quantistico.

#### 3.1.1 Esempio di crittografia classica

Classicamente entrambi possiedono una sequenza  $S$  di bit casuali, chiamata **codepad**. Immaginiamo che Alice voglia inviare a Bob un messaggio  $M$ : un modo classico di inviare il messaggio criptato è quello di inviare la sequenza  $M \oplus S$ , dove il simbolo " $\oplus$ " indica l'**addizione bit a bit modulo 2**. Ad esempio supponiamo che il codepad sia  $S = 0110$  e il messaggio sia  $M = 1111$ : la sequenza  $M \oplus S$  è data da

$$\begin{array}{r|rrrr|r} S & 0 & 1 & 1 & 0 & = 6 \\ M & 1 & 1 & 1 & 1 & = 15 \\ \hline M \oplus S & 1 & 0 & 0 & 1 & = 9 \end{array}$$

dove nell'ultima colonna abbiamo inserito il numero associato a quel messaggio (ad esempio, leggendo da destra verso sinistra, per  $S$  si ha  $0 \times 2^0 + 1 \times 2^1 + 1 \times 2^2 + 0 \times 2^3 = 6$ ).

---

<sup>i</sup>Inventata nel 1977 da Ronald Rivest, Adi Shamir e Leonard Adleman.

Il vantaggio di questo modo di crittografare messaggi risiede nel fatto che, anche se si parte con una stringa  $M$  sensata, l'operazione  $M \oplus S$  la trasforma in una sequenza apparentemente casuale di 0 e 1 che può essere decifrata solamente se si possiede il codepad. Infatti, una volta che Bob riceve  $M \oplus S$ , si può facilmente ricostruire il messaggio originale calcolando  $(S \oplus M) \oplus S = M \oplus (S \oplus S) = M$  dato che

$$x \oplus x = \begin{cases} 0 \oplus 0 = 0 \\ 1 \oplus 1 = 0 \end{cases}, \quad \forall x.$$

Il problema di un tale protocollo crittografico, oltre al fatto che il codepad non debba essere scoperto da nessun altro al di fuori di Alice e Bob, risiede nel fatto che non sia molto efficiente essendo un **one-time codepad**, dato che la stringa  $S$  può essere utilizzata una volta sola. Per capirne il motivo supponiamo che Alice invii due messaggi  $M_1$  e  $M_2$ : la composizione dei due messaggi è  $(M_1 \oplus S) \oplus (M_2 \oplus S) = M_1 \oplus M_2$ , il quale è costituito da una sequenza di 0 e 1 abbastanza randomica. Supponiamo ora che i due messaggi vengano intercettati da qualcuno. Se costui è abbastanza abile e conosce almeno una parte del messaggio che Alice voleva inviare allora ci sono possibilità che riesca a decifrare  $M_1$  e  $M_2$  separatamente riconoscendo degli opportuni schemi in  $M_1 \oplus M_2$ ; tuttavia non è detto che chi intercetti il messaggio sia sempre così abile!

### 3.1.2 Il protocollo BB84

La versione quantistica viene chiamata **protocollo BB84**, sviluppato da Charles H. Bennett e Gilles Brassard nel 1984, ed è abbastanza simile al caso classico, ma molto più potente: lo scopo è quello di creare un codepad  $S$  che non possa essere in alcun modo (o quasi<sup>ii</sup>) intercettato da una terza persona, che chiameremo Eve, la quale vuole rovinare i piani di Alice e Bob. Il protocollo funziona come segue: Alice possiede una serie di qubit che vorrebbe inviare a Bob tramite un canale sicuro; invia allora casualmente dei qubit che sono preparati nella base computazionale  $C = \{|0\rangle, |1\rangle\}$  oppure nella base di Hadamard  $H = \{|+\rangle, |-\rangle\}$  (si vedano le (1.2.3)). Quindi Alice, prima di inviare i qubit, effettua due scelte: sceglie la base e poi sceglie uno stato di quella base da inviare. Nel frattempo, Bob riceve i qubit inviati e tiene attentamente conto dell'ordine di ricezione di questi qubit, dopodiché effettua una misurazione scegliendo randomicamente la base  $C$  oppure la base  $H$ <sup>iii</sup>. Dato che Bob sceglie una delle due basi, per ogni qubit che riceve ci sono due possibilità:

- Sceglie la stessa base di Alice. Ad esempio se Alice avesse scelto  $(C, |0\rangle)$  allora necessariamente, dai postulati della QM, sappiamo che Bob misura obbligatoriamente  $(C, |0\rangle)$  con probabilità 1 (nel caso in cui nessuno abbia intercettato il messaggio).
- Sceglie una base differente da quella di Alice. Ad esempio se Alice invia  $(C, |0\rangle)$  e Bob sceglie la base  $H$  allora sappiamo che ha il 50% di possibilità di trovare  $|0\rangle$  nella propria misurazione.

---

<sup>ii</sup>Si sfrutta la natura probabilistica della QM quindi, se i qubit inviati da Alice sono in gran numero, è solo una questione di tempo prima che una terza persona venga scoperta intercettare i messaggi. Si veda la discussione di seguito per chiarimenti più esplicativi.

<sup>iii</sup>Ad esempio, se Alice invia delle particelle dotate di spin, Bob può scegliere, mediante un apparato simile a quello dell'esperimento di Stern e Gerlach, di misurare lo spin lungo la direzione  $z$  (base  $C$ ) oppure lungo la direzione  $x$  (base  $H$ ).

Notiamo che i risultati ottenuti da Bob nelle proprie misurazioni non sono in alcun modo correlati con le informazioni che Alice vuole inviare. Riassumendo, gli step necessari sono i seguenti:

1. Alice sceglie una base e invia casualmente i qubit.
2. Bob riceve i qubit tenendo conto dell'ordine di arrivo e misura con il proprio apparato scegliendo casualmente una delle due basi.
3. Alice e Bob comparano **soltamente le basi** di un numero arbitrario di qubit concordato a priori dai due (alcuni e non tutti perché in generale Alice potrebbe inviare un numero altissimo di qubit) tramite una linea non sicura (ossia che può essere intercettata da Eve). Questo significa che per ogni qubit che confrontano, i due si scambiano la base in cui è stata effettuata la preparazione e la misura, non lo stato misurato.
4. La parte dei qubit che Bob ha misurato nella stessa base in cui sono stati preparati da Alice, viene usata per costruire un codepad comune (si veda l'Esempio 3.1).
5. Confrontando ulteriormente una **frazione sacrificabile** dei qubit che compongono il codepad, Alice e Bob possono stabilire se qualcuno ha intercettato i qubit inviati (si veda la discussione dopo l'Esempio 3.1).

Per capire al meglio il funzionamento di questo meccanismo illustriamolo con un esempio.

**Esempio 3.1.** *Immaginiamo che le basi scelte e i risultati delle misurazioni effettuate da Alice e Bob siano quelli mostrati nella Tabella 3.1.*

Alice	base	$\rightarrow$	C	H	H	C	C	H	C	H	C
	qubit	$\rightarrow$	0	1	0	0	0	0	1	0	1
Bob	base	$\rightarrow$	H	H	H	C	C	H	C	C	
	qubit	$\rightarrow$	1	1	0	0	0	0	1	1	1

Tabella 3.1: Basi scelte e rispettive misurazioni effettuate da Alice e Bob. Si noti che nelle righe dei qubit misurati si è indicato solamente il bit di informazione inviato da Alice o ottenuto da Bob, ossia:  $|0\rangle, |+\rangle \rightarrow 0$  e  $|1\rangle, |-\rangle \rightarrow 1$ . Nella tabella sono state colorate in grigio le colonne corrispondenti alle misurazioni effettuate nella medesima base.

*Una volta che Alice ha terminato<sup>iv</sup> la sequenza di qubit che voleva inviare, comunica a Bob, mediante un canale classico, la sequenza di basi scelte, ossia la prima riga della tabella: dalle regole della QM sappiamo che ogniqualvolta che Bob sceglie (per coincidenza) la medesima base di Alice, il risultato della misurazione che ottiene è obbligatoriamente il medesimo qubit che Alice ha scelto di inviare (a tal proposito si vedano infatti le colonne colorate). Notiamo che per una coincidenza fortuita le misurazioni nelle colonne 4 e 7 sono le medesime sebbene la base scelta fosse differente: in questa situazione, ossia*

<sup>iv</sup>In generale esistono varie versioni di questa procedura perché dal punto di vista pratico è molto difficile accumulare una sequenza di qubit mantenendoli tutti inalterati. Una versione alternativa più conveniente e realistica prevede Alice che invia il suo qubit e subito dopo comunica immediatamente la base che ha scelto, in maniera tale che una volta che Bob abbia ricevuto il qubit possa scartare quelli misurati in basi differenti.

*quando i due sperimentatori scelgono una base diversa, Bob ottiene casualmente 0 o 1 con probabilità 1/2. Una volta effettuata la chiamata, i due decidono di tenere solamente i risultati in cui hanno scelto le stesse basi e formano con tali misure un codepad comune: nella situazione della Tabella 3.1, solo le colonne colorate hanno la stessa base, quindi il codepad non è altro che  $S = 10001$ . Ovviamente questo codepad è comune perché Alice e Bob si sono scambiati, oltre alle basi, anche i qubit delle misure effettuate nella stessa base.*

Per quale ragione il codepad comune formato da Alice e Bob è più protetto di quello classico? Come interviene Eve nella trasmissione delle informazioni per capire ciò che è stato inviato? Eve può semplicemente intercettare il qubit durante il transito: dalla QM sappiamo che è obbligata ad effettuare una misurazione, la quale disturba inevitabilmente il sistema. Dato che Eve non conosce la base in cui il qubit è stato preparato è costretta a fare una scelta! Nel caso in cui sia fortunata, scegliendo cioè la stessa base di Alice, Eve vede il qubit inviato senza modificare lo stato, tuttavia quando sceglie la base opposta ottiene un numero casuale 0 o 1 con probabilità 1/2 e causa il collasso dello stato in uno dei due stati della base utilizzata.

Capiamo meglio questo discorso con un esempio.

**Esempio 3.2.** *Supponiamo che Alice abbia scelto di inviare  $(C, |0\rangle)$  e che Eve scelga di misurare nella base  $H$  ottenendo  $|+\rangle$ : lo stato è ora collassato in  $|+\rangle$ , quindi se Bob effettua una misurazione in  $C$ , egli può ottenere sia  $|0\rangle$  sia  $|1\rangle$  con probabilità 1/2, nonostante Alice avesse inviato  $(C, |0\rangle)$ . Se dovesse succedere che Bob misuri  $(C, |1\rangle)$ , allora Alice e Bob concludono che hanno misurato due stati differenti, nonostante abbiano scelto la medesima base, ma questo è impossibile dalla QM se nessuno è intervenuto sullo stato!*

A seguito del collasso dello stato in uno stato di una base differente da quella scelta da Alice, può accadere che nelle colonne colorate della Tabella 3.1 (misurazioni con stesse basi) i due sperimentatori ottengano uno stato differente: se nessuno sta intercettando gli stati in transito questo è impossibile per le leggi della QM! In questo modo, una volta comunicati i qubit misurati nelle stesse basi, Bob capisce che qualcuno ha interferito con i qubit che Alice sta inviando.

Statisticamente, quante volte Eve sta ascoltando sistematicamente il messaggio e vi è una possibilità che Alice e Bob non concordino su una misura effettuata nella stessa base? Tipicamente per 1/4 delle volte. Il motivo è dato dal fatto che Eve può essere fortunata e misurare nella stessa base di Alice (probabilità 1/2 per questa scelta) e inoltre anche se Eve sceglie la base sbagliata, Bob deve effettuare una misurazione in cui ottiene lo stesso qubit di Alice il 50% delle volte: quindi  $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$ , dove il primo 1/2 deriva dalla scelta di Eve e il secondo dalla misura di Bob.

La quantità di qubit che devono venire sacrificati per verificare se Eve sta ascoltando, comunicando attraverso una linea non sicura il risultato delle misurazioni, dipenderà dal grado di sicurezza richiesto. Per maggior efficienza, si potrà anche usare una linea classica criptata.

### 3.1.3 Quantum nondemolition measurement

Chiaramente ci si potrebbe domandare se Eve possa fare di meglio. Esiste una possibilità in cui possa misurare senza recare alcun disturbo allo stato? Delle volte queste misure vengono chiamate in letteratura **quantum nondemolition measurement**: si trattano

di particolari misure in cui Eve effettua la misurazione senza disturbare lo stato oppure disturba lo stato, ma è in grado di resettarlo all'originale inviato da Alice. La risposta alla domanda precedente è no per un motivo simile alla dimostrazione del teorema di no-cloning.

Supponiamo che Alice stia inviando l'insieme di stati  $|\phi_\mu\rangle = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ , dove  $\mu = 0, 1, 2, 3$ , e inoltre assumiamo che Eve possiede un proprio computer quantistico sul quale può effettuare operazioni. Nell'intercettare il messaggio, Eve osserva lo stato  $|\phi_\mu\rangle \otimes |\phi\rangle$ , dove  $|\phi\rangle$  si trova nel suo computer. Supponiamo inoltre che nel suo computer ci sia un altro insieme di stati  $|\psi_\mu\rangle$ , con  $\mu = 0, 1, 2, 3$ , tale che possa essere distinto da una misura effettuata da Eve stessa. La domanda è: esiste qualche sorta di processo quantistico (gate unitario  $U$ ) che agisce come

$$U(|\phi_\mu\rangle \otimes |\phi\rangle) = |\phi_\mu\rangle \otimes |\psi_\mu\rangle , \quad (3.1.1)$$

ossia tale che quando Eve misura  $|\psi_\mu\rangle$  e legge il valore  $\mu$  allora con probabilità 1 legge anche lo stesso  $\mu$  che Alice sta inviando, senza però disturbare  $|\phi_\mu\rangle$ ? La risposta è no, similmente al teorema di no-cloning. Per dimostrare questo fatto calcoliamo il prodotto scalare di ambo i membri della (3.1.1), il quale, come sappiamo a seguito dell'unitarietà di  $U$ , deve rimanere preservato:

$$\begin{aligned} (\langle \phi_\mu | \otimes \langle \phi |) (|\phi_\nu\rangle \otimes |\phi\rangle) &\stackrel{?}{=} (\langle \phi_\mu | \otimes \langle \psi_\mu |) (|\phi_\nu\rangle \otimes |\psi_\nu\rangle) , \quad \text{con } \mu \neq \nu \text{ in generale.} \\ \Rightarrow \quad \langle \phi_\mu | \phi_\nu \rangle \underbrace{\langle \phi | \phi \rangle}_1 &\stackrel{?}{=} \langle \phi_\mu | \phi_\nu \rangle \langle \psi_\mu | \psi_\nu \rangle , \quad \forall \text{ paia di indici } (\mu, \nu) . \end{aligned}$$

Analizziamo i casi in cui  $\mu \neq \nu$ . Quando  $(\mu = 2, \nu = 3)$  e  $(\mu = 0, \nu = 1)$  (o viceversa) si ha l'identità 0 = 0, che non è interessante (ricordare sopra gli stati  $|\phi_\mu\rangle$  di Alice). Nei casi invece  $(\mu = 0, \nu = 2)$ ,  $(\mu = 0, \nu = 3)$ ,  $(\mu = 1, \nu = 2)$  oppure  $(\mu = 1, \nu = 3)$  (o viceversa) i prodotti scalari  $\langle \phi_\mu | \phi_\nu \rangle$  non sono nulli e possono essere semplificati ad entrambi i membri. Per queste scelte otteniamo quindi che  $\langle \psi_\mu | \psi_\nu \rangle = 1$ , ossia  $|\psi_\mu\rangle = |\psi_\nu\rangle$  a meno di una fase. Ma questo significa allora che  $|\psi_0\rangle = |\psi_1\rangle = |\psi_2\rangle = |\psi_3\rangle$  e quindi, non essendo stati differenti, Eve non può in alcun modo distinguere ciò che ha inviato Alice.

La conclusione è che non esiste alcun modo di effettuare una misura con operazioni unitarie che distingua il qubit inviato da Alice senza necessariamente disturbare il sistema. Per comprendere al meglio il protocollo BB84 si può provare dal punto di vista pratico a realizzare la situazione di Alice e Bob (ed eventualmente di Eve) tramite una simulazione presente a [questo indirizzo](#).

## 3.2 Proprietà dei gate

Nella Sezione 1.5 abbiamo introdotto alcuni concetti preliminari riguardanti i gate, i circuiti e i computer quantistici. In molti casi nei computer si hanno degli algoritmi, ossia una ben precisa sequenza di istruzioni, che permettono di calcolare risultati desiderati. Approfondiamo le analogie e differenze dei gate classici e quantistici.

### 3.2.1 Gate classici: il Toffoli-gate

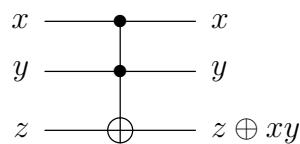
In CC si hanno i bit 0 e 1 e le funzioni classiche sono tali che  $f : \{0, 1\}^{\otimes n} \rightarrow \{0, 1\}^{\otimes m}$ , sono cioè mappe da  $n$  a  $m$  bit classici. Quindi in generale abbiamo una collezione di  $m$

funzioni a valori in un bit

$$f_i(x_1, x_2, \dots, x_n) = \{0, 1\}, \text{ dove } i = 1, \dots, m, \text{ e } x_j = 0, 1.$$

Si vorrebbe che il computer sia in grado di calcolare tali funzioni e che inoltre gli strumenti a disposizione siano sufficientemente efficienti per farlo: quello che uno vorrebbe è poter calcolare funzioni generali con l'ausilio di solamente pochi gate. In CC si ha che con le seguenti operazioni è possibile calcolare quasi tutti i conti di algebra e aritmetica: NOT,  $a \rightarrow -a$ ; AND, indicato con  $a \wedge b$  e OR, indicato con  $a \vee b$ . Questo insieme di operazioni è detto **universale** perché utilizzando questi pochi gate è possibile calcolare tutte le operazioni di aritmetica di interesse.

Sempre nella Sezione 1.5 abbiamo osservato che il CC **non** è **reversibile**<sup>v</sup> (in generale). Si pensi ad esempio all'**AND-gate**. Nel corso degli anni si sono studiati numerosi metodi per implementare operazioni reversibili: questo è possibile mediante il cosiddetto **Toffoli gate** o **Control-Control-NOT**. Il circuito classico è



Quando uno dei due tra  $x$  e  $y$  è 0, allora  $xy$  è 0 e niente succede all'output di  $z$ . L'output si modifica solamente quando sono 1 perché controllano entrambi il risultato di  $z$ : quando  $xy = 1$  allora  $z \oplus 1$  inverte il valore iniziale di  $z$ .

**Esempio 3.3** (Azione Toffoli gate). *In pratica il TOFFOLI-gate agisce come mostrato in Tabella 3.2:*

Bit iniziali			Bit finali		
$x$	$y$	$z$	$x$	$y$	$z \oplus xy$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

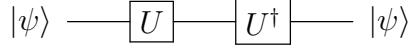
Tabella 3.2: Azione del TOFFOLI-gate su tutti i possibili bit.

È possibile dimostrare che mediante l'uso del **TOFFOLI-gate** si possono realizzare tutte le operazioni base, quindi è universale e reversibile. Notiamo che è reversibile poiché, come evidenziato nelle ultime due righe della Tabella 3.2, esso agisce sulle stringhe facendo una **permutazione**, la quale è invertibile.

<sup>v</sup>Si pensi ad esempio al fatto che le operazioni non reversibili dissipino calore all'interno della macchina. Si tratta di tutte quelle situazioni in cui si parte con molta informazione e si giunge alla fine ad un singolo risultato, creando nel frattempo numerosi risultati di scarto.

### 3.2.2 Gate quantistici: reversibili e continui

Consideriamo ora il caso dei gate quantistici. Per definizione, essendo implementati da operatori unitari, sono sempre dei gate **reversibili**. Questo significa ad esempio che



dato che  $UU^\dagger = \mathbb{I}$ . È possibile implementare il **TOFFOLI-gate** anche in un computer quantistico? La risposta è sì: consideriamo una base di stati per 3 qubit

$$\{|000\rangle, |001\rangle, |010\rangle, |100\rangle, |101\rangle, |011\rangle, |110\rangle, |111\rangle\}.$$

La matrice unitaria  $U_T$   $8 \times 8$  che agisce sul vettore contenenti gli stati della base è

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} |000\rangle \\ |001\rangle \\ |010\rangle \\ |100\rangle \\ |101\rangle \\ |011\rangle \\ |110\rangle \\ |111\rangle \end{pmatrix} = \begin{pmatrix} |000\rangle \\ |001\rangle \\ |010\rangle \\ |100\rangle \\ |101\rangle \\ |011\rangle \\ |111\rangle \\ |110\rangle \end{pmatrix}.$$

Notiamo infatti che  $U_T$  è unitaria ( $U_T U_T^\dagger = \mathbb{I}$ ). Tramite  $U_T$  possiamo realizzare su un computer quantistico le stesse operazioni che faremmo su un computer classico. Fino ad ora non abbiamo ancora detto se effettivamente queste operazioni possano essere eseguite in maniera più efficiente su un QC.

Il secondo fatto importante dei gate quantistici è che sono **continui**: matrici unitarie possono dipendere da parametri reali continui. Ad esempio, per un sistema di 1 qubit abbiamo visto nella (1.5.4) come si scrive la più generale matrice  $2 \times 2$  unitaria (gruppo  $U(2)$ ) tramite l'implementazione delle rotazioni di angolo  $\lambda$  sulla sfera di Bloch e lungo la direzione generica  $\vec{n}$  (si veda la (1.5.3)). Abbiamo visto che la (1.5.4) dipende in generale da 4 parametri reali arbitrari, quindi persino per un singolo qubit si ha un insieme continuo di gate! Il problema è che le cose si complicano notevolmente se si passa ad un sistema generico di  $n$ -qubit. In tale situazione lo spazio di Hilbert associato ha dimensione  $2^n$ , quindi le matrici unitarie che agiscono su tale spazio sono  $2^n \times 2^n$ , le quali formano il gruppo  $U(2^n)$ . Ognuna di queste matrici contiene in generale  $2^{2n}$  parametri reali! Il problema è quindi dato dal fatto che il numero di parametri cresce esponenzialmente con il numero di qubit: il numero di gate è estremamente grande e non vogliamo un QC in cui possiamo implementare qualsiasi trasformazione con  $2^{2n}$  parametri reali. Una tale situazione è troppo difficile da realizzare, tuttavia preferiamo considerare un numero limitato di gate e costruire le operazioni desiderate tramite composizione. Si noti inoltre che un insieme continuo di operazioni è impossibile per la memoria limitata di un computer.

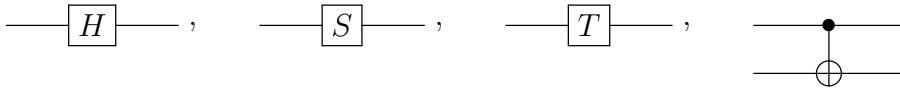
Il meglio che possiamo fare è introdurre una nozione di **universalità** e approssimare abbastanza bene una generica trasformazione unitaria utilizzando solamente un insieme finito di gate. Qual è il significato di tale approssimazione? Dobbiamo definire un'opportuna nozione di **distanza** tra matrici:

**Definizione 3.1 (Distanza tra matrici).** Date due matrici  $U$  e  $V$ , definiamo la seguente funzione *distanza*

$$E(U, V) = \max_{|\psi\rangle} \|(U - V)|\psi\rangle\|,$$

dove  $|\psi\rangle$  è un vettore arbitrario.

È possibile trovare un insieme discreto di matrici tale che tutte le possibili matrici unitarie possano essere realizzate a partire da tale insieme a meno di un errore  $\varepsilon$  arbitrario? La risposta è sì: un possibile insieme di gate che soddisfa la precedente nozione di "approssimazione universale" è dato dai seguenti 4



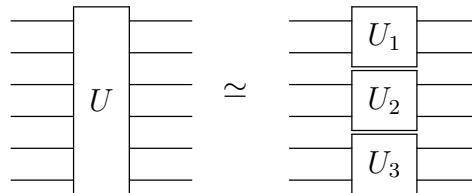
Si vedano esplicitamente le matrici in (1.5.1) e (1.5.2). Questi gate prendono il nome di **H-gate**  $H$  (Hadamard gate), **Phase-gate**  $S$ ,  $\pi/8$ -gate  $T$  e il già noto **CNOT-gate**. Si noti che il nome della matrice  $T$  deriva dal fatto che

$$T = e^{i\frac{\pi}{8}} \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix}.$$

Non lo dimostriamo esplicitamente, ma l'insieme di questi 4 gate è universale. È importante sottolineare che  $H$ ,  $S$  e  $T$  sono gate agenti sui singoli qubit, mentre il **CNOT-gate** agisce sempre su almeno 2 qubit. Dato che avevamo visto che  $T^2 = S$  potrebbe sorgere spontanea la domanda: perché è necessario considerare entrambi  $T$  e  $S$ ? Di solito si preferisce tenere anche  $S$  per la cosiddetta **fault tolerance computation**, che approfondiremo quando parleremo di propagazione degli errori nei circuiti quantistici. Alcune importanti proprietà che ci servirà sapere sui gate quantistici sono le seguenti:

1. Tutti i gate agenti su  $n$  qubit possono essere scritti come prodotto di un opportuno numero di gate agenti su 2 qubit.

Chiaramente il numero di gate agenti su 2 qubit deve essere sufficientemente grande per ricostruire una matrice  $2^n \times 2^n$  (matrice agente su  $n$  qubit). Per capire il significato di questa affermazione si pensi al circuito seguente di 6 qubit:



In questo esempio il gate originale  $U$  è stato approssimato fattorizzandolo in 3 gate agenti ciascuno localmente solo su 2 qubit: il numero di operazioni per ricostruire la matrice  $2^n \times 2^n$  del circuito a LHS è di ordine  $\mathcal{O}(2^{2n})$ . Chiaramente si tratta solamente di algebra: questo non è un modo molto efficiente di approssimare un gate agente su  $n$  qubit perché tipicamente si hanno comunque  $2^{2n}$  fattori da tenere in considerazione.

2. I gate agenti su 2 qubit possono essere scritti come prodotti di un certo numero di CNOT-gate e di gate agenti su un singolo qubit.

In termini di circuiti stiamo dicendo che la generica matrice  $U_4 \in U(4)$  può essere decomposta in prodotti di operazioni più semplici, CNOT-gate e matrici  $U_2 \in U(2)$

$$\begin{array}{c} \text{---} \\ \text{---} \end{array} \boxed{U_4} \begin{array}{c} \text{---} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \text{---} \end{array} \bullet \begin{array}{c} \text{---} \\ \oplus \end{array} \begin{array}{c} \text{---} \\ \text{---} \end{array} + \begin{array}{c} \text{---} \\ \text{---} \end{array} \boxed{U_2} \begin{array}{c} \text{---} \\ \text{---} \end{array}$$

Notiamo che questa proprietà, come la precedente, è esatta e può essere svolta senza alcuna approssimazione. In generale potrebbe essere più efficiente approssimare un gate piuttosto che usare una rappresentazione esatta come prodotto di un numero di elementi che potrebbe essere grande. In questo contesto è possibile dimostrare che si può approssimare ogni matrice di  $SU(4)$  come prodotto di generiche matrici  $A, B \in SU(4)$  con  $[A, B] \neq 0$  (la proprietà può essere falsa per coppie speciali di matrici), in analogia con la discussione della proprietà seguente.

3. I gate agenti sui singoli qubit possono essere approssimati come prodotto di matrici  $H$  e  $T$  con un errore, il quale può essere arbitrariamente scelto più piccolo di  $\varepsilon$ .

Questo significa che data  $V$  la generica matrice unitaria  $2 \times 2$  da approssimare (ricordare che contiene  $2^2 = 4$  parametri reali) possiamo scrivere un'opportuna sequenza di prodotti tra  $H$  e  $T$  tali che

$$E(V, \dots HHTH \dots T \dots H \dots) < \varepsilon.$$

Chiaramente più lunga è la sequenza più piccolo sarà l'errore entro il quale si può approssimare  $V$ . In realtà  $H$  e  $T$  non sono matrici speciali: questo argomento funziona con una coppia generica di matrici  $A, B \in SU(2)$  tali che  $[A, B] \neq 0$ . Matematicamente questa proprietà è dovuta al fatto che il sottogruppo generato dai prodotti di  $H$  e  $T$  è **denso** in  $SU(2)$ . Notiamo l'importanza di usare  $T$ : la coppia  $H, S$  è non generica; il sottogruppo generato dai prodotti di  $H$  e  $S$  è infatti un sottogruppo discreto che non è denso in  $SU(2)$ .

Ci si può chiedere se un'approssimazione mediante prodotti di  $H$  e  $T$  possa essere efficiente. Ancora una volta, fortunatamente la risposta è sì: esiste un teorema, chiamato **teorema di Solovay-Kitaev**, che stabilisce che il numero di prodotti tra  $H$  e  $T$  per approssimare una generica matrice di  $U(2)$  è dell'ordine di  $\mathcal{O}(\log_{10}^c(1/\varepsilon))$  dove  $c \sim 2$ .

### 3.3 Quantum Parallelism

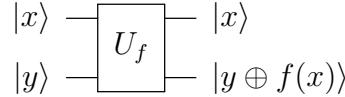
**Definizione 3.2 (Quantum Parallelism).** Il **quantum parallelism** è una delle caratteristiche fondamentali di molti algoritmi quantistici. Consente ai computer quantistici di valutare una funzione  $f(x)$  per molti valori diversi di  $x$  contemporaneamente.

Supponiamo di considerare la più semplice funzione possibile  $f(x) : \{0, 1\}^{\otimes n} \rightarrow \{0, 1\}$  definita su un dominio (insieme di numeri costruiti con  $n$  cifre di 0 e 1) e a elementi in un intervallo di bit. Assumiamo inoltre di saper calcolare efficientemente nel nostro computer tale funzione. Ciò che calcoliamo, dal punto di vista della computazione classica, lo possiamo valutare nella computazione quantistica, pertanto tutte le operazioni aritmetiche possono essere svolte dal calcolo quantistico. Un modo quindi di calcolare questa funzione su un computer quantistico è quello di considerare due differenti stati: immaginiamo un qubit  $|y\rangle$  e uno stato che può essere un prodotto tensoriale di qubit, come ad esempio  $|0\rangle^{\otimes n}$ . Spesso considereremo lo stato  $|0\rangle^{\otimes n}$  come stato iniziale in cui il computer quantistico viene preparato mediante una misurazione nella base computazionale perché è facilmente costruibile: ad esempio nel caso  $n = 3$  se, a seguito di una misurazione, lo stato nel QC collassa in  $|\psi\rangle \rightarrow |1\rangle \otimes |0\rangle \otimes |1\rangle$ , basterà applicare un X-gate al primo e al terzo qubit per costruire lo stato voluto  $|0\rangle^{\otimes 3}$ .

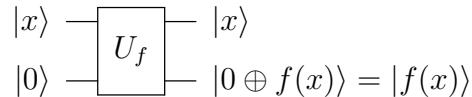
Chiamiamo lo stato iniziale totale  $|x, y\rangle$ , dove  $x$  contiene l'informazione iniziale data in input e  $y$  conterrà, dopo delle opportune operazioni, il risultato cercato. Con un'appropriata sequenza di gate è possibile effettuare la trasformazione

$$|x, y\rangle \xrightarrow{U_f} |x, y \oplus f(x)\rangle , \quad (3.3.1)$$

dove  $U_f$  è un opportuno gate unitario che implementa l'operazione desiderata. Il circuito che implementa la (3.3.1) è



dove  $|x\rangle$  prende il nome di **data register** e  $|y\rangle$  prende il nome di **target register**. Questa rappresentazione è utile perché quando  $|y\rangle = |0\rangle$  l'output del target register è esattamente l'oggetto che si vuole calcolare



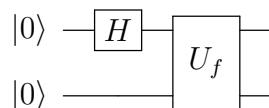
Notiamo che la (3.3.1) è invertibile: se applichiamo  $U_f$  due volte, otteniamo:

$$|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle \rightarrow |x, y \oplus f(x) \oplus f(x)\rangle = |x, y\rangle ,$$

siccome  $f(x) \oplus f(x) = 0$  indipendentemente dai valori di  $f$ . Fino ad ora avremmo potuto effettuare tutte queste operazioni in CC. L'importanza del QC risiede nel fatto che si possano considerare sovrapposizioni di stati appartenenti ad una base. Consideriamo il caso  $n = 1$  (il data register è un qubit) e assumiamo il seguente stato iniziale

$$|x, y\rangle \equiv \underbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}_{|x\rangle} \otimes \underbrace{|0\rangle}_{|y\rangle} = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) ;$$

Se assumiamo che il computer sia preparato in  $|0\rangle \otimes |0\rangle$  come possiamo rappresentare  $|x, y\rangle$  in un circuito? Possiamo sfruttare l'H-gate in questo modo:



infatti, utilizzando la (3.3.1), avremo

$$|0, 0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{U_f} \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle).$$

Questo circuito è particolarmente interessante perché l'output è una sovrapposizione di differenti stati contenenti informazioni riguardo la funzione:  $f(0)$  e  $f(1)$  appaiono simultaneamente nel medesimo stato. È come se avessimo valutato  $f(x)$  per due valori di  $x$  contemporaneamente, parallelamente! A differenza del classic parallelism, in cui più circuiti vengono costruiti per calcolare  $f(x)$  ed eseguiti simultaneamente, qui viene impiegato un singolo circuito per valutare la funzione  $f(x)$  per più valori di  $x$  nello stesso momento: si sta sfruttando la capacità di un computer quantistico di essere in sovrapposizioni di stati diversi. Qui risiede il **quantum parallelism**.

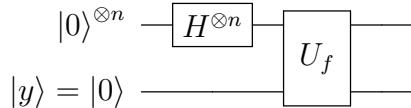
Questo discorso può essere facilmente generalizzato al caso di  $n$ -qubit. Supponiamo che il data register si trovi in  $|0\rangle^{\otimes n}$ . Usiamo il fatto che l'azione dell'H-gate su  $n$ -qubit possa essere scritta nel seguente modo:

$$\begin{aligned} H^{\otimes n} |0\rangle^{\otimes n} &= \underbrace{H \otimes \cdots \otimes H}_{n\text{-volte}} |0\rangle \otimes \underbrace{\cdots \otimes |0\rangle}_{n\text{-volte}} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^n}}(|000\dots 0\rangle + |010\dots 0\rangle + \dots + |111\dots 1\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle, \end{aligned} \quad (3.3.2)$$

dove  $x$  rappresenta tutte le possibili stringhe di  $n$ -volte 0 e 1. Se il target si trova in  $|y\rangle = |0\rangle$  e applichiamo ora  $U_f$ , il risultato è:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle,$$

dove si è fatto uso della (3.3.1) con  $|y\rangle = |0\rangle$ . In termini di circuiti avremo



In un certo senso, il quantum parallelism consente di valutare simultaneamente tutti i possibili valori della funzione  $f(x)$ , anche se apparentemente abbiamo valutato  $f(x)$  in una singola volta. Precisiamo che la misura dello stato nel caso del qubit singolo ci darà solamente  $|0, f(0)\rangle$  oppure  $|1, f(1)\rangle$ . In maniera analoga per il caso generale, la misura dello stato  $\sum_x |x, f(x)\rangle$  ci darà un solo  $f(x_0)$  per un singolo valore casuale  $x_0$ . Ovviamente un computer classico può farlo più facilmente! La computazione quantistica richiede qualcosa di più del semplice quantum parallelism per essere utile; richiede cioè la capacità di estrarre informazioni su più di un valore di  $f(x)$  da stati di sovrapposizione, come  $\sum_x |x, f(x)\rangle$ . Come vedremo nella prossima sezione, il trucco di considerare una sovrapposizione lineare ci permetterà di estrarre alcune informazioni su  $f$  in un modo più efficiente del CC.

## 3.4 Algoritmo di Deutsch

Una semplice modifica del circuito precedente dimostra come i circuiti quantistici possano essere più performanti rispetto a quelli classici. Nelle ultime righe del paragrafo

precedente abbiamo detto che la computazione quantistica richiede qualcosa di più oltre al quantum parallelism per essere utilizzabile. L'**algoritmo di Deutsch** combina il meccanismo del **quantum parallelism** con la proprietà della meccanica quantistica dell'**interferenza**.

Si tratta di un algoritmo un po' accademico (le funzioni sono banali), tuttavia utile per illustrare l'idea di algoritmo quantistico. Lasciamo che entrambi input e output register contengano ciascuno un solo qubit, quindi stiamo esplorando le funzioni  $f(x)$  che convertono un singolo bit in un singolo bit:  $f(x) : \{0, 1\} \rightarrow \{0, 1\}$ . Ci sono due modi piuttosto diversi di pensare a tali funzioni. Il primo modo è notare che ci sono solo quattro di queste funzioni, come mostrato nella Tabella 3.3.

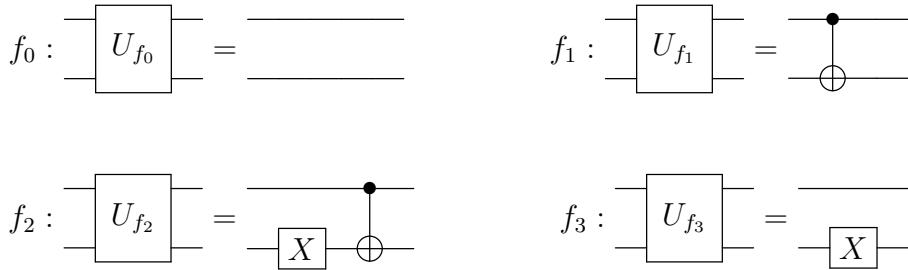
	$x = 0$	$x = 1$
$f_0$	0	0
$f_1$	0	1
$f_2$	1	0
$f_3$	1	1

Tabella 3.3: Possibili output delle sole quattro funzioni distinte  $f_j(x)$  che convertono un bit in un bit. Esse sono tutte facilmente implementabili sia in un computer classico che quantistico.

Supponiamo che ci venga data una black-box (ossia un gate ignoto che indicheremo con **U-gate**) che calcola una di queste quattro funzioni eseguendo la seguente trasformazione unitaria:

$$U_{f_j} |x, y\rangle = |x, y \oplus f_j(x)\rangle .$$

In questo caso, se implementiamo in circuiti la Tabella 3.3 avremo:



Dato che la regola che vogliamo implementare è  $|x, 0\rangle \rightarrow |x, f(x)\rangle$  ( $|y\rangle$  inizializzato a  $|0\rangle$ ), in termini matematici questo significa scrivere:

$$\begin{aligned} f_0 : & \quad |x, 0\rangle \longrightarrow |x, 0\rangle , \\ f_1 : & \quad |x, 0\rangle \xrightarrow{\text{CNOT}} \begin{cases} |0, 0\rangle , & \text{per } x = 0 \\ |1, 1\rangle , & \text{per } x = 1 \end{cases} , \\ f_2 : & \quad |x, 0\rangle \xrightarrow{X} |x, 1\rangle \xrightarrow{\text{CNOT}} \begin{cases} |0, 1\rangle , & \text{per } x = 0 \\ |1, 0\rangle , & \text{per } x = 1 \end{cases} , \\ f_3 : & \quad |x, 0\rangle \xrightarrow{X} |x, 1\rangle , \end{aligned}$$

Supponiamo che ci venga data una black-box che esegua  $U_f$  per una delle quattro funzioni, ma non ci venga detto quale delle quattro operazioni. Ovviamente possiamo scoprirla

lasciando agire due volte la black-box, prima su  $|0\rangle\otimes|0\rangle$  e poi su  $|1\rangle\otimes|0\rangle$ . Ma supponiamo di poter far agire la black-box solo una volta. Cosa possiamo conoscere di  $f(x)$ ?

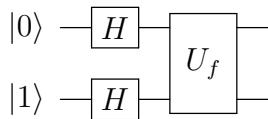
In un computer classico, dove siamo effettivamente limitati a lasciare che la black-box agisca sui qubit in uno dei quattro stati di base computazionale, possiamo conoscere il valore di:

- $f(0)$ , lasciando che  $U_f$  agisca su uno dei due  $|0\rangle\otimes|0\rangle$  o  $|0\rangle\otimes|1\rangle$ ;
  - In tal caso possiamo limitare la scelta a  $f_0$  o  $f_1$  (se  $f(0) = 0$ ) oppure  $f_2$  o  $f_3$  (se  $f(0) = 1$ ).
- $f(1)$ , lasciando che  $U_f$  agisca su  $|1\rangle\otimes|0\rangle$  o  $|1\rangle\otimes|1\rangle$ ;
  - In questa situazione abbiamo ristretto la funzione ad essere  $f_0$  o  $f_2$  (se  $f(1) = 0$ ) oppure  $f_1$  o  $f_3$  (se  $f(1) = 1$ ).

In definitiva, un computer classico necessita di due esecuzioni per determinare se  $f$  sia costante o meno. Sorprendentemente, risulta che con un computer quantistico questo non è necessario perché il problema può essere risolto con una singola esecuzione. Il punto interessante è che l'algoritmo non riguarda il calcolo preciso della funzione, ma piuttosto la comprensione di una o più sue proprietà: quando l'algoritmo viene lanciato non impariamo nulla sui valori individuali di  $f(0)$  e  $f(1)$ , ma siamo comunque in grado di rispondere alla domanda sui loro valori relativi. Chiaramente otteniamo meno informazioni di quelle che otterremmo rispondendo alla domanda con un computer classico, ma, rinunciando alla possibilità di acquisire quella parte dell'informazione che è irrilevante per la domanda a cui vogliamo rispondere, possiamo ottenere la risposta con una sola applicazione di  $U_f$ . Come sottolineato in precedenza l'algoritmo combina il quantum parallelism e l'interferenza: possiamo preparare il computer nello stato  $|0\rangle\otimes|1\rangle$  della base canonica e applicare l'H-gate a entrambi i qubit:

$$(H \otimes H) |0\rangle \otimes |1\rangle = \underbrace{\frac{|0\rangle + |1\rangle}{\sqrt{2}}}_{\text{quantum parallelism}} \otimes \underbrace{\frac{|0\rangle - |1\rangle}{\sqrt{2}}}_{\text{interferenza}}; \quad (3.4.1)$$

in un circuito significa scrivere



Chiamando per semplicità  $|x\rangle \equiv \{|0\rangle, |1\rangle\}$  e applicando  $U_f$  alla (3.4.1) tramite (3.3.1), possiamo esplicitamente vedere che cosa implica il termine di interferenza:

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

Combinando i due casi in un'unica espressione compatta abbiamo ottenuto

$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{U_f} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \quad (3.4.2)$$

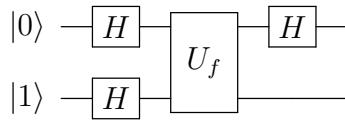
Sostituendo  $|x\rangle$  con lo stato iniziale che implementava il quantum parallelism avremo

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{U_f} \frac{1}{\sqrt{2}} [(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle] \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}};$$

dato che il segno relativo nella parentesi quadra dipende dal fatto che  $f(0)$  e  $f(1)$  siano uguali o meno, possiamo riscrivere quest'ultima espressione come

$$\begin{cases} (-1)^{f(0)} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}, & \text{per } f(0) = f(1) \\ (-1)^{f(0)} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}, & \text{per } f(0) \neq f(1) \end{cases}.$$

Come ultimo passaggio si applica l'**H-gate** al primo qubit in maniera tale che il circuito totale diventi:



Questa modifica trasforma il risultato precedente in

$$\begin{cases} (-1)^{f(0)} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{H} (-1)^{f(0)} |0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}, & \text{per } f(0) = f(1) \\ (-1)^{f(0)} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{H} (-1)^{f(0)} |1\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}, & \text{per } f(0) \neq f(1) \end{cases}.$$

Il risultato finale ci suggerisce che possiamo effettuare solamente una misurazione sul primo qubit: ottenendo  $|0\rangle$  o  $|1\rangle$  siamo in grado, con una singola misura, di stabilire se  $f(0) = f(1)$  oppure  $f(0) \neq f(1)$ . Questo significa che siamo in grado di escludere 2 delle 4 funzioni con una singola esecuzione dell'algoritmo.

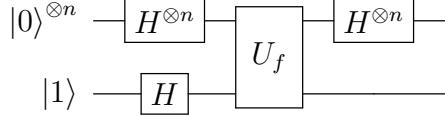
Questo esempio permette di evidenziare quale sia la differenza tra il quantum parallelism e gli algoritmi randomizzati classici. Ingenuamente, si potrebbe pensare che lo stato finale corrisponda piuttosto a un calcolatore classico probabilistico che valuta  $f(0)$  con probabilità  $\frac{1}{2}$ , o  $f(1)$  con probabilità  $\frac{1}{2}$ . La differenza è che in un computer classico queste due alternative si escludono sempre mentre in un computer quantistico è possibile che le due alternative interferiscano l'una con l'altra per ottenere alcune proprietà globali della funzione  $f(x)$ . Utilizzando un opportuno gate (nel nostro caso l'**H-gate**) siamo in grado di ricombinare le diverse alternative.

### 3.5 Algoritmo di Deutsch-Jozsa

L'algoritmo di Deutsch è un semplice caso di un algoritmo quantistico più generale, noto come **algoritmo di Deutsch-Jozsa**, che evidenzia esplicitamente come il QC offra un grosso miglioramento rispetto ai metodi del CC. Supponiamo di avere una black-box che calcoli una funzione booleana  $f(x) : \{0, 1\}^{\otimes n} \rightarrow \{0, 1\}$  e supponiamo di sapere per certo che  $f(x)$  sia solamente una delle seguenti alternative:

- **Funzione costante (constant):** l'output è sempre 0 oppure 1 indipendentemente dall'input.
- **Funzione bilanciata (balanced):** l'output è costituito per metà dal valore 0 e metà dal valore 1.

Lo scopo dell'algoritmo è quello di capire quale delle due sia l'alternativa corretta con il minor numero di esecuzioni. Classicamente potremmo risolvere questo problema calcolando  $2^{n-1} + 1$  valori della funzione perché è necessario calcolare almeno una metà dei valori più un valore aggiuntivo. Chiaramente si tratta di un numero esponenzialmente grande. Quello che fa l'algoritmo di Deutsch-Jozsa è risolvere il problema perfettamente con una sola query quantistica. Cominciamo scrivendo il circuito che descrive tale algoritmo, il quale è molto simile a quello di Deutsch con la sola differenza che il data register non è un singolo qubit, ma piuttosto un prodotto tensoriale di  $n$ -qubit:



Vediamo nello specifico cosa succede all'interno del circuito:

1. Viene inizializzato (preparato) lo stato in  $|0\rangle^{\otimes n} \otimes |1\rangle$ ;
2. Creiamo una sovrapposizione di stati usando l'H-gate su tutti gli  $n + 1$  qubit:

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

dove si è fatto uso della (3.3.2). Notiamo che ora nell'output register è presente lo stato che nella sezione precedente avevamo visto essere associato all'interferenza.

3. Valutiamo la funzione  $f(x)$  usando la black-box di  $U_f$

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{U_f} \sum_{x=0}^{2^n-1} \frac{(-1)^{f(x)}}{\sqrt{2^n}} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

dove, essendo  $|x\rangle$  arbitrario, abbiamo fatto uso della (3.4.2).

4. Applichiamo nuovamente l'H-gate ai primi  $n$  qubit. Per capire il risultato di  $H^{\otimes n} |x\rangle$  consideriamo per semplicità il caso  $n = 1$ : formalmente avremo

$$H|x\rangle = \sum_{z=0}^1 \frac{(-1)^{xz}}{\sqrt{2}} |z\rangle, \quad \text{dove } x = 0 \text{ oppure } 1.$$

Per  $n$  generico possiamo generalizzare scrivendo

$$\begin{aligned} H^{\otimes n} |x\rangle &= (H \otimes \dots \otimes H) |x_0\rangle \otimes |x_1\rangle \otimes \dots \otimes |x_{n-1}\rangle \\ &= \sum_{z_0=0}^1 \dots \sum_{z_{n-1}=0}^1 \frac{(-1)^{x_0 z_0} (-1)^{x_1 z_1} \dots (-1)^{x_{n-1} z_{n-1}}}{\sqrt{2^n}} |z\rangle, \end{aligned}$$

dove  $|z\rangle \equiv |z_0, z_1, \dots, z_{n-1}\rangle$ . In maniera più compatta possiamo scrivere quindi l'azione dell'H-gate sugli  $n$  qubit (nonché risultato finale del circuito) come

$$\sum_{z=0}^{2^n-1} \sum_{x=0}^{2^n-1} \frac{(-1)^{f(x)+x \cdot z}}{2^n} |z\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \tag{3.5.1}$$

dove abbiamo indicato con  $x \cdot z$  il **prodotto bit a bit modulo 2**:

$$x \cdot z = (x_0 z_0 + \dots + x_{n-1} z_{n-1}) \mod 2.$$

5. Infine misuriamo per ottenere lo stato finale  $|z\rangle$ .

Ricordiamo che il problema è quello di determinare se  $f$  sia constant o balanced. Notiamo dal risultato in (3.5.1) che il data register ora contiene una sovrapposizione lineare di tutti i possibili stati che si scrivono come stringhe contenenti  $n$  volte 0 e 1. In  $|z\rangle$  è presente un caso particolare: consideriamo la situazione in cui  $|z\rangle = |00\dots 0\rangle = |0\rangle^{\otimes n}$  e cerchiamo la probabilità di ottenere tale stato guardando il modulo quadro del coefficiente:

$$P(|z\rangle = |0\rangle^{\otimes n}) = \left| \sum_{x=0}^{2^n-1} \frac{(-1)^{f(x)}}{2^n} \right|^2 = \begin{cases} 1, & \text{se } f(x) \text{ è constant} \\ 0, & \text{se } f(x) \text{ è balanced} \end{cases}.$$

Notiamo che quando la probabilità è 1 a numeratore si hanno  $2^n$  termini tutti uguali ( $(-1)^1$  oppure  $(-1)^0$ ) che si semplificano con il fattore  $1/2^n$ ; quando invece la probabilità è nulla a numeratore si ha uno stesso numero di  $(-1)^1$  e  $(-1)^0$  che si cancellano esattamente. Come abbiamo detto  $|z\rangle = |0\rangle^{\otimes n}$  è un caso particolare molto importante perché permette di risolvere il problema mediante la misura dello stato. Se misurando  $z$  otteniamo  $|0\rangle^{\otimes n}$  allora, con probabilità 1 (quindi sempre), lo stato è  $|0\rangle^{\otimes n}$  e la funzione è constant; al contrario quando la misura di  $z$  produce un qualsiasi stato differente da  $|0\rangle^{\otimes n}$  allora, necessariamente  $P(|z\rangle = |0\rangle^{\otimes n}) = 0$ , lo stato  $|0\rangle^{\otimes n}$  non è nemmeno presente in  $z$  e possiamo stabilire con assoluta certezza che la funzione è balanced. Il fatto importante è che essendo queste misure mutualmente esclusive, possiamo determinare se  $f$  sia constant o balanced con una singola misurazione. Quindi si tratta di effettuare una sola misurazione in QC contro  $\mathcal{O}(2^n)$  misure in CC.

Osserviamo che il confronto tra algoritmi classici e quantistici è in qualche modo un confronto delicato, poiché il metodo per valutare la funzione è abbastanza diverso nei due casi. Se fosse consentito utilizzare un computer probabilistico classico, per valutare  $f(x)$  per pochi  $x$  scelti a caso, si può determinare molto rapidamente con alta probabilità se  $f(x)$  è *constant* o *balanced*. Questo scenario probabilistico è forse più realistico dello scenario deterministico che abbiamo considerato.

Ribadiamo nuovamente che questo algoritmo è un esempio molto accademico in quanto non esistono problemi fisici o matematici reali che necessitano di sapere se una funzione sia constant o balanced. Nonostante ciò il fatto importante è che grazie a questo algoritmo quantistico non è più necessario aspettare un tempo esponenzialmente<sup>vi</sup> crescente nel numero di bit per sapere il risultato.

## 3.6 Algoritmo di Bernstein-Vazirani

Consideriamo un altro algoritmo di black-box per il quale gli algoritmi quantistici forniscono un vantaggio: l'**algoritmo di Bernstein-Vazirani**. Qui, a differenza dei due casi precedenti, abbiamo accesso alla funzione della black-box  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ . Supponiamo che la funzione sia data da<sup>vii</sup>:

$$f(x) = a \cdot x = (a_0 x_0 + \dots + a_{n-1} x_{n-1}) \mod 2, \quad \text{dove } a \geq 0 \text{ e } x < 2^n.$$

---

<sup>vi</sup>Talvolta non si vuole sapere con precisione assoluta se  $f$  sia constant o balanced, ma è sufficiente stabilirlo entro un errore dato  $\varepsilon$ . Un ipotetico algoritmo classico e probabilistico di questo tipo diventa di ordine polinomiale in  $n$ : passare da  $\mathcal{O}(\text{polinomio in } n)$  a  $\mathcal{O}(1)$  mediante la controparte quantistica non è più un miglioramento così estremo come passare da  $\mathcal{O}(2^n)$  ad  $\mathcal{O}(1)$ !

<sup>vii</sup>Come prima il simbolo "·" indica il prodotto bit a bit modulo 2

Sappiamo che la funzione è lineare, tuttavia l'obiettivo di questo algoritmo è trovare il valore di  $a$ . Classicamente, questo problema potrebbe richiedere  $n$  query poiché ogni query può fornire solo un nuovo bit di informazioni su  $a$ , ma  $a$  possiede  $n$  bit: dobbiamo valutare  $f(1000\dots) = a_0$ ,  $f(0100\dots) = a_1$  e così via con  $n$  valutazioni fino a  $f(111\dots1) = a_{n-1}$ . L'algoritmo di Bernstein-Vazirani, invece, risolve il problema quantisticamente utilizzando una sola query!

Consideriamo il medesimo circuito dell'algoritmo di Deutsch-Josza e il suo output in (3.5.1): nel caso in cui  $f(x) = a \cdot x$  esso diventa

$$\sum_{z=0}^{2^n-1} \sum_{x=0}^{2^n-1} \frac{(-1)^{x \cdot (a+z)}}{2^n} |z\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Come nell'algoritmo precedente guardiamo il coefficiente di  $|z\rangle$ :

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{x \cdot (a+z)} = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{x_0(a_0+z_0) + \dots + x_{n-1}(a_{n-1}+z_{n-1})} = \frac{1}{2^n} \prod_{j=0}^{n-1} \left( \sum_{x_j=0}^1 (-1)^{x_j(a_j+z_j)} \right),$$

ma ogni termine nella parentesi tonda è la somma di termini che possono essere  $\pm 1$  a seconda dell'esponente. Distinguiamo i due casi:

- Se  $(a_j + z_j = 0) \pmod 2$  allora il coefficiente è

$$\frac{1}{2^n} \prod_{j=0}^{n-1} (2) = 1, \Rightarrow \text{Probabilità } 1.$$

- Al contrario quando  $(a_j + z_j = 1) \pmod 2$  allora il coefficiente diventa

$$\frac{1}{2^n} \prod_{j=0}^{n-1} [(-1)^{0 \cdot 1} + (-1)^{1 \cdot 1}] = 0, \Rightarrow \text{Probabilità } 0.$$

Ancora una volta, i due casi della probabilità sono mutualmente esclusivi e quindi avremo

$$\begin{aligned} (a_j + z_j = 0) \pmod 2 \quad \forall j, & \Rightarrow a = z, \Rightarrow \text{Probabilità } 1, \\ (a_j + z_j = 1) \pmod 2 \text{ for some } j, & \Rightarrow a \neq z, \Rightarrow \text{Probabilità } 0. \end{aligned}$$

Questo significa che il nostro stato, in realtà, non è una sovrapposizione lineare, ma contiene bensì solamente lo stato

$$|a\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}};$$

e quindi attraverso un'unica operazione di misura sui primi  $n$ -qubit, otteniamo  $a$ , la nostra incognita.

LEZIONE 7 - 25/10/2021

I prossimi due algoritmi sono tra quelli più conosciuti, in termini di algoritmi quantistici, sia dal punto di vista storico del QC sia dal punto di vista applicativo:

- L'algoritmo di ricerca del periodo di una funzione: l'**algoritmo di Shor**;
- L'algoritmo di ricerca di particolari elementi in un database: l'**algoritmo di Grover**.

Prima di addentrarci nello studio del più difficile (non vedremo tutto il discorso legato alla teoria dei numeri) dei due, l'algoritmo di Shor, introduciamo il seguente concetto:

### 3.7 Quantum Fourier Transform

Il cuore dell'algoritmo di Shor è la **QFT** o **Quantum Fourier Transform**, che può essere eseguita da un circuito quantistico. La QFT di  $n$  qubit è definita come quella trasformazione unitaria  $\hat{U}_{\text{FT}}$  la cui azione su un elemento  $|x\rangle \in \mathcal{H}$  è data da:

$$\hat{U}_{\text{FT}} |x\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{xy}{2^n}} |y\rangle \quad (3.7.1)$$

dove con la notazione precedente intendiamo  $|x\rangle \equiv |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes \dots \otimes |x_0\rangle$ , in cui ciascun qubit  $|x_i\rangle$  può essere un elemento della base computazionale, quindi  $|0\rangle$  o  $|1\rangle$ . Notiamo inoltre che il prodotto  $xy$  ad esponente è un prodotto tra interi e non un prodotto bit a bit modulo 2. Lo stato  $|x\rangle$  può essere scritto utilizzando anche la codifica digitale degli interi, ossia

$$x = 2^{n-1}x_{n-1} + 2^{n-2}x_{n-2} + \dots + 2^0x_0, \quad \text{dove } 0 \leq x \leq 2^n - 1.$$

Notiamo che il fattore davanti alla sommatoria in (3.7.1) è un fattore di normalizzazione perché abbiamo diviso per la radice del numero totale degli stati: lo spazio di Hilbert di  $|x\rangle$  ha infatti  $\dim \mathcal{H} = 2^n$  poiché è frutto del prodotto tensoriale degli  $n$  spazi associati ai singoli qubit. Dato che  $\hat{U}_{\text{FT}}$  è un operatore che agisce su  $\mathcal{H}$ , possiamo applicare la (3.7.1) ad una sovrapposizione di stati  $|x\rangle$  con ampiezze complesse  $\gamma(x)$ :

$$\hat{U}_{\text{FT}} \left( \sum_{x=0}^{2^n-1} \gamma(x) |x\rangle \right) = \sum_{x,y=0}^{2^n-1} \frac{\gamma(x)}{2^{\frac{n}{2}}} e^{2\pi i \frac{xy}{2^n}} |y\rangle = \sum_{y=0}^{2^n-1} \hat{\gamma}(y) |y\rangle, \quad (3.7.2)$$

dove abbiamo ottenuto un'altra sovrapposizione con ampiezze che sono legate a  $\gamma(x)$  dalla **DFT** o **Discrete Fourier Transform**:

$$\hat{\gamma}(y) = \sum_{x=0}^{2^n-1} \frac{e^{2\pi i \frac{xy}{2^n}}}{2^{\frac{n}{2}}} \gamma(x). \quad (3.7.3)$$

Si noti che la (3.7.1) agisce sui coefficienti  $\gamma(x)$  come in (3.7.3), ossia tramite una versione discretizzata della trasformata di Fourier standard. In generale la DFT è largamente utilizzata nella teoria dei segnali.

Per calcolare ciascun coefficiente  $\hat{\gamma}(x)$  in (3.7.3) si richiedono  $2^n \times 2^n = 2^{2n}$  operazioni (dimensione della matrice), le quali sono un'enormità! In CC esiste un celebre algoritmo chiamato **FFT** o **Fast Fourier Transform** che migliora il numero precedente fino a  $\mathcal{O}(n2^n)$ , ottenendo quindi un modo molto più efficiente per calcolare  $\hat{\gamma}(x)$ . In realtà esiste un algoritmo quantistico per eseguire la trasformazione unitaria  $\hat{U}_{\text{FT}}$  in un tempo esponenzialmente più veloce, perché cresce solo come  $\mathcal{O}(n^2)$ . Il problema, come al solito,

è che non si può conoscere l'insieme completo dei coefficienti di Fourier, come si fa dopo aver applicato la FFT: il risultato è infatti una sovrapposizione  $\sum_y \hat{\gamma}(y) |y\rangle$  sulla quale è necessario effettuare una misurazione che permetterà di ottenere solamente 1 coefficiente. Nonostante quindi l'algoritmo per il calcolo della QFT non migliori l'algoritmo classico della FFT, la (3.7.1) si è rivelata molto utile per la risoluzione di problemi del mondo quantistico. Ad esempio, se  $\gamma$  è una funzione periodica con un periodo  $r$  non maggiore di  $2^{\frac{n}{2}}$ , allora un registro nello stato in (3.7.2) può fornire potenti indizi sul valore preciso del periodo, anche se  $r$  può essere lungo centinaia di cifre. Per il momento il nostro scopo è mostrare che è possibile costruire un circuito che calcoli in un numero di step di ordine  $\mathcal{O}(n^2)$  la QFT.

Consideriamo, come al solito, come punto di partenza lo stato  $|0\rangle^{\otimes n}$ . Sappiamo dalla (3.3.2) che se applichiamo l'**H-gate** su tale stato avremo

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} |y\rangle ,$$

ossia una somma su tutti gli stati nella base computazionale. Definiamo ora un operatore  $\mathcal{Z}$  che agisce nel modo seguente:

$$\mathcal{Z} |y\rangle = e^{2\pi i \frac{y}{2^n}} |y\rangle ;$$

in questo modo l'operatore  $\hat{U}_{\text{FT}}$  della (3.7.1) può essere riscritto come

$$\hat{U}_{\text{FT}} |x\rangle = \mathcal{Z}^x H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} \mathcal{Z}^x |y\rangle , \quad \text{con } \mathcal{Z} = e^{2\pi i \frac{y}{2^n}} ; \quad (3.7.4)$$

si ricordi sempre che  $x$  è un intero. Cerchiamo di capire cosa sia  $\mathcal{Z}$ . Consideriamo il caso del qubit singolo ( $n = 1$ ):

$$\mathcal{Z} |y\rangle = e^{\pi i y} |y\rangle = \begin{cases} |y\rangle , & \text{per } y = 0 \\ -|y\rangle , & \text{per } y = 1 \end{cases} , \quad \Rightarrow \quad \mathcal{Z} = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} .$$

Si noti che un altro modo conveniente di scriverlo è come esponenziale

$$Z = e^{i\pi n} , \quad \text{dove } n = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} .$$

Per passare alla generalizzazione per  $n$  qubit ricordiamo che, come lo stato  $|x\rangle$  di (3.7.1), possiamo scrivere nella base computazionale che  $|y\rangle = |y_{n-1}\rangle \otimes \dots \otimes |y_0\rangle$  e analogamente come intero avremo  $y = 2^{n-1}y_{n-1} + \dots + 2^0y_0$ . Introduciamo  $n$  differenti matrici, che chiameremo  $n_i$  con  $i = 0, \dots, n-1$ , che agiscono sul corrispondente qubit di  $|y\rangle$  dando 0 o 1 a seconda del valore del qubit: questo significa scrivere che

$$(2^{n-1}n_{n-1} + 2^{n-2}n_{n-2} + \dots + n_0) |y\rangle = 2^{n-1}y_{n-1} |y_{n-1}\rangle \otimes \dots \otimes |y_0\rangle + \dots = y |y\rangle ,$$

quindi si tratta di un particolare modo di calcolare la codifica digitale, ossia l'intero  $y$ , dello stato  $|y\rangle$ . Notiamo che la matrice  $n_{n-1}$  agisce su  $|y_{n-1}\rangle$ ,  $n_{n-2}$  agisce su  $|y_{n-2}\rangle$  e così via fino a  $n_0$  che agisce su  $|y_0\rangle$ , questo perché in generale  $n_p |y_p\rangle = y_p |y_p\rangle$ . Utilizzando quindi questa notazione possiamo riscrivere l'operatore  $\mathcal{Z}$  in questo modo:

$$\mathcal{Z} |y\rangle = e^{\frac{2\pi i}{2^n} y} |y\rangle = e^{\frac{2\pi i}{2^n} (2^{n-1}n_{n-1} + \dots + n_0)} |y\rangle ,$$

dove si è utilizzata la formula  $n_p |y_p\rangle = y_p |y_p\rangle$  ad esponente e si è riconosciuta la codifica digitale di  $y$ . Per calcolare la QFT come in (3.7.4) ci serve saper calcolare  $\mathcal{Z}^x$ . Al posto che farlo in generale, focalizziamoci su un esempio perché vedremo alla fine che otterremo un circuito il cui schema è facilmente generalizzabile per il calcolo della QFT per un numero generico di qubit.

**Esempio 3.4 (QFT per 3 qubit).** Vogliamo valutare  $\mathcal{Z}^x$ . Usando l'espressione di  $\mathcal{Z}$  in (3.7.4) e ricordando la codifica digitale di  $x$  e  $y$  per  $n = 3$  possiamo facilmente scrivere

$$\mathcal{Z}^x = e^{\frac{2\pi i}{8}(4x_2+2x_1+x_0)(4n_2+2n_1+n_0)}.$$

Semplifichiamo questa espressione ricordando che  $e^{2\pi i n} = \mathbb{I}$ , dato che  $n = 0, 1$ , e molti termini nel prodotto delle onde ad esponente sono in realtà multipli interi di  $2\pi i n$ . Più in dettaglio possiamo scrivere la precedente come

$$\mathcal{Z}^x = e^{\pi i [n_2 x_0 + n_1 (x_1 + \frac{x_0}{2}) + n_0 (x_2 + \frac{x_1}{2} + \frac{x_0}{4})]}.$$

Scriviamo quindi la (3.7.4):

$$\mathcal{Z}^x H^{\otimes 3} |0\rangle^{\otimes 3} = e^{i\pi n_2 x_0} H_2 |0\rangle_2 \otimes e^{i\pi n_1 (x_1 + \frac{x_0}{2})} H_1 |0\rangle_1 \otimes e^{i\pi n_0 (x_2 + \frac{x_1}{2} + \frac{x_0}{4})} H_0 |0\rangle_0, \quad (3.7.5)$$

dove il label su ogni *H-gate* indica su quale qubit quell'operatore sta agendo. Per calcolare l'azione di ciascun operatore sul rispettivo qubit utilizziamo il seguente stratagemma: le matrici  $H_i$  non commutano con gli esponenziali alla loro sinistra, tuttavia possiamo scrivere che

$$e^{i\pi x n} H |0\rangle = H |x\rangle, \quad \text{dove } x = 0, 1;$$

infatti, ricordando le (1.2.3), avremo

$$\begin{cases} H |0\rangle = H |0\rangle, & x = 0 \\ e^{i\pi x n} H |0\rangle = Z H |0\rangle = Z |+\rangle = |-\rangle = H |1\rangle, & x = 1 \end{cases}.$$

Usando questo risultato, la (3.7.5) può essere riscritta nel seguente modo

$$\begin{aligned} \mathcal{Z}^x H^{\otimes 3} |0\rangle^{\otimes 3} &= H_2 |x_0\rangle_2 \otimes e^{i\pi n_1 \frac{x_0}{2}} H_1 |x_1\rangle_1 \otimes e^{i\pi n_0 (\frac{x_1}{2} + \frac{x_0}{4})} H_0 |x_2\rangle_0 \\ &= H_2 e^{i\pi n_1 \frac{x_0}{2}} H_1 e^{i\pi n_0 \frac{x_1}{2}} e^{i\pi n_0 \frac{x_0}{4}} H_0 |x_0\rangle_2 \otimes |x_1\rangle_1 \otimes |x_2\rangle_0, \end{aligned}$$

dove nell'ultimo passaggio abbiamo raggruppato tutti gli operatori a sinistra e diviso gli esponenziali contenenti  $n_0$  dato che commutano tra loro. Notiamo che durante questo conto abbiamo ottenuto una permutazione dei qubit iniziali ( $x_0 \leftrightarrow x_2$ ). Lo stato  $|x_0\rangle_2 \otimes |x_1\rangle_1 \otimes |x_2\rangle_0$  è un autostato degli operatori numerici  $n_2, n_1, n_0$  con i rispettivi autovalori  $x_0, x_1, x_2$ . Consideriamo il primo qubit  $H_2 e^{i\pi n_1 \frac{x_0}{2}} |x_0\rangle_2$ : sappiamo che  $n_2 |x_0\rangle_2 = x_0 |x_0\rangle_2$  quindi possiamo tranquillamente rimpiazzare  $n_2 \leftrightarrow x_0$  ad esponente. Chiaramente lo possiamo fare perché solamente la matrice di Hadamard  $H_2$  agisce su  $|x_0\rangle_2$ , ed essa si trova a sinistra dell'esponenziale (in generale le matrici di Hadamard non commutano con questi esponenziali, tuttavia in questa situazione si trovano tutte a sinistra). Un discorso analogo vale anche per gli altri due qubit. Riassumendo: possiamo sostituire ad esponente ogni  $x_i$  con l'operatore numerico  $n_{2-i}$ :

$$\mathcal{Z}^x H^{\otimes 3} |0\rangle^{\otimes 3} = H_2 e^{i\pi \frac{n_1 n_2}{2}} H_1 e^{i\pi \frac{n_0 n_1}{2}} e^{i\pi \frac{n_0 n_2}{4}} H_0 |x_0\rangle_2 \otimes |x_1\rangle_1 \otimes |x_2\rangle_0;$$

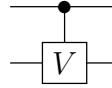
infine, se definiamo l'operatore unitario  $P$  che realizza la permutazione degli stati della base computazionale, ossia  $P|x\rangle = P(|x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle) = |x_0\rangle \otimes |x_1\rangle \otimes |x_2\rangle$ , possiamo scrivere

$$U_{FT}|x\rangle = \mathcal{Z}^x H^{\otimes 3} |0\rangle^{\otimes 3} = H_2 e^{i\pi \frac{n_1 n_2}{2}} H_1 e^{i\pi \frac{n_0 n_1}{2}} e^{i\pi \frac{n_0 n_2}{4}} H_0 P |x\rangle .$$

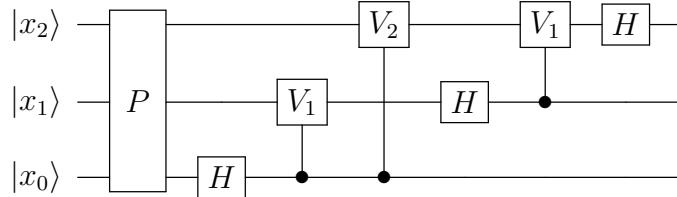
Per capire che tipologia di operatore sia  $U_{FT}$  ricordiamo che sappiamo bene come agiscono gli  **$H$ -gate**, inoltre non è difficile costruire un opportuno  **$P$ -gate** che inverta l'ordine dei qubit. Gli esponenziali, invece, sono operatori che contengono delle paia di matrici  $n_i$  agenti sui singoli qubit: tutti questi sono della forma

$$V_{ij} = e^{i\pi \frac{n_i n_j}{2^{|i-j|}}} ,$$

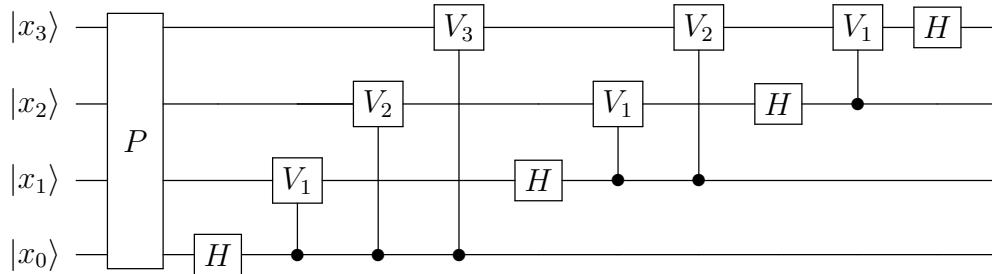
dove  $|i - j|$  è la distanza tra i qubit  $i$  e  $j$  nell'array contenente tutti i qubit. Qual è l'effetto esplicito di ciascun  $V_{ij}$  sui qubit  $i$  e  $j$ ? Quando  $i$  è nello stato  $|0\rangle$  allora  $n_i = 0$  e l'esponenziale non fa nulla; ma quando  $i$  è nello stato  $|1\rangle$  allora  $n_i = 1$  e l'esponenziale agisce come  $e^{i\pi \frac{n_j}{2^{|i-j|}}}$ . Quindi si tratta di una sorta di **Controlled-V-gate** che agisce solamente quando il primo qubit è  $|1\rangle$ :



Si noti che il **CNOT-gate** è un caso particolare del **Controlled-V-gate** quando  $V = X$ . In termini di circuiti, ponendo  $V_k = e^{i\pi \frac{n}{2^k}}$ , l'azione dell'operatore che calcola la QFT per 3 qubit può essere rappresentata come:



Cosa succede nel caso in cui  $n = 4$ ? La struttura del circuito dell'esempio precedente può essere facilmente generalizzata, infatti:



Qual è il numero totale di gate necessari? Dal circuito precedente ( $n = 4$ ) si hanno  $4+3+2+1 = 10 \sim \mathcal{O}(4^2)$  gate, quindi in generale avremo  $n+(n-1)+(n-2)+\dots \sim \mathcal{O}(n^2)$ , dove il massimo è proprio  $n^2$ . Dunque l'algoritmo quantistico per il calcolo della QFT è di ordine  $\mathcal{O}(n^2)$  nel numero di qubit  $n$ .

### 3.8 Algoritmo di Shor: period finding

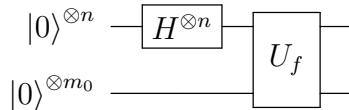
La ricerca del periodo di una funzione è importante per diverse ragioni: vedremo in che modo possiamo usare questo risultato per rompere la crittografia RSA standard, tuttavia è importante anche per simulazioni quantistiche, come ad esempio quando si vogliono trovare gli autovalori di matrici unitarie molto grandi.

Supponiamo di avere una funzione di interi e periodica di periodo  $r$ :

$$f : \mathbb{Z} \rightarrow \{0, 1\}^{\otimes m_0},$$

dove sappiamo per certo che  $\exists r \in \mathbb{Z} : f(x + r) = f(x)$  dove  $r \leq N \equiv 2^{n_0}$ . Quindi si tratta di trovare il periodo di una funzione periodica data in input: chiaramente se la funzione fosse definita sui reali il problema sarebbe banale perché richiederebbe un semplice disegno di un plot. Il miglior algoritmo classico ("general number field sieve") richiede un numero di operazioni di ordine  $\mathcal{O}\left(\exp\left\{n_0^{1/3} \log^{2/3} n_0\right\}\right)$ , quindi presenta un comportamento esponenziale in  $n_0$ . L'algoritmo di Shor, invece, richiede solamente un numero di operazioni di ordine  $\mathcal{O}(n_0^2 \log^2 n_0)$ , un bel vantaggio rispetto al caso classico perché presenta un comportamento polinomiale in  $n_0$ .

L'algoritmo funziona come segue: innanzitutto consideriamo un data register costituito da  $n$  qubit preparati in  $|0\rangle^{\otimes n}$  e un output register (che conterrà il risultato della funzione  $f$ ) fatto di  $m_0$  qubit preparati in  $|0\rangle^{\otimes m_0}$ . Il circuito che vogliamo applicare è il seguente:



I qubit nel data register sono tipicamente di più di quanti si necessitano per valutare il periodo ( $n_0$ ), infatti di solito  $n \sim 2n_0$  in maniera tale che  $2^n \sim N^2$ . Come ben sappiamo, l'H-gate e  $U_f$  agiranno nel seguente modo:

$$U_f [(H^{\otimes n} |0\rangle^{\otimes n}) \otimes |0\rangle^{\otimes m_0}] = U_f \left( \sum_{x=0}^{2^n-1} \frac{1}{2^{\frac{n}{2}}} |x\rangle \otimes |0\rangle^{\otimes m_0} \right) = \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |f(x)\rangle.$$

Come al solito, dopo  $U_f$  abbiamo una sovrapposizione di tutti i possibili valori di  $f(x)$  in un colpo solo. Ora facciamo una misura sull'output register, cioè su  $|f(x)\rangle$ : dalla meccanica quantistica, che valuta tutti i valori di  $f(x)$  all'interno della black-box, otteniamo un valore random della funzione

$$f_0 = f(x_0) = f(x_0 + r);$$

ma questa funzione, in realtà, è valutata in differenti valori di  $x$  in quanto periodica: abbiamo trovato diversi valori  $x_0 + jr$  dell'input register che sono associati al medesimo output; più precisamente il vincolo che deve essere soddisfatto è che  $0 \leq x_0 + jr \leq 2^n$ . Chiaramente il numero preciso di valori  $x_0 + jr$  dipende da quanto  $2^n$  è più grande rispetto a  $r$ : supponiamo di aver trovato  $m$  valori di output, allora, siccome  $r \leq N$  e  $2^n \sim N^2$ , asintoticamente avremo  $0 \leq x_0 + jN \lesssim N^2$  e quindi  $m$  sarà dell'ordine di  $N$  (un numero molto grande). Per cui il nostro stato complessivo è collassato in

$$|\psi\rangle = \underbrace{\frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle}_{\text{Data register}} \otimes \underbrace{|f(x_0)\rangle}_{\text{Output register}}. \quad (3.8.1)$$

A questo punto lo stato  $|f(x_0)\rangle$  è lo stesso per qualsiasi valore di  $|x_0 + kr\rangle$ , perciò nella discussione che segue è irrilevante e possiamo dimenticarcene. Ricordiamo che il nostro scopo è quello di ottenere  $r$ : se ora si effettuasse una misura si otterrebbe  $x_0 + kr$ , il quale sarebbe un ottimo risultato se non ci fosse il numero casuale  $x_0$ , il quale non conosciamo. Analogamente sarebbe bello poter effettuare due misurazioni (non lo possiamo fare per la regola di Born e il teorema di no-cloning): gli ipotetici risultati  $x_0 + kr$  e  $x_0 + k'r$  potrebbero essere sottratti per ottenere la differenza  $(k - k')r$ , la quale è un multiplo del periodo cercato. Naturalmente, se eseguissimo di nuovo l'intero algoritmo, ci ritroveremmo con uno stato della forma (3.8.1) per un altro valore casuale di  $x_0$ , che non consentirebbe alcun confronto utile con quanto appreso dalla prima esecuzione. In realtà possiamo fare qualcosa di più allo stato (3.8.1) prima di effettuare la misurazione finale. Come evidenziato, il problema risiede nella presenza del numero casuale  $x_0$ , che trasla  $kr$  e impedisce di estrarre qualsiasi informazione su  $r$  in una singola misura. Abbiamo bisogno di una trasformazione unitaria che trasformi la dipendenza da  $x_0$  in un fattore di fase complessivo (e innocuo). Ciò si ottiene applicando la Quantum Fourier Transform in (3.7.1) a (3.8.1):

$$\begin{aligned} U_{\text{FT}} \left( \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle \right) &= \frac{1}{\sqrt{m} 2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} \sum_{k=0}^{m-1} e^{\frac{2\pi i}{2^n} (x_0 + kr)y} |y\rangle \\ &= \sum_{y=0}^{2^n-1} \underbrace{e^{2\pi i \frac{x_0 y}{2^n}}}_{\text{coefficiente di ogni } |y\rangle} \sum_{k=0}^{m-1} \frac{e^{2\pi i \frac{kry}{2^n}}}{\sqrt{m} 2^{\frac{n}{2}}} |y\rangle ; \end{aligned}$$

in questo modo abbiamo ottenuto una sovrapposizione di tutti i possibili interi nella base computazionale, i cui coefficienti sono dati dai fattori sottolineati. Se ora effettuiamo una misura, la probabilità  $P(|y\rangle)$  di ottenere il risultato  $y$  è data dal modulo quadro dell'ampiezza del coefficiente di  $|y\rangle$ :

$$P(|y\rangle) = \left| e^{\frac{2\pi i}{2^n} (x_0 y)} \sum_{k=0}^{m-1} \frac{e^{\frac{2\pi i}{2^n} (kry)}}{\sqrt{m} 2^{\frac{n}{2}}} \right|^2 = \frac{1}{m 2^n} \left| \sum_{k=0}^{m-1} e^{\frac{2\pi i}{2^n} (kry)} \right|^2 ; \quad (3.8.2)$$

è evidente come lo scomodo  $x_0$  sia scomparso a seguito del fatto che apparisse unicamente come una pura fase all'interno del modulo quadro. Studiamo la probabilità (3.8.2) in dettaglio.

Un esempio di plot è mostrato nel Grafico 3.1. Notiamo che vi sono differenti picchi di diverse ampiezze: ciò è dovuto al fatto che ci sono valori di  $y$  dove abbiamo interferenza costruttiva, mentre in altri si ha interferenza distruttiva. Nel realizzare tale grafico, però, abbiamo assunto che  $y \in \mathbb{R}$ , ma bisogna ricordare che  $y \in \mathbb{Z}$ , quindi si tratta di un'approssimazione perché non tutti i punti della curva devono essere disegnati! In realtà, per valori di  $n$  molto grandi  $2^n$  è enorme quindi la discretizzazione è minima e quasi impercettibile. Nei punti in cui la probabilità è maggiore, in corrispondenza dei picchi più alti, si ha  $y = j \frac{2^n}{r}$  dove  $j \in \mathbb{N}$ . Per tali valori, gli esponenziali dentro la probabilità in (3.8.2) non sono altro che  $e^{2\pi i j k} = 1$  perché  $j, k \in \mathbb{Z}$ , quindi la (3.8.2) diventa:

$$P(|y\rangle) = \frac{1}{m 2^n} \left| \sum_{k=0}^{m-1} 1 \right|^2 = \frac{m^2}{m 2^n} = \frac{m}{2^n},$$

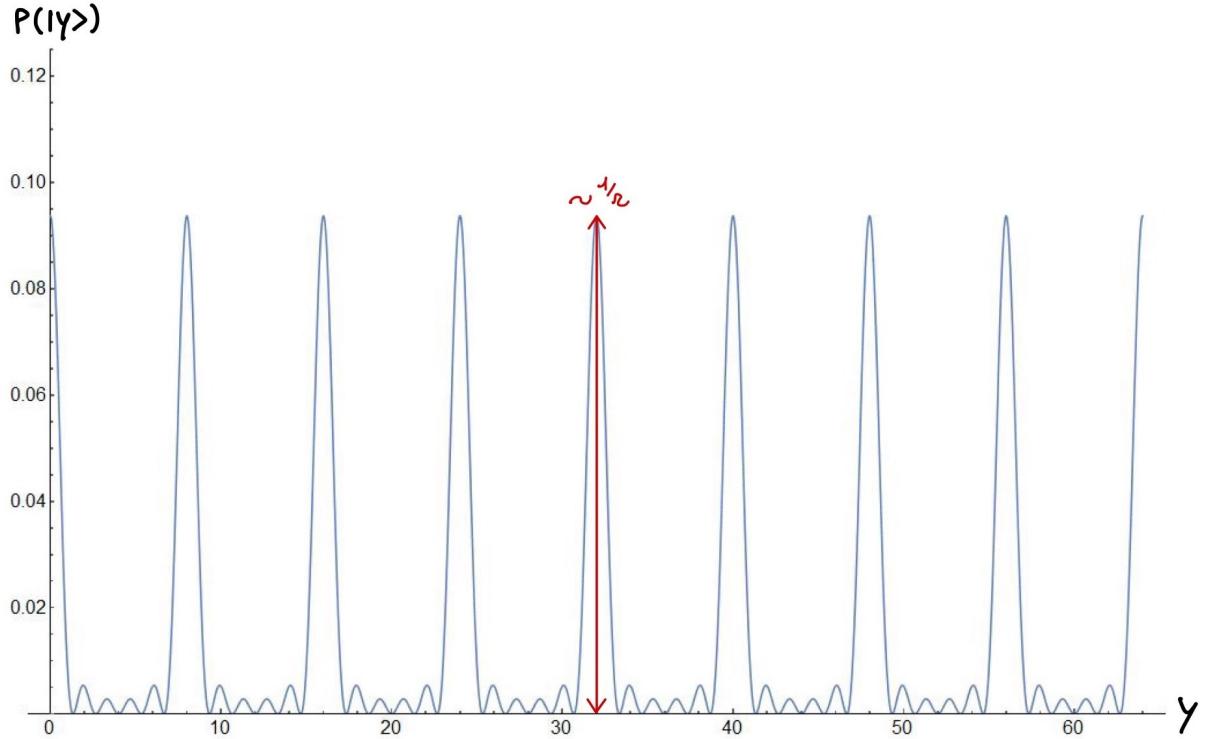


Figura 3.1: Esempio di grafico della probabilità di misurare  $y$  della formula (3.8.2), dove  $0 \leq y \leq 2^n$ . In questo esempio si è usato  $n = m = 6$  e  $r = 8$ . Si noti come il numero di picchi sia  $\mathcal{O}(r)$  e la loro altezza, come ordine di grandezza, comparabile a  $1/r$ .

il quale è il valore massimo della probabilità. Per capire per quale ragione abbiamo indicato nel Grafico 3.1 che l'altezza dei picchi è di circa  $1/r$ , ricordiamo che  $2^n \sim N^2$ ,  $r \sim N$  e anche  $m \sim N$ , per cui:

$$P(|y\rangle) = \frac{m}{2^n} \sim \frac{N}{N^2} \sim \frac{1}{N} \sim \frac{1}{r}.$$

Notiamo che sebbene abbiamo disegnato una funzione continua, l'approssimazione è comunque molto buona perché la probabilità totale è correttamente normalizzata a 1: infatti l'altezza dei picchi per il loro numero non è altro che  $\frac{1}{r} \times m \sim \frac{1}{r} \times r \simeq 1$ , quindi gran parte della probabilità è saturata i corrispondenza dei picchi (si può dimostrare che nel limite in cui  $n \rightarrow \infty$  i picchi tendono a delle delta function).

Un risultato fondamentale è che passando attraverso delle manipolazioni algebriche di seno e coseno, si può dimostrare che si ha circa il 40% di possibilità ( $P(|y\rangle) = \frac{4}{\pi^2}$ ) di misurare  $y$  e ottenere un valore che si trovi in prossimità di uno di questi picchi con un errore di circa  $\frac{1}{2}$ : ricordando che i picchi sono situati in  $y = j \frac{2^n}{r}$ , possiamo formalmente scrivere che

$$\left| y - j \frac{2^n}{r} \right| < \frac{1}{2}, \quad \Rightarrow \quad \left| \frac{y}{2^n} - \frac{j}{r} \right| < \frac{1}{2^{n+1}}, \quad (3.8.3)$$

dove abbiamo diviso per  $2^n$ . Stiamo quindi dicendo che una misura di  $y$  soddisfa la diseguaglianza (3.8.3) il 40% delle volte. Possiamo estrarre  $r$  dalla (3.8.3)? Innanzitutto notiamo che, essendo  $0 \leq y \leq 2^n$ , abbiamo  $0 \leq \frac{y}{2^n} \leq 1$ . Se  $n \geq 2n_0$  allora avremo  $2^n \geq 2^{2n_0} = N^2$ , quindi quando la (3.8.3) è verificata esiste un singolo numero razionale della forma  $\frac{j}{r}$  che la soddisfa e dalla quale è possibile estrarre  $r$ .

La logica è mostrata nel disegno della Figura 3.2: prendendo il segmento  $[0, 1]$  e suddividendolo in step uguali di lunghezza  $\frac{1}{2^n}$ , possiamo rappresentare con delle barrette verticali

tutti i possibili valori di  $y$  tali che  $0 \leq \frac{y}{2^n} \leq 1$ . La disegualanza (3.8.3) ci dice che il numero  $\frac{j}{r}$  (indicato con una "x" azzurra) è vicino a  $\frac{y}{2^n}$  con una distanza minore di  $\frac{1}{2^{n+1}}$ .

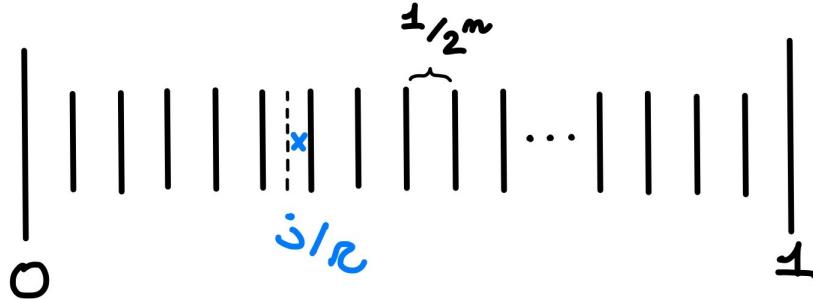


Figura 3.2: Rappresentazione geometrica della disegualanza (3.8.3).

La domanda che possiamo porci è se esista più di un numero razionale che soddisfi questa particolare proprietà. Supponiamo per assurdo che esistano due numeri razionali  $\frac{j_1}{r_1}$  e  $\frac{j_2}{r_2}$  che soddisfano la disegualanza (3.8.3) (e la condizione per cui  $r_1, r_2 < N$ ). Allora la differenza tra questi due numeri è

$$\frac{j_1}{r_1} - \frac{j_2}{r_2} = \frac{r_2 j_1 - r_1 j_2}{r_1 r_2}, \quad (3.8.4)$$

tuttavia il numeratore è un intero e il denominatore è di ordine  $\mathcal{O}(N^2)$ : essendo  $r_1, r_2 < N$  allora il denominatore è strettamente minore di  $N^2$  quindi la (3.8.4) è  $\geq \frac{1}{N^2} \geq \frac{1}{2^n}$ , che è proprio la larghezza degli step in cui abbiamo suddiviso  $[0, 1]$ . Questo significa che se ci sono due soluzioni della (3.8.3) allora la distanza tra le due deve necessariamente essere più grande della misura dello step: in un dato step è possibile trovare una sola soluzione, ossia un solo numero razionale che verifica la (3.8.3).

Riassumendo: misurando un valore  $y$  che soddisfa la (3.8.3) otteniamo un unico numero razionale  $\frac{j}{r}$ . Il punto chiave è quindi trovare  $\frac{j}{r}$ , tuttavia questo non è così semplice, perché quello che si ottiene dalla misura è un numero scritto in forma decimale, il quale vorremmo poterlo scrivere come rapporto tra razionali. Nonostante ciò facciamo uso del seguente risultato di teoria dei numeri che non dimostreremo. Usando  $\frac{1}{2^{n+1}} \leq \frac{1}{2N^2} \leq \frac{1}{2r^2}$ , riscriviamo la disegualanza (3.8.3) come

$$\left| x - \frac{j}{r} \right| \leq \frac{1}{2r^2}, \quad \text{dove } x \in [0, 1].$$

Il valore  $x$  è dato dalla misura mentre lo scopo è quello di trovare un numero razionale  $\frac{j}{r}$  che soddisfi questa disegualanza. Il risultato dalla teoria dei numeri asserisce che questo valore appare nell'espansione in frazione continua del numero  $x$ :

$$x = \frac{1}{x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \dots}}}.$$

**Esempio 3.5** (Espansione in frazione continua). *Supponiamo di considerare il numero  $x = 0.256789$ . Prendendone l'inverso avremo  $\frac{1}{x} = \frac{1}{0.256789} = 3.8942478\dots$ . Da questo risultato è evidente che  $x_0 = 3$ . Nello step successivo si calcola  $x_1$ : calcoliamo  $\frac{1}{x} - 3$  e poi*

$(\frac{1}{x} - 3)^{-1}$ , la cui parte intera è  $x_1$ . Iterando all'infinito questo procedimento si ottiene l'espansione in frazione continua di  $x$ :

$$x = \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{8 + \dots}}}.$$

Ad ogni step si ottiene quindi un'approssimazione razionale di  $x$ , infatti il set di numeri razionali che approssimano il suo valore è dato da  $\{\frac{1}{3}, \frac{1}{4}, \frac{9}{35}, \frac{19}{74}, \frac{104}{405}, \dots\}$ . Più si procede, meglio approssimato sarà il valore di  $x$ . Il teorema ci dice che a un certo punto possiamo trovare il valore di  $\frac{j}{r}$  all'interno di questo insieme e questo con una probabilità del 100%.

Tuttavia di questo procedimento vanno fatte delle opportune precisazioni:

- Supponiamo che  $j$  e  $r$  abbiano dei fattori comuni (e questo ovviamente non lo sapremo mai), allora il valore di  $r$  può essere diverso, infatti:

$$\frac{j}{r} = \frac{j_0 k}{r_0 k} = \frac{j_0}{r_0},$$

quindi mediante la procedura sopraelencata, al posto di trovare il periodo cercato, si ottiene  $r_0$ . Nonostante ciò si è trovato un divisore di  $r$ , quindi prendendo la forma analitica di  $f$  si può provare a calcolare  $f(x + r_0)$ ,  $f(x + 2r_0)$ ,  $f(x + 3r_0)$ , ... fino a quando effettivamente si trova un valore uguale a  $f(x)$ .

- Talvolta si possono misurare dei valori  $y$  che non soddisfano la disuguaglianza (3.8.3) (la probabilità di soddisfarla è infatti del 40%). In tal caso basta semplicemente ricominciare l'algoritmo da capo con una nuova esecuzione del circuito e della QFT fino a quando non si ottiene un valore di  $y$  che soddisfi la (3.8.3). Inoltre è possibile dimostrare che la probabilità che la (3.8.3) sia soddisfatta cresce fino al 90% se si sa a priori che  $r < \frac{N}{2}$ .

Concludiamo la discussione dicendo che lo stesso tipo di algoritmo può essere utilizzato per calcolare i *logaritmi discreti*, oppure per la simulazione di sistemi quantistici (si possono calcolare gli autovalori di matrici unitarie molto grandi che servono per il calcolo degli autovalori delle relative hamiltoniane e degli evoluti temporali).

LEZIONE 8 - 29/10/2021

### 3.8.1 Violazione della crittografia RSA

Dal momento che l'algoritmo quantistico del period finding di Shor è spesso descritto come un algoritmo di fattorizzazione di numeri interi, concludiamo questa sezione illustrando come questo algoritmo porti alla fattorizzazione. Consideriamo solo il caso relativo alla **crittografia RSA** (R. Rivest, A. Shamir e L. Adleman), dove si vuole fattorizzare un numero molto grande in prodotto di due numeri primi, sebbene la connessione tra period finding e fattorizzazione sia più generale.

Supponiamo di avere un numero  $N = pq$ , tale per cui  $N, p$  e  $q$  siano molto grandi e  $p, q$  siano numeri primi. Nel CC non esiste un modo efficiente di risolvere questo problema perché fattorizzare  $N$  richiederebbe un tempo di esecuzione esponenziale di ordine  $\mathcal{O}(e^N)$ ;

al contrario nel QC si può ridurre il tempo di attesa a un tempo polinomiale in  $N$ . Vediamo ora come interviene esplicitamente l'algoritmo di Shor.

Consideriamo la funzione  $f(x) = a^x \pmod{N}$ , dove  $a, x \in \mathbb{Z}$ . Il fatto che la funzione sia periodica è equivalente a richiedere che  $f(x+r) = f(x)$ , ossia  $a^r \equiv 1 \pmod{N}$ . In tal caso, quando  $r$  è la più piccola soluzione della condizione precedente, il periodo è chiamato **ordine di  $a$  (mod  $N$ )**. Un risultato in teoria dei numeri ci dice che, quando  $a$  è coprimo<sup>viii</sup> con  $N$ , si ha  $r < N$ . In particolare, vale il seguente teorema

**Teorema 3.1 (Teorema di Eulero).** *Se prendiamo un numero  $a$  coprimo con  $p$  e  $q$ , allora vale*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

Quindi, se  $N = pq$ , l'ordine di  $a$  (mod  $N$ ) esiste ed è più piccolo di  $(p-1)(q-1) < N$ . Il punto importante è che l'algoritmo di Shor può essere utilizzato per trovare l'ordine di  $a$  (mod  $N$ ), cioè  $r$ .

Iniziamo con il considerare  $N = pq$  e lo scopo è chiaramente trovare i valori di  $p$  e  $q$ . Scegliamo  $a$  coprimo con  $N$ : in generale verificare che siano coprimi tra loro non è difficile perché esiste un teorema (di Euclide) molto famoso che può essere eseguito su un computer classico; ciò che è invece difficile è trovare tutti i possibili divisori di un numero  $N$ . A questo punto usiamo il QC per trovare  $r$  tale che  $a^r \equiv 1 \pmod{N}$  e in particolar modo facciamo due assunzioni:

1. Supponiamo che  $r$  sia **pari**. Sotto questa ipotesi possiamo definire  $x = a^{\frac{r}{2}} \pmod{N}$ , con  $x \in \mathbb{Z}$ , che ha la seguente proprietà:

$$[0 = a^r - 1 = x^2 - 1 = (x - 1)(x + 1)] \pmod{N};$$

notiamo inoltre che  $x - 1 \neq 0 \pmod{N}$  perché se non fosse così allora  $a^{\frac{r}{2}} \equiv 1 \pmod{N}$  e quindi l'ordine non sarebbe più  $r$ , ma  $r/2$ .

2. Supponiamo di essere fortunati e che anche  $x + 1 \neq 0 \pmod{N}$ .

Ora, dato che  $0 = (x - 1)(x + 1) \pmod{N}$ , allora il prodotto  $(x - 1)(x + 1)$  è un multiplo di  $N$ , ma i singoli fattori non sono un multiplo di  $N$ , in quanto  $x + 1 \neq 0 \pmod{N}$  e  $x - 1 \neq 0 \pmod{N}$ : si tratta di una situazione in cui il prodotto  $(x - 1)(x + 1)$  è un multiplo di  $N$ , ma i singoli non lo sono. Essendo  $N = pq$  allora  $(x - 1)$  è multiplo di  $p$  e  $(x + 1)$  è multiplo di  $q$  (o viceversa) e allora possiamo andare a calcolare classicamente  $p$  e  $q$  usando i massimi comuni divisori ( $\gcd = \text{"greatest common divisor"}$ ):

$$p = \gcd(x - 1, N), \quad q = \gcd(x + 1, N).$$

Quando non siamo fortunati e le assunzioni precedenti non sono soddisfatte, basta semplicemente provare a scegliere degli  $a$  differenti fino a quando ci troviamo nelle ipotesi di cui sopra.

Uno potrebbe porsi la seguente domanda: perché saper fattorizzare degli interi molto grandi è così importante? Perché è possibile violare il protocollo crittografico RSA.

**Esempio 3.6 (Protocollo RSA).** Consideriamo come al solito i due sperimentatori Alice e Bob. Iniziamo facendo delle premesse: supponiamo che Bob possieda due grandi numeri primi  $p$  e  $q$ , il cui prodotto sia un grande intero  $N$ ; Bob considera inoltre un

---

<sup>viii</sup>Dire che un intero  $c$  è coprimo con  $d$  significa che  $c$  e  $d$  hanno solamente 1 come divisore comune.

numero  $c$  che non ha alcun fattore in comune con  $(p-1)(q-1)$ . Consideriamo ora Alice e immaginiamo che conosca  $N$  e  $c$ , ma non possieda alcuna informazione su  $p$  e  $q$ . Il protocollo RSA lavora nel seguente modo:

- Alice possiede un messaggio codificato in una stringa di 0 e 1, che chiamiamo  $a$ .
- Alice calcola  $b = a^c \pmod{N}$  e invia  $b$  a Bob.
- Bob decodifica il messaggio calcolando  $d$  tale che  $cd = 1 \pmod{(p-1)(q-1)}$ . Questo passaggio non è difficile con un computer classico.
- Da un risultato di teoria dei numeri Bob può risalire al messaggio di Alice tramite il calcolo di  $a = b^d \pmod{N}$ .

Il punto importante è che se si conosce  $b$ ,  $c$  e  $d$ , si può ricavare  $a$ , cioè il messaggio.

Dal funzionamento del protocollo RSA è evidente che per decodificare il messaggio si necessita di conoscere  $d$ , ossia si ha bisogno di  $p$  e  $q$ , questo perché conoscere solo  $N$  e  $c$  non è sufficiente per ricavare  $d$ . È qui che si evidenzia l'importanza di fattorizzare gli interi se si vuole decodificare il messaggio: la potenza del protocollo RSA sta nel fatto che nel CC sarebbero richieste risorse esponenziali per poter trovare i fattori primi mentre nel QC parliamo di tempi polinomiali.

L'algoritmo di Shor può essere impiegato per violare anche altri protocolli crittografici, come ad esempio il **protocollo Diffie-Hellman**, perché è in grado di calcolare i logaritmi discreti, utilizzati in tale protocollo.

### 3.9 Algoritmo di Grover

L'ultimo algoritmo che affrontiamo per mostrare ancora una volta che le prestazioni del QC sono nettamente migliori rispetto a quelle del CC è l'**algoritmo di Grover** per la ricerca di elementi in un database. L'idea è quella di considerare  $N$  oggetti e di cercarne uno specifico che identifichiamo con  $a$ . In maniera astratta potremmo pensare di avere una funzione  $f(x) : \{0, \dots, N-1\} \rightarrow \{0, 1\}$  la quale assume valori

$$f(x) = \begin{cases} 1, & x = a \\ 0, & x \neq a \end{cases}. \quad (3.9.1)$$

Esistono molte situazioni in cui un algoritmo di questo tipo può essere applicato.

**Esempio 3.7** (Problema matematico). Consideriamo un intero  $p$  definito come

$$p = x^2 + y^2,$$

dove  $x, y$  sono due numeri interi che vogliamo trovare. Per tutti gli  $x$  possiamo valutare la funzione  $g(x) = \sqrt{p - x^2}$  tale che  $g(x)$  sia un intero in corrispondenza di  $y$ : ogni volta che  $g$  è un intero esiste una funzione corrispondente uguale 1, in maniera tale da poterci ricondurre alla (3.9.1).

Nel CC, questo tipo di algoritmo può essere risolto con una probabilità del 50% che corrisponde a  $N/2$  operazioni; siccome  $N/2$  è dell'ordine di  $N$ , in termini di esecuzione sono richieste  $\mathcal{O}(N)$  operazioni. Dal punto di vista invece del QC, sono richieste  $\mathcal{O}(\sqrt{N})$

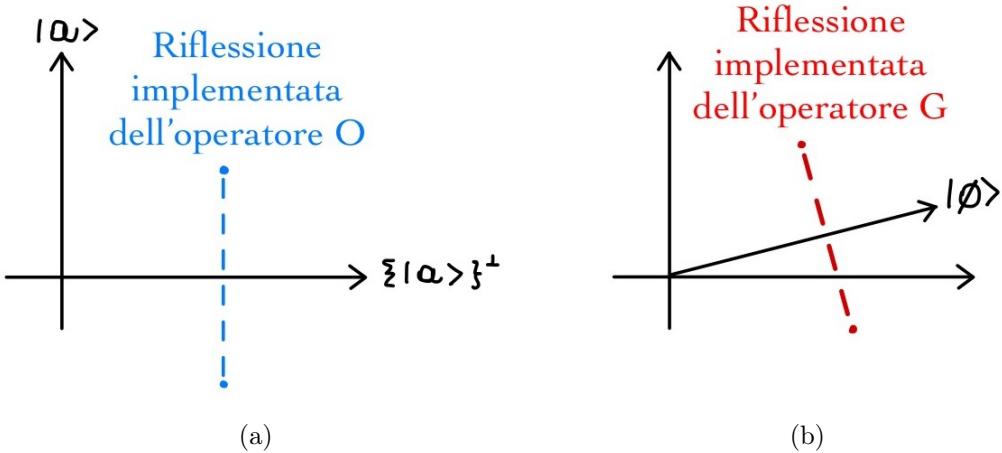
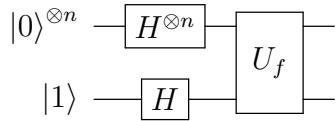


Figura 3.3: (3.3a) L’operatore  $O$  effettua una riflessione rispetto all’asse individuato da tutti gli stati perpendicolari ad  $|a\rangle$ . (3.3b) L’operatore  $G$ , invece, effettua una riflessione rispetto all’asse individuato dalla sovrapposizione di stati che abbiamo chiamato  $|\phi\rangle$ .

operazioni, quindi si tratta di un deciso miglioramento nei casi in cui  $N$  è veramente grande. Iniziamo con il nostro solito circuito per capire come funziona l’algoritmo di Grover:



quindi come al solito il data register ha  $n$  qubit inizializzati in  $|0\rangle^{\otimes n}$  e l’output register è preparato in  $|1\rangle$ . Tale circuito produce lo stato

$$\frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \otimes \underbrace{\frac{|0\rangle - |1\rangle}{\sqrt{2}}}_{\text{termine irrilevante}}.$$

Ricordiamo che l’azione di  $f(x)$  produce i valori 0 o 1 (non fa nulla nella maggior parte dei casi), quindi ciò che si realizza è un termine di fase. Nel gergo comune, si è soliti identificare la nostra black-box  $U_f$  con il nome **oracle**: chiamiamo  $O$  l’operatore la cui azione è data da

$$O|x\rangle = (-1)^{f(x)} |x\rangle = \begin{cases} -|x\rangle, & x = a \\ |x\rangle, & x \neq a \end{cases}$$

L’applicazione di  $O$  su un generico stato  $|x\rangle$  non è altro che una **riflessione** rispetto all’asse che individua tutti gli stati ortogonali ad  $|a\rangle$ . Consideriamo lo spazio di Hilbert  $\mathcal{H}$  costituito dal sottospazio contenente  $|a\rangle$  e dal sottospazio ortogonale ad  $|a\rangle$  che definiamo come:

$$\{|a\rangle\}^\perp = \{|x\rangle \in \mathcal{H} : \langle a|x\rangle = 0\}.$$

Allora l’azione di  $O$  è mostrata nella Figura 3.3a:  $O$  esegue una riflessione rispetto all’asse  $\{|a\rangle\}^\perp$ . In termini matematici possiamo definire  $O$  come

$$O = \mathbb{I} - 2|a\rangle\langle a|, \quad (3.9.2)$$

infatti

$$\begin{aligned} O|a\rangle &= |a\rangle - 2|a\rangle \underbrace{\langle a|a\rangle}_1 = |a\rangle - 2|a\rangle = -|a\rangle, & \text{per } |x\rangle = |a\rangle, \\ O|x\rangle &= |x\rangle - 2|a\rangle \underbrace{\langle a|x\rangle}_0 = |x\rangle, & \text{per } |x\rangle \in \{|a\rangle\}^\perp. \end{aligned}$$

Chiamiamo lo stato finale del data register nel modo seguente

$$|0\rangle^{\otimes n} \rightarrow H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} |x\rangle \equiv |\phi\rangle; \quad (3.9.3)$$

notiamo che si tratta di una sovrapposizione uniforme di tutti i possibili interi con la stessa ampiezza data da  $1/2^{\frac{n}{2}}$ . Definiamo ora un'altra operazione di riflessione, che chiamiamo  $G$ , rispetto a  $|\phi\rangle$  tale per cui

$$\begin{cases} G|\phi\rangle = |\phi\rangle, & \text{per } |x\rangle = |\phi\rangle \\ G|x\rangle = -|x\rangle, & \text{per } \langle x|\phi\rangle = 0 \end{cases}.$$

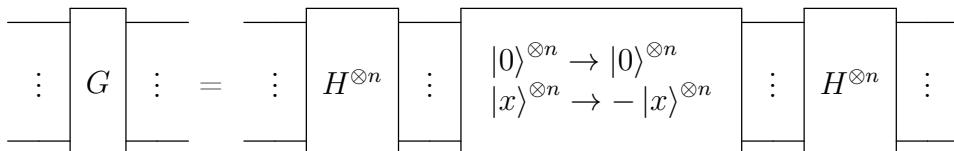
Si veda la Figura 3.3b per una semplice rappresentazione grafica. In questo modo vediamo che  $G$  è simile alla forma della (3.9.2), ma con un segno invertito:

$$G = 2|\phi\rangle\langle\phi| - \mathbb{I}. \quad (3.9.4)$$

Consideriamo ora l'operazione seguente:

$$\begin{cases} |0\rangle^{\otimes n} \rightarrow |0\rangle^{\otimes n} \\ |x\rangle \rightarrow -|x\rangle, \quad x \neq 0 \end{cases}, \quad (3.9.5)$$

il quale mantiene il "ground state" inalterato e inverte qualsiasi altro stato della base computazionale. Se supponiamo di poter trovare un circuito che implementi l'operazione precedente, allora l'operatore  $G$  può essere costruito in termini di gate nel seguente modo



Notiamo che il circuito precedente riproduce la (3.9.4): ricordando infatti che  $H^2 = \mathbb{I}$  ( $H$ -gate è unitario) e  $|\phi\rangle \equiv H^{\otimes n}|0\rangle^{\otimes n}$  avremo

$$G = H^{\otimes n} (2|0\rangle^{\otimes n}\langle 0|^{\otimes n} - \mathbb{I}) H^{\otimes n} = 2|\phi\rangle\langle\phi| - \mathbb{I}.$$

Abbiamo quindi le due operazioni  $O$  e  $G$  di Figura 3.3. L'idea alla base dell'algoritmo di Grover è l'applicazione ripetuta della successione di operazioni  $O$  e  $G$ : dimostreremo tra un attimo che se applichiamo la successione  $\dots GOGOG\dots OGOGO$  (termina con  $O$ , quindi  $O$  è il primo operatore che viene applicato) costituita da  $k$  volte l'applicazione di tali operazioni allora per  $k = \mathcal{O}(\sqrt{N})$  la probabilità che lo stato finale rimanente sia  $|a\rangle$  è prossima ad 1.

Vediamo due semplici modi per descrivere questo procedimento.

### 3.9.1 Interpretazione geometrica

Vediamo il motivo della conclusione precedente secondo un semplice argomento geometrico. Il vettore  $|a\rangle$  è un particolare stato della sovrapposizione (3.9.3), quindi possiamo chiedere di calcolare il seguente prodotto scalare:

$$\langle a|\phi\rangle = \frac{1}{2^{\frac{n}{2}}} \ll 1;$$

il risultato è un numero molto piccolo perché stiamo assumendo che  $n$  sia molto grande (come detto all'inizio, un algoritmo di ricerca è sensato solamente se il database contiene un numero enorme di oggetti). Questo significa che  $|\phi\rangle$  è quasi ortogonale ad  $|a\rangle$ , ossia coincide quasi con l'asse orizzontale (si pensi alla Figura 3.3b). Si noti dalla Figura 3.4a che

$$\sin \theta = \cos\left(\frac{\pi}{2} - \theta\right) = \langle a|\phi\rangle = \frac{1}{2^{\frac{n}{2}}} \ll 1, \quad \Rightarrow \quad \sin \theta \approx \theta = \frac{1}{2^{\frac{n}{2}}}.$$

Siccome i nostri oggetti nel database sono  $N = 2^n$  (con  $N$  grande e  $n$  numero di qubit), allora  $\theta \sim 1/\sqrt{N}$ . Cosa succede a  $|\phi\rangle$  quando si applica la sequenza di  $G$  ed  $O$ ? Si veda l'esempio di Figura 3.4b: il primo step è  $O$ , ossia una riflessione lungo  $\{|a\rangle\}^\perp$ , quindi  $|\phi\rangle$  viene ribaltato al di sotto dell'asse orizzontale di un angolo  $\theta$ ; lo step successivo è  $G$ , ossia una riflessione lungo  $|\phi\rangle$ , che riporta il vettore nel primo quadrante con un angolo  $2\theta$  da  $|\phi\rangle$ . Si noti che l'azione complessiva di  $O$  e  $G$  è una doppia riflessione, cioè una rotazione, per cui lo stato  $\phi$  è passato da un angolo  $\theta$  a un angolo  $3\theta$  dall'asse orizzontale. Applicando, nei due step successivi, nuovamente la sequenza  $GO$  (prima  $O$  poi  $G$ ) si passerà da un angolo  $3\theta$  a  $5\theta$ . Iterando questo procedimento per  $r$  iterazioni, avremo che l'angolo finale diventa  $\theta + 2r\theta$ . Dopo quante iterazioni il vettore risulta essenzialmente verticale? In termini di angoli significa imporre che  $\theta + 2r\theta \simeq \frac{\pi}{2}$ , quindi  $r \simeq \frac{\pi}{4\theta} - \frac{1}{2}$ . Ma  $\theta$  è piccolo, per cui il secondo termine è trascurabile e si ottiene

$$r \approx \frac{\pi}{4\theta} = \frac{\pi}{4}\theta^{-1} \approx \frac{\pi}{4}\sqrt{N};$$

quindi dopo  $\mathcal{O}(\sqrt{N})$  iterazioni di  $GO$  si arriva allo stato  $|a\rangle$  con probabilità prossima

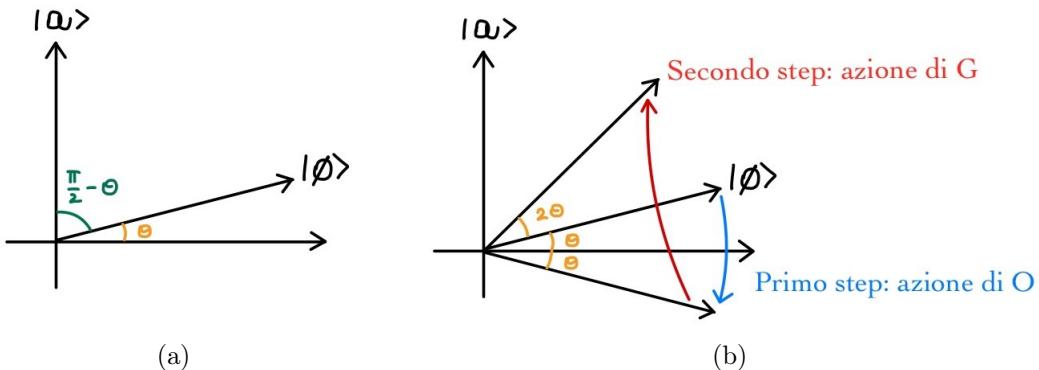


Figura 3.4: (3.4a) Il prodotto scalare tra  $|a\rangle$  e  $|\phi\rangle$  è dato da  $\cos(\frac{\pi}{2} - \theta) = \sin \theta$ . (3.4b) Implementazione dei primi due step  $GO$ . Si noti che le due riflessioni corrispondono ad una rotazione: lo stato finale  $GO|\phi\rangle$  è ruotato di angolo  $2\theta$  rispetto a  $|\phi\rangle$  e di angolo  $3\theta$  rispetto all'asse orizzontale.

ad 1: possiamo infatti trovare  $|a\rangle$  attraverso una misura finale dello stato  $(GO)^r |\phi\rangle$ ; si dimostra che

$$(GO)^r |\phi\rangle = \sqrt{1 - \varepsilon^2} |a\rangle + \varepsilon |a\rangle^\perp , \quad \varepsilon \ll 1 .$$

Se siamo sfortunati e non otteniamo  $|a\rangle$ , possiamo eseguire nuovamente l'algoritmo magari incrementando il numero di iterazioni e provare a misurare nuovamente. Dopo un numero limitato di tentativi troveremo  $a$ !

### 3.9.2 Interpretazione grafica: inversione rispetto alla media

Esiste un altro modo grafico per visualizzare il risultato dell'algoritmo di Grover. Supponiamo di partire con un generico stato  $|\psi\rangle = \sum_x \alpha_x |x\rangle$  espanso nella base computazionale. Scriviamo esplicitamente l'azione di  $O$  e  $G$  su  $|\psi\rangle$ :

- L'operatore  $O$  è la riflessione rispetto alla direzione individuata da  $\{|a\rangle\}^\perp$ , quindi inverte l'ampiezza solamente per  $x = a$ :

$$O : \begin{cases} \alpha_a \rightarrow -\alpha_a , & x = a \\ \alpha_x \rightarrow \alpha_x , & x \neq a \end{cases} .$$

- Per capire l'azione di  $G$ , invece, ricordiamo la (3.9.4) dove  $|\phi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$ . Calcoliamo  $G|\psi\rangle$ :

$$\begin{aligned} G|\psi\rangle &= (2|\phi\rangle\langle\phi| - \mathbb{I})|\psi\rangle = \frac{2}{N} \sum_{x=0}^{2^n-1} |x\rangle \sum_{y=0}^{2^n-1} \langle y| \left( \sum_{z=0}^{2^n-1} \alpha_z |z\rangle \right) - \sum_{x=0}^{2^n-1} \alpha_x |x\rangle \\ &= \sum_{x=0}^{2^n-1} \left( 2 \sum_{y=0}^{2^n-1} \frac{\alpha_y}{N} - \alpha_x \right) |x\rangle , \end{aligned}$$

dove a secondo passaggio abbiamo utilizzato  $\langle y|z\rangle = \delta_{yz}$  (si ricordi l'ortonormalizzazione degli stati della base computazionale). Perciò l'azione dell'operatore  $G$  non è altro che una riflessione rispetto al valor medio dell'ampiezza:

$$G : \alpha_x \rightarrow 2\langle\alpha\rangle - \alpha_x , \quad \text{dove } \langle\alpha\rangle \equiv \sum_{y=0}^{2^n-1} \frac{\alpha_y}{N} .$$

Ricordiamo che nell'algoritmo si parte dallo stato  $|\phi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$ . Disegnando in ascissa i diversi stati e in ordinata l'ampiezza di ciascun stato, l'azione grafica ripetuta degli operatori  $O$  e  $G$  su  $|\phi\rangle$  è mostrata nei diversi plot di Figura 3.5. È evidente come la continua applicazione di  $O$  e  $G$  ad ogni step faccia in modo che l'ampiezza di  $|a\rangle$  aumenti sempre di più fino a 1 e le ampiezze degli stati rimanenti diminuiscano sempre di più tendendo a 0.

Questo modo di procedere per visualizzare l'azione dell'algoritmo di Grover è utile anche nel caso in cui si voglia effettuare una ricerca di  $M$  numeri speciali all'interno degli  $N$  oggetti del database. Come evidenziano i plot di Figura 3.6, dopo un certo numero di applicazioni di  $O$  e  $G$ , le  $M$  ampiezze cercate tendono al valore  $1/M$  e si isolano automaticamente rispetto a tutte le altre.

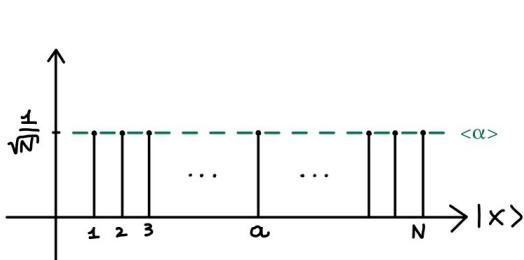
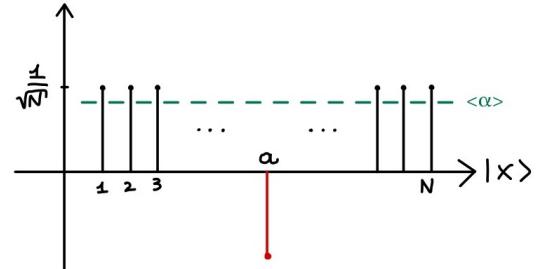
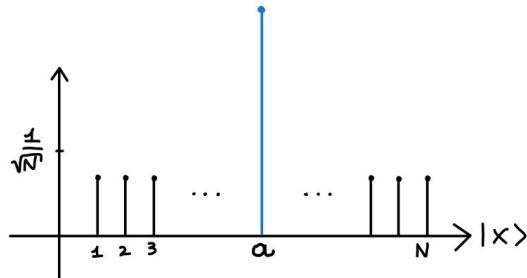
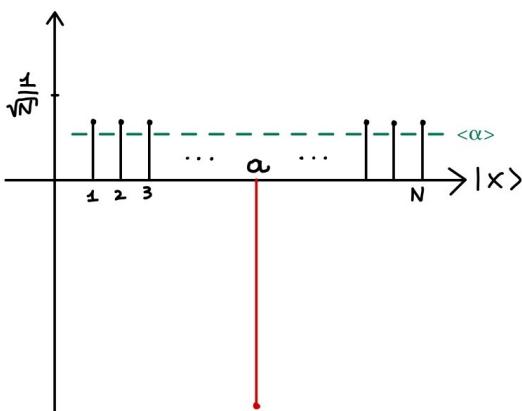
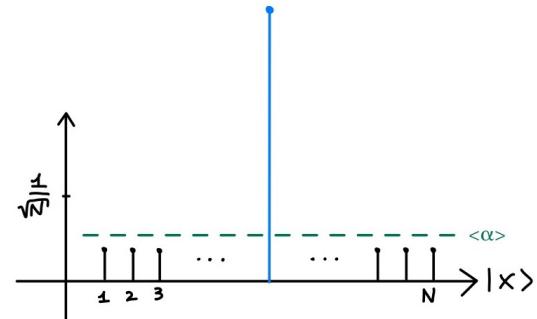
(a) Stato iniziale  $|\phi\rangle$ .(b) Azione di  $O$ : stato  $O|\phi\rangle$ .(c) Azione di  $G$ : stato  $GO|\phi\rangle$ .(d) Azione di  $O$ : stato  $OGO|\phi\rangle$ .(e) Azione di  $G$ : stato  $GOGO|\phi\rangle$ .

Figura 3.5: Esempio dell'applicazione dei primi due step  $GOGO$  allo stato  $|\phi\rangle$ . In rosso e in blu sono indicate le azioni di  $O$  e  $G$  rispettivamente sullo stato  $|a\rangle$ ; in verde scuro (con una linea tratteggiata orizzontale) è mostrata la media  $\langle\alpha\rangle$  delle ampiezze. Si noti come  $O$  porti ogni volta ad una diminuzione della media (solo l'ampiezza di  $|a\rangle$  è invertita);  $G$ , invece, causa una diminuzione di tutte le ampiezze di  $|x\rangle \neq |a\rangle$  e un aumento dell'ampiezza di  $|a\rangle$ . Ad ogni step l'ampiezza di  $|a\rangle$  diventa sempre più alta tendendo ad 1.

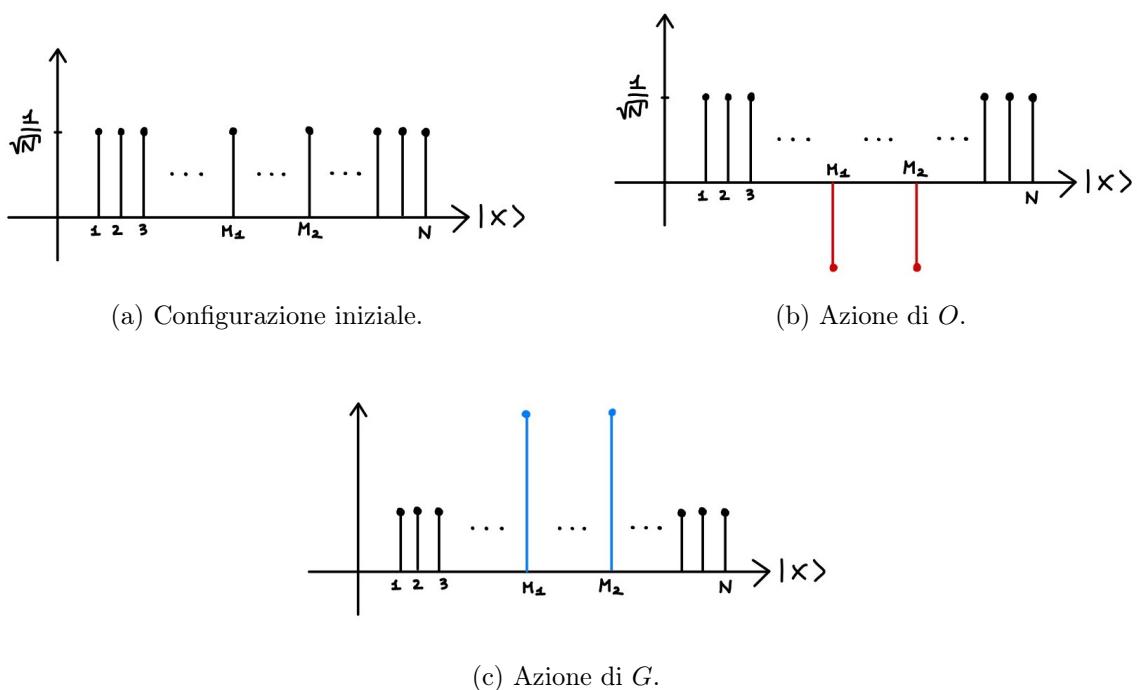


Figura 3.6: Esempio di applicazione dell'algoritmo di ricerca di Grover per un database contenente due oggetti speciali, indicati con  $M_1$  e  $M_2$ . In rosso e in blu sono mostrate le azioni di  $O$  e  $G$  sulle due ampiezze cercate.

# Capitolo 4

## Sistemi aperti

LEZIONE 9 - 05/11/2021

### 4.1 Matrice densità

Il formalismo della **matrice densità** viene solitamente introdotto per affrontare situazioni in cui sono presenti sia un'incertezza quantistica, intrinseca alla QM, che un'incertezza classica, dovuta all'ignoranza su alcune configurazioni del sistema. Spesso viene introdotta nell'ambito della fisica statistica, tuttavia viene largamente utilizzata anche in altri contesti.

Ad esempio: supponiamo di considerare un laboratorio e un ambiente esterno in cui è immerso; spesso, per descrivere la fisica del sistema completo, non si possono tenere in considerazione tutti i gradi di libertà dell'ambiente, così si assume che esista un'opportuna descrizione del laboratorio (nel quale potrebbe esserci un qubit o un apparato sperimentale) più l'ambiente e si prende una traccia (capiremo tra un attimo cosa significhi) su tutti i gradi di libertà dell'ambiente. In questo modo si ottiene una **descrizione efficace** del laboratorio, la quale contiene "nascosta" la nostra ignoranza relativa all'ambiente.

Vediamo la definizione generale:

**Definizione 4.1 (Matrice Densità).** Siano  $|\psi_i\rangle$  un insieme di stati quantistici con probabilità classica  $p_i$  ( $\sum_i p_i = 1$ ), ossia la probabilità di realizzare ogni stato  $|\psi_i\rangle$  è data da  $p_i$ . Indichiamo con  $\{p_i, |\psi_i\rangle\}$  l'insieme di tali stati con le rispettive probabilità (assumiamo che  $\langle \psi_i | \psi_i \rangle = 1$ ). Si definisce **matrice densità** (o **operatore densità**)  $\rho$  la seguente

$$\rho = \sum_i p_i |\psi_i\rangle \otimes \langle \psi_i| . \quad (4.1.1)$$

Si noti che, come evidenziato, le  $p_i$  sono probabilità *classiche* poiché è già intrinseca ad ogni stato  $|\psi_i\rangle$  la descrizione mediante probabilità *quantistica*. Chiaramente  $\rho$ , in quanto prodotto esterno, agisce come un operatore sugli stati dello spazio di Hilbert. È importante sottolineare che gli stati  $|\psi_i\rangle$  sono normalizzati ma non necessariamente ortogonali.

L'introduzione della (4.1.1) è utile perché permette di scrivere differenti quantità in forma compatta. Ad esempio, la media di un'osservabile  $A$  può essere scritta come

$$\langle A \rangle = \text{Tr}(\rho A) . \quad (4.1.2)$$

*Dimostrazione.* Scriviamo

$$\mathrm{Tr}(\rho A) = \sum_i p_i \mathrm{Tr}(|\psi_i\rangle\langle\psi_i| A) = \sum_i p_i \langle\psi_i|A|\psi_i\rangle = \langle A \rangle ,$$

dove nel secondo passaggio abbiamo utilizzato la proprietà ciclica della traccia per muovere il ket a destra. Notiamo che questa operazione può essere svolta per la ragione seguente: in generale per gli operatori si ha  $\mathrm{Tr} B = \sum_n \langle n|B|n\rangle$  dove  $\{|n\rangle\}$  è una base ortonormale, perciò nel passaggio sopra possiamo scrivere

$$\mathrm{Tr}(|\psi_i\rangle\langle\psi_i| A) = \sum_n \langle n|\psi_i\rangle \langle\psi_i|A|n\rangle = \sum_n \langle\psi_i|A|n\rangle \langle n|\psi_i\rangle = \langle\psi_i|A|\psi_i\rangle ,$$

dove nell'ultimo passaggio abbiamo utilizzato la relazione di completezza  $\mathbb{I} = \sum_n |n\rangle\langle n|$ .  $\square$

Se si possiede solamente uno stato  $|\psi\rangle$ , esso viene chiamato **stato puro**, quindi la matrice densità si scriverà come  $\rho = |\psi\rangle\langle\psi|$ . Al contrario, un insieme di stati  $\{p_i, |\psi_i\rangle\}$ , con almeno 2 probabilità  $p_i \neq 0$ , avrà matrice densità  $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$  ed è chiamato **stato misto o miscela di stati** (nota anche come **mixture**). Ribadiamo nuovamente che in quest'ultima situazione l'incertezza classica  $p_i$  si va ad aggiungere all'incertezza puramente quantomeccanica degli stati quantistici.

**Esempio 4.1 (Miscela in Meccanica Statistica).** *Il più semplice esempio di miscela di stati in meccanica statistica è costituito dall'insieme di stati  $\{E_n, |n\rangle\}$ , dove  $H|n\rangle = E_n|n\rangle$ , in cui assegniamo ad ogni stato una probabilità classica*

$$P(E_n) = \frac{e^{-\frac{E_n}{k_B T}}}{Z}, \quad \text{con } Z = \sum_n e^{-\frac{E_n}{k_B T}},$$

dove  $Z$  è chiamata **funzione di partizione**. Quindi per studiare un tale sistema dal punto di vista quantistico possiamo dire che in aggiunta all'incertezza quantistica ci sono altre probabilità classiche  $P(E_n)$  dipendenti dalla temperatura. Per un tale sistema la matrice densità non è altro che

$$\rho = \sum_n p_n |n\rangle\langle n|, \quad \text{dove } p_n \equiv P(E_n) = \frac{e^{-\frac{E_n}{k_B T}}}{Z}.$$

Vediamo immediatamente l'esempio dei qubit per capire la differenza della matrice densità nel caso di uno stato puro e per miscele di stati:

**Esempio 4.2 (Singolo qubit: stato puro).** *Immaginiamo un qubit nello stato  $|0\rangle$ . La matrice (4.1.1) non è altro che*

$$\rho = |0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes (1 \ 0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} ,$$

dove nell'ultimo passaggio abbiamo utilizzato il prodotto di Kronecker della definizione 1.5.

**Esempio 4.3 (Singolo qubit: miscela di stati).** Si consideri un qubit nella miscela di stati in cui  $|0\rangle$  è dato con probabilità  $p$  e  $|1\rangle$  con probabilità  $1-p$  (non stiamo prendendo la solita sovrapposizione di stati della QM). Allora la matrice densità risulterà

$$\rho = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1| = p \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + (1-p) \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p & 0 \\ 0 & 1-p \end{pmatrix}.$$

Notiamo che dal punto di vista dell'informazione, nello stato puro la matrice densità ha solamente un'entrata: non vi è alcuna incertezza classica (solamente quantistica). Al contrario, per la miscela di stati abbiamo il caso della maggior incertezza possibile quando  $p = \frac{1}{2}$  perché  $\rho = \frac{1}{2}\mathbb{I}$ . In generale, per matrici diagonali, sono miscele le configurazioni in cui più di un'entrata diagonale è non nulla. Si noti dall'esempio 4.3 che sulle entrate diagonali di  $\rho$  si può leggere l'incertezza classica collegata agli stati  $|0\rangle$  e  $|1\rangle$ .

Questi esempi erano molto semplici perché  $\rho$  è diagonale: la matrice densità non è in generale diagonale né per gli stati puri né per le miscele. Vediamo alcuni esempi:

**Esempio 4.4 (Stato puro:  $\rho$  non diagonale).** Consideriamo il caso dello stato puro di un qubit nella sua forma più generale, ossia  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ . La (4.1.1) diventa una matrice non diagonale, infatti

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes (\alpha^* \quad \beta^*) = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}.$$

Si noti dall'esempio precedente la differenza tra le entrate diagonali e non: su quelle diagonali vi sono le probabilità quantistiche del risultato di una misura, mentre su quelle non diagonali sono presenti dei prodotti tra  $\alpha$  e  $\beta$  che misurano, in un certo senso, l'interferenza (sovraposizione) tra  $|0\rangle$  e  $|1\rangle$ .

**Esempio 4.5 (Miscela:  $\rho$  non diagonale).** Supponiamo di avere la miscela costituita dal 50% di probabilità di avere  $|0\rangle$  e dal 50% di probabilità di avere  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ . In questo caso  $\rho$  non è diagonale ed è data da una combinazione lineare di stati non ortogonali:

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +| = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{4} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes (1 \quad 1) = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix}.$$

Vediamo alcune proprietà generali della matrice densità:

1.  $\rho$  è hermitiana e positiva.

*Dimostrazione.* Ricordando che  $p_i \geq 0 \in \mathbb{R}$  allora

$$\left( \sum_i p_i |\psi_i\rangle\langle\psi_i| \right)^\dagger = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

La positività di un operatore  $A$  è data dalla proprietà  $\langle\phi|A|\phi\rangle \geq 0$  per ogni  $|\phi\rangle$ , quindi

$$\langle\phi|\rho|\phi\rangle = \langle\phi| \sum_i p_i |\psi_i\rangle\langle\psi_i|\phi\rangle = \sum_i p_i \langle\phi|\psi_i\rangle \underbrace{\langle\psi_i|\phi\rangle}_{\langle\phi|\psi_i\rangle^*} = \sum_i p_i |\langle\phi|\psi_i\rangle|^2 \geq 0.$$

□

2.  $\text{Tr } \rho = 1$ .

*Dimostrazione.*

$$\text{Tr} \left[ \sum_i p_i |\psi_i\rangle\langle\psi_i| \right] = \sum_i p_i \text{Tr} |\psi_i\rangle\langle\psi_i| = \sum_i p_i \langle\psi_i|\psi_i\rangle = 1,$$

dove nel penultimo passaggio abbiamo usato la proprietà ciclica della traccia come nella dimostrazione della (4.1.2).  $\square$

3.  $\text{Tr } \rho^2 \leq 1$  e  $\text{Tr } \rho^2 = 1$  solo per gli stati puri.

*Dimostrazione.* Dato che  $\rho$  è hermitiana allora può essere diagonalizzata, quindi  $\rho |n\rangle = \rho_n |n\rangle$ . In particolare avremo

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \equiv \sum_n \rho_n |n\rangle\langle n|; \quad (4.1.3)$$

quindi la matrice densità è scrivibile come somma del prodotto tra i proiettori nella direzione degli autospazi e dei corrispondenti autovalori. Notiamo che la formula precedente consiste di fatto nella diagonalizzazione in notazione di Dirac. Chiaramente in generale  $p_i \neq \rho_i$ ! Dato che  $\text{Tr } \rho = 1$  allora dalla precedente si ha che  $\sum_n \rho_n = 1$ . Cerchiamo di valutare  $\text{Tr } \rho^2 = \sum_n \rho_n^2$ : dato che la matrice densità è hermitiana e positiva allora  $\rho_n \geq 0 \in \mathbb{R}$ , ma al tempo stesso si deve avere  $0 \leq \rho_n \leq 1$  poiché  $\sum_n \rho_n = 1$ . Ma allora

$$0 \leq \rho_n^2 \leq \rho_n \leq 1, \Rightarrow \sum_n \rho_n^2 \leq \sum_n \rho_n = 1.$$

Il caso limite è dato da

$$\sum_n \rho_n^2 = 1 = \sum_n \rho_n \Leftrightarrow \rho_n = \rho_n^2, \forall n,$$

ma per numeri tra 0 e 1 questo è vero solamente per  $\rho_n = 1 \vee \rho_n = 0$ : solamente un valore è diverso da 0 (uguale a 1) mentre tutti gli altri sono 0, quindi  $\rho = |n\rangle\langle n|$  per un particolare  $n$ , ossia si tratta di uno stato puro.  $\square$

Si noti che la formula  $[\text{Tr } \rho^2 = 1 \Leftrightarrow \text{stato puro}]$  è un criterio per stabilire se effettivamente uno stato è puro. Inoltre, essendo  $\rho$  hermitiana, può sempre essere diagonalizzata secondo la (4.1.3) e quindi la sua forma non è unica (si pensi ai casi degli esempi 4.4 e 4.5 che possono essere diagonalizzati).

Torniamo al caso dei qubit. Avevamo visto che la più generale matrice hermitiana  $2 \times 2$  può essere scritta come  $\rho = a_0 \mathbb{I} + \vec{a} \cdot \vec{\sigma}$  con  $a_0, \vec{a} \in \mathbb{R}$ , ma  $\text{Tr } \rho = 1$  e quindi, dato che le matrici di Pauli hanno traccia nulla, avremo  $1 = 2a_0$ , ossia  $a_0 = \frac{1}{2}$ . Possiamo allora scrivere la matrice densità come

$$\rho = \frac{\mathbb{I} + \vec{r} \cdot \vec{\sigma}}{2}, \text{ dove } r_i \in \mathbb{R}. \quad (4.1.4)$$

Quali sono gli autovalori di  $\rho$ ? Sappiamo che  $\vec{r} \cdot \vec{\sigma}$  è lo spin in direzione  $\vec{r}$ , il quale ha autovalori  $|\vec{r}|$  e  $-|\vec{r}|$ , inoltre  $\rho$  è hermitiana, quindi

$$\text{eig}(\rho) \equiv \lambda = \frac{1 \pm |\vec{r}|}{2} \geq 0, \quad \Rightarrow \quad |\vec{r}| \leq 1.$$

Calcoliamo ora  $\text{Tr } \rho^2$  sempre usando la (4.1.4):

$$\text{Tr } \rho^2 = \text{Tr} \left[ \frac{1}{4} (\mathbb{I} + 2\vec{r} \cdot \vec{\sigma} + |\vec{r}|^2) \right] = \frac{1 + |\vec{r}|^2}{2} \leq 1,$$

dove abbiamo usato il risultato seguente

$$r_i r_j \sigma_i \sigma_j = r_i r_j (\delta_{ij} \mathbb{I} + i \varepsilon_{ijk} \sigma_k) = |\vec{r}|^2 + i (\varepsilon_{kij} r_i r_j) \sigma_k = |\vec{r}|^2 + i \underbrace{(\vec{r} \times \vec{r}) \cdot \vec{\sigma}}_0 = |\vec{r}|^2.$$

Notiamo che per gli stati puri  $\frac{1+|\vec{r}|^2}{2} = 1 \Leftrightarrow |\vec{r}|^2 = 1$ , quindi possiamo impiegare nuovamente la descrizione grafica con la sfera di Bloch che abbiamo introdotto nella Sottosezione 1.1.1. Associamo il punto dato da  $\vec{r}$  con la matrice densità (4.1.4) in maniera tale da estendere questa descrizione anche ai punti interni della sfera (si veda la Figura 1.1 a Pagina 8): i punti sulla superficie sono stati puri, mentre quelli all'interno sono delle miscele di stati. Tenendo presente la Figura 1.2 a Pagina 10, focalizziamo la nostra attenzione su due direzioni precise:

- Consideriamo l'asse  $z$ : in tal caso avremo  $\vec{r} = (0, 0, r)$  con  $r \in [-1, 1]$ . Chiaramente i due stati corrispondenti ai punti sulla superficie sono  $|0\rangle$  per  $z = 1$  e  $|1\rangle$  per  $z = -1$ . La matrice densità non è altro che

$$\rho = \frac{\mathbb{I}}{2} + \frac{r}{2} \sigma_3 = \begin{pmatrix} \frac{1+r}{2} & 0 \\ 0 & \frac{1-r}{2} \end{pmatrix} \equiv \begin{pmatrix} p & 0 \\ 0 & 1-p \end{pmatrix}, \quad \text{con } p = \frac{1+r}{2}; \quad (4.1.5)$$

si tratta della stessa forma dell'Esempio 4.3: si ha una miscela di stati con probabilità classiche  $p$  di avere  $|0\rangle$  e  $1-p$  di avere  $|1\rangle$ .

- Consideriamo ora, invece, l'asse  $x$ : in tal caso  $\vec{r} = (r, 0, 0)$  e gli stati sulla superficie (intersezione sfera con asse  $x$ ) sono  $|+\rangle$  per  $x = 1$  e  $|-\rangle$  per  $x = -1$ . La (4.1.4) non è altro che

$$\rho = \frac{\mathbb{I}}{2} + \frac{r}{2} \sigma_1 = \begin{pmatrix} \frac{1}{2} & \frac{r}{2} \\ \frac{r}{2} & \frac{1}{2} \end{pmatrix}; \quad (4.1.6)$$

perciò i punti corrispondenti a  $|+\rangle$  e  $|-\rangle$  sono gli stati puri nella direzione in cui si sta misurando lo spin, mentre tutti gli altri punti intermedi lungo  $x$  sono una miscela di  $|+\rangle$  e  $|-\rangle$ .

Notiamo che il punto  $\vec{r} = 0$  è l'unico punto comune a tutti e 3 gli intervalli nelle 3 direzioni spaziali: esso corrisponde alla massima indeterminazione possibile, infatti

$$\rho = \frac{\mathbb{I}}{2} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix},$$

il quale non è altro che una sovrapposizione dei due autostati corrispondenti ognuno una probabilità classica del 50%. Un fatto importante da sottolineare è che la matrice precedente può essere ottenuta sia dalla (4.1.5) che dalla (4.1.6) ponendo  $p = \frac{1}{2}$  e  $r = 0$ : solamente conoscendo la matrice densità di un sistema non siamo in grado di distinguere la miscela di stati in cui ci troviamo!

## 4.2 Sottosistemi e traccia parziale

Torniamo ad affrontare alcuni casi interessanti dal punto di vista della fisica dei qubit. Il formalismo della matrice densità risulta utile quando si hanno sistemi bipartiti tali che  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ . Supponiamo che Alice si trovi in un laboratorio descritto da  $\mathcal{H}_A$  e che Bob invece sia in un altro laboratorio descritto da  $\mathcal{H}_B$ : la matrice densità è utile quando si vuole studiare la fisica dal punto di vista di Alice, la quale ignora il laboratorio di Bob; Alice vorrebbe ignorare parte dello spazio di Hilbert totale perché non ne ha l'accesso completo. Questo fatto, vedremo, porta ad una descrizione fisica in termini di miscele di stati anche se si era partiti da uno stato puro in  $\mathcal{H}$ .

Che cosa significa fare esperimenti dal punto di vista di Alice? Significa che Alice effettua misure di osservabili della forma  $O = O_A \otimes \mathbb{I}_B$ , quindi agisce solamente nel proprio laboratorio senza fare nulla sul laboratorio di Bob. Immaginiamo che i due laboratori siano soggetti a dell'indeterminazione classica, quindi il sistema totale è ben descritto da un'opportuna matrice densità  $\rho$ . Siamo interessati al sottosistema descritto da  $\mathcal{H}_A$ : chiamiamo  $\{|nm\rangle\}$  la base dello spazio di Hilbert totale  $\mathcal{H}$  dove  $|nm\rangle \equiv |n\rangle_A \otimes |m\rangle_B$  con  $|n\rangle_A \in \mathcal{H}_A$  e  $|m\rangle_B \in \mathcal{H}_B$ . Calcoliamo il valor medio di  $O$  mediante la (4.1.2):

$$\begin{aligned}\langle O \rangle &= \text{Tr}(O\rho) = \sum_{n,m} \langle nm|O\rho|nm\rangle \\ &= \sum_{\substack{n,m \\ n',m'}} \langle nm|O_A \otimes \mathbb{I}_B|n'm'\rangle \langle n'm'| \rho |nm\rangle \\ &= \sum_{\substack{n,m \\ n',m'}} \langle n|O_A|n'\rangle \underbrace{\langle m|m'\rangle}_{\delta_{mm'}} \langle n'm'| \rho |nm\rangle \\ &= \sum_{n,m,n'} \langle n|O_A|n'\rangle \langle n'm| \rho |nm\rangle \\ &= \sum_{n,n'} \langle n|O_A|n'\rangle \sum_m \langle n'm| \rho |nm\rangle ,\end{aligned}$$

dove nella seconda riga abbiamo inserito una relazione di completezza nello spazio  $\mathcal{H}$ :  $\mathbb{I} = \sum_{n',m'} |n'm'\rangle\langle n'm'|$ . Definiamo ora il seguente oggetto

$$\langle n'|\rho_A|n\rangle \equiv \sum_m \langle n'm| \rho |nm\rangle , \quad (4.2.1)$$

dove chiaramente  $\rho_A$  agisce solamente su  $\mathcal{H}_A$ . In questo modo la precedente diventa

$$\langle O \rangle = \sum_{n,n'} \langle n|O_A|n'\rangle \langle n'|\rho_A|n\rangle = \sum_n \langle n|O_A\rho_A|n\rangle = \text{Tr}(O_A\rho_A) ,$$

dove abbiamo tolto, nel penultimo passaggio, una relazione di completezza in  $\mathcal{H}_A$ . In definitiva abbiamo ricavato

$$\langle O \rangle = \text{Tr}(O_A\rho_A) . \quad (4.2.2)$$

Siamo partiti dal considerare un valor medio di una grandezza di tutto lo spazio di Hilbert, ma abbiamo ricavato una formula che considera solamente oggetti che agiscono su  $\mathcal{H}_A$ ! La relazione (4.2.2) permette di dare una **descrizione efficace** di tutti i gradi di libertà del sistema prendendo una cosiddetta "traccia parziale sullo spazio di Hilbert  $\mathcal{H}_B$ ".

Omettendo  $n, n'$  ad entrambi i membri, possiamo scrivere la definizione (4.2.1) in forma più compatta come

$$\rho_A = \sum_m \langle m | \rho | m \rangle \equiv \text{Tr}_B \rho ;$$

risulta ancora più evidente che  $\rho_A$  sia costruita prendendo una traccia sui gradi di libertà del laboratorio di Bob, tuttavia notiamo che quest'ultima formula è un po' fuorviante dato che  $\rho_A$  è un operatore e il RHS sembrerebbe invece un numero: il simbolo " $\text{Tr}_B$ " non produce un numero, bensì un operatore agente unicamente su  $\mathcal{H}_A$ .

Vediamo immediatamente due semplici esempi per fissare meglio questi concetti.

**Esempio 4.6 (Fisica "fattorizzata").** Supponiamo che la fisica di un sistema possa essere "fattorizzata" scrivendo  $\rho = \rho_A \otimes \rho_B$ . Supponiamo di voler studiare il sistema dal punto di vista di Alice:

$$\text{Tr}_B \rho = \text{Tr}_B (\rho_A \otimes \rho_B) = \sum_m \langle m | \rho_A \otimes \rho_B | m \rangle = \rho_A \otimes \sum_m \langle m | \rho_B | m \rangle = \rho_A \underbrace{\text{Tr} \rho_B}_1 = \rho_A ;$$

quindi se si vuole studiare la fisica di  $\mathcal{H}_A$  e la fisica totale è disaccoppiata, ci si aspetta che prendere una traccia sui gradi di libertà esterni produca  $\rho_A$ : per effettuare una misura nel laboratorio di Alice bisogna solamente utilizzare  $\rho_A$ .

**Esempio 4.7 (Qubit in stati separabili).** Supponiamo che Alice e Bob condividano due qubit in uno stato separabile,  $|00\rangle$  ad esempio, dove la prima entrata appartiene ad Alice e la seconda a Bob. Anche in una situazione come questa la fisica è fattorizzata e le misurazioni sono indipendenti perché il collasso dello stato non produce alcunché di nuovo. Cosa succede a  $\rho$  dal punto di vista di Alice? Sappiamo che  $\rho = |00\rangle\langle 00|$  quindi

$$\rho_A \equiv \text{Tr}_B \rho = \text{Tr}_B |00\rangle\langle 00| = \sum_m \langle m | 00 \rangle \langle 00 | m \rangle = |0\rangle\langle 0| ,$$

dove nell'ultimo passaggio sopravvivono solamente i prodotti scalari per  $m = 0$ . In questa situazione abbiamo ottenuto che  $\rho_A$  corrisponde alla matrice densità di uno stato puro, perché metà delle paia di qubit appartengono ad Alice.

Chiaramente, in analogia con gli stati separabili, i casi degli esempi precedenti non sono molto utili e interessanti. Vediamo, invece, che per stati entangled l'effetto della traccia diventa del tutto non banale:

**Esempio 4.8 (Qubit in stati entangled).** Supponiamo che Alice e Bob condividano lo stato entangled  $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  (come nell'esempio precedente ad Alice appartiene la prima entrata mentre a Bob la seconda). Scriviamo la matrice densità totale:

$$\rho = |\psi\rangle\langle\psi| = \frac{1}{2} (|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|) ;$$

si noti che lo stato  $|\psi\rangle$  è puro nello spazio di Hilbert totale. Vediamo la matrice densità di Alice:

$$\rho_A = \text{Tr}_B \rho = \sum_m \langle m | \rho | m \rangle = \langle 0 | \rho | 0 \rangle + \langle 1 | \rho | 1 \rangle ;$$

calcoliamo separatamente i due termini:

$$\begin{aligned} \langle 0 | \rho | 0 \rangle &= \frac{1}{2} (\langle 0 | 00 \rangle \langle 00 | 0 \rangle + \langle 0 | 00 \rangle \langle 11 | 0 \rangle + \langle 0 | 11 \rangle \langle 00 | 0 \rangle + \langle 0 | 11 \rangle \langle 11 | 0 \rangle) = \frac{1}{2} |0\rangle\langle 0| , \\ \langle 1 | \rho | 1 \rangle &= \frac{1}{2} (\langle 1 | 00 \rangle \langle 00 | 1 \rangle + \langle 1 | 00 \rangle \langle 11 | 1 \rangle + \langle 1 | 11 \rangle \langle 00 | 1 \rangle + \langle 1 | 11 \rangle \langle 11 | 1 \rangle) = \frac{1}{2} |1\rangle\langle 1| , \end{aligned}$$

quindi avremo semplicemente che

$$\rho_A = \frac{1}{2} (|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2} \sum_n |n\rangle\langle n| = \frac{\mathbb{I}}{2}.$$

Come sottolineato in precedenza, si tratta del caso peggiore possibile in cui tutto è completamente indeterminato: dal punto di vista di Alice c'è una totale casualità.

Perciò anche se si parte da uno stato puro nello spazio di Hilbert totale (universo) e si decide di effettuare un esperimento solo localmente, la traccia parziale può trasformarlo in una matrice densità: tracce parziali producono tipicamente matrici densità.

Come ultima curiosità enunciamo il teorema seguente:

**Teorema 4.1 (Teorema di purificazione).** *Data la traccia parziale  $\rho_A$  agente su  $\mathcal{H}_A$ , esiste sempre uno spazio di Hilbert più grande  $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$  e uno stato puro  $|\psi\rangle \in \mathcal{H}$  tale che*

$$\rho_A = \text{Tr}_B \rho, \quad \text{con } \rho = |\psi\rangle\langle\psi|.$$

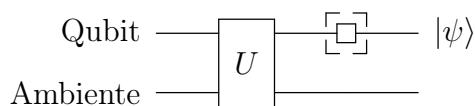
LEZIONE 10 - 08/11/2021

### 4.3 Interazione con l'ambiente

Focalizziamo la nostra attenzione sul discorso riguardante i qubit e sul modo con cui interagiscono con l'ambiente in cui sono immersi, ossia come sono influenzati dal rumore, dalla temperatura, ecc. Lo spazio di Hilbert generale è il prodotto tensoriale tra quello del qubit e quello dell'ambiente:  $\mathcal{H} = \mathcal{H}_q \otimes \mathcal{H}_E$  (pedice  $E$  per "environment"). Come visto dai postulati della QM, possiamo assumere che l'evoluzione temporale in  $\mathcal{H}$  sia unitaria: se assumiamo uno stato puro iniziale  $|\psi\rangle \in \mathcal{H}$ , allora esso evolverà in  $|\psi'\rangle = U|\psi\rangle$  dove  $U$  è un operatore unitario.

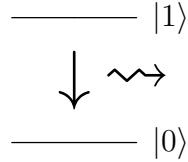
Come evidenziato nella sezione precedente, non vogliamo studiare il qubit mantenendo tutti i gradi di libertà dell'ambiente, quindi possiamo calcolare una traccia parziale su  $\mathcal{H}_E$ : si ricordi che anche se  $|\psi\rangle$  è uno stato puro, alla fine otteniamo una matrice densità  $\rho$  che descrive il sottosistema  $\mathcal{H}_q$ . Ad esempio, se il qubit è preparato nella sovrapposizione  $|\psi\rangle = a|0\rangle + b|1\rangle$ , dal punto di vista della fisica del qubit esso si trova in uno stato puro; quando si considera tuttavia l'intero sistema costituito anche dall'ambiente, la traccia parziale su  $\mathcal{H}_E$  produce una matrice densità del qubit tale che possa corrispondere ad una miscela di stati nonostante si partisse da uno stato puro!

Un punto importante da tenere sempre in considerazione è che l'evoluzione temporale del sottosistema del qubit non è necessariamente unitaria: supponiamo ad esempio che l'evoluzione di  $\mathcal{H}$  sia descritta dal seguente circuito



dove l'evoluzione totale  $U$  è unitaria. Il problema è che il risultato  $|\psi\rangle \in \mathcal{H}_q$  dell'evoluzione del qubit potrebbe derivare da un operatore non unitario di  $\mathcal{H}_q$ ! (si veda il gate ignoto nel riquadro tratteggiato).

Uno dei modi per realizzare un qubit è quello di considerare un atomo che presenta due livelli energetici vicini tra loro, ma facilmente isolabili rispetto ai livelli restanti. Chiamiamo  $|1\rangle$  e  $|0\rangle$  lo stato eccitato e il ground state rispettivamente. Un fenomeno che accade spontaneamente in natura è l'**emissione spontanea** di fotoni



(la freccia verticale indica la transizione  $|1\rangle \rightarrow |0\rangle$ , mentre quella orizzontale indica l'emissione del fotone). In generale questo accade sempre se si aspetta un tempo sufficientemente lungo. Chiaramente il fotone emesso viene perso nell'ambiente, quindi dal punto di vista del qubit,  $\mathcal{H}_q$  è lo spazio di Hilbert dei livelli energetici, mentre la radiazione ambientale di background, che è parte del campo elettromagnetico quantizzato, costituisce l'ambiente in cui il qubit è immerso. Come detto sopra, dal punto di vista del sistema totale l'evoluzione è unitaria, tuttavia in  $\mathcal{H}_q$  l'emissione spontanea è descritta dal seguente operatore  $\tilde{U}$

$$\tilde{U} : \begin{cases} |1\rangle \rightarrow |0\rangle \\ |0\rangle \rightarrow |0\rangle \end{cases}, \Rightarrow \tilde{U} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

e chiaramente la matrice  $\tilde{U}$  non è unitaria!

Diamo uno sguardo più dettagliato a questi processi generali. Supponiamo che  $\mathcal{H}$  sia un sistema **chiuso** descritto da un evoluzione unitaria  $U$  tale che

$$|\psi\rangle \rightarrow U|\psi\rangle, \\ \langle\psi| \rightarrow \langle\psi|U^\dagger;$$

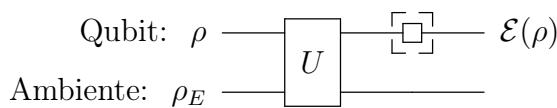
usando il formalismo della matrice densità possiamo scrivere  $\rho = |\psi\rangle\langle\psi|$ : come evolve  $\rho$  a seguito di evoluzioni unitarie degli stati? Semplicemente

$$\rho = |\psi\rangle\langle\psi| \rightarrow U|\psi\rangle\langle\psi|U^\dagger = U\rho U^\dagger,$$

quindi la matrice densità evolve per **coniugazione**. Questo vale anche nel caso di miscele, infatti

$$\rho = \sum_i \rho_i |\psi_i\rangle\langle\psi_i| \rightarrow \sum_i \rho_i U |\psi_i\rangle\langle\psi_i| U^\dagger = U\rho U^\dagger.$$

Ritorniamo al sistema totale descritto da  $\tilde{\mathcal{H}} = \mathcal{H}_q \otimes \mathcal{H}_E$ : chiamiamo  $\tilde{\rho}$  la matrice densità totale di  $\tilde{\mathcal{H}}$ , la quale può descrivere sia stati puri sia miscele (in generale a seguito della presenza di una temperatura finita si parte sempre con una miscela di stati). Scriviamo  $\tilde{\rho} = \rho \otimes \rho_E$ , dove chiaramente  $\rho$  è la matrice densità in  $\mathcal{H}_q$ . Cosa succede se si aspetta un tempo abbastanza lungo? Analizziamo la seguente situazione



dove  $\mathcal{E}(\rho)$  è l'evoluto di  $\rho$  in  $\mathcal{H}_q$ . Sappiamo che se il sistema totale qubit-ambiente è chiuso allora  $\tilde{\rho}$  evolverà per coniugazione come  $\tilde{\rho} \rightarrow U(\rho \otimes \rho_E)U^\dagger$ . Come al solito, per ignorare

i gradi di libertà dell'ambiente prendiamo una traccia parziale su di esso: definiamo la matrice densità

$$\mathcal{E}(\rho) = \text{Tr}_E [U(\rho \otimes \rho_E)U^\dagger], \quad (4.3.1)$$

che dà una descrizione efficace del qubit e ne descrive la fisica dal suo punto di vista. La mappa  $\rho \rightarrow \mathcal{E}(\rho)$  non è unitaria in generale! Come possiamo caratterizzare l'evoluzione dal punto di vista del qubit? Abbiamo detto che



Supponiamo che  $\mathcal{H}_E$  possieda la base  $\{|e_k\rangle\}$ , allora la (4.3.1) diventa

$$\mathcal{E}(\rho) = \sum_k \langle e_k | U(\rho \otimes \rho_E)U^\dagger | e_k \rangle,$$

dove sottolineiamo che la notazione non deve trarre in inganno perché  $U$  e  $U^\dagger$  agiscono sia sul qubit sia sull'ambiente (il RHS rimane un operatore, non una somma di elementi di matrice). Supponiamo che l'ambiente sia in uno stato puro iniziale, che chiamiamo  $|e_0\rangle$ : possiamo sempre assumere questa condizione senza alcuna perdita di generalità grazie al teorema di purificazione; quindi  $\rho_E = |e_0\rangle\langle e_0|$ . In questo modo la precedente diventa

$$\mathcal{E}(\rho) = \sum_k \langle e_k | U | e_0 \rangle \rho \langle e_0 | U^\dagger | e_k \rangle,$$

dove come prima notiamo che  $\langle e_k | U | e_0 \rangle$  e  $\langle e_0 | U^\dagger | e_k \rangle$  non sono elementi di matrice ma rimangono operatori agenti sul qubit. Chiamiamo

$$E_k \equiv \langle e_k | U | e_0 \rangle, \quad (4.3.2)$$

questi operatori ottenuti come elementi di matrice parziali con  $e_k$  e  $e_0$ : spesso vengono chiamati **operation elements**. In questo modo  $\mathcal{E}(\rho)$  può essere scritto come

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger, \quad (4.3.3)$$

il quale prende il nome di **operator-sum representation**; la mappa  $\mathcal{E}(\rho)$ , invece, prende il nome di **quantum operation**. Dato che  $\mathcal{E}(\rho)$  è una matrice densità deve soddisfare la condizione  $\text{Tr } \mathcal{E}(\rho) = 1$ :

$$\text{Tr } \mathcal{E}(\rho) = \text{Tr} \left( \sum_k E_k \rho E_k^\dagger \right) = \sum_k \text{Tr} \left( E_k \rho E_k^\dagger \right) = \sum_k \text{Tr} \left( \rho E_k^\dagger E_k \right) \stackrel{!}{=} 1;$$

dove nell'ultimo passaggio abbiamo usato la proprietà ciclica della traccia. Dato che  $\text{Tr } \rho = 1$ , allora gli operation elements devono soddisfare il vincolo seguente

$$\sum_k E_k^\dagger E_k = \mathbb{I}. \quad (4.3.4)$$

Notiamo che nella (4.3.4) si ha in generale  $E_k^\dagger E_k \neq \mathbb{I}$ , quindi  $E_k$  non sono unitari!

Qual è l'interpretazione fisica della (4.3.3)? Si assume che esistano numerosi processi, etichettati da  $k$ , ognuno dei quali è visto come un sottosistema in cui è eseguita una particolare evoluzione temporale, data da  $\rho \rightarrow E_k \rho E_k^\dagger$ . Ancora una volta, non si tratta di una coniugazione perché gli  $E_k$  non sono in generale unitari. Ciascun operatore  $E_k$  descritto dalla (4.3.2) è visto come un salto degli stati dell'ambiente da  $|e_0\rangle$  a  $|e_k\rangle$ .

Cominciamo a capire meglio come l'ambiente interagisce con i qubit guardando degli esempi esplicativi. Supponiamo un qubit nella sovrapposizione  $a|0\rangle + b|1\rangle$  che interagisce con l'ambiente: gli stati possono essere invertiti, possono essere aggiunte delle fasi (cambiano i segni dei coefficienti) e più in generale i coefficienti stessi possono cambiare. Vediamo esplicitamente che cosa può succedere.

**Esempio 4.9 (Bit flip channel).** Il primo esempio che analizziamo è il caso in cui gli stati vengano invertiti:  $|0\rangle \rightarrow |1\rangle$  e  $|1\rangle \rightarrow |0\rangle$ . Che cosa ci aspettiamo per gli operatori  $E_k$ ? Chiaramente uno degli operatori può essere  $X$ , dato che agisce sui singoli qubit; tuttavia  $X$  da solo non è sufficiente per soddisfare il vincolo (4.3.4), quindi aggiungiamo anche l'identità: scriviamo

$$E_0 = \sqrt{p} \mathbb{I} = \sqrt{p} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad E_1 = \sqrt{1-p} X = \sqrt{1-p} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

se imponiamo che  $0 \leq p \leq 1$  allora possiamo interpretarla come una probabilità:  $p$  è la probabilità che non accada nulla, mentre  $1-p$  è la probabilità che lo stato venga invertito. Ricordando che  $X^2 = \mathbb{I}$ , ora il vincolo (4.3.4) è soddisfatto:

$$E_0^\dagger E_0 + E_1^\dagger E_1 = p\mathbb{I} + (1-p)X^2 = \mathbb{I}.$$

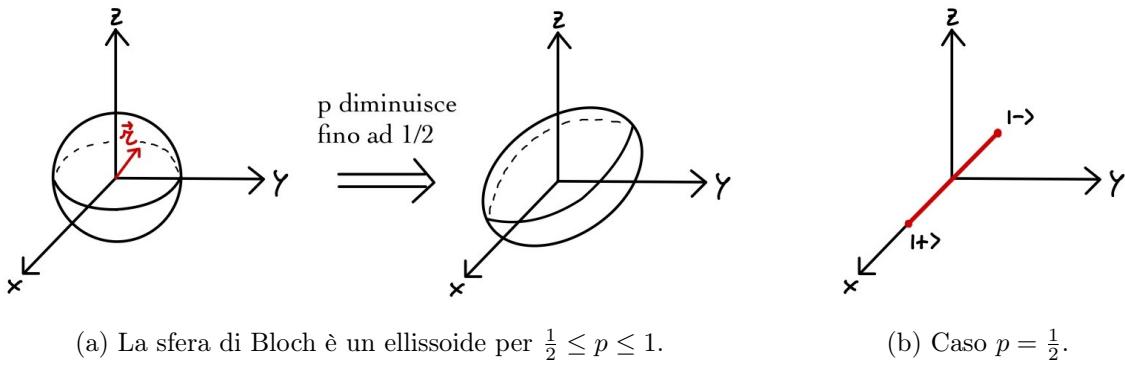
Vediamo cosa accade esplicitamente alla matrice densità del qubit: usiamo la (4.3.3) sulla (4.1.4)

$$\begin{aligned} \rho \rightarrow \sum_k E_k \rho E_k^\dagger &= E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger = p \frac{\mathbb{I} + \vec{r} \cdot \vec{\sigma}}{2} + (1-p)X \frac{\mathbb{I} + \vec{r} \cdot \vec{\sigma}}{2} X \\ &= p \frac{\mathbb{I} + r_1 \sigma_1 + r_2 \sigma_2 + r_3 \sigma_3}{2} + (1-p) \frac{\mathbb{I} + r_1 \sigma_1 - r_2 \sigma_2 - r_3 \sigma_3}{2} \\ &= \frac{\mathbb{I} + r_1 \sigma_1 + (2p-1)r_2 \sigma_2 + (2p-1)r_3 \sigma_3}{2} \equiv \mathcal{E}(\rho), \end{aligned}$$

dove nella seconda linea abbiamo utilizzato  $\sigma_i \sigma_j = i \varepsilon_{ijk} \sigma_k$  per  $i \neq j$ . Esplicitamente, in funzione del punto  $\vec{r}$  della sfera di Bloch avremo

$$(r_1, r_2, r_3) \rightarrow [r_1, (2p-1)r_2, (2p-1)r_3].$$

Come evidenziano i plot di Figura 4.1a, quando  $p$  diminuisce, allora anche  $2p-1$  diminuisce: più  $p$  è prossima a  $\frac{1}{2}$ , più la sfera di Bloch risulta schiacciata lungo  $y$  e  $z$  (lungo  $x$  rimane costante). In corrispondenza del valore  $p = \frac{1}{2}$ , come evidenziato nel plot 4.1b, la sfera collassa ad un segmento lungo  $x$ : dato che i punti sulla superficie della sfera erano gli stati  $|+\rangle$  e  $|-\rangle$ , allora ogni generico punto del segmento consiste in una sovrapposizione classica (miscela) di  $|+\rangle$  e  $|-\rangle$  con pesi dati dalla distanza dai due estremi del segmento. Notiamo che, viceversa, al diminuire di  $p$  con  $0 \leq p \leq \frac{1}{2}$  la sfera di Bloch ritorna ad essere un ellissoide: passa dall'essere il segmento di Figura 4.1b fino alla sfera unitaria originale per  $p = 0$ .

Figura 4.1: Cambiamento della sfera di Bloch nel bit flip channel al variare di  $p$ .

**Esempio 4.10 (Phase flip channel).** Si tratta del caso analogo all'esempio precedente in cui  $X$  è sostituita da  $Z$ . In questa situazione sappiamo che  $Z$  agisce come  $a|0\rangle+b|1\rangle \rightarrow a|0\rangle-b|1\rangle$  (si ricordi che  $-1 = e^{i\pi}$ ), quindi cambia la fase relativa tra gli stati (importante per fenomeni di interferenza). In questo caso gli operatori  $E_k$  sono

$$E_0 = \sqrt{p}\mathbb{I} = \sqrt{p} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad E_1 = \sqrt{1-p}Z = \sqrt{1-p} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix};$$

dove analogamente  $1-p$  ha l'interpretazione della probabilità che lo stato possa subire un cambio di fase. Come nell'esempio precedente la trasformazione di  $\rho$  sarà

$$\begin{aligned} \rho \rightarrow \sum_k E_k \rho E_k^\dagger &= E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger = p \frac{\mathbb{I} + \vec{r} \cdot \vec{\sigma}}{2} + (1-p) Z \frac{\mathbb{I} + \vec{r} \cdot \vec{\sigma}}{2} Z \\ &= p \frac{\mathbb{I} + r_1 \sigma_1 + r_2 \sigma_2 + r_3 \sigma_3}{2} + (1-p) \frac{\mathbb{I} - r_1 \sigma_1 - r_2 \sigma_2 + r_3 \sigma_3}{2} \\ &= \frac{\mathbb{I} + r_3 \sigma_3 + (2p-1)r_1 \sigma_1 + (2p-1)r_2 \sigma_2}{2} \equiv \mathcal{E}(\rho); \end{aligned}$$

perciò in termini della sfera di Bloch avremo

$$(r_1, r_2, r_3) \rightarrow [(2p-1)r_1, (2p-1)r_2, r_3].$$

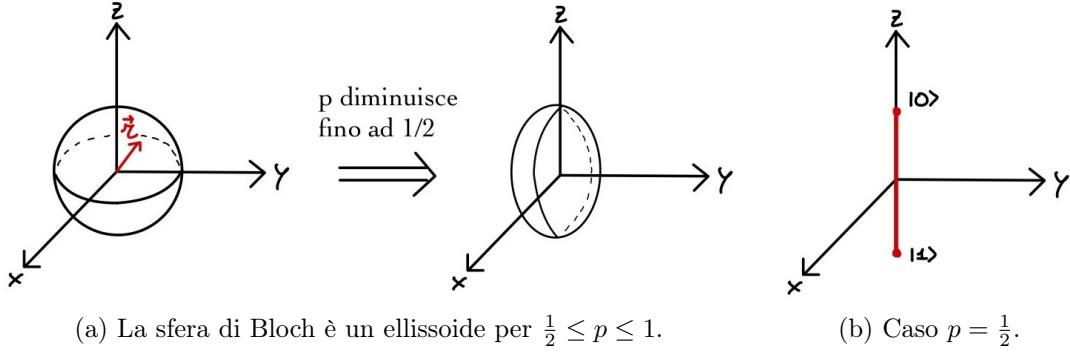
Le situazioni sono mostrate in Figura 4.2. Il caso è simile al precedente esempio, tuttavia l'ellissoide risulta questa volta schiacciato lungo  $y$  e  $x$  mantenendo  $z$  costante. Quando  $p = \frac{1}{2}$  la sfera collissa ad un segmento lungo  $z$ : a seconda del valore di  $r_3$  lo stato corrisponde ad una miscela classica di  $|0\rangle$  e  $|1\rangle$ .

Esplícitamente per  $p = \frac{1}{2}$  avremo

$$\mathcal{E}(\rho) = \frac{\mathbb{I} + \sigma_3 r_3}{2} = \begin{pmatrix} \frac{1+r_3}{2} & 0 \\ 0 & \frac{1-r_3}{2} \end{pmatrix} = \frac{1+r_3}{2} |0\rangle\langle 0| + \frac{1-r_3}{2} |1\rangle\langle 1|.$$

Notiamo che questo fenomeno accade anche quando si parte da uno stato puro: se si partisse dallo stato  $|+\rangle$  (intersezione della sfera di Bloch con l'asse positivo delle  $x$ ), allora esso sarebbe spinto, al diminuire di  $p$ , verso l'origine fino a quando  $\rho = \frac{\mathbb{I}}{2}$ .

Il cambiamento della fase relativa a seguito dell'interazione con l'ambiente è correlato al fenomeno (lo analizzeremo in dettaglio più avanti) che va sotto il nome di **decoerenza**.

Figura 4.2: Cambiamento della sfera di Bloch nel phase flip channel al variare di  $p$ .

Per capire di che cosa si tratta supponiamo di partire con lo stato puro  $|\psi\rangle$ , dato dalla sovrapposizione generica  $|\psi\rangle = a|0\rangle + b|1\rangle$ . In termini di  $\rho$  abbiamo visto che

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} a \\ b \end{pmatrix} \otimes (a^* & b^*) = \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix};$$

i termini non diagonali misurano la sovrapposizione degli stati  $|0\rangle$  e  $|1\rangle$ , quindi hanno a che fare con la fase relativa dello stato. Se si aspetta un tempo sufficientemente lungo, il qubit interagirà con l'ambiente tramite i phase flip channel producendo la seguente matrice diagonale:

$$\rho = \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix} \rightarrow \mathcal{E}(\rho) = \begin{pmatrix} (\dots) & 0 \\ 0 & (\dots) \end{pmatrix};$$

si ottiene quindi una miscela di stati (non è più uno stato puro) in cui tutte le informazioni legate alle fasi relative (termini non-diagonali) vengono perse! Questo fenomeno è la **decoerenza**: l'interazione con l'ambiente tramite phase flip channel tende a sopprimere tutti i termini non-diagonali di  $\rho$ .

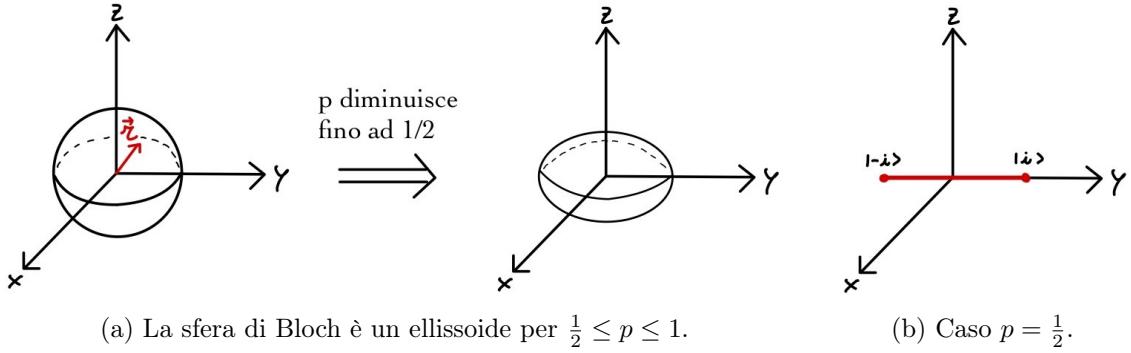
**Esempio 4.11 (Bit-phase flip channel).** Ricordando che  $XZ = -iY$ , se combiniamo il bit flip channel con il phase flip channel possiamo scrivere l'interazione con l'ambiente dovuta ai seguenti operatori

$$E_0 = \sqrt{p}\mathbb{I} = \sqrt{p} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad E_1 = \sqrt{1-p}Y = \sqrt{1-p} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix};$$

la trasformazione di  $\rho$  non è altro che

$$\begin{aligned} \rho \rightarrow \sum_k E_k \rho E_k^\dagger &= E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger = p \frac{\mathbb{I} + \vec{r} \cdot \vec{\sigma}}{2} + (1-p)Y \frac{\mathbb{I} + \vec{r} \cdot \vec{\sigma}}{2} Y \\ &= p \frac{\mathbb{I} + r_1\sigma_1 + r_2\sigma_2 + r_3\sigma_3}{2} + (1-p) \frac{\mathbb{I} - r_1\sigma_1 + r_2\sigma_2 - r_3\sigma_3}{2} \\ &= \frac{\mathbb{I} + r_2\sigma_2 + (2p-1)r_1\sigma_1 + (2p-1)r_3\sigma_3}{2} \equiv \mathcal{E}(\rho); \end{aligned}$$

e quindi la sfera di Bloch si modifica come in Figura 4.3.

Figura 4.3: Cambiamento della sfera di Bloch nel bit phase flip channel al variare di  $p$ .

**Esempio 4.12 (Depolarizing channel).** Un altro possibile modo di interagire con l'ambiente porta al cosiddetto **canale di depolarizzazione** per il quale la matrice densità del qubit diventa

$$\mathcal{E}(\rho) = (1 - p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z), \quad (4.3.5)$$

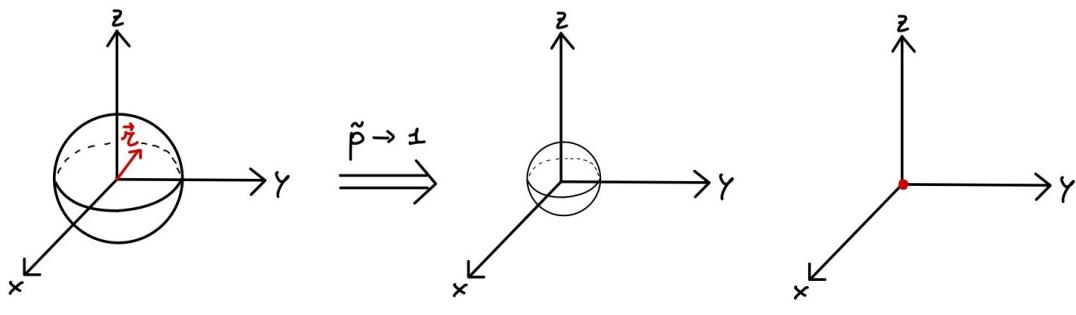
dove  $\frac{p}{3}$  non è altro che la probabilità che l'ambiente interagisca tramite ognuno dei termini nella parentesi tonda. Se utilizziamo la formula

$$\frac{\mathbb{I}}{2} = \frac{\rho + X\rho X + Y\rho Y + Z\rho Z}{4}, \quad \forall \rho = \frac{\mathbb{I} + \vec{r} \cdot \vec{\sigma}}{2},$$

la quale è facilmente dimostrabile con la proprietà  $\sigma_i\sigma_j = i\varepsilon_{ijk}\sigma_k$  per  $i \neq j$ , allora la (4.3.5) può essere scritta come

$$\mathcal{E}(\rho) = \tilde{p}\frac{\mathbb{I}}{2} + (1 - \tilde{p})\rho, \quad \text{con } \tilde{p} = \frac{4}{3}p. \quad (4.3.6)$$

Quest'ultima formula asserisce che nel canale di depolarizzazione vi è una probabilità di  $1 - \tilde{p}$  che nulla accada a  $\rho$  e una probabilità di  $\tilde{p}$  che ci sia un improvviso salto da  $\rho$  a  $\frac{\mathbb{I}}{2}$ , ossia alla situazione in cui lo stato è il più indeterminato o depolarizzato possibile. In termini di effetti sulla sfera di Bloch, la situazione è mostrata nella Figura 4.4: quando  $\tilde{p} \rightarrow 1$  la sfera di Bloch viene "schiacciata" in tutte le 3 possibili direzioni fino a quando, per  $\tilde{p} = 1$ , collassa ad un punto nell'origine.

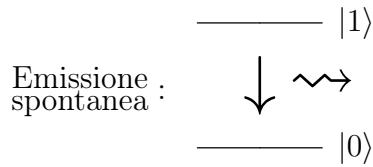
Figura 4.4: Cambiamento della sfera di Bloch nel canale di depolarizzazione al variare di  $\tilde{p}$ .

La caratterizzazione più completa dell'interazione dei qubit con l'ambiente è offerta dai fenomeni dell'**amplitude damping** ("smorzamento dell'ampiezza") e **phase damping** ("smorzamento della fase"): il primo è associato alla perdita di energia, tipicamente a seguito dell'emissione spontanea di fotoni, mentre il secondo è dovuto alla perdita di fase, a causa degli scattering (in realtà sono una sorta di diffusioni) con le particelle dell'ambiente (gli stati rimangono tali,  $|0\rangle \rightarrow |0\rangle$  e  $|1\rangle \rightarrow |1\rangle$ ). Cominciamo con l'analisi del primo dei due.

LEZIONE 11 - 12/11/2021

### 4.3.1 Amplitude damping

Un'importante applicazione delle **quantum operations** è la descrizione della dissipazione di energia, ossia effetti dovuti alla perdita di energia da un sistema quantistico. Quali sono le dinamiche di un atomo che emette spontaneamente un fotone? In che modo un sistema di spin ad alta temperatura si avvicina all'equilibrio con il suo ambiente? Qual è lo stato di un fotone in un interferometro o in una cavità quando è soggetto a diffusione e attenuazione? Ciascuno di questi processi ha le sue caratteristiche uniche, ma il comportamento generale di un qubit è ben caratterizzato da un'operazione quantistica nota come **amplitude damping** (smorzamento dell'ampiezza), che possiamo ricavare considerando il caso dell'emissione spontanea nella seguente schematizzazione:



dove, d'ora in avanti, assumeremo che lo stato  $|1\rangle$  ha un'energia associata maggiore di quella dello stato  $|0\rangle$ . Possiamo descrivere la fisica dell'emissione spontanea dal punto di vista dell'ambiente nel modo seguente: assumiamo che esso presenti una base ortonormale costituita dai due stati seguenti

$$\begin{aligned} |0\rangle_E &= \text{Nessuna emissione di fotoni.} \\ |1\rangle_E &= 1 \text{ fotone emesso.} \end{aligned}$$

In questo modo il sistema totale  $\mathcal{H}_q \otimes \mathcal{H}_E$  evolve con un'evoluzione unitaria  $U$  tale che

$$U : \begin{cases} |0\rangle \otimes |0\rangle_E & \rightarrow |0\rangle \otimes |0\rangle_E \\ |1\rangle \otimes |0\rangle_E & \rightarrow \sqrt{1-p}|1\rangle \otimes |0\rangle_E + \sqrt{p}|0\rangle \otimes |1\rangle_E \end{cases} ; \quad (4.3.7)$$

nel primo caso non succede nulla, il nostro sistema è nello stato fondamentale per cui non ci sarà mai emissione di fotoni. Nel secondo caso, invece, c'è una probabilità  $p$  che il nostro sistema, essendo nello stato eccitato, emetta spontaneamente un fotone, per cui dopo si troverà nello stato fondamentale, e una probabilità  $1 - p$  che il nostro sistema rimanga nello stato eccitato senza alcuna emissione di fotoni. Precisiamo che le trasformazioni (4.3.7) sono unitarie: è immediatamente evidente che, essendo ciascun stato ortogonale agli altri, il prodotto scalare è conservato. Come al solito, siamo interessati a studiare il nostro sistema ignorando i gradi di libertà dell'ambiente, per cui valutiamo la traccia

parziale su  $\mathcal{H}_E$  mediante il calcolo degli operation elements (4.3.2). Per semplicità di scrittura identifichiamo  $|e_0\rangle \equiv |0\rangle_E$  e  $|e_1\rangle \equiv |1\rangle_E$ . Prima di procedere ricordiamo che  $E_k = \langle e_k|U|e_0\rangle$  è equivalente a scrivere  $\langle x|E_k|y\rangle = \langle xe_k|U|ye_0\rangle$ , dove  $|x\rangle, |y\rangle \in \mathcal{H}_q$ , dunque abbiamo un modo operativo per poter calcolare ciascun termine. Valutiamo le matrici  $E_0$  ed  $E_1$ :

$$E_0 = {}_E\langle 0|U|0\rangle_E \Rightarrow \begin{cases} \langle 0|E_0|0\rangle = \langle 00|U|00\rangle = 1 \\ \langle 1|E_0|1\rangle = \langle 10|U|10\rangle = \sqrt{1-p} \\ \langle 0|E_0|1\rangle = \langle 00|U|10\rangle = 0 \\ \langle 1|E_0|0\rangle = \langle 10|U|00\rangle = 0 \end{cases} \Rightarrow E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix},$$

$$E_1 = {}_E\langle 1|U|0\rangle_E \Rightarrow \begin{cases} \langle 0|E_1|0\rangle = \langle 01|U|00\rangle = 0 \\ \langle 1|E_1|1\rangle = \langle 11|U|10\rangle = 0 \\ \langle 0|E_1|1\rangle = \langle 01|U|10\rangle = \sqrt{p} \\ \langle 1|E_1|0\rangle = \langle 11|U|00\rangle = 0 \end{cases} \Rightarrow E_1 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}.$$

Per verificare se quanto ottenuto sia consistente possiamo controllare che le matrici soddisfino il vincolo (4.3.4)

$$\sum_k E_k^\dagger E_k = E_0^\dagger E_0 + E_1^\dagger E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1-p \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & p \end{pmatrix} = \mathbb{I}.$$

A questo punto siamo pronti a valutare  $\mathcal{E}(\rho)$  per mezzo della (4.3.3). Consideriamo una generica matrice densità

$$\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix},$$

e andiamo a calcolare la sua trasformazione:

$$\begin{aligned} \mathcal{E}(\rho) &= \sum_k E_k \rho E_k^\dagger = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger \\ &= \begin{pmatrix} \rho_{00} & \sqrt{1-p}\rho_{01} \\ \sqrt{1-p}\rho_{10} & (1-p)\rho_{11} \end{pmatrix} + \begin{pmatrix} p\rho_{11} & 0 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} \rho_{00} + p\rho_{11} & \sqrt{1-p}\rho_{01} \\ \sqrt{1-p}\rho_{10} & (1-p)\rho_{11} \end{pmatrix}. \end{aligned} \quad (4.3.8)$$

Scritta in questo modo,  $\mathcal{E}(\rho)$  risulta di difficile interpretazione fisica, quindi solitamente quello che si fa in QM è introdurre una *probabilità di decadimento per unità di tempo*, detta  $\Gamma$ , tale per cui la probabilità  $p$  che avvenga un'emissione spontanea risulti definita come  $p = \Gamma\Delta t$ . Ma  $\Gamma$  definita così lo è per tempi infinitesimi, quindi per poterla usare per tempi finiti dobbiamo valutarla su un lasso di tempo finito  $t = n\Delta t$ , dove  $n$  è il numero di intervalli considerati, e mandare  $n \rightarrow \infty$ . A questo punto, ricordando che in ogni intervallo abbiamo una probabilità di  $1 - p$  che il decadimento non avvenga, in un tempo finito avremo

$$(1 - p)^n = (1 - \Gamma\Delta t)^n = \left(1 - \frac{\Gamma t}{n}\right)^n \xrightarrow{n \rightarrow \infty} e^{-\Gamma t},$$

quindi  $(1 - p) = e^{-\Gamma t}$ . Con questa nuova definizione possiamo riscrivere la (4.3.8) come

$$\mathcal{E}(\rho) = \begin{pmatrix} \rho_{00} + (1 - e^{-\Gamma t})\rho_{11} & e^{-\frac{\Gamma t}{2}}\rho_{01} \\ e^{-\frac{\Gamma t}{2}}\rho_{10} & e^{-\Gamma t}\rho_{11} \end{pmatrix}; \quad (4.3.9)$$

osserviamo che gli elementi sulla diagonale contengono  $\Gamma$  mentre quelli off-diagonal  $\Gamma/2$ . Possiamo definire anche il *tempo di vita* come  $\Gamma = 1/T$  dimodoché  $e^{-\Gamma t} = e^{-t/T}$ . Vediamo cosa succede per tempi molto grandi:

$$\mathcal{E}(\rho) \xrightarrow{t \rightarrow \infty} \begin{pmatrix} \rho_{00} + \rho_{11} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = |0\rangle\langle 0| ,$$

dove nel secondo passaggio abbiamo fatto uso di  $\text{Tr } \rho = 1$  (si ricordi anche che essendo  $\mathcal{E}(\rho)$  una matrice densità deve valere  $\text{Tr } \mathcal{E}(\rho) = 1$ ). Il motivo per cui abbiamo ottenuto una matrice densità corrispondente ad uno stato puro è molto semplice: se lasciamo che il qubit interagisca con l'ambiente per un lungo periodo di tempo, allora, con probabilità 1, se si trova nello stato eccitato decadrà sempre nel suo stato fondamentale emettendo un fotone. In termini della sfera di Bloch, il processo è rappresentato in Figura 4.5.

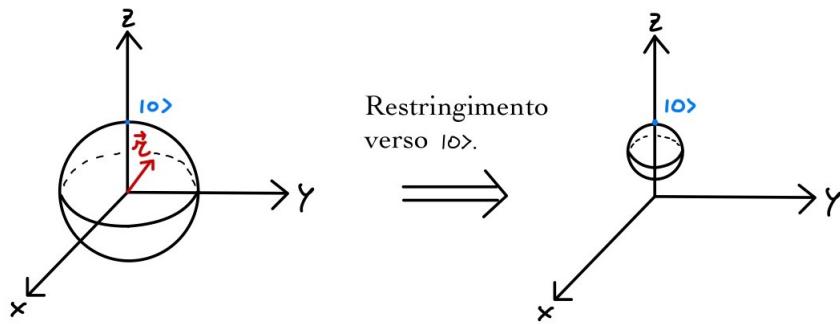


Figura 4.5: La sfera di Bloch si restringe verso lo stato  $|0\rangle$  per tempi molto lunghi.

### 4.3.2 Phase damping

Un processo di rumore che è unicamente quantistico e descrive la perdita di *coerenza*, ossia di informazioni quantistiche senza perdita di energia, è il **phase damping** (smorzamento della fase). Fisicamente descrive, ad esempio, cosa succede quando un fotone si disperde casualmente mentre viaggia attraverso una guida d'onda, o come gli stati elettronici in un atomo vengono perturbati quando interagisce con cariche elettriche distanti. Gli autostati energetici di un sistema quantistico non cambiano in funzione del tempo, ma accumulano una fase proporzionale all'autovalore. Quando un sistema evolve per un periodo di tempo non noto con precisione, le informazioni parziali su questa fase relativa, tra gli autostati energetici, vengono perse, quindi questo fenomeno affligge unicamente la fase relativa di una sovrapposizione quantistica di stati.

In maniera analoga a quanto visto nell'amplitude damping, possiamo descrivere la fisica dietro al phase damping considerando lo scattering di particelle presenti nell'ambiente con il nostro sistema quantistico. Modellizziamo la situazione dal punto di vista dell'ambiente introducendo la seguente base

$|0\rangle_E$  = Ground state: nessuno scattering.

$|1\rangle_E$  = Scattering che porta al I stato eccitato.

$|2\rangle_E$  = Scattering che porta al II stato eccitato,

dove lo stato eccitato finale dell'ambiente dipenderà dallo stato del qubit. In questo modo il sistema totale  $\mathcal{H}_q \otimes \mathcal{H}_E$  evolve con l'evoluzione unitaria  $U$  tale che

$$U : \begin{cases} |0\rangle \otimes |0\rangle_E & \rightarrow \sqrt{1-p}|0\rangle \otimes |0\rangle_E + \sqrt{p}|0\rangle \otimes |1\rangle_E \\ |1\rangle \otimes |0\rangle_E & \rightarrow \sqrt{1-p}|1\rangle \otimes |0\rangle_E + \sqrt{p}|1\rangle \otimes |2\rangle_E \end{cases} ; \quad (4.3.10)$$

abbiamo indicato con  $p$  la probabilità che lo scattering cambi in qualche modo lo stato dell'ambiente: in tutti i casi, trattandosi di scattering, il qubit rimane nel suo stato mentre lo stato che descrive l'ambiente cambia. Come nel caso dell'amplitude damping, l'operatore che descrive le trasformazioni (4.3.10) è unitario poiché i prodotti scalari sono conservati. L'obiettivo è quello di valutare il nostro sistema (qubit) ignorando l'ambiente e lo facciamo prendendo una traccia della matrice densità  $\rho$ , ancora una volta, su  $\mathcal{H}_E$ . Calcoliamo gli operation elements della (4.3.2) ricordando, come in precedenza, che  $E_k = {}_E\langle k|U|0\rangle_E \Leftrightarrow \langle x|E_k|y\rangle = \langle xk|U|y0\rangle$ . In questo caso avremo 3 matrici  $E_0$ ,  $E_1$  ed  $E_2$ :

$$\begin{aligned} E_0 = {}_E\langle 0|U|0\rangle_E &\Rightarrow \begin{cases} \langle 0|E_0|0\rangle = \langle 00|U|00\rangle = \sqrt{1-p} \\ \langle 1|E_0|1\rangle = \langle 10|U|10\rangle = \sqrt{1-p} \\ \langle 0|E_0|1\rangle = \langle 00|U|10\rangle = 0 \\ \langle 1|E_0|0\rangle = \langle 10|U|00\rangle = 0 \end{cases} \Rightarrow E_0 = \sqrt{1-p} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\ E_1 = {}_E\langle 1|U|0\rangle_E &\Rightarrow \begin{cases} \langle 0|E_1|0\rangle = \langle 01|U|00\rangle = \sqrt{p} \\ \langle 1|E_1|1\rangle = \langle 11|U|10\rangle = 0 \\ \langle 0|E_1|1\rangle = \langle 01|U|10\rangle = 0 \\ \langle 1|E_1|0\rangle = \langle 11|U|00\rangle = 0 \end{cases} \Rightarrow E_1 = \sqrt{p} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \\ E_2 = {}_E\langle 2|U|0\rangle_E &\Rightarrow \begin{cases} \langle 0|E_2|0\rangle = \langle 02|U|00\rangle = 0 \\ \langle 1|E_2|1\rangle = \langle 12|U|10\rangle = \sqrt{p} \\ \langle 0|E_2|1\rangle = \langle 02|U|10\rangle = 0 \\ \langle 1|E_2|0\rangle = \langle 12|U|00\rangle = 0 \end{cases} \Rightarrow E_2 = \sqrt{p} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Le matrici ottenute soddisfano coerentemente la (4.3.4):

$$\begin{aligned} \sum_k E_k^\dagger E_k &= E_0^\dagger E_0 + E_1^\dagger E_1 + E_2^\dagger E_2 \\ &= \begin{pmatrix} 1-p & 0 \\ 0 & 1-p \end{pmatrix} + \begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & p \end{pmatrix} = \mathbb{I}. \end{aligned}$$

Avendo ora a disposizione  $E_0$ ,  $E_1$  ed  $E_2$ , possiamo calcolare la (4.3.3):

$$\begin{aligned} \rho \rightarrow \mathcal{E}(\rho) &= \sum_k E_k \rho E_k^\dagger = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger + E_2 \rho E_2^\dagger \\ &= (1-p)\rho + p \frac{\mathbb{I} + \sigma_3}{2} \rho \frac{\mathbb{I} + \sigma_3}{2} + p \frac{\mathbb{I} - \sigma_3}{2} \rho \frac{\mathbb{I} - \sigma_3}{2} \\ &= (1-p)\rho + \frac{1}{2}(p\rho + p\sigma_3\rho\sigma_3) \\ &= \left(1 - \frac{p}{2}\right)\rho + \frac{p}{2}\sigma_3\rho\sigma_3, \end{aligned} \quad (4.3.11)$$

dove nella seconda linea abbiamo utilizzato  $E_1 = \sqrt{p}\frac{\mathbb{I} + \sigma_3}{2}$  e  $E_2 = \sqrt{p}\frac{\mathbb{I} - \sigma_3}{2}$ . Questo risultato non è nient'altro che il conto che avevamo svolto nell'Esempio 4.10 del phase flip channel. Un altro modo per rendere più esplicito questo fatto è quello di introdurre il cambio di variabili  $\tilde{p} = 1 - \frac{p}{2}$  nella precedente

$$\mathcal{E}(\rho) = \tilde{p}\rho + (1 - \tilde{p})Z\rho Z, \quad (4.3.12)$$

e ricordare che **Z-gate** introduce, in un generico stato, una fase relativa

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{Z} \alpha|0\rangle - \beta|1\rangle;$$

(si veda direttamente l'Esempio 4.10 per capire la trasformazione di  $\vec{r}$  e visualizzarne l'effetto sulla sfera di Bloch). Perciò, esplicitando la (4.3.11), la generica matrice densità si trasformerà nel seguente modo

$$\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} \longrightarrow \mathcal{E}(\rho) = \begin{pmatrix} \rho_{00} & (1-p)\rho_{01} \\ (1-p)\rho_{10} & \rho_{11} \end{pmatrix};$$

Ancora una volta, possiamo introdurre un'opportuna ampiezza di scattering  $\Gamma$  e sostituire la probabilità con il termine di decadimento esponenziale  $(1-p) = e^{-\Gamma t}$  nel limite in cui  $n \rightarrow \infty$ :

$$\mathcal{E}(\rho) = \begin{pmatrix} \rho_{00} & e^{-\Gamma t}\rho_{01} \\ e^{-\Gamma t}\rho_{10} & \rho_{11} \end{pmatrix}; \quad (4.3.13)$$

solamente le componenti off-diagonal risentono dell'interazione con l'ambiente a differenza di quanto avveniva nell'amplitude damping! Ricapitolando: una singola azione del phase flip channel produce una singola aggiunta di una fase, tuttavia molte azioni ripetute dell'ambiente (scattering con le particelle) causano una diminuzione delle componenti off-diagonal di  $\rho$ , ossia una perdita di coerenza nei termini di interferenza degli stati quantistici.

Evidenziamo un aspetto particolare che è opportuno menzionare e che incontreremo nuovamente nella sezione successiva sulla **quantum error-correction**. In questa situazione abbiamo ricavato il risultato (4.3.12) da una prospettiva differente rispetto all'Esempio 4.10 poiché abbiamo visto che lo stato del qubit può essere invertito a seguito degli scattering con le particelle esterne dell'ambiente. Vi è una sorta di **universalità**: quando, in fisica, si ritrova un comportamento universale è sempre un fatto positivo, tuttavia è bene ricordare che i qubit, a differenza del CC, sono continui (sovraposizione di stati, gate unitari dipendenti da parametri continui, ecc.) e quindi sembrerebbe molto difficoltoso controllare tutte le possibili situazioni perché si potrebbe ingenuamente pensare che ci siano un'infinità di errori agenti sui qubit! Il punto fondamentale è che se si aspetta un tempo sufficientemente lungo tutti questi effetti sono indistinguibili e si finisce sempre in una delle due situazioni appena esaminate: si perde energia (amplitude damping) o si perde coerenza (phase damping).

Storicamente, il phase damping era un processo che è stato quasi sempre pensato, fisicamente, come risultato di un processo casuale di kick di fase o scattering. Non lo è stato fino a quando fu scoperta la connessione al phase flip channel, il quale è stato analizzato nella teoria della correzione degli errori quantistici: si pensava infatti che gli errori di fase fossero continui e non potessero quindi essere descritti come un processo discreto! In effetti, gli errori di fase del singolo qubit possono sempre essere pensati come il risultato di un processo in cui, con probabilità  $p$ , non accade nulla a un qubit o, con probabilità

$1 - p$ , il qubit viene capovolto dallo Z-gate. Sebbene questo potrebbe non essere l'effettivo processo fisico microscopico che sta accadendo, dal punto di vista della trasformazione che si verifica in un qubit su un intervallo di tempo discreto, ampio rispetto al processo casuale sottostante, non c'è alcuna differenza.

Vediamo un altro esempio di modello molto semplice che produce il medesimo effetto sul qubit, ossia il phase damping e la conseguente perdita di coerenza. Supponiamo di avere un qubit nello stato  $|\psi\rangle = a|0\rangle + b|1\rangle$  che interagisce con l'ambiente, il quale aggiunge al qubit delle fasi casuali in qualche direzione particolare, diciamo una rotazione  $R_z(\theta) = e^{-\frac{i\theta\sigma_3}{2}}$  attorno a  $z$ , dove l'angolo di rotazione  $\theta$  è casuale:

$$|\psi\rangle \rightarrow R_z(\theta)|\psi\rangle = e^{-i\frac{\theta}{2}\sigma_3}|\psi\rangle = ae^{-i\frac{\theta}{2}}|0\rangle + be^{i\frac{\theta}{2}}|1\rangle , \quad (4.3.14)$$

quindi il suo effetto è quello di frapporre una fase relativa tra  $|0\rangle$  e  $|1\rangle$ . Non vogliamo studiare il caso di un valore particolare di  $\theta$ , ma vogliamo invece capire che cosa succede quando si hanno errori multipli. Consideriamo un'interazione continua con l'ambiente, il quale causa  $|\psi\rangle \rightarrow R_z(\theta)|\psi\rangle$  per qualche valore casuale di  $\theta$ , e supponiamo che l'angolo di rotazione sia una variabile casuale con una ben definita distribuzione di probabilità. Immaginiamo che tale distribuzione sia una gaussiana con media  $\theta$  e varianza  $2\lambda$ : la probabilità di avere un angolo  $\theta$  è data da

$$P(\theta) = \frac{1}{\sqrt{4\pi\lambda}}e^{-\frac{\theta^2}{4\lambda}}.$$

Vediamo cosa succede al qubit aspettando del tempo: l'effetto di una singola rotazione sullo stato finale del qubit dopo questo processo è descritto dalla seguente matrice densità

$$\rho = |\psi\rangle\langle\psi| \rightarrow \mathcal{E}(\rho) = R_z(\theta)|\psi\rangle\langle\psi|R_z^\dagger(\theta),$$

quindi se integriamo su tutti i valori di  $\theta$  possiamo calcolare un effetto totale mediato

$$\begin{aligned} \langle \mathcal{E}(\rho) \rangle_\theta &= \frac{1}{\sqrt{4\pi\lambda}} \int d\theta e^{-\frac{\theta^2}{4\lambda}} R_z(\theta)|\psi\rangle\langle\psi|R_z^\dagger(\theta) \\ &= \frac{1}{\sqrt{4\pi\lambda}} \int d\theta e^{-\frac{\theta^2}{4\lambda}} R_z(\theta) \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix} R_z^\dagger(\theta) \\ &= \frac{1}{\sqrt{4\pi\lambda}} \int d\theta e^{-\frac{\theta^2}{4\lambda}} \begin{pmatrix} |a|^2 & ab^*e^{-i\theta} \\ a^*be^{i\theta} & |b|^2 \end{pmatrix}, \end{aligned}$$

dove nell'ultima riga abbiamo letto l'effetto di  $R_z(\theta)$  su  $a$  e  $b$  dalla (4.3.14):  $a \rightarrow ae^{-i\theta/2}$  e  $b \rightarrow be^{i\theta/2}$ . L'integrale dei termini diagonali è banale perché cancella esattamente la normalizzazione, mentre l'integrale dei termini off-diagonal è un semplice integrale gaussiano

$$\frac{1}{\sqrt{4\pi\lambda}} \int d\theta e^{-\frac{\theta^2}{4\lambda} \pm i\theta} = \frac{1}{\sqrt{4\pi\lambda}} \int d\theta e^{-\frac{1}{4\lambda}(\theta \mp 2\lambda i)^2 - \lambda} = e^{-\lambda},$$

dove nel penultimo passaggio abbiamo ricostruito il quadrato ad esponente e nell'ultimo abbiamo usato la formula dell'integrale gaussiano. Perciò la matrice densità finale si è modificata in

$$\langle \mathcal{E}(\rho) \rangle_\theta = \begin{pmatrix} |a|^2 & ab^*e^{-\lambda} \\ a^*be^{-\lambda} & |b|^2 \end{pmatrix}.$$

Ancora una volta abbiamo ottenuto che la media sugli effetti dell'ambiente risulta una soppressione dei termini off-diagonal (legati all'interferenza tra gli stati) per la presenza dei fattori  $e^{-\lambda}$ .

### 4.3.3 Combinazione di amplitude e phase damping

Riassumiamo quanto abbiamo ottenuto per l'**amplitude damping** e il **phase damping**. Le matrici densità risultanti sono la (4.3.9) e la (4.3.13):

$$\begin{aligned} \text{Amplitude damping : } \rho &\rightarrow \mathcal{E}(\rho) = \begin{pmatrix} \rho_{00} + (1 - e^{-\Gamma_a t})\rho_{11} & e^{-\frac{\Gamma_a t}{2}}\rho_{01} \\ e^{-\frac{\Gamma_a t}{2}}\rho_{10} & e^{-\Gamma_a t}\rho_{11} \end{pmatrix}, \\ \text{Phase damping : } \rho &\rightarrow \mathcal{E}(\rho) = \begin{pmatrix} \rho_{00} & e^{-\Gamma_\varphi t}\rho_{01} \\ e^{-\Gamma_\varphi t}\rho_{10} & \rho_{11} \end{pmatrix}, \end{aligned}$$

dove  $\Gamma_a$  è il rateo di decadimento dell'emissione spontanea e  $\Gamma_\varphi$  è l'ampiezza di scattering (o equivalentemente la varianza della distribuzione del segnale che causa il rumore). Combinandoli insieme otteniamo

$$\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} \rightarrow \mathcal{E}(\rho) = \begin{pmatrix} \rho_{00} + (1 - e^{-\Gamma_1 t})\rho_{11} & e^{-\Gamma_2 t}\rho_{01} \\ e^{-\Gamma_2 t}\rho_{10} & e^{-\Gamma_1 t}\rho_{11} \end{pmatrix}, \quad (4.3.15)$$

dove abbiamo definito

- $\Gamma_1 = \Gamma_a \equiv \frac{1}{T_1}$ ;
- $\Gamma_2 = \frac{\Gamma_a}{2} + \Gamma_\varphi \equiv \frac{1}{T_2}$ .

La relazione (4.3.15) descrive in maniera standard ciò che accade alla matrice densità di un qubit a seguito dell'interazione con l'ambiente: gli elementi off-diagonal vengono modificati sia dalla perdita di energia (amplitude damping) sia dalla perdita di coerenza (phase damping) mentre gli elementi sulla diagonale vengono influenzati unicamente dalla perdita di energia attraverso un amplitude damping. Si noti che la (4.3.15) non è data dalla somma dei due effetti (somma di matrici) ma si tratta di una loro opportuna combinazione: spegnendo  $\Gamma_\varphi$  riotteniamo la (4.3.9), viceversa sopprimendo  $\Gamma_a$  avremo la (4.3.13).



# Capitolo 5

## Quantum error correction

LEZIONE 12 - 15/11/21

Entrambi il CC e il QC sono soggetti ad errori: si pensi ad esempio all'imperfezione dei fili nei circuiti elettrici, ai gate difettosi che non restituiscono il corretto risultato oppure anche al caso dell'interazione con l'ambiente che, come visto nel capitolo precedente, porta sempre ad una perdita di coerenza e di ampiezza nella sovrapposizione quantistica del qubit. A tal proposito, tipicamente il tempo di decoerenza è molto più piccolo rispetto al tempo di decadimento dell'ampiezza, quindi la perdita di interferenza nello stato avviene quasi immediatamente.

Nonostante la gestione degli errori di un qubit sia molto più complessa rispetto al caso classico, a causa della continua influenza dell'ambiente, cominciamo la nostra discussione analizzando il caso del CC.

### 5.1 Correzione classica degli errori

In CC esistono alcuni protocolli standard per affrontare i problemi sopraelencati: il più famoso prevede una **codifica** del messaggio contenuto nella stringa di bit in esame in una ripetizione di questi ultimi. Questo significa rimpiazzare, ad esempio,  $0 \rightarrow 000$  e  $1 \rightarrow 111$ : chiaramente la sequenza di 3 bit finali, chiamati **bit logici**, ha il medesimo significato del bit iniziale (3 bit uguali = 1 bit), tuttavia la differenza è che si hanno molti più bit.

A quale vantaggio porta questa sostituzione? Assumendo che gli errori tipici siano equivalenti ad un **OR** (bit flip:  $0 \rightarrow 1$  e  $1 \rightarrow 0$ ) e che siano statisticamente indipendenti tra loro, allora la probabilità che due o più errori avvengano simultaneamente nella sequenza finale è molto più piccola rispetto ad averne solamente uno: possiamo quindi correggere un qualsiasi errore usando la **majority rule**. Se la sequenza di bit ricevuti è costituita da  $xxx$ , allora il ricevente legge "bit inviato = 0" se la maggior parte dei bit sono 0, viceversa, quando la maggior parte sono degli 1 allora legge "bit inviato = 1".

Più formalmente, chiamiamo  $p$  la probabilità di avere un singolo bit flip. Quando si codifica il messaggio in un bit singolo si ha probabilità  $p$  di avere una qualche sorta di errore, tuttavia se la codifica avviene in 3 bit allora la sicurezza è maggiore. Per vederlo più esplicitamente calcoliamo la probabilità di avere 2 o 3 bit flip contemporaneamente: nel caso di due bit flip avremo  $3pp(1-p) = 3p^2(1-p)$  (il 3 indica che il primo errore può avvenire in uno dei 3 bit qualsiasi), mentre la probabilità di avere 3 errori è ovviamente  $p^3$ , dunque la probabilità totale di avere 2 o più errori è data dalla somma  $3p^2 - 2p^3$ . Ma

si ha

$$3p^2 - 2p^3 < p \quad \text{per} \quad p < \frac{1}{2}; \quad (5.1.1)$$

bastano quindi probabilità minori del 50%, di avere un singolo bit flip, per fare in modo che la probabilità di avere 2 o più errori simultanei sia trascurabile. Codificare il messaggio in 3 bit è più sicuro che lasciare il singolo bit. In generale questo discorso funziona ragionevolmente bene in CC.

Analizziamo ora l'analogo quantistico.

## 5.2 Introduzione alla correzione quantistica degli errori

Proviamo a svolgere il medesimo procedimento in QC: rimpiazziamo i singoli qubit con  $|0\rangle \rightarrow |000\rangle$  e  $|1\rangle \rightarrow |111\rangle$ . Nonostante il problema della duplicazione dei qubit (non è affatto banale raddoppiarli o triplicarli), esistono altri problemi concettuali da tenere necessariamente in considerazione:

- A. **Teorema di no-cloning**: non possiamo clonare stati generici.
- B. **Errori continui**: in CC tutti gli errori che avvengono sono discreti, ma in QC, dato che i gate dipendono da parametri continui, gli errori possono essere continui (si pensi banalmente all'amplitude e phase damping).
- C. **Regola di Born**: sappiamo dalla QM che la misurazione porta al collasso della funzione d'onda; per applicare la majority rule sui qubit è quindi necessario interagire con essi e causare irreversibilmente il collasso dello stato.

Nelle prossime sezioni vedremo che tutte queste problematiche possono essere affrontate nella teoria generale della correzione degli errori.

Cominciamo ad introdurre il procedimento che si attua per rimpiazzare i qubit iniziali con dei **qubit logici**. Come prima cosa si vuole rimpiazzare

$$\begin{aligned} |0\rangle &\rightarrow |000\rangle \equiv |\bar{0}\rangle \equiv |0\rangle_L, \\ |1\rangle &\rightarrow |111\rangle \equiv |\bar{1}\rangle \equiv |1\rangle_L, \end{aligned}$$

dove il pedice  $L$  sta per "logico". Ricordiamo che un qubit si trova quasi sempre in una sovrapposizione quantistica di stati, quindi si vuole scrivere

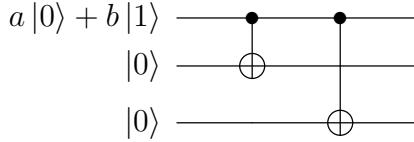
$$a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle. \quad (5.2.1)$$

Possiamo effettuare questa operazione senza violare il punto A.? La risposta è sì ed è quasi banale perché l'operazione precedente non è la stessa che clonare lo stato. Ciò che non è permesso dal *teorema di no-cloning* è

$$\begin{aligned} a|0\rangle + b|1\rangle &\equiv |\psi\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle \\ &= (a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle); \end{aligned} \quad (5.2.2)$$

chiaramente  $(5.2.1) \neq (5.2.2)$  perché ciò che vogliamo fare è molto più semplice.

Possiamo disegnare un circuito che sia in grado di operare la codifica (5.2.1) ricordando che il CNOT-gate inverte lo stato solamente quando il control qubit è in  $|1\rangle$ :



è chiaro vedere che quando il primo qubit è in  $|0\rangle$  allora si ottiene  $|000\rangle$  e viceversa quando è in  $|1\rangle$  i due **CNOT-gate** agiscono e producono  $|111\rangle$ . Questo circuito non contraddice il teorema di no-cloning: ad esempio se il primo qubit si trova in  $|1\rangle$  allora il circuito avrà come output

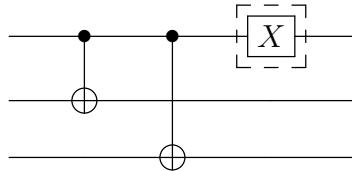
$$b|1\rangle \otimes |0\rangle \otimes |0\rangle \rightarrow b|1\rangle \otimes |1\rangle \otimes |1\rangle ,$$

il quale è effettivamente il risultato di una clonazione perché se chiamiamo  $|1\rangle \equiv |\psi\rangle$  allora l'operazione è

$$|\psi\rangle \otimes |0\rangle \otimes |0\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle ;$$

nonostante ciò, la dimostrazione del teorema di no-cloning falliva per stati ortogonali, il che significa che non c'è contraddizione fisica nel clonare stati appartenenti ad una base. Il teorema non è violato perché lo stato clonato non è uno stato generico.

Vogliamo cercare di capire come rilevare possibili errori. Supponiamo che si possano verificare errori di bit flip: gli errori causano  $|0\rangle \rightarrow |1\rangle$  e  $|1\rangle \rightarrow |0\rangle$  e questa operazione può essere implementata in un circuito con un **X-gate**. Immaginiamo che il circuito precedente sia soggetto ad un errore di questo tipo:



(il gate è stato inserito nel primo qubit, ma il discorso è analogo anche se fosse stato nel secondo o terzo). Il nostro scopo è quello di correggere l'errore tratteggiato senza disturbare in maniera eccessiva il sistema. Chiaramente essendo l'output il seguente

$$a|000\rangle + b|111\rangle \xrightarrow{X} a|100\rangle + b|011\rangle ,$$

dobbiamo cercare di capire come rilevare questo errore senza causare il collasso dello stato e come intervenire per ripristinare l'informazione desiderata.

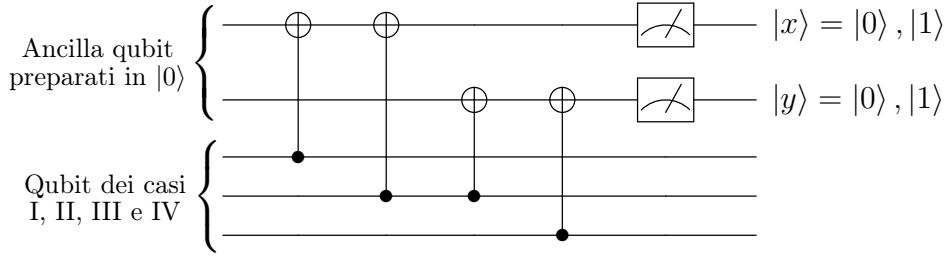
Vediamo questo errore in generale. Se solamente singoli **X-gate** su singoli qubit possono intervenire allora, a seconda della posizione di questo gate in uno dei 3 qubit, possono verificarsi 4 casi (compresa la situazione in cui non avviene alcun errore):

$$a|000\rangle + b|111\rangle \rightarrow \begin{cases} a|000\rangle + b|111\rangle , & \text{Caso I} \\ a|100\rangle + b|011\rangle , & \text{Caso II} \\ a|010\rangle + b|101\rangle , & \text{Caso III} \\ a|001\rangle + b|110\rangle , & \text{Caso IV} \end{cases} \quad (5.2.3)$$

Come possiamo distinguere in quale dei 4 casi ci troviamo? Possiamo pensare di costruire un circuito che distingua le situazioni senza disturbare i 3 qubit in gioco. Per farlo aggiungiamo, dopo i due **CNOT-gate** che servono per produrre (5.2.1), due qubit extra, chiamati **ancilla qubit**<sup>ii</sup>, e costruiamo il seguente circuito:

<sup>i</sup>Stiamo assumendo che la probabilità che avvengano 2 o più errori simultaneamente è soppressa rispetto alla probabilità che avvenga un singolo bit flip. Si veda l'equazione (5.1.1) per ulteriori dettagli.

<sup>ii</sup>Il nome "ancilla" deriva dal latino *ancilla*, che significa "ancella", "serva", "schiava". Sì, sono qubit schiavi.



In questo circuito i 3 qubit in esame agiscono sempre da control qubit, quindi rimangono tali non essendo soggetti ad alcun flip dovuto ai diversi CNOT-gate (questo significa che il punto C. è rispettato). Come indicato, si svolge una misurazione sugli ancilla qubit: il risultato, che non causa alcun collasso dei 3 qubit in esame, è un insieme di due numeri  $(x, y)$  che possono essere utilizzati per distinguere quale dei 4 errori è avvenuto. Tenendo presente gli stati indicati in (5.2.3) nei differenti casi, avremo le seguenti situazioni:

**1. Caso I:**  $(x, y) = (0, 0)$ .

La parte che riguarda  $|000\rangle$  non produce alcuna modifica perché i 4 CNOT-gate non agiscono; la parte di  $|111\rangle$ , invece, attiva tutti e 4 i CNOT-gate ma non produce alcuna variazione finale degli stati  $|x\rangle = |0\rangle$  e  $|y\rangle = |0\rangle$  perché si hanno due flip consecutivi.

**2. Caso II:**  $(x, y) = (1, 0)$ .

Lo stato  $|100\rangle$  attiva solamente il primo CNOT-gate sul primo ancilla; lo stato  $|011\rangle$  attiva gli altri 3, di cui uno sul primo ancilla (come in precedenza) e due consecutivi sul secondo ancilla. Il risultato è quindi  $|x\rangle = |1\rangle$  e  $|y\rangle = |0\rangle$  per entrambi.

**3. Caso III:**  $(x, y) = (1, 1)$ .

Lo stato  $|010\rangle$  attiva i due CNOT-gate centrali che agiscono sui due diversi ancilla; lo stato  $|101\rangle$  attiva il primo e il quarto CNOT-gate, che anch'essi agiscono su due diversi ancilla. In entrambi i casi si ha un flip su ogni stato e quindi avremo  $|x\rangle = |1\rangle$  e  $|y\rangle = |1\rangle$ .

**4. Caso IV:**  $(x, y) = (0, 1)$ .

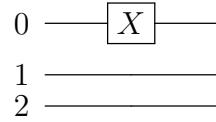
Lo stato  $|001\rangle$  attiva solamente l'ultimo CNOT-gate, che modifica il secondo ancilla; lo stato  $|110\rangle$  attiva i primi 3 CNOT-gate: i primi due non producono alcuna differenza sul primo ancilla, mentre il terzo inverte il secondo ancilla. Il risultato per entrambe le situazioni è quindi  $|x\rangle = |0\rangle$  e  $|y\rangle = |1\rangle$ .

Una volta effettuata la misurazione sugli ancilla e distinto il caso in esame, si può facilmente intervenire sul qubit corrotto inserendo un X-gate che lo riporti alla situazione iniziale. Si noti, ancora una volta, che non si è misurato il qubit difettoso, ma si sa della sua presenza grazie al risultato degli ancilla. In generale, al posto che effettuare le misure sugli ancilla, è possibile implementare un circuito che svolga questo lavoro in automatico (compreso l'inserimento dell'X-gate per correggere il qubit).

### 5.3 Stabilizers

Qual è il significato fisico in termini di osservabili della misurazione  $(x, y)$  che viene effettuata sugli ancilla qubit?

Prima di rispondere a questa domanda fissiamo le notazioni: i 3 qubit soggetti ad errori vengono generalmente indicati con un numero, come ad esempio



L'**X-gate** mostrato, invece, corrisponde, in termini di operatori agenti sui 3 qubit, al prodotto tensoriale  $X_0 \otimes \mathbb{I}_1 \otimes \mathbb{I}_2$ . Per semplicità scriveremo sempre  $X_0 \otimes \mathbb{I}_1 \otimes \mathbb{I}_2 \equiv X_0$ ,  $\mathbb{I}_0 \otimes X_1 \otimes \mathbb{I}_2 \equiv X_1$  e così via: i pedici sugli operatori indicano il qubit su cui esso sta agendo.

Lo spazio di Hilbert dei 3 qubit, che indicheremo con  $\mathcal{H}$ , ha dimensione  $\dim \mathcal{H} = 2^3 = 8$  perché i qubit logici che stiamo considerando sono triplettie dei qubit singoli iniziali:  $|\bar{0}\rangle = |000\rangle$  e  $|\bar{1}\rangle = |111\rangle$ . Chiamiamo **codewords** gli stati del seguente sottospazio

$$C = \{|\psi\rangle \in \mathcal{H} : |\psi\rangle = a|000\rangle + b|111\rangle\} \subset \mathcal{H}, \quad (5.3.1)$$

ossia l'insieme di tutti i vettori di  $\mathcal{H}$  che si scrivono come in (5.2.1). Gli operatori che agiscono su  $\mathcal{H}$  che ci interessano particolarmente sono della forma  $M = M_0 \otimes M_1 \otimes M_2$  dove  $M_i = \{\mathbb{I}, X, Y, Z\}$ . Questi operatori  $M$  sono molto speciali perché sono fattorizzati come prodotto di matrici: non stiamo agendo su  $|\bar{0}\rangle$  e  $|\bar{1}\rangle$  con generiche matrici  $8 \times 8$ ; in aggiunta, se consideriamo le singole matrici  $M_i$   $2 \times 2$  che agiscono sui singoli qubit esse non sono matrici generali di  $U(2)$ . Alcuni semplici esempi di operatori  $M$  sono:  $X \otimes \mathbb{I} \otimes \mathbb{I}$ ,  $X \otimes Z \otimes \mathbb{I}$  e  $Y \otimes Z \otimes X$ .

Perché questi operatori sono così importanti? In primo luogo perché grazie alla proprietà  $\sigma_i^2 = \mathbb{I}$  allora  $M^2 = \mathbb{I}$ . Ad esempio se  $M = X \otimes Z \otimes \mathbb{I}$  avremo

$$M^2 = (X \otimes Z \otimes \mathbb{I})(X \otimes Z \otimes \mathbb{I}) = X^2 \otimes Z^2 \otimes \mathbb{I}^2 = \mathbb{I} \otimes \mathbb{I} \otimes \mathbb{I} \equiv \mathbb{I}.$$

In secondo luogo, le matrici di Pauli sono hermitiane, il che vuol dire che possono essere diagonalizzate. I possibili autovalori ( $\lambda = \pm 1$ ) e autovettori delle matrici di Pauli sono mostrati nella Tabella 1.1 della Sezione 1.2.

Grazie alla due ragioni precedenti vale il seguente risultato: se  $M$  è non banale (almeno una  $M_i \neq \mathbb{I}$ ) allora lo spazio di Hilbert dei qubit può essere decomposto come somma diretta di due sottospazi della medesima dimensione corrispondenti agli autovalori  $\lambda = \pm 1$  dell'operatore  $M$  (autospazi di  $M$ ). In termini matematici possiamo scrivere

$$\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2, \quad \text{con} \quad \dim \mathcal{H}_1 = \dim \mathcal{H}_2; \quad (5.3.2)$$

questo significa quindi che  $\mathcal{H}$  è "tagliato" da  $M$  in due sottospazi della stessa dimensione. Cerchiamo di capirlo meglio con un esempio:

**Esempio 5.1.** Supponiamo che l'operatore sia  $M = X \otimes \mathbb{I} \otimes \mathbb{I}$ . Dato che abbiamo la matrice  $\sigma_x$  è meglio utilizzare la base composta dai suoi autostati: si ha  $X|\pm\rangle = \pm|\pm\rangle$ , quindi la triplettia di qubit è costituita dagli stati della forma  $\{|\pm\pm\pm\rangle\}$ . Lo spazio di Hilbert totale è tagliato negli autospazi:

$$\mathcal{H}_1 = \{|+\pm\pm\rangle\}, \quad \mathcal{H}_2 = \{|-\pm\pm\rangle\}, \quad (5.3.3)$$

dove entrambi gli spazi hanno dimensione 4 poiché sono costituiti da 4 stati differenti. Tutti gli stati di  $\mathcal{H}_1$  sono autostati di  $M$  con autovalore 1 e similmente tutti gli stati di  $\mathcal{H}_2$  sono autostati di  $M$  con autovalore -1.

Il fatto che valga la (5.3.2) non è una coincidenza perché per ogni operatore  $M$  non banale esiste un operatore invertibile  $S$  tale che  $S : \mathcal{H}_1 \rightarrow \mathcal{H}_2$  (i due sottospazi  $\mathcal{H}_1$  e  $\mathcal{H}_2$  sono infatti isomorfi perché possiamo sempre tornare indietro).

**Esempio 5.2.** In riferimento all’Esempio 5.1, possiamo scegliere una matrice che anticommuta con  $X$ , come  $Z$  ad esempio, e scrivere  $S = Z \otimes \mathbb{I} \otimes \mathbb{I}$ . Come agisce  $Z$  su  $|\pm\rangle$ ? Ricordiamo che

$$Z |\pm\rangle = Z \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} = \frac{|0\rangle \mp |1\rangle}{\sqrt{2}} = |\mp\rangle ;$$

in riferimento ai sottospazi in (5.3.3), è evidente che se partiamo da  $|\psi_1\rangle \in \mathcal{H}_1$  allora  $S|\psi_1\rangle = |-\pm\pm\rangle \equiv |\psi_2\rangle \in \mathcal{H}_2$ . Chiaramente è invertibile perché basta applicare nuovamente  $S$  a  $|\psi_2\rangle$  per ottenere uno stato di  $\mathcal{H}_1$ .

L’esempio precedente funzionava perché l’operatore scelto anticommutava con  $M$ : se possiamo trovare un operatore  $S$  tale che  $\{S, M\} = 0$  allora tale operatore agisce come  $S : \mathcal{H}_1 \rightarrow \mathcal{H}_2$  per una ragione algebrica molto semplice. Consideriamo uno stato  $|\psi_1\rangle \in \mathcal{H}_1$ , quindi  $M|\psi_1\rangle = |\psi_1\rangle$  perché  $\mathcal{H}_1$  è autosazio di  $M$  con autovalore associato  $\lambda = +1$ . Allora

$$M(S|\psi_1\rangle) = -S(M|\psi_1\rangle) = -S|\psi_1\rangle ,$$

quindi  $S|\psi_1\rangle$  è autovettore di  $M$  con autovalore associato  $\lambda = -1$ : questo significa necessariamente che  $S|\psi_1\rangle \in \mathcal{H}_2$ .

Dopo questa digressione matematica ritorniamo al nostro problema originale nel capire qual è il significato fisico delle misure effettuate sugli ancilla qubit. Cosa c’è di speciale negli stati che si scrivono come in (5.3.1)? Possiamo identifierli in qualche modo? Definiamo gli operatori

$$\begin{aligned} Z_0 Z_1 &= Z \otimes Z \otimes \mathbb{I} , \\ Z_1 Z_2 &= \mathbb{I} \otimes Z \otimes Z , \end{aligned}$$

dove i pedici indicano su quali qubit le matrici  $Z$  stanno agendo. Tutti gli stati di  $C$  in (5.3.1) sono autostati di questi due operatori con autovalori  $+1$  per entrambi: questo è ovvio perché  $Z|0\rangle = |0\rangle$  e  $Z|1\rangle = -|1\rangle$ , infatti

$$\begin{aligned} Z_0 Z_1 |000\rangle &= |000\rangle , & Z_1 Z_2 |000\rangle &= |000\rangle , \\ Z_0 Z_1 |111\rangle &= |111\rangle , & Z_1 Z_2 |111\rangle &= |111\rangle . \end{aligned}$$

Affermiamo inoltre che gli stati di  $C$  sono il più generale autovettore comune di  $Z_0 Z_1$  e  $Z_1 Z_2$ . La ragione è la seguente: entrambi gli operatori sono della forma di  $M$  e ognuno dei due, come autosazio, taglia lo spazio di Hilbert totale  $\mathcal{H}$  in 2 sottospazi, le cui dimensioni sono la metà della dimensione dello spazio di partenza (ossia 4). Entrambi gli operatori  $Z_0 Z_1$  e  $Z_1 Z_2$  possono avere autovalori  $\pm 1$ : focalizzandoci sull’autovalore in comune, ossia  $+1$ , abbiamo che la dimensionalità viene tagliata in  $8/2/2 = 2$ , dove il primo taglio è operato da  $Z_0 Z_1$  e il secondo da  $Z_1 Z_2$ . La dimensionalità rimanente, ossia 2, indica che l’autosazio comune agli operatori ha dimensione 2, e infatti  $C$  ha proprio dimensione 2 (tutti gli stati della (5.3.1) dipendono da due coefficienti generici, quindi  $\dim C = 2$ ).

Alla luce di questo discorso affermiamo che le misure sugli ancilla qubit sono legate agli autovalori  $x$  di  $Z_0 Z_1$  e  $y$  di  $Z_1 Z_2$ . Gli autovalori dell’azione di questi operatori sugli stati della (5.2.3) sono mostrati nella Tabella 5.1. Si noti che ciascun caso è un sottospazio di  $\mathcal{H}$  di dimensione 2 (gli stati dipendono da due coefficienti generici) quindi riempiono

tutto lo spazio di Hilbert totale ( $8 = 2 + 2 + 2 + 2$ ). Gli autovalori di questi operatori permettono di distinguere i 4 differenti autospazi, ossia le 4 differenti situazioni (qubit intatto o qubit corrotto da uno dei 3 errori).

Caso	Autospazio	Autovalore di $Z_0Z_1$	Autovalore di $Z_1Z_2$
I	$C = \{a 000\rangle + b 111\rangle\}$	+1 ( $x = 0$ )	+1 ( $y = 0$ )
II	$E_{II} = \{a' 100\rangle + b' 011\rangle\}$	-1 ( $x = 1$ )	+1 ( $y = 0$ )
III	$E_{III} = \{a'' 010\rangle + b'' 101\rangle\}$	-1 ( $x = 1$ )	-1 ( $y = 1$ )
IV	$E_{IV} = \{a''' 001\rangle + b''' 110\rangle\}$	+1 ( $x = 0$ )	-1 ( $y = 1$ )

Tabella 5.1: Autovalori degli operatori  $Z_0Z_1$  e  $Z_1Z_2$  sugli autospazi delle differenti situazioni in (5.2.3). Se associamo agli autovalori le misure ( $\lambda = +1$ )  $\rightarrow (x, y = 0)$  e ( $\lambda = -1$ )  $\rightarrow (x, y = 1)$  allora questi autovalori permettono di distinguere i 4 differenti autospazi perché i valori corrispondenti di  $(x, y)$  sono esattamente le misurazioni effettuate sugli ancilla qubit.

Abbiamo detto che un errore non è altro che un **X-gate** agente su un qubit: dato che  $\{X, Z\} = 0$  allora, come evidenzia anche la Tabella 5.2, le misure sugli ancilla qubit non sono altro che i segni rimanenti nelle anticommutazioni di  $X_i$  con gli operatori  $Z_0Z_1$  e  $Z_1Z_2$ . Esplicitamente avremo:

$$\begin{aligned} (Z_0Z_1)\mathbb{I} &= \mathbb{I}(Z_0Z_1), & (Z_1Z_2)\mathbb{I} &= \mathbb{I}(Z_1Z_2), \\ (Z_0Z_1)X_0 &= -X_0(Z_0Z_1), & (Z_1Z_2)X_0 &= X_0(Z_1Z_2), \\ (Z_0Z_1)X_1 &= -X_1(Z_0Z_1), & (Z_1Z_2)X_1 &= -X_1(Z_1Z_2), \\ (Z_0Z_1)X_2 &= X_2(Z_0Z_1), & (Z_1Z_2)X_2 &= -X_2(Z_1Z_2). \end{aligned}$$

Si noti che un determinato  $X_i$  commuta sempre con le matrici appartenenti ad un differente sottospazio (differenti qubit).

Operatore	Segno $\mathbb{I}$	Segno $X_0$	Segno $X_1$	Segno $X_2$
$Z_0Z_1$	+1 ( $x = 0$ )	-1 ( $x = 1$ )	-1 ( $x = 1$ )	+1 ( $x = 0$ )
$Z_1Z_2$	+1 ( $y = 0$ )	+1 ( $y = 0$ )	-1 ( $y = 1$ )	-1 ( $y = 1$ )

Tabella 5.2: Il segno rimanente dell'anticommutazione degli operatori  $X_i$  (gli **X-gate** che implementano l'errore) con gli operatori  $Z_0Z_1$  e  $Z_1Z_2$  è esattamente la misura (mostrata tra parentesi) che viene effettuata sui due ancilla qubit.

Questo formalismo che abbiamo utilizzato per rilevare gli errori è spesso chiamato **syndrome error correction**. In generale il prodotto delle matrici di Pauli in questi operatori è molto utile per scrivere degli algoritmi per la rilevazione di errori: codici basati su questa logica vengono detti **stabilizer codes**; gli operatori  $Z_0Z_1$  e  $Z_1Z_2$  sono detti **stabilizers**. Nelle sezioni successive vedremo alcuni di questi codici famosi.

Abbiamo detto che lo spazio di Hilbert totale dei 3 qubit può essere visto come somma dei sottospazi  $C$ ,  $E_{II}$ ,  $E_{III}$  e  $E_{IV}$  perché ciascuno ha dimensione 2, quindi  $2^3 = 8$  è scrivibile come  $2 + 2 + 2 + 2$ . Gli spazi degli errori sono 3 poiché stiamo studiando solamente i bit flip errors, i quali possono accadere in 3 posizioni differenti dei qubit logici. La domanda è: avremmo potuto fare di meglio se avessimo scelto di codificare il messaggio in un numero maggiore di qubit? Se si vuole correggere gli errori di bit flip codificando 1 qubit in  $n$  qubit, qual è il minimo valore di  $n$  da utilizzare? Per rispondere a queste domande

ripartiamo dalla (5.3.1): sappiamo che  $C$  ha dimensione 2 e immaginiamo che codifichi i singoli qubit di partenza in  $n$  qubit logici, che chiamiamo  $|\bar{0}\rangle$  e  $|\bar{1}\rangle$ ; per ognuno di essi è possibile il verificarsi di un errore e in tal caso si necessita uno "spazio dell'errore" ortogonale<sup>iii</sup> a tutti gli altri. Il numero degli spazi necessari sarà quindi  $2 + 2n$ : il primo termine è la dimensione del codewords mentre il secondo è la dimensione del numero di spazi necessari per correggere  $n$  qubit<sup>iv</sup>. Dato che la dimensione dello spazio di Hilbert di  $n$  qubit è  $2^n$ , allora per avere un codewords e degli spazi degli errori mutualmente ortogonali dovremo avere

$$2^n \geq 2 + 2n, \Rightarrow 2^{n-1} \geq 1 + n.$$

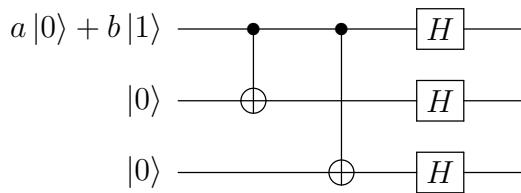
Il minimo numero che soddisfa la disegualanza precedente è proprio  $n = 3$ .

Il **bit flip error** appena analizzato non è l'unico errore che si può verificare: talvolta può accadere ad esempio un **phase flip error**, il quale è facilmente implementabile nei circuiti con un semplice Z-gate ricordando che  $Z|0\rangle = |0\rangle$  e  $Z|1\rangle = -|1\rangle$ . Per analizzare una situazione di questo tipo bisogna ricordarsi che per cambiare base da quella di  $Z$ ,  $\{|0\rangle, |1\rangle\}$ , a quella di  $X$ ,  $\{|+\rangle, |-\rangle\}$ , basta applicare un H-gate (si ricordi la matrice (1.5.1)):  $H|0\rangle = |+\rangle$  e  $H|1\rangle = |-\rangle$ .

Per correggere gli errori di phase flip è quindi necessario codificare gli stati in maniera differente:  $|0\rangle \rightarrow |+++ \rangle$  e  $|1\rangle \rightarrow |--- \rangle$ . Se si parte con uno stato generico  $a|+++ \rangle + b|--- \rangle$  allora l'azione dello Z-gate è semplicemente quella di scambiare  $+ \leftrightarrow -$ :

$$\begin{aligned} a|+++ \rangle + b|--- \rangle &\xrightarrow{Z_0} a|--- \rangle + b|+++\rangle , \\ a|+++ \rangle + b|--- \rangle &\xrightarrow{Z_1} a|+-+ \rangle + b|-+-\rangle , \\ a|+++ \rangle + b|--- \rangle &\xrightarrow{Z_2} a|+-+ \rangle + b|-+-\rangle . \end{aligned}$$

A questo punto la logica è esattamente la stessa di quella che abbiamo adoperato in precedenza! In termini di circuiti, per costruire una tale codifica è necessario aggiungere 3 H-gate al termine del circuito originale:



Infatti dopo i due CNOT-gate lo stato è come in (5.2.1), mentre dopo i 3 H-gate si avrà

$$a|000\rangle + b|111\rangle \xrightarrow{H^{\otimes 3}} a|+++ \rangle + b|---\rangle . \quad (5.3.4)$$

Da qui in poi per correggere gli errori si agisce esattamente come prima: questa volta lo stato (5.3.4) è autostato degli operatori  $X_0X_1$  e  $X_1X_2$  con autovalore +1 e ogni qualvolta avverrà un phase flip error si potrà rilevare l'errore per mezzo del cambiamento di tale

<sup>iii</sup>Se lo spazio è ortogonale a tutti gli altri allora la misurazione non influenza in alcun modo gli altri spazi.

<sup>iv</sup>Il 2 deriva dal fatto che si debbano correggere entrambi i qubit logici  $|\bar{0}\rangle$  e  $|\bar{1}\rangle$ , mentre il fattore  $n$  indica che l'errore si può trovare in uno degli  $n$  qubit di quello logico. Ad esempio per  $n = 4$  si avrà  $|\bar{0}\rangle = |0000\rangle$  e  $|\bar{1}\rangle = |1111\rangle$ : vanno corretti entrambi i qubit logici e in più l'errore si può trovare in ciascuno dei quattro "posti" nel ket di stato.

autovalore. La discussione è identica alla precedente sostituendo  $Z \leftrightarrow X$ ,  $|0\rangle \leftrightarrow |+\rangle$  e  $|1\rangle \leftrightarrow |-\rangle$ : si tratta solamente di un cambio di base!

Chiaramente può sorgere spontanea la domanda: come faccio se voglio correggere entrambi i bit-phase flip errors? Nelle prossime sezioni vedremo che il codice che si utilizza, dovuto nuovamente a Shor, utilizza solamente 9 qubit per correggere qualsiasi tipologia di errore (assicurando in questo modo che anche il problema B. di inizio sezione sia risolto). Vedremo che correggere tutti gli errori riguardanti i gate  $X, Y, Z$  è equivalente a correggere qualsiasi tipologia di errore continuo!

LEZIONE 13 - 19/11/21

## 5.4 Codice di correzione di Shor a 9 qubit

Nel 1995 Peter Shor propose il primo codice di correzione degli errori quantistici in grado di correggere errori arbitrari a singolo qubit. La sua proposta, in breve, consisteva in una concatenazione dei circuiti di bit flip error e phase flip error che abbiamo visto nelle sezioni precedenti. Per il primo livello di codifica, si garantisce la protezione dagli errori legati al phase flip codificando i qubit logici  $|\bar{0}\rangle$  e  $|\bar{1}\rangle$  utilizzando il codice di phase flip a 3 qubit:

$$|\bar{0}\rangle \rightarrow |+++ \rangle, \quad |\bar{1}\rangle \rightarrow |--- \rangle. \quad (5.4.1)$$

Come abbiamo notato sopra, tuttavia, questa codifica è suscettibile a errori di bit flip. Per proteggerci da questo tipo di errori prendiamo ciascuno degli stati  $|+\rangle$  e  $|-\rangle$  e, ricordando le (1.2.3), codifichiamo ciascun  $|0\rangle$  e  $|1\rangle$  utilizzando il codice di bit flip a 3 qubit. In questo modo la codifica finale è costituita da 9 qubit in totale:

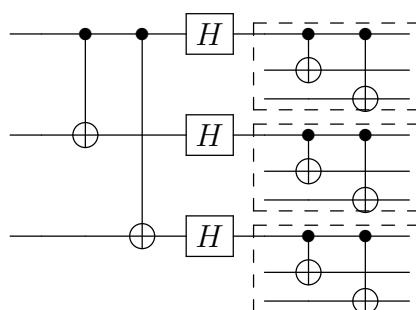
$$|+++ \rangle \rightarrow \frac{|000\rangle + |111\rangle}{\sqrt{2}} \frac{|000\rangle + |111\rangle}{\sqrt{2}} \frac{|000\rangle + |111\rangle}{\sqrt{2}} \equiv |\bar{0}\rangle, \quad (5.4.2)$$

$$|--- \rangle \rightarrow \frac{|000\rangle - |111\rangle}{\sqrt{2}} \frac{|000\rangle - |111\rangle}{\sqrt{2}} \frac{|000\rangle - |111\rangle}{\sqrt{2}} \equiv |\bar{1}\rangle. \quad (5.4.3)$$

Mettendo insieme i due passaggi che coinvolgono prima la correzione di eventuali phase flip in (5.4.1) e dopo la correzione di eventuali bit flip in (5.4.2) e (5.4.3) avremo quindi la codifica

$$|\bar{0}\rangle = \left( \frac{|000\rangle + |111\rangle}{\sqrt{2}} \right)^{\otimes 3}, \quad |\bar{1}\rangle = \left( \frac{|000\rangle - |111\rangle}{\sqrt{2}} \right)^{\otimes 3}.$$

Questi passaggi possono essere implementati nel circuito seguente



Come sopra descritto, la prima parte del circuito (fino a dopo gli H-gate) codifica il qubit utilizzando il codice relativo al phase flip a tre qubit. La seconda parte del circuito codifica ciascuno di questi tre qubit mediante il codice relativo al bit flip; in particolare fa uso di tre copie del circuito di codifica bit flip (si vedano le 3 subroutine tratteggiate). Questo metodo di codifica che utilizza una gerarchia di livelli è noto come *concatenazione*. Per capire se il codice di Shor sia effettivamente in grado di proteggere da errori di phase flip e bit flip su qualsiasi qubit dobbiamo trovare un insieme di operatori tali che  $|\bar{0}\rangle$  e  $|\bar{1}\rangle$  siano autostati col medesimo autovalore. Per capire la logica generale di funzionamento facciamo un semplice esempio.

**Esempio 5.3.** *Supponiamo che si verifichi un bit flip sul primo qubit (blocco I). Per quanto riguarda il codice relativo al bit flip, possiamo eseguire una misurazione di  $Z_0Z_1$  per confrontare i primi due qubit, scoprendo che sono diversi ( $x = 1$ ). In questo modo stabiliamo che si è verificato un errore di bit flip sul primo o sul secondo qubit. Successivamente possiamo confrontare il secondo e il terzo qubit eseguendo una misurazione di  $Z_1Z_2$ : in tal caso scopriremmo che sono uguali ( $y = 0$ ), quindi non potrebbe essere stato il secondo qubit a capovolgersi. Concludiamo che il primo qubit deve essere stato capovolto e risolviamo l'errore invertendo nuovamente il primo qubit, riportandolo allo stato originale attraverso il gate  $X_0$ .*

In modo del tutto analogo all'esempio precedente possiamo rilevare e correggere gli effetti degli errori legati al bit flip su uno qualsiasi dei nove qubit nel codice. Riassumiamo gli stabilizers coinvolti nella rilevazione nella Tabella 5.3:

Operatori	Blocco
$Z_0Z_1, Z_1Z_2$	I
$Z_3Z_4, Z_4Z_5$	II
$Z_6Z_7, Z_7Z_8$	III

Tabella 5.3: Stabilizers coinvolti nei diversi blocchi per identificare eventuali errori legati al bit flip. Il blocco I coinvolge i primi 3 qubit, il blocco II i qubit 3, 4 e 5 e infine il blocco III contiene i qubit 6, 7 e 8.

Vediamo ora come affrontare errori di phase flip sui 9 qubit. Supponiamo che si verifichi un phase flip sul primo qubit, quindi

$$Z_0 (|000\rangle + |111\rangle) = (|000\rangle - |111\rangle) ;$$

in questa situazione notiamo che c'è qualcosa di strano, perché se si verificasse un phase flip sul secondo o terzo qubit avremmo

$$\begin{aligned} Z_1 (|000\rangle + |111\rangle) &= |000\rangle - |111\rangle , \\ Z_2 (|000\rangle + |111\rangle) &= |000\rangle - |111\rangle , \end{aligned}$$

dunque questi due errori producono entrambi lo stesso effetto di  $Z_0$ : non possiamo stabilire con precisione in quale qubit si trovi l'errore, ma solamente il blocco di appartenenza. Per tale ragione il codice di Shor si dice **degenero** in quanto  $Z_0$ ,  $Z_1$  e  $Z_2$  producono lo stesso effetto, o meglio, in generale qualunque errore di phase flip che comporta un cambiamento di segno sui 3 qubit all'interno dello stesso blocco (I, II o III) è lo stesso (degenerazione = 3).

Per trovare un errore legato al phase flip dobbiamo quindi utilizzare un **X-gate**, ma deve essere eseguito come tripletta, cioè

$$X_0 X_1 X_2 (|000\rangle \pm |111\rangle) = \pm (|000\rangle \pm |111\rangle) ,$$

quindi lo stato di partenza è autostato di questa tripletta di operatori con autovalore  $\pm 1$ . Per tale ragione, gli stabilizers, i cui autostati sono (5.4.2) e (5.4.3), da considerare nel codice di Shor per individuare in quale blocco avvengono errori di phase flip sono

$$X_0 X_1 X_2 X_3 X_4 X_5 , \quad X_3 X_4 X_5 X_6 X_7 X_8 . \quad (5.4.4)$$

Un fatto importante da evidenziare è che nonostante gli operatori (5.4.4) permettano di stabilire solamente il blocco in cui è avvenuto l'errore, ciò non limita la sua risoluzione. Più precisamente, in riferimento ai casi scritti sopra, supponiamo che si verifichi un phase flip error nel blocco I: indipendentemente dall'operatore  $Z_i$  che ha causato l'errore ( $i = 0, 1, 2$ ), possiamo sempre applicare nuovamente al primo blocco uno qualsiasi di questi 3 operatori per correggere e riportare lo stato alla situazione originale. Il discorso è analogo per gli altri due blocchi.

Riassumendo<sup>v</sup>:

- I sei operatori contenenti  $Z$  della Tabella 5.3 identificano la posizione di un eventuale bit flip sui 9 qubit;
- I due operatori  $X$  in (5.4.4) identificano la posizione di un eventuale phase flip nei 3 diversi blocchi.

Questa tipologia di misurazioni vengono definite **syndrome measurements**.

Per chiarire al meglio il funzionamento del codice di Shor consideriamo il seguente esempio che coinvolge tutte le casistiche possibili: bit flip, phase flip e bit-phase-flip.

**Esempio 5.4 (Errori sul primo qubit).** Consideriamo la Tabella 5.4: supponiamo di considerare separatamente tutti i possibili tre tipi di errori discreti che possono avvenire sul primo qubit

Si noti che, come nella Tabella 5.2, gli autovalori mostrati possono essere verificati ulteriormente andando a vedere se gli operatori che implementano i vari errori anticommutano con i rispettivi stabilizers. Ad esempio  $\{Z_0 Z_1, X_0\} = 0$  (prima riga e seconda colonna). È sempre possibile distinguere il tipo di errore (syndrome), dove avviene (in che blocco o qubit) e automatizzare questo processo.

Alla luce di questo discorso ci possiamo chiedere: che cosa ne è stata della problematica B. di inizio Sezione 5.2? Il codice di Shor è sufficiente a correggere tutte le tipologie di errori, comprese quelli continui?

In effetti, il codice Shor protegge da molto più di semplici errori di bit e phase flip su un singolo qubit: ora mostriamo che protegge da errori completamente arbitrari, a condizione che influiscano solo su un singolo qubit! La cosa interessante è che non è necessario eseguire alcun lavoro aggiuntivo per proteggersi da errori arbitrari: la procedura già descritta funziona perfettamente. Questo è un esempio del fatto straordinario che l'apparente continuum di errori che può verificarsi su un singolo qubit può essere corretto

---

<sup>v</sup>Per esercizio si può dimostrare che effettivamente gli 8 operatori del codice di Shor (6 in Tabella 5.3 e 2 in (5.4.4)) possono rilevare qualsiasi errore di bit flip, phase flip e bit-phase flip.

correggendo solo un sottoinsieme discreto di quegli errori; tutti gli altri possibili errori vengono corretti automaticamente da questa procedura! La procedura di discretizzazione degli errori è fondamentale per il motivo per cui la correzione degli errori quantistico funziona e dovrebbe essere considerata in contrasto con la correzione degli errori classica per i sistemi analogici, dove tale discretizzazione degli errori non è possibile.

Che cosa produce un generico errore? Immaginiamo di avere un sistema quantistico descritto da una matrice densità  $\rho = |\psi\rangle\langle\psi|$  e di considerare solamente il nostro qubit tracciando  $\rho$  sull'ambiente descritto dallo spazio di Hilbert  $\mathcal{H}_E$ :

$$\rho = |\psi\rangle\langle\psi| \rightarrow \mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger.$$

Supponendo che lo stato del qubit codificato sia  $|\psi\rangle = \alpha |\bar{0}\rangle + \beta |\bar{1}\rangle$  prima che il rumore agisca, allora successivamente all'interazione con l'ambiente lo stato è descritto dalla matrice densità  $\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_k E_k |\psi\rangle\langle\psi| E_k^\dagger$ . Per analizzare gli effetti della correzione dell'errore è più facile concentrarsi sull'effetto che essa ha su un singolo termine in questa somma, diciamo  $E_k |\psi\rangle\langle\psi| E_k^\dagger$ . Come operatore sul solo qubit,  $E_k$  può essere espanso come una generica (si veda la (1.2.1)) combinazione lineare dell'identità, del bit flip  $X$ , del phase flip  $Z$  e del bit-phase flip  $Y$ :

$$E_k |\psi\rangle = (\alpha \mathbb{I} + \beta_x X + \beta_y Y + \beta_z Z) |\psi\rangle ,$$

dove  $\alpha, \beta_x, \beta_y$  e  $\beta_z$  sono coefficienti arbitrari reali: il comportamento continuo è chiaramente in questi coefficienti! La syndrome measurement dell'errore fa collassare<sup>vi</sup> questa sovrapposizione in uno dei quattro stati  $|\psi\rangle, X|\psi\rangle, Y|\psi\rangle$  o  $Z|\psi\rangle$  da cui poi si può recuperare lo stato iniziale  $|\psi\rangle$  applicando l'opportuna operazione di inversione. Lo stesso vale per tutti gli altri operation elements  $E_k$ : la misura causa il collasso dello stato in  $S|\psi\rangle$ , dove  $S = \{\mathbb{I}, X, Y, Z\}$ , e tutti gli stati  $S|\psi\rangle$  appartengono a differenti sottospazi degli errori mutualmente ortogonali tra loro.

Pertanto, la correzione degli errori comporta il ripristino dello stato originale, nonostante il fatto che l'errore sul qubit fosse arbitrario. Questo è un fatto fondamentale e profondo sulla correzione degli errori quantistico: correggendo solo un insieme discreto di errori (il

---

<sup>vi</sup>Il coefficiente è irrilevante perché possiamo sempre normalizzare lo stato.

Stabilizers	Codewords	bit flip ( $X_0$ )	phase flip ( $Z_0$ )	Bit-phase flip ( $Y_0$ )
$Z_0 Z_1$	+1	-1	+1	-1
$Z_1 Z_2$	+1	+1	+1	+1
$Z_3 Z_4$	+1	+1	+1	+1
$Z_4 Z_5$	+1	+1	+1	+1
$Z_6 Z_7$	+1	+1	+1	+1
$Z_7 Z_8$	+1	+1	+1	+1
$X_0 X_1 X_2 X_3 X_4 X_5$	+1	+1	-1	-1
$X_3 X_4 X_5 X_6 X_7 X_8$	+1	+1	+1	+1

Tabella 5.4: Autovalori degli stabilizers del codice di Shor per tutti i possibili errori discreti che avvengono sul primo qubit (il codewords è dato dalla generica combinazione lineare degli stati (5.4.2) e (5.4.3)). Essendo tutti i casi distinguibili, tutti i tre tipi di errori discreti possono essere identificati e corretti.

bit flip, il phase flip e il bit-phase flip) un codice di correzione quantistica degli errori è in grado di correggere automaticamente una classe di errori apparentemente molto più ampia (continua!). Ricordiamo però che tutto questo discorso è basato sull'assunzione che il rumore può coinvolgere solo un singolo qubit.

## 5.5 Codice di correzione di Steane a 7 qubit

Nel 1996 il fisico inglese Andrew Steane propose un codice di correzione degli errori basato sull'utilizzo di soli 7 qubit. Il codice di Steane utilizza i seguenti 6 operatori per la diagnostica degli errori:

$$\begin{aligned} M_0 &= X_0 X_4 X_5 X_6, & N_0 &= Z_0 Z_4 Z_5 Z_6, \\ M_1 &= X_1 X_3 X_5 X_6, & N_1 &= Z_1 Z_3 Z_5 Z_6, \\ M_2 &= X_2 X_3 X_4 X_6, & N_2 &= Z_2 Z_3 Z_4 Z_6. \end{aligned}$$

Notiamo che soddisfano le proprietà seguenti:

1.  $M_i^2 = N_i^2 = \mathbb{I}$  per  $i = 0, 1, 2$ ;
2. Sono operatori commutanti, quindi  $[M_i, M_j] = [N_i, N_j] = [M_i, N_j] = 0$ .

I primi due commutatori sono ovvi. L'ultimo commutatore, invece, è meno immediato. È utile osservare che i termini che agiscono sullo stesso qubit anticommutano (da  $\{X_i, Z_i\} = 0$ ) e producono un segno meno. Nel caso in cui  $i = j$ , abbiamo quattro meno moltiplicati tra loro mentre per  $i \neq j$  solo due meno moltiplicati tra loro: in ogni caso i segni meno scompaiono e la commutazione è dimostrata.

Trattandosi di operatori commutanti possiamo simultaneamente diagonalizzarli: l'idea è quella di utilizzare questo autospazio comune per codificare i qubit logici del codewords. Lavorando con 7 qubit, lo spazio totale di cui necessitiamo deve essere di dimensione  $\dim \mathcal{H} = 2^7$ : se ci restringiamo agli autovettori di  $M_i$  e  $N_i$  che hanno autovalore +1 allora effettivamente la dimensione del codewords sarà  $2^7 / 2 / 2 / 2 / 2 / 2 / 2 = 2$ , ossia la dimensione di uno spazio di un singolo qubit logico.

Il problema è quindi come costruire questo autospazio comune per  $|\bar{0}\rangle$  e  $|\bar{1}\rangle$ . Il punto importante è che non è necessario conoscere la forma degli stati  $|\bar{0}\rangle$  e  $|\bar{1}\rangle$ . Consideriamo uno stato generico  $|\psi\rangle$ ; notiamo che

$$M_i ((\mathbb{I} + M_i) |\psi\rangle) = (M_i + \mathbb{I}) |\psi\rangle , \quad (5.5.1)$$

quindi  $(\mathbb{I} + M_i) |\psi\rangle$  è autostato di  $M_i$  con autovalore +1 indipendentemente dalla forma di  $|\psi\rangle$ . L'idea è quindi quella di iniziare con gli stati  $|0000000\rangle$  e  $|1111111\rangle$  e di applicare degli operatori come in (5.5.1):

$$\begin{aligned} |\bar{0}\rangle &= \frac{\mathbb{I} + M_2}{\sqrt{2}} \frac{\mathbb{I} + M_1}{\sqrt{2}} \frac{\mathbb{I} + M_0}{\sqrt{2}} |0000000\rangle , \\ |\bar{1}\rangle &= \frac{\mathbb{I} + M_2}{\sqrt{2}} \frac{\mathbb{I} + M_1}{\sqrt{2}} \frac{\mathbb{I} + M_0}{\sqrt{2}} |1111111\rangle . \end{aligned}$$

Questo rappresenta il modo corretto per codificare i qubit logici  $|\bar{0}\rangle$  e  $|\bar{1}\rangle$  perché sono entrambi autostati di tutti gli operatori  $M_i$  e  $N_i$ .

Dimostriamolo esplicitamente. Il fatto che siano autostati di  $M_i$  con autovalore +1 è evidente dalla (5.5.1), perciò la domanda è: che cosa succede agli  $N_i$ ? Ricordiamo che  $[N_i, M_j] = 0$  per qualsiasi  $i, j$  e notiamo inoltre che ciascun  $N_i$  è dato da un prodotto di 4 operatori  $Z$ , i quali hanno autostati  $|0\rangle$  e  $|1\rangle$  con autovalori +1 e -1 rispettivamente: il fatto che  $N_i |\bar{0}\rangle = |\bar{0}\rangle$  è quindi ovvio, mentre  $N_i |\bar{1}\rangle = (-1)^4 |\bar{1}\rangle = |\bar{1}\rangle$  perché si hanno sempre 4 operatori  $Z$ .

È possibile verificare<sup>vii</sup> che i qubit  $|\bar{0}\rangle$  e  $|\bar{1}\rangle$ , definiti a partire da  $M_0$ ,  $M_1$  ed  $M_2$ , possono essere utilizzati come qubit logici perché sono un sistema ortonormale:

$$\begin{aligned} \langle \bar{0} | \bar{0} \rangle &= \langle \bar{1} | \bar{1} \rangle = 1, \\ \langle \bar{0} | \bar{1} \rangle &= \langle \bar{1} | \bar{0} \rangle = 0. \end{aligned}$$

Consideriamo ora il generico stato del codewords nella base logica, ossia  $|\psi\rangle = \alpha |\bar{0}\rangle + \beta |\bar{1}\rangle$ , e supponiamo che avvenga un'interazione esterna, ad esempio con l'ambiente. Lo stato dopo l'interazione, la quale è implementata da un opportuno operatore che agisce come errore, sarà descritto da  $E_k |\psi\rangle$  con l'assunzione che l'errore possa avvenire su un singolo qubit. I possibili errori che possono avvenire non sono altro che generiche matrici  $2 \times 2$  che possono essere parametrizzate da una combinazione lineare di matrici di Pauli. Questo significa che gli  $E_k$  non sono altro che una collezione di

$$\{X_i, Y_i, Z_i\}_{i=0,\dots,6};$$

in totale ci sono quindi  $3 \times 7 = 21$  possibili errori da distinguere: il 3 è dovuto al fatto che abbiamo come sorgente di errore  $X$ ,  $Y$  e  $Z$  (3 errori indipendenti su ciascun qubit) mentre il 7 perché stiamo lavorando con un codice a 7 qubit. Necessitiamo quindi di 21 "spazi degli errori" mutualmente ortogonali per correggere tutti i possibili errori. Consideriamo ora la Tabella 5.5, la quale mostra se un determinato operatore  $M_i$  o  $N_i$  contiene o meno l'operatore corrispondente.

bit flip	$X_0$	$X_1$	$X_2$	$X_3$	$X_4$	$X_5$	$X_6$
$M_0$	•				•	•	•
$M_1$		•		•		•	•
$M_2$			•	•	•		•
phase flip	$Z_0$	$Z_1$	$Z_2$	$Z_3$	$Z_4$	$Z_5$	$Z_6$
$N_0$	•				•	•	•
$N_1$		•		•		•	•
$N_2$			•	•	•		

Tabella 5.5: I 6 error-syndrome operators  $M_i$  e  $N_i$  ( $i = 0, 1, 2$ ) per il codice di Steane a 7 qubit. Un punto (•) indica se un dato operatore  $X_i$  appare in  $M_j$  e se un dato operatore  $Z_i$  appare in  $N_j$ .

Abbiamo già discusso la logica generica del codice di correzione degli errori nella Sezione 5.3: il codice deve essere realizzato in maniera tale che se ho un errore tale per cui

<sup>vii</sup>Esercizio! Si utilizzi  $(\mathbb{I} + M_i)^2 = 2(\mathbb{I} + M_i)$ . Per verificare la normalizzazione si noti che nei 3 prodotti di questi operatori solamente il prodotto delle 3 identità sopravvive: il motivo deriva dal fatto che l'azione di ciascun  $M_i$  su  $|\bar{0}\rangle$  o  $|\bar{1}\rangle$  inverte  $0 \leftrightarrow 1$ , quindi il braket rimanente coinvolgerà sempre almeno un prodotto scalare  $\langle 0|1\rangle = \langle 1|0\rangle = 0$ .

$[E_k, M] = 0$  ( $M$  è uno degli error-syndrome) e sono in un autostato  $|\psi\rangle$  di  $M$  ( $M|\psi\rangle = |\psi\rangle$ ), allora  $M(E|\psi\rangle) = EM|\psi\rangle = E|\psi\rangle$  e rimaniamo quindi nel medesimo autospazio; viceversa se  $\{E_k, M\} = 0$ , allora  $M(E|\psi\rangle) = -EM|\psi\rangle = -E|\psi\rangle$  e quindi finiamo in un autospazio con un valore differente dell'osservabile. Per capire meglio questo discorso e il significato della Tabella 5.5 si veda il seguente esempio.

**Esempio 5.5.** Supponiamo di avere un bit flip error  $X_2$ : sappiamo che  $[X_2, M_i] = 0$  per ogni  $i$ , ma  $[X_2, N_2] \neq 0$  perché è l'unico operatore che contiene  $Z_2$ . Se eseguissimo una misura degli error-syndrome avremmo tutti autovalori +1, tranne che per la riga corrispondente a  $N_2$ , nella quale si ha un autovalore pari a -1 per la presenza di  $Z_2$ . Questo non solo ci dice se c'è un bit flip error, ma ci dice anche dove è localizzato, così da poterlo correggere. I simboli "•" nella Tabella 5.5 indicano dove il segno sarà invertito, ossia dove l'autovalore della misura dell'error-syndrome sarà -1! Lo stesso discorso ovviamente lo si può fare per un phase flip error  $Z_i$ : si otterrà un segno -1 nella corrispondente riga di  $M_j$  che conterrà l'operatore  $X_i$  dello stesso autospazio dell'errore. Questa procedura può essere utilizzata anche per errori di bit-phase flip  $Y_i$ : in questo caso i segni -1 appaiono in entrambi gli operatori  $M_j$  e  $N_j$ .

Ricapitolando:

- I bit flip error  $X$  sono rilevati da dei "•" nella parte bassa della tabella.
- I phase flip error  $Z$  sono rilevati da dei "•" nella parte alta della tabella.
- I bit-phase flip error sono rilevati da dei "•" sia nella parte bassa sia in quella alta della tabella.

In questo modo siamo in grado di distinguere separatamente senza alcuna degenerazione tutti i possibili 21 errori perché tutti gli errori a singolo qubit sono localizzati in **singole colonne**.

Supponiamo di considerare errori multipli: saremmo in grado di rilevarli utilizzando la medesima trattazione? La risposta è affermativa perché lo spazio di Hilbert  $\mathcal{H}$  dei 7 qubit ha dimensione  $2^7 = 128$ , quindi è grande abbastanza da poter trattare anche questo tipo di errori. Per capire questo fatto notiamo che fino ad ora abbiamo lavorato con spazi del tipo  $C \oplus E_a C$ , ossia spazi che contenevano la somma diretta tra il codewords e gli spazi degli errori che servivano per correggere  $C$ . In questo caso avremo  $\dim(C \oplus E_a C) = 2 + 2 \times 21 = 44$ : se valutiamo la differenza di dimensione tra lo spazio di Hilbert totale  $\mathcal{H}$  e lo spazio  $C \oplus E_a C$  che serve per correggere tutti i possibili 21 errori a singolo qubit, ci rimane un sottospazio di dimensione  $128 - 44 = 84$ . Questi spazi rimanenti non sono nient'altro che gli spazi degli errori multipli! Ad esempio, se si verifica un errore simultaneo sui qubit  $i$  e  $j$  con  $i \neq j$ , possiamo implementarlo come  $X_i Z_j |\bar{0}\rangle$  e  $X_i Z_j |\bar{1}\rangle$ : in totale avremo quindi  $7 \times 6 + 7 \times 6 = 84$  errori simultanei, i quali sono rilevabili per mezzo della Tabella 5.5 dalla presenza di "•" in **2 colonne simultaneamente**. In principio siamo quindi in grado di correggere tutti i tipi di errori su singoli qubit o su coppie di qubit.

Chiaramente, dopo aver analizzato il funzionamento del codice di Steane potrebbe sorgere spontanea la domanda: se esistono, quali sono i vantaggi del codice di Steane rispetto al codice di Shor?

- Innanzitutto nel codice di Steane è relativamente più semplice il meccanismo di localizzazione e correzione degli errori, dal momento che il numero di qubit coinvolti è minore (7 rispetto a 9). In generale, una volta rilevati gli errori, è necessario

intervenire con degli opportuni gate per risolverli: lavorare con un sistema a 7 qubit è più semplice rispetto a 9 qubit in quanto le matrici (gate) con cui si è costretti a lavorare sono  $2^7 \times 2^7$ , molto più piccole rispetto ai gate di risoluzione degli errori nel codice di Shor. Inoltre gli operatori logici **X-gate**, **Z-gate** e **H-gate** che implementano le operazioni elementari sulle codewords hanno una forma particolarmente semplice nel codice di Steane:

$$\begin{aligned}\overline{X} &= X_0 X_1 X_2 X_3 X_4 X_5 X_6, \\ \overline{Z} &= Z_0 Z_1 Z_2 Z_3 Z_4 Z_5 Z_6, \\ \overline{H} &= H_0 H_1 H_2 H_3 H_4 H_5 H_6.\end{aligned}$$

- Un altro vantaggio del codice di Steane riguarda il concetto della **fault tolerance**, che approfondiremo nelle prossime sezioni. Il punto fondamentale verte sul fatto che sia necessario correggere gli errori in maniera sufficientemente veloce per poter effettuare correttamente il calcolo desiderato.

Se volessimo codificare un qubit logico usando  $n$  qubit necessiteremmo uno spazio di Hilbert di dimensione  $\dim \mathcal{H} = 2^n$ , il quale dovrebbe necessariamente contenere  $C \oplus E_a C$ : la condizione per  $n$  che deve essere soddisfatta prende il nome di **Quantum Hamming Bound** ed è data da

$$\dim \mathcal{H} \geq \dim(C \oplus E_a C), \quad \Rightarrow \quad 2^n \geq 2 + 2 \times 3 \times n,$$

( $2 \times 3$  perché è necessario correggere entrambi i qubit logici di  $C$  per tutti e 3 gli errori  $X, Y, Z$ ). Semplificando un 2, la relazione non è altro che

$$2^{n-1} \geq 1 + 3n, \tag{5.5.2}$$

la quale ci dice qual è la dimensione minima che possiamo usare. Questo risultato è applicabile unicamente a codici **non-degeneri**, ossia codici in cui possiamo distinguere e localizzare precisamente l'errore. Per contro, il codice di Shor è degenere quindi ad esso non si applica la diseguaglianza (5.5.2). Il Quantum Hamming Bound è saturato per  $n = 5$ , ci chiediamo quindi se esiste un codice che, sfruttando soli 5 qubit, corregga efficientemente tutti i possibili errori. La risposta è affermativa ed è possibile verificare che gli error-syndrome operators sono i seguenti

$$\begin{array}{ll} M_0 = Z_1 X_2 X_3 Z_4, & M_1 = Z_0 X_3 X_4 Z_0, \\ M_2 = Z_3 X_4 X_0 Z_1, & M_3 = Z_4 X_0 X_1 Z_2. \end{array}$$

Non ci addentriamo nel suo studio, ma ci limitiamo a dire che lavora in maniera simile al codice di Steane a 7 qubit perché è possibile dimostrare che esistono dei qubit logici con  $n = 5$  che sono autovettori degli operatori precedenti con autovalore +1. Lo spazio di Hilbert è quindi diviso da questi operatori in  $2^5 / 2 / 2 / 2 / 2 = 2$ , ossia proprio la dimensione del codewords.

Infine ci chiediamo: che cosa succederebbe se abbandonassimo l'ipotesi di codice non-degeneri? Esiste un codice di correzione con  $n < 5$ ? Intuitivamente possiamo pensare che, dato che lo spazio degli errori  $E_a C$  diventa più piccolo, allora si necessiterebbe di dimensioni inferiori per  $\mathcal{H}$  poiché serve meno spazio per correggere gli errori. Nonostante ciò, la risposta, che è complicata da dimostrare, è no:  $n = 5$  è il numero minimo di qubit per un generico codice di correzione degli errori anche per codici degeneri.

## 5.6 Fault tolerance

Prima di discutere in dettaglio il successivo codice di correzione degli errori spendiamo alcune parole riguardanti le diverse tipologie di codici. Ne esistono di diversi esempi:

- I **CSS codes** (da Calderbank-Shor-Steane), i quali generalizzano gli analoghi classici della correzione degli errori al contesto del QC;
- Gli **stabilizer codes**, dei quali abbiamo visto alcuni esempi nelle sezioni precedenti;
- Vi è il cosiddetto **toric/surface code**, il quale fornisce un approccio topologico<sup>viii</sup> al QC;
- E molti altri...

In generale esiste un'intera teoria generale riguardante questi codici, la quale evidenzia tutte le loro analogie e differenze. Si pensi ad esempio al modo con cui correggono gli errori, al numero di qubit utilizzati, ecc.

Quanto velocemente questi codici correggono gli errori? Questo è il soggetto della cosiddetta **fault tolerance** in QC (esiste un analogo classico), perché quando si ha un errore bisogna essere certi di non averne troppi (nel senso che sono talmente tanti da non poter essere corretti in un tempo ragionevole) e inoltre bisogna assicurarsi che i circuiti non possiedano gate che propaghino questi errori. Anche in questo caso esiste una teoria generale riguardante il come costruire circuiti quantistici che siano ottimizzati per la correzione degli errori.

La logica della fault tolerance è la seguente: si fissa un probabilità  $p$  che un qualche elemento del circuito non svolga correttamente il proprio lavoro (si pensi ad esempio alla probabilità di fallimento di un filo o un gate) e, data  $p$ , si vuole conoscere quanti qubit aggiuntivi è necessario introdurre per correggere tutti questi errori. In generale si fissa una soglia, la quale non è altro che la probabilità che il circuito fornisca l'output desiderato: lo scopo è quello di bilanciare opportunamente le componenti del circuito affinché esso lavori al di sotto di tale soglia. Più precisamente: il fine ultimo è quello di conoscere la probabilità che un singolo componente del circuito fallisca; in questo modo, con un numero polinomiale di qubit extra, si possono correggere gli errori avendo la certezza che il risultato sia corretto a meno di una soglia fissata. In generale, i codici fault tolerant sono quelli in cui si introducono un ragionevole ammontare di componenti extra senza modificare l'efficienza e la velocità di esecuzione dei codici.

Non entreremo nel dettaglio, tuttavia è bene ricordare ciò che sottolineammo nella Sottosezione 3.2.2: l'insieme di gate  $\{H, T, S, \text{CNOT}\}$  è universale sebbene  $S$  e  $T$  non siano indipendenti perché  $S = \sqrt{Z}$  e  $T = \sqrt{S}$ ; nonostante  $S$  sembra ridondante nella descrizione, affinché si abbia un codice fault tolerant è necessario tenere in considerazione anche questo gate.

---

<sup>viii</sup>Si tratta di codici particolarmente ben protetti rispetto all'interazione dei qubit con l'ambiente.

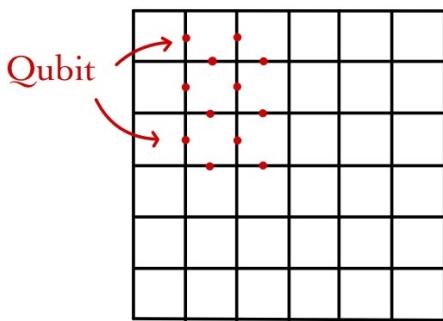
## 5.7 Toric code

L'ultimo esempio che analizziamo di codice di correzione degli errori è il cosiddetto **toric code** (conosciuto con questo nome nella letteratura della fisica della materia condensata), detto anche più genericamente **surface code**. È un codice peculiare per diverse ragioni: innanzitutto, dal punto di vista della correzione degli errori, è un codice fault tolerant perché è molto "robusto" contro gli errori; in secondo luogo è molto interessante perché è legato ad altre branche della fisica oltre al QC: si tratta di un esempio di una situazione in cui appare una fase topologica non banale della materia e, per tale motivo, è stato in passato uno dei modelli che ha condotto all'idea della cosiddetta **topological quantum computing**. Dal nostro punto di vista è interessante per la correzione degli errori e per l'approccio topologico al QC.

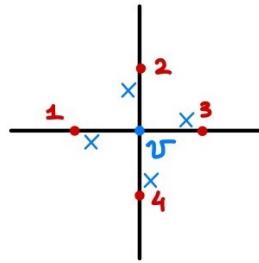
Come mostra la Figura 5.1a, consideriamo un reticolo  $L \times L$  di qubit in cui questi ultimi "vivono" sui link (collegamenti) del reticolo (si vedano i puntini rossi sui lati dei quadrati). Dal punto di vista pratico si costruisce un array periodico di qubit su un reticolo. Dato che sono presenti 2 qubit indipendenti per ogni faccia (assumiamo il qubit a sinistra e in basso nei diversi quadrati) allora la dimensione dello spazio di Hilbert totale non è altro che

$$\dim \mathcal{H} = 2^n = 2^{2L^2},$$

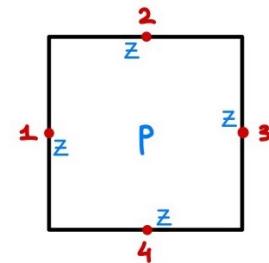
dove  $L^2$  è il numero di link/facce (si hanno  $L$  righe e  $L$  colonne). Quindi in totale avremo  $n = 2L^2$  qubit indipendenti. In generale questo codice funziona molto bene quando si ha un grande numero di qubit.



(a) Reticolo di qubit.



(b) Operatore  $A_v$ .



(c) Operatore  $B_p$ .

Figura 5.1: (5.1a) Reticolo  $L \times L$  costituito da  $2L^2$  qubit indipendenti. Per ogni plaquette ci sono 2 qubit indipendenti, quello in basso e quello a sinistra. (5.1b) L'operatore rappresentato è esplicitamente  $A_v = X_1X_2X_3X_4$ . (5.1c) L'operatore rappresentato è esplicitamente  $B_p = Z_1Z_2Z_3Z_4$ .

Il codice fu proposto per la prima volta dal fisico Alexei Kitaev ed è realizzato su un reticolo con condizioni al bordo periodiche (PBC: Periodic Boundary Conditions): dal punto di vista topologico considerare PBC sul quadrato di Figura 5.1a significa porre il reticolo di qubit su un **toro** (il reticolo è bidimensionale, ma il volume è tridimensionale). Per realizzazioni concrete il toro risulta tuttavia poco pratico: in realtà la fisica del codice può essere ben rappresentata anche mediante strutture planari con opportune condizioni al bordo (per tale motivo il codice è anche detto **surface code**); anche l'idea di realizzazione di questa procedura su strutture planari fu proposta da Kitaev.

Ancora una volta la logica del codice è la stessa di quelle viste nelle precedenti sezioni perché è un **stabilizer code**. Vi sono due tipologie di stabilizers: per ogni vertice  $v$

del reticolo si costruisce un operatore  $A_v$ , dato dal prodotto degli **X-gate** di ogni link appartenente al vertice  $v$ , similmente, per ogni faccia  $p$  del reticolo (detta **plaquette**) si definisce l'operatore  $B_p$  come prodotto dei 4 **Z-gate** sui link della plaquette. Si faccia riferimento alle Figure 5.1b e 5.1c per una rappresentazione grafica di questi operatori (chiaramente, così come i qubit, anche i gate si trovano sui link del reticolo). Dal punto di vista degli operatori avremo

$$A_v = \prod_{j \in v} X_j, \quad B_p = \prod_{j \in p} Z_j. \quad (5.7.1)$$

In totale si hanno  $L^2$  differenti operatori  $A_v$  (uno per ognuno degli  $L^2$  vertici) e  $L^2$  differenti operatori  $B_p$  (uno per ognuna delle  $L^2$  plaquette): abbiamo quindi  $2L^2$  differenti stabilizers. L'idea è, come al solito negli stabilizer codes, quello di codificare i qubit logici nel sottospazio (dato un certo autovalore) di questo insieme di operatori: più precisamente sappiamo che possiamo codificare il codewords nell'autospazio comune di questi operatori se commutano tra loro e il loro quadrato è l'identità. È evidente che per ogni  $v$  e  $p$ , in quanto prodotto di matrici di Pauli, avremo  $A_v^2 = B_p^2 = \mathbb{I}$ . Inoltre si ha

$$[A_v, B_p] = 0, \quad [A_v, A_{v'}] = 0, \quad [B_p, B_{p'}] = 0 \quad \forall v, p, v', p'; \quad (5.7.2)$$

il secondo e il terzo commutatore sono banali, tuttavia il primo è meno ovvio. Chiaramente questo commutatore è nullo quando  $A_v$  e  $B_p$  agiscono su qubit diversi (vertice e plaquette disgiunti), tuttavia potrebbe non essere nullo nel caso in cui  $A_v$  sia localizzato in uno dei quattro vertici di una plaquette  $p$  (si pensi al vertice 5.1b posto su uno dei quattro vertici della plaquette 5.1c): nonostante questa situazione, le matrici  $X$  e  $Z$  che agiscono sui qubit di un medesimo sottospazio sono sempre 2. Questo significa che i due anticommutatori  $\{Z_i, X_i\} = 0$  producono  $(-1)^2 = 1$ , quindi anche in questo caso il primo commutatore è dimostrato.

Possiamo definire come codewords il sottospazio di  $\mathcal{H}$  corrispondente all'autospazio comune agli operatori  $A_v$  e  $B_p$  con autovalore +1, ossia

$$C = \{\text{Sottospazio comune agli operatori con autovalore } A_v = B_p = +1\}.$$

Qual è la dimensione di  $C$ ? Ricordando dalla (5.7.1) che gli stabilizers sono prodotti di matrici di Pauli, essi "tagliano" sempre  $\mathcal{H}$  in due sottospazi della medesima dimensione: dato che abbiamo  $L^2$  operatori  $A_v$  e  $L^2$  operatori  $B_p$  allora si ha  $\dim C = 2^{2L^2}/2^{L^2}/2^{L^2} = 1$ , quindi sembrerebbe che non possiamo codificare i qubit in  $C$ . Il problema è che ci siamo dimenticati che non tutti questi stabilizers sono indipendenti! Essi soddisfano infatti

$$\prod_v A_v = \mathbb{I}, \quad \prod_p B_p = \mathbb{I}; \quad (5.7.3)$$

queste proprietà derivano dal fatto che nei prodotti di tutti i possibili vertici e plaquette ci sono sempre almeno 2 matrici di Pauli in comune tali che  $X_i^2 = \mathbb{I}$  e  $Z_i^2 = \mathbb{I}$ . Si pensi ad esempio all'operatore  $A_{v_1}$  della Figura 5.1b adiacente ad un altro  $A_{v_2}$ , i quali hanno un link in comune e quindi gli **X-gate** di quel link daranno  $X^2 = \mathbb{I}$ ; discorso simile per due plaquette adiacenti  $B_{p_1}$  e  $B_{p_2}$  della Figura 5.1c, le quali hanno un link comune che darà  $Z^2 = \mathbb{I}$ . I vincoli (5.7.3) fanno sì che si abbiano in totale  $(L^2 - 1) + (L^2 - 1)$  operatori  $A_v$  e  $B_p$  indipendenti: dunque il codewords ha dimensione

$$\dim C = 2^{2L^2}/2^{L^2-1}/2^{L^2-1} = 4.$$

Questo significa che nel toro possiamo codificare fino a 4 stati logici, ovvero 2 qubit logici. In realtà nel caso planare si ha  $\dim C = 2$ , quindi possiamo codificare un singolo qubit logico (come nei codici precedenti).

Come costruiamo gli stati logici del codewords  $C$ ? Possiamo procedere in maniera esattamente analoga al caso di Steane: partiamo dallo stato  $|000\dots 0\rangle$  (prodotto tensoriale dei  $2L^2$  qubit indipendenti del reticolo) e calcoliamo

$$|\overline{00}\rangle = \prod_v \frac{(\mathbb{I} + A_v)}{\sqrt{2}} |000\dots 0\rangle ; \quad (5.7.4)$$

sappiamo che in questo modo otteniamo automaticamente un autostato di qualsiasi  $A_v$  con autovalore +1 perché  $A_v(\mathbb{I} + A_v)|\psi\rangle = (A_v + \mathbb{I})|\psi\rangle$ . Analogamente avremo che  $|\overline{00}\rangle$  è anche autostato di ogni  $B_p$  con autovalore +1 perché valgono i commutatori (5.7.2) e perché  $B_p$  è un prodotto di Z-gate ( $Z|0\rangle = |0\rangle$ ):

$$B_p(\mathbb{I} + A_v)|000\dots 0\rangle = (\mathbb{I} + A_v)B_p|000\dots 0\rangle = (\mathbb{I} + A_v)|000\dots 0\rangle .$$

In aggiunta allo stato  $|\overline{00}\rangle$ , dato che  $\dim C = 4$ , ci sono altri 3 stati logici che chiamiamo  $|\overline{01}\rangle$ ,  $|\overline{10}\rangle$  e  $|\overline{11}\rangle$ . Al posto che costruirli scrivendo formule analoghe alla (5.7.4) possiamo identificare degli opportuni operatori logici  $\overline{X}_1$ ,  $\overline{X}_2$ ,  $\overline{Z}_1$  e  $\overline{Z}_2$  tali che permettano di costruire questi ultimi a partire da  $|\overline{00}\rangle$ :  $\overline{X}_1|\overline{00}\rangle = |\overline{10}\rangle$ , ecc. Come riferimento grafico per la discussione che segue si vedano i due reticolati di Figura 5.2.

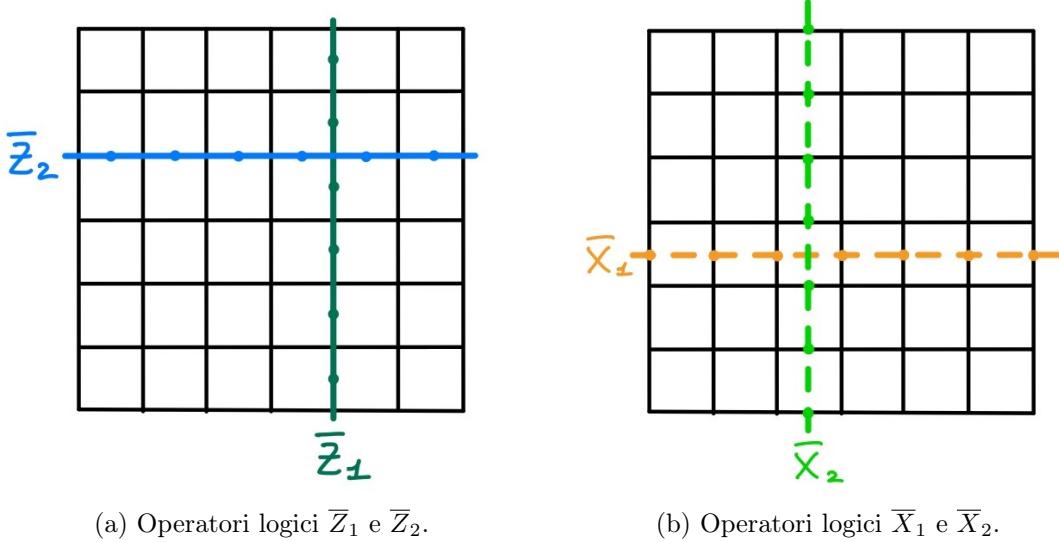


Figura 5.2: Le linee che rappresentano gli operatori logici  $\overline{Z}_1$ ,  $\overline{Z}_2$ ,  $\overline{X}_1$  e  $\overline{X}_2$  non sono altro che linee chiuse grazie alle PBC, quindi sono loop attorno al reticolo toroidale. I pallini rappresentati in corrispondenza dei link indicano i singoli gate che costituiscono il prodotto di quell'operatore logico.

Come mostrato nella Figura 5.2a, definiamo  $\overline{Z}_1$  come prodotto di tutti gli Z-gate individuati dall'intersezione della linea verticale passante per i link del reticolo; similmente  $\overline{Z}_2$  è definito come prodotto degli Z-gate individuati dall'intersezione della linea orizzontale passante per i link. Esplicitamente avremo

$$\overline{Z}_1 = \prod_{i \in \text{vline}} Z_i, \quad \overline{Z}_2 = \prod_{i \in \text{hline}} Z_i, \quad (5.7.5)$$

dove le diciture "vline" e "hline" indicano rispettivamente la linea verticale e la linea orizzontale passante per i link del reticolo.

Similmente agli operatori (5.7.5) consideriamo ora la Figura 5.2b. Se consideriamo questa volta il **reticolo duale**, ossia l'analogo reticolo che si costruisce passando per i punti medi dei link del reticolo di partenza, possiamo definire  $\bar{X}_2$  come prodotto degli **X-gate** intercettati dalla linea verticale passante per il reticolo duale; infine definiamo  $\bar{X}_1$  come prodotto degli **X-gate** intercettati dalla linea orizzontale passante per il reticolo duale. In termini di operatori scriviamo

$$\bar{X}_1 = \prod_{i \in \text{hline}} X_i, \quad \bar{X}_2 = \prod_{i \in \text{vline}} X_i, \quad (5.7.6)$$

dove questa volta le diciture "hline" e "vline" indicano rispettivamente la linea orizzontale e la linea verticale passante per i link del reticolo duale. È importante notare che grazie alle PBC le linee degli operatori  $\bar{Z}_1$ ,  $\bar{Z}_2$ ,  $\bar{X}_1$  e  $\bar{X}_2$  rappresentate nella Figura 5.2 non sono altro che **loop** (linee chiuse) passanti attorno al reticolo toroidale. D'ora in avanti ci riferiremo a queste linee chiamandole equivalentemente con il termine "loop".

Come possiamo essere certi che gli operatori (5.7.5) e (5.7.6) siano i corretti operatori logici? Sappiamo che gli operatori logici agiscono sul sottospazio  $C$  e producono un nuovo stato  $|\psi\rangle \in C$ ; questo significa che se gli operatori appena definiti commutano con tutti gli  $A_v$  e  $B_p$  allora la loro azione su stati del codewords produce altri stati di  $C$ , altrimenti, se anticommutano con  $A_v$  e  $B_p$ , la loro azione su  $C$  produce nuovi stati non più facenti parte del codewords, ossia si tratta di operatori corrispondenti ad errori. In altre parole dobbiamo quindi verificare che per ogni  $i = 1, 2$  e per qualsiasi  $v$  e  $p$  avremo

$$[\bar{X}_i, A_v] = 0, \quad [\bar{Z}_i, B_p] = 0 \quad (5.7.7)$$

$$[\bar{X}_i, B_p] = 0, \quad [\bar{Z}_i, A_v] = 0. \quad (5.7.8)$$

Chiaramente, ricordando le definizioni (5.7.1), le (5.7.7) sono banali. Per quanto riguarda invece le (5.7.8) il discorso è più sottile: se si considerano operatori  $A_v$  (vertici di Figura 5.1b) e  $B_p$  (plaquette di Figura 5.1c) disgiunti rispetto alle linee individuate rispettivamente da  $\bar{Z}_i$  e  $\bar{X}_i$  allora i commutatori sono ancora una volta banali. Se si considera tuttavia un vertice  $A_v$  sulla linea  $\bar{Z}_i$  allora esso presenterà alcuni operatori agenti sul medesimo sottospazio di quelli del loop: gli **X-gate** di  $A_v$  sul loop  $\bar{Z}_i$  saranno sempre due (sopra e sotto per  $\bar{Z}_1$  e destra e sinistra per  $\bar{Z}_2$ ), quindi come per (5.7.2), le due anticommutazioni producono  $(-1)^2 = +1$  e il commutatore è dimostrato. Vale un discorso analogo per gli operatori  $B_p$ : quando la plaquette di  $B_p$  si interseca con una delle due linee  $\bar{X}_i$  allora saranno sempre e solamente 2 gli **Z-gate** di  $B_p$  agenti sul medesimo sottospazio degli **X-gate** del loop  $\bar{X}_i$  (sopra e sotto per  $\bar{X}_2$  e destra e sinistra per  $\bar{X}_1$ ); perciò le due anticommutazioni producono come prima  $(-1)^2 = +1$  e il commutatore è verificato<sup>ix</sup>.

Affinché  $\bar{Z}_1$ ,  $\bar{Z}_2$ ,  $\bar{X}_1$  e  $\bar{X}_2$  siano i corretti operatori logici non solo devono essere verificati i commutatori sopra, ma inoltre deve valere

$$\{\bar{X}_1, \bar{Z}_1\} = 0, \quad \{\bar{X}_2, \bar{Z}_2\} = 0;$$

queste relazioni sono ovvie se si pensano ai loop di Figura 5.2: nell'intersezione di  $\bar{X}_1$  con  $\bar{Z}_1$  e di  $\bar{X}_2$  con  $\bar{Z}_2$  vi è precisamente un solo operatore ( $X$  per  $\bar{X}_i$  e  $Z$  per  $\bar{Z}_i$ ) che

<sup>ix</sup>Per capire ancora meglio questo discorso si provi a sovrapporre gli operatori  $A_v$  e  $B_p$  delle Figure 5.1b e 5.1c con le linee delle Figure 5.2a e 5.2b rispettivamente: apparirà evidente come sono sempre due gli operatori anticommutanti agenti sul medesimo sottospazio.

agisce sul medesimo sottospazio comune perché l'intersezione tra le due linee avviene in un solo punto. Questo fatto fa in modo che grazie all'anticommutatore  $\{X, Z\} = 0$  gli anticommutatori logici precedenti siano anch'essi verificati.

Dati quindi gli operatori logici in (5.7.5) e (5.7.6) possiamo calcolare i 3 stati logici rimanenti ( $|\bar{0}\bar{1}\rangle$ ,  $|\bar{1}\bar{0}\rangle$  e  $|\bar{1}\bar{1}\rangle$ ) a partire dallo stato (5.7.4). Nonostante ciò qui si evidenzia la natura topologica del codice: avremmo potuto proporre come operatori logici moltissimi altri loop oltre alle linee di Figura 5.2, ma ciò non avrebbe fatto alcuna differenza perché si tratta sempre di loop omotopi a quelle linee!

Il motivo profondo dell'affermazione precedente è mostrato nell'esempio di Figura 5.3.

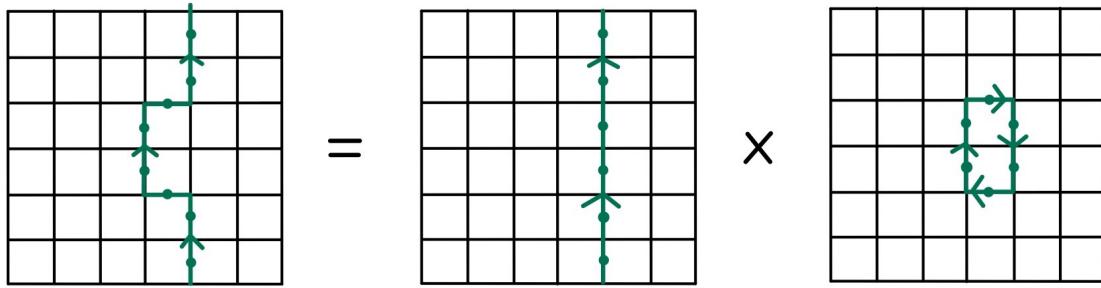


Figura 5.3: Una possibile scelta di operatore logico  $\bar{Z}_1$  è dato dal loop spezzato a sinistra. Questo loop è in realtà equivalente al loop dritto della Figura 5.2a per il loop chiuso a destra, il quale è omotopo a zero, ossia all'identità quando agisce sul codewords.

Nella parte sinistra della figura è presentato un esempio di scelta differente di  $\bar{Z}_1$ , il quale non è altro che un loop (linea) lungo il toro che non è più dritto. Si può infatti dimostrare con argomenti analoghi ai precedenti che è un operatore logico  $\bar{Z}_1$  perché soddisfa i commutatori (5.7.7) e (5.7.8). Sembrerebbe da questa scelta che possiamo avere un'infinità di loop analoghi, tuttavia ora dimostriamo che in realtà il loop a sinistra è equivalente al prodotto del loop dritto al centro della Figura 5.3 (ossia quello della Figura 5.2a) per il loop chiuso a destra, dove quest'ultimo è dato dal prodotto di tutti gli Z-gate lungo tale loop. Per capire questo fatto consideriamo il loop chiuso a destra: con la stessa logica possiamo pensare a questo loop, che circonda due plaquette, come al prodotto dei due loop più piccoli che circondano ciascuno una singola plaquette. In tale situazione il link orizzontale intermedio comune ai due loop conta 2 operatori  $Z$ , ciascuno da uno dei due loop: grazie alla proprietà  $Z^2 = \mathbb{I}$  allora effettivamente questo loop attorno alle due plaquette è equivalente al prodotto dei due loop singoli.

Quale sarà il loop più piccolo possibile? Chiaramente questo non è altro che il prodotto di 4 Z-gate attorno ad una plaquette, ossia, dalla definizione (5.7.1), proprio lo stabilizer  $B_p$  di Figura 5.1c; ma ricordiamo che ciascun  $B_p$  sul codewords ha autovalore +1! Questo significa che ciascun loop non dritto del reticolo è equivalente ad un loop dritto (Figura 5.2a) grazie al fatto che ogni loop chiuso abbia un contributo banale su  $C$ : 2 loop omotopi sono equivalenti quando agiscono sul codewords! È questo il motivo fondamentale per cui il codice è chiamato **topologico**: è possibile deformare i contorni di  $\bar{Z}_i$  e  $\bar{X}_i$  senza cambiare l'azione di questi operatori logici sugli stati del codewords!

Notiamo che con la stessa logica precedente un qualsiasi prodotto di Z-gate lungo un loop chiuso contraibile è equivalente all'identità quando agisce su  $C$ :

$$\prod_{\substack{i \in \text{loop} \\ \text{chiuso} \\ \text{contraibile}}} Z_i \equiv \mathbb{I} \text{ agendo su } C. \quad (5.7.9)$$

Perciò il contributo del prodotto precedente è banale su  $C$  perché un qualsiasi loop chiuso può essere decomposto come prodotto di plaquette singole, ossia come prodotto di  $B_p$ , le quali hanno autovalore +1 sul codewords. Questo fatto può essere espresso in altre parole dicendo che qualsiasi loop chiuso contraibile sia omotopo a zero, ossia è equivalente all'azione dell'identità sul codewords.

Qual è quindi la ragione per cui abbiamo esattamente 4 operatori logici non banali? Il motivo è che qualsiasi operatore non banale sul toro deve essere periodico: i due loop della Figura 5.4 (ricordare che sono prodotti di operatori), a differenza di qualsiasi altro loop, non sono omotopi a zero e ciascuno dei due può essere costituito dal prodotto di Z-gate oppure X-gate. Abbiamo quindi in totale 4 operatori non banali (2 loop non-contraibili con prodotti di  $Z$  più 2 loop con prodotti di  $X$ ).

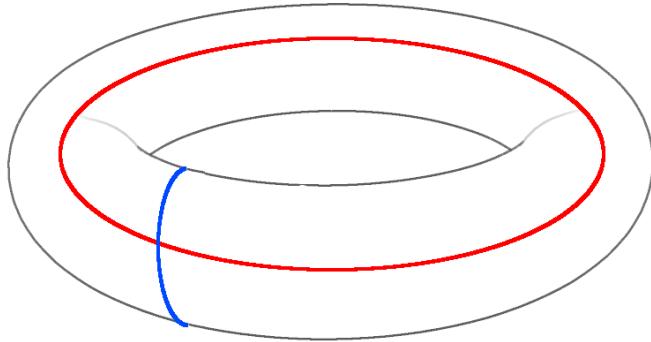


Figura 5.4: Abbiamo in totale 4 operatori logici non banali: 2 loop rossi e 2 loop blu . Ogni tipologia di loop (rosso o blu) può essere originata da prodotti di Z-gate o X-gate. Qualsiasi altro loop non rappresentato in figura è banale, ossia è omotopo a zero e agisce come un'identità sul codewords. Notare che questi 4 operatori, se pensati in una rappresentazione planare con PBC, non sono altro che le 4 linee (loop) delle Figure 5.2a e 5.2b.

### 5.7.1 Correzione degli errori

Discutiamo ora come avviene la correzione degli errori nel toric code. Ricordiamo ancora una volta che negli stabilizer codes gli operatori commutanti con gli stabilizers sono operatori logici, mentre coloro che non commutano, ma anticommutano, sono errori.

Cominciamo col considerare un **bit flip error**. Immaginiamo, come in Figura 5.5a, di avere un qubit su un link qualsiasi con un errore dato da un X-gate. In tale situazione solamente le due plaquette adiacenti al link contano: in generale  $[X, A_v] = 0$ , ma dato che  $B_p = \prod_{j \in p} Z_j$  allora solamente per le due plaquette mostrate avremo  $[X, B_p] \neq 0$ . Dato che in particolare si ha  $\{X, B_p\} = 0$  per la presenza di uno Z-gate agente sullo stesso sottospazio di  $X$  in ciascuna delle due plaquette, allora l'autovalore di questi due  $B_p$  su  $C$  è diventato  $-1$ . In questo modo possiamo rilevare un bit flip error misurando l'autovalore di queste due plaquette. Questo significa, in generale, che quando si ha una situazione in cui tutti gli operatori  $B_p$  hanno autovalore +1 eccetto per due plaquette adiacenti allora sia ha la certezza che è presente un bit flip error nel qubit tra le due.

Consideriamo ora un **phase flip error**. Come evidenziato nella Figura 5.5b la situazione è simile alla precedente, ma questa volta l'errore è rappresentato da uno Z-gate su un link: per ogni plaquette avremo  $[Z, B_p] = 0$ , ma essendo  $A_v = \prod_{i \in v} X_i$  allora per i due vertici adiacenti mostrati si ha  $[Z, A_v] \neq 0$ . Come in precedenza, l'errore agisce sul medesimo

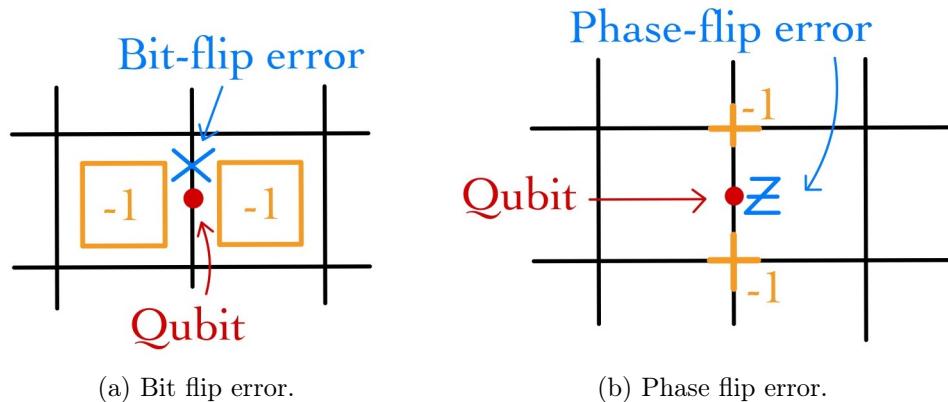
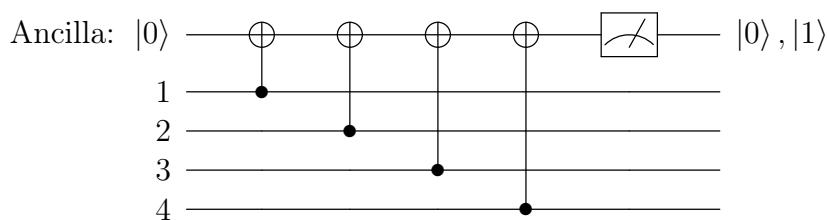


Figura 5.5: (5.5a) Esempio di rilevazione di un bit flip error. Solamente le due plaquette (riquadri arancioni) adiacenti all’errore contano perché viene invertito il loro autovalore. (5.5b) Esempio di rilevazione di un phase flip error. Solamente i due vertici (croci arancioni) adiacenti all’errore contano perché viene invertito il loro autovalore.

sottospazio degli operatori  $X$  nei due  $A_v$ , quindi a causa dell’anticommutatore  $\{Z, A_v\} = 0$  l’autovalore di questi due vertici sarà  $-1$ . Esattamente come il caso precedente, quando tutti gli operatori  $A_v$  hanno autovalore  $+1$  tranne due vertici adiacenti allora si ha la certezza che è presente un phase flip error nel qubit tra i due.

Ricapitolando, abbiamo esplicitamente mostrato che gli operatori  $A_v$  e  $B_p$  agiscono come stabilizers: misurando gli autovalori degli (5.7.1) è possibile rilevare direttamente bit flip error e phase flip error. Gli altri errori, ossia la combinazione bit-phase flip, sono semplicemente dati da una combinazione dei casi precedenti.

Una delle ragioni principali per cui questo codice di correzione degli errori è così popolare nella letteratura del QC è data dal fatto che sia possibile rilevare e correggere gli errori aggiungendo qubit extra (che chiamiamo anche qui **ancilla qubits**) nei vertici e nelle facce del reticolo. Tutte le tipologie di qubit presenti nel reticolo (compresi gli ancilla) sono mostrate in Figura 5.6a. I qubit sui link (pallini rossi pieni) sono i qubit fisici, ossia coloro che codificano l’informazione. Viceversa, i qubit aggiunti sui vertici e al centro delle facce del reticolo (pallini arancio vuoti) sono gli ancilla qubit che hanno lo scopo di effettuare la misurazione e correggere eventuali errori. Chiamiamo **qubit of type Z** gli ancilla nelle facce perché effettuano la misurazione di  $B_p$  sui 4 qubit dei link della plaquette, mentre definiamo **qubit of type X** gli ancilla presenti nei vertici, i quali similmente effettuano una misurazione di  $A_v$  sui 4 qubit dei link entranti in quel vertice. Più precisamente, consideriamo la singola plaquette di qubit di Figura 5.6b. L’ancilla qubit effettua una misurazione dell’operatore  $B_p = Z_1Z_2Z_3Z_4$ : questa misurazione può essere portata a termine per mezzo del seguente circuito



L’autovalore del prodotto dei 4 Z-gate di  $B_p$  sarà  $+1$  o  $-1$  a seconda del numero di flip che vengono operati dai CNOT-gate: un numero dispari di stati  $|1\rangle$  nei 4 qubit produrrà

$B_p = -1$  perché l'ancilla sarà in  $|1\rangle$ , viceversa un numero pari di  $|1\rangle$  vorrà dire  $B_p = +1$  perché la misurazione sull'ancilla ha output  $|0\rangle$ . Misurando quindi lo stato dell'ancilla siamo in grado di stabilire l'autovalore di  $B_p$ .

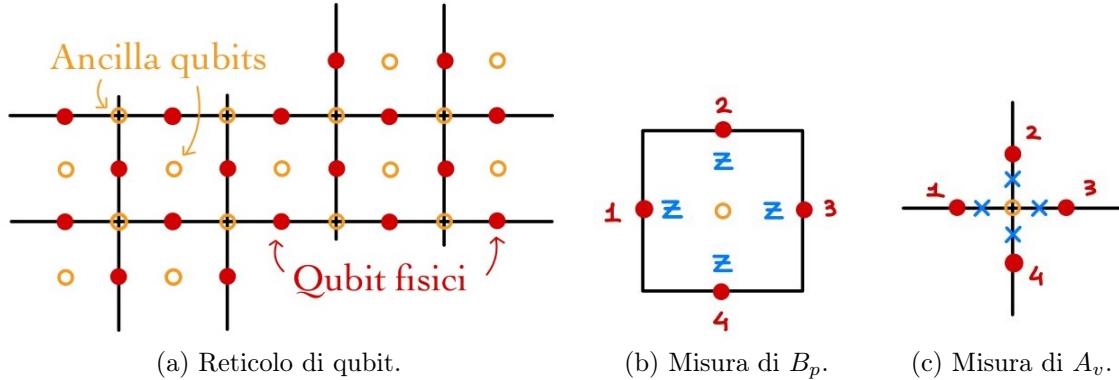


Figura 5.6: Il reticolo è cosparso di qubit fisici (pallini rossi pieni sui link) e di ancilla qubits (pallini arancio vuoti nelle facce e sui vertici). Gli ancilla delle plaquette permettono di effettuare una misurazione dell'autovalore di  $B_p$ , mentre gli ancilla dei vertici effettuano una misurazione dell'autovalore di  $A_v$ .

In maniera del tutto analoga consideriamo ora il singolo vertice di Figura 5.6c. È possibile dimostrare che l'ancilla sul vertice effettua una misurazione dell'operatore  $A_v = X_1X_2X_3X_4$  utilizzando un circuito analogo al precedente (vengono solamente inseriti alcuni H-gate): anche in questo caso, una misurazione sullo stato finale dell'ancilla permette di stabilire se l'autovalore è  $A_v = +1$  oppure  $A_v = -1$ .

Analizziamo ora gli errori mostrati in Figura 5.7a. Come evidenziato anche nella Figura 5.5a, la misura nel reticolo di due autovalori  $B_p = -1$  corrisponde ad un bit flip error sul qubit tra le due plaquette adiacenti (situazione azzurra in alto nel reticolo). Nonostante la situazione precedente possono avvenire altre tipologie di errori: supponiamo di misurare due autovalori  $B_p = -1$  in corrispondenza di due plaquette non adiacenti (si vedano i  $-1$  in rosso nelle due facce). Da che cosa sono prodotti errori come i precedenti? Questi non sono altro che il risultato di una serie di bit flip lungo una linea che connette le due plaquette (si veda le "X" in arancio): dato che tutti i link tra le plaquette intermedie hanno cambiato segno due volte a seguito del bit flip, allora per tali facce la misura produce  $B_p = +1$ , mentre per le plaquette iniziali e finali l'autovalore risulta invertito! Siamo quindi in grado di dare una corretta interpretazione anche di questa tipologia di errore.

Perché la natura topologica del codice è così importante? Come possiamo essere certi che l'errore appena spiegato sia dovuto alla linea arancio di bit flip e non, ad esempio, alla linea verde? In principio ogni possibile cammino di X-gate che connette le due plaquette invertite potrebbe dare lo stesso identico errore. Se non sappiamo distinguere quale percorso di X-gate ha causato l'errore, come possiamo correggerlo? Il punto fondamentale è che non importa quale sia il giusto percorso di errori: possiamo correggere gli errori applicando un cammino arbitrario di X-gate lungo un qualsiasi cammino aperto che connette le due plaquette invertite: si tratta quindi di scegliere un cammino di X-gate che connette le due plaquette invertite! Il cammino originale che causa l'errore (non lo conosciamo) più il cammino di X-gate scelto è un operatore banale perché uno compensa l'altro: il percorso finale risultante non è altro che un cammino chiuso nel reticolo duale, quindi la combinazione di errori risulta in un prodotto di X-gate lungo un loop chiuso

(Figura 5.7b)! Dato che, come illustra la Figura 5.7b, un qualsiasi prodotto di **X-gate** su un loop chiuso contraibile può essere scritto come prodotto di  $A_p$ , allora in analogia alla (5.7.9) avremo

$$\prod_{i \in \substack{\text{loop} \\ \text{chiuso} \\ \text{contraibile}}} X_i \equiv \mathbb{I} \text{ agendo su } C. \quad (5.7.10)$$

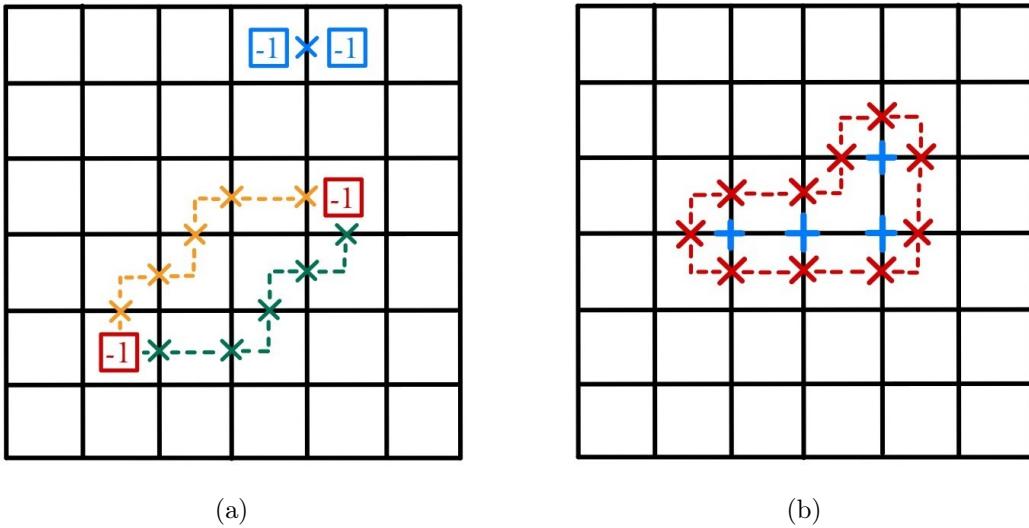


Figura 5.7: (5.7a) La misura di due autovalori  $B_p = -1$  in corrispondenza di due plaquette non adiacenti (facce in rosso) può essere causata da una concatenazione di bit flip errors lungo un cammino che connette le due plaquette. Per correggere tale errore basta applicare un percorso di **X-gate** che connette le due plaquette. (5.7b) Un prodotto di **X-gate** su un loop chiuso nel reticolo duale è equivalente ad un prodotto di operatori  $A_v$  (vertici azzurri), i quali hanno contributo banale su  $C$ .

Ricapitolando: un cammino chiuso di **X-gate** nel reticolo duale può sempre essere visto come prodotto di tutti i vertici (operatori  $A_v$ ) contenuti nel loop; ogni  $A_p$  inserisce un **X-gate** sui link esterni mentre, grazie a  $X^2 = \mathbb{I}$ , nulla accade nei link interni comuni ai vertici. Dato che su  $C$  tutti gli  $A_p$  hanno autovalore +1, allora i loop chiusi di **X-gate** nel reticolo duale sono omotopi a zero, ossia sono l'operatore banale (identità).

## 5.7.2 Interpretazione in meccanica statistica

Esiste una curiosa interpretazione del toric code alla luce della meccanica statistica considerando un reale modello di spin quantistici. Supponiamo un reticolo in cui, su ogni link, è possibile avere uno spin quantistico (up o down). In un tale sistema l'hamiltoniana è data da

$$H = -J \sum_v A_v - J \sum_p B_p, \quad J > 0. \quad (5.7.11)$$

Come mostra la Figura 5.8a, l'interazione degli spin avviene in due modi: interagiscono i 4 spin in un vertice (prima somma in  $H$ ) oppure i 4 spin di una plaquette (seconda somma in  $H$ ). Qual è lo stato (o gli stati) di minima energia? I ground state corrispondono a tutte quelle situazioni in cui gli autovalori sono  $A_v = B_p = +1$  per ogni vertice e plaquette del reticolo. In un'interpretazione di questo tipo i 4 qubit logici  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  e  $|11\rangle$

(con autovalori  $A_v = B_p = +1$ ) del QC sono mappati nei ground state dell'hamiltoniana (5.7.11); viceversa gli errori nel reticolo corrispondono a delle eccitazioni, ossia a delle configurazioni in cui almeno un autovalore di  $A_v$  e/o  $B_p$  è uguale a  $-1$ .

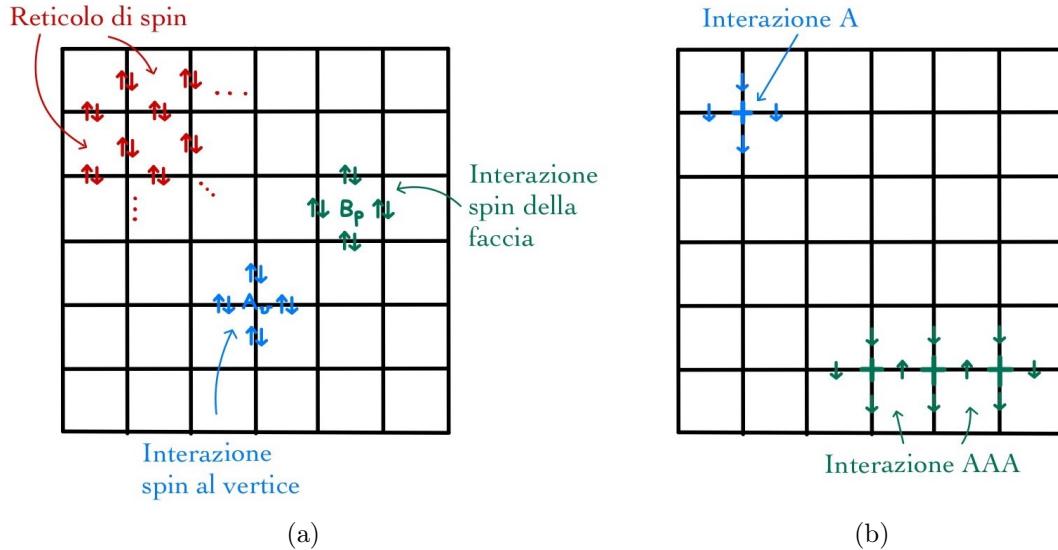


Figura 5.8: (5.8a) L'analogo sistema in meccanica statistica del toric code è costituito da un reticolo di spin in cui questi ultimi possono interagire in un vertice oppure in una plaquette. (5.8b) Se si espande la produttoria in (5.7.4) si hanno diverse interazioni di spin a causa delle combinazioni degli operatori  $A_v$ .

Dal punto di vista dei singoli spin lo stato (5.7.4) è estremamente complicato perché è uno stato molto entangled. Se si espande la produttoria in  $|\overline{00}\rangle$  si ottengono dei termini del tipo  $\mathbb{I} + A + AA + AAA + \dots$ , quindi avvengono diverse interazioni: come illustra la Figura 5.8b, il singolo operatore  $A$  agisce sul vertice e inverte i 4 spin (in blu in alto a sinistra dove gli spin  $\uparrow$  sono diventati  $\downarrow$ ); gli operatori della forma  $AAA$ , invece, creano un loop di spin capovolti nel reticolo originale (si vedano i tre vertici in basso in verde). In totale la produttoria in (5.7.4) produce una sovrapposizione lineare di tutti i possibili loop costituiti da spin invertiti: c'è entanglement tra tutti gli spin del reticolo, persino tra quelli più distanti.

Che cosa sono gli errori in QC? Non sono altro che operatori che agiscono sui link del reticolo: ad esempio se si pensa ad un singolo bit flip error (**X-gate** su un link) allora esso cambia autovalore agli operatori  $B_p$  delle placchette adiacenti (si veda la Figura 5.5a); similmente quando si ha un phase flip error (Figura 5.5b), allora lo **Z-gate** sul link corrotto cambierà autovalore ai due operatori  $A_v$  adiacenti.

Data l'hamiltoniana (5.7.11), agli errori nel QC corrispondono delle eccitazioni nel sistema di spin: avremo una variazione di energia  $\Delta E_z = 2J$  per il singolo bit flip e una variazione di  $\Delta E_x = 2J$  per il singolo phase flip. In teoria della materia condensata questi stati eccitati corrispondono alle cosiddette **quasiparticles**. In questo contesto ne esistono di due tipologie: le quasiparticle **elettriche**, a seguito dell'errore causato da  $Z$  e le quasiparticle **magnetiche**, generate dall'errore di  $X$ ; entrambe hanno la medesima energia e vedremo nelle prossime sezioni che presentano alcune proprietà strane e insolite. Dato che per ogni errore (bit flip o phase flip) si hanno due autovalori  $-1$  ( $A_v = -1$  per  $Z$  e  $B_p = -1$  per  $X$ ) allora è come se potessimo associare due paia di quasiparticle: 2 elettriche e 2 magnetiche.

Una delle proprietà più insolite (vedremo) è la seguente: se si considera una quasiparticle elettrica e la si muove attorno ad una quasiparticle magnetica ritornando poi al punto di origine allora, a seguito della QM, si origina una fase: questo fenomeno può essere interpretato come un doppio scambio di particelle; per tale ragione questa particolare tipologia di particelle costituiscono un perfetto "toy model" per i cosiddetti **anyons** (diffusi in letteratura nella teoria della materia condensata). Queste particolari quasiparticle, presenti unicamente in sistemi bidimensionali, sono simili a particelle che presentano una statistica frazionaria, ossia non sono né bosoni né fermioni!

LEZIONE 15 - 26/11/2021

### 5.7.3 Topological quantum computing

Nella sezione precedente abbiamo associato le eccitazioni nel sistema di spin (errori nel toric code) a due diverse tipologie di quasiparticle: elettriche e magnetiche. Queste quasiparticle si originano in coppia quando si verifica un bit flip o un phase flip in un qualunque punto del reticolo. Notiamo che queste quasiparticle possono essere separate all'interno del reticolo senza alcun costo in termini energetici, perché possiamo costruire un percorso generico che le colleghi attraverso l'applicazione ripetuta di X-gate (quasiparticle magnetiche) o Z-gate (quasiparticle elettriche). In Figura 5.9 è evidenziata come la posizione delle quasiparticle (magnetiche ed elettriche) all'interno dei due reticolati abbia la stessa differenza in energia  $\Delta E = 2J$  indipendentemente dalla loro vicinanza.

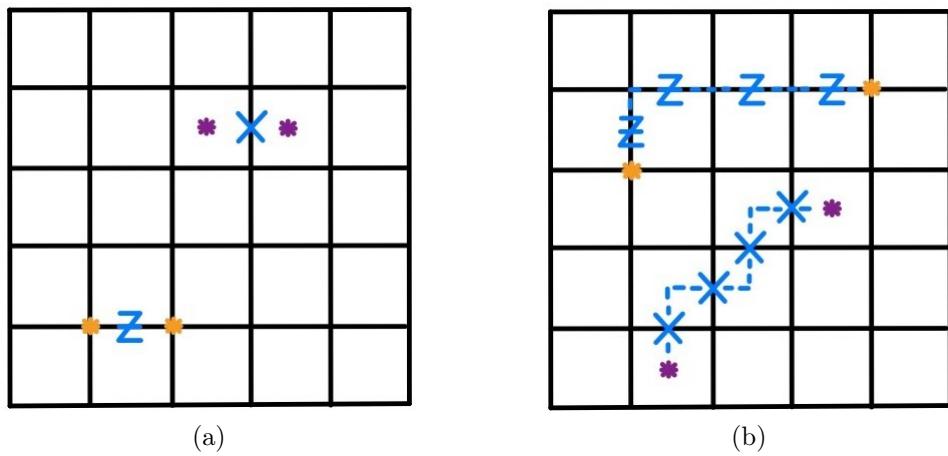


Figura 5.9: (5.9a) Coppia di quasiparticle elettriche (asterischi arancio per  $A_v = -1$ ) e magnetiche (asterischi viola per  $B_p = -1$ ) create da un singolo errore. (5.9b) Indipendentemente dal cammino di errori che origina queste particelle, il costo di energia  $E - E_0 = 2J$  è sempre lo stesso.

In aggiunta queste quasiparticle presentano delle ulteriori proprietà interessanti. Supponiamo di considerare due coppie, una di quasiparticle elettriche e l'altra di quasiparticle magnetiche, come mostrato in Figura 5.10. Immaginiamo di considerare solamente la coppia elettrica: come visto nella scorsa sottosezione, se muoviamo una delle due particelle applicando una stringa di Z-gate lungo un loop chiuso, allora l'effetto è banale perché il percorso può essere fattorizzato in un prodotto di operatori  $B_p$ , i quali hanno tutti autovalori +1 sul codewords.

Il comportamento risulta tuttavia differente se consideriamo in aggiunta una coppia di particelle magnetiche. Come in figura, realizziamo un circuito chiuso (quindi tornerà nel suo punto iniziale) a partire da una particella elettrica che passi tra le due quasiparticle magnetiche. Quando il percorso va ad avvolgere una quasiparticle magnetica, siccome  $X$  e  $Z$  anticommutano tra loro, lo stato ottiene un termine di fase  $|\psi\rangle \rightarrow -|\psi\rangle = e^{i\pi} |\psi\rangle$  dovuto al fatto che questa volta il prodotto di plaquette abbia autovalore  $-1$ . Questo risultato assomiglia un po' all'effetto Aharonov-Bohm<sup>x</sup>: per questo motivo si dice che queste quasiparticle abbiano una statistica reciproca non banale.

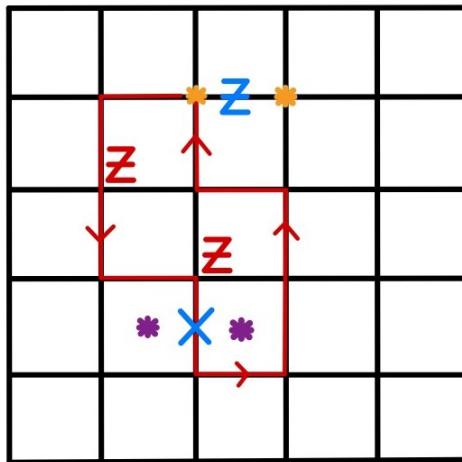


Figura 5.10: Il loop chiuso di Z-gate (loop rosso) della quasiparticle elettrica attorno a quella magnetica produce un termine di fase a seguito di  $\{X, Z\} = 0$ .

Riassumiamo ciò che abbiamo imparato sull'interpretazione in meccanica statistica del toric code. Questo codice di correzione degli errori presenta un approccio topologico: mentre gli errori agenti sui singoli qubit possono essere corretti similmente ai codici visti in precedenza, la situazione è differente quando si considerano errori agenti su più di un qubit simultaneamente. Immaginiamo che in un codice di protezione dagli errori come quello di Shor o di Steane avvengano 3 errori simultanei che causino  $|000\rangle \rightarrow |111\rangle$ . In generale, dato che un qubit logico si è trasformato in un altro qubit logico, una tale situazione è molto difficile da distinguere e correggere per quel tipo di codici. Al contrario, nel toric code, errori tali che trasformino qubit logici in altri qubit logici sono molto difficili da avere perché sono necessari degli interi loop di errori che attraversano tutto il reticolo (si pensi a  $\bar{Z}_i$  e  $\bar{X}_i$  della Figura 5.4). Se il reticolo è grande abbastanza questi errori sono molto improbabili: un reticolo sufficientemente grande assicura una protezione da questa tipologia di errori!

Dal punto di vista della sua interpretazione in meccanica statistica, questa robustezza del toric code contro gli errori si traduce in una robustezza della degenerazione dei vuoti, ossia degli stati di ground, contro le perturbazioni. Possiamo formalizzare questa proprietà nel seguente modo. Per tutti gli operatori locali<sup>xi</sup>  $\hat{O}$ , chiamando  $|\bar{x}\bar{y}\rangle$  e  $|\bar{x}'\bar{y}'\rangle$  due differenti stati di ground, vale

$$\langle \bar{x}\bar{y} | \hat{O} | \bar{x}'\bar{y}' \rangle = \delta_{\bar{x}\bar{x}'} \delta_{\bar{y}\bar{y}'} , \quad \text{per } \bar{x}, \bar{y}, \bar{x}', \bar{y}' = 0, 1 .$$

<sup>x</sup>Dopo aver percorso un circuito chiuso torniamo allo stato iniziale con una fase extra.

<sup>xi</sup>Operatori costruiti a partire da una collezione di  $X$ ,  $Z$  e  $Y$  che agiscono solo localmente in una regione finita del piano del reticolo; non sono gli operatori  $\bar{Z}_i$  e  $\bar{X}_i$ , ossia tali che attraversino l'intero reticolo.

Questo significa che operatori locali non possono tramutare stati di ground in altri stati di ground. Il motivo della precedente proprietà è il seguente: se  $\hat{O}$  è locale allora è un loop di  $X$  o  $Z$ , che agisce banalmente come identità, oppure è un singolo errore  $X$  o  $Z$ , il quale sappiamo che genera uno stato non più facente parte del codewords. L'unico modo per ottenere qualcosa di non banale è quello di utilizzare un operatore non locale: qualsiasi perturbazione può agire solo localmente!

Il toric code è un esempio di **fase della materia con ordine topologico**. Queste sono caratterizzate da un entanglement a lungo raggio (LRE = long range entanglement, soprattutto per gli stati fondamentali) e presentano alcune proprietà comuni:

- Degenerazione robusta dello stato fondamentale su varietà compatte (ad esempio un toro). Questo fatto è associato alla topologia della varietà: è molto difficile eliminare la degenerazione del ground state utilizzando perturbazioni locali;
- Ci sono eccitazioni (quasiparticles elettriche e magnetiche) che presentano proprietà non locali, come ad esempio statistiche non banali. Si pensi all'effetto Aharonov-Bohm tipico di fasi topologiche della materia;
- La low-energy theory è in qualche modo topologica, ossia dipende unicamente dalla topologia della varietà che si sta considerando. Si tratta di una descrizione in termini di una cosiddetta **topological quantum field theory** (TQFT)<sup>xii</sup>. Per esempio ampiezze di processi in QM dipendono solo dalla topologia del cammino della particella e non dalla sua forma o velocità (Figura 5.11).

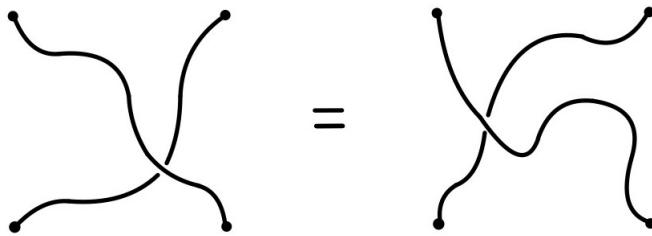


Figura 5.11: Equivalenza delle ampiezze dei processi in una TQFT, i quali non dipendono dalla forma o dalla velocità dei cammini.

Queste caratteristiche erano dal punto di vista della teoria della materia condensata. Ritornando al QC, il toric code è solitamente discusso come uno dei primi esempi di **topological quantum computing**, poiché alcune generalizzazioni di ciò che abbiamo visto nel corso di questa sezione possono essere utilizzate per il QC. Senza alcuna pretesa di essere formali, cerchiamo di comprendere quale sia l'idea che ne sta alla base.

Dal punto di vista dell'interpretazione in meccanica statistica (sistema fisico di spin su reticolo), consideriamo l'ampiezza in QM generata dal processo in Figura 5.12a: se la quasiparticle elettrica circonda quella magnetica, allora, come abbiamo visto, otteniamo un termine di fase  $(-1) = e^{i\pi}$  tale per cui la funzione d'onda passa da uno stato  $|\psi\rangle$  (stato iniziale delle 4 quasiparticle) a uno stato  $-|\psi\rangle$ . Questa situazione, come mostra la Figura 5.12b, è assimilabile ad uno scambio di particelle: a metà del processo (linea tratteggiata in rosso in 5.12a) si ha una situazione in cui la particella elettrica è stata mossa nel passato di quella magnetica, quindi è come se si avesse uno scambio delle due.

<sup>xii</sup>Introdotta da Edward Witten nel 1988.

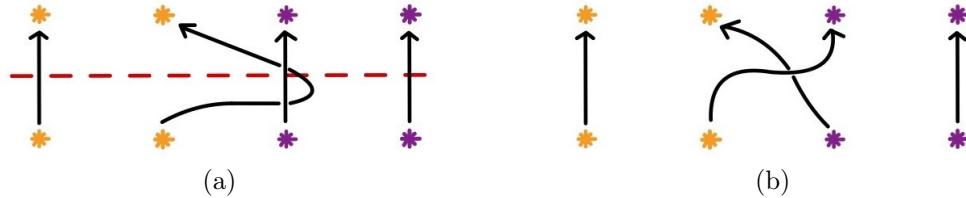


Figura 5.12: (5.12a) Ampiezza del processo in cui una quasiparticle elettrica gira attorno ad una magnetica. (5.12b) L'ampiezza qui a sinistra è analoga ad una situazione di scambio di queste particelle.

In una situazione di scambio di particelle dobbiamo stare attenti in QM quando si tratta di particelle identiche (si pensi alla Figura 5.12b con 4 particelle identiche come stato iniziale e finale): dobbiamo prestare attenzione al principio di esclusione di Pauli!

Supponiamo di avere un sistema (in teoria della materia condensata) con un insieme di quattro<sup>xiii</sup> quasiparticle tali per cui lo stato iniziale sia descritto dalla sovrapposizione  $|\psi\rangle = \alpha|\psi_1\rangle + \beta|\psi_2\rangle$ , la quale è degenere: ci sono due stati quantistici  $|\psi_1\rangle$  e  $|\psi_2\rangle$  che corrispondono alle quattro particelle identiche con i medesimi numeri quantici. Quando scambiamo due di loro come in Figura 5.12b avremo in generale

$$|\psi\rangle = \alpha|\psi_1\rangle + \beta|\psi_2\rangle \longrightarrow |\psi'\rangle = \alpha'|\psi_1\rangle + \beta'|\psi_2\rangle .$$

La relazione che lega questo scambio può essere vista come una rotazione non banale operata dalla matrice unitaria  $\hat{U}$ :

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \longrightarrow \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = \hat{U} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} ;$$

in particolare ritorniamo alla condizione iniziale, ma con lo stato che può essere trasformato in un altro stato dello stesso spazio di Hilbert degenere. L'unico vincolo quantomeccanico è il fatto che  $\hat{U}$  sia unitario.

Questi stati presentano quella che si definisce **statistica non-abeliana** (il toric code ha solo uno stato per cui la statistica era abeliana, ossia data da una semplice fase del gruppo  $U(1)$ ). Quando le particelle sono identiche e presentano statistica frazionaria, allora, non essendo né fermioni né bosoni, sono note come **anyons** e possono esistere solamente in una situazione bidimensionale<sup>xiv</sup>.

La cosa curiosa è che, in teoria, gli anyons non-abeliani possono essere usati per il QC! Costruendo in laboratorio un array di quasiparticle e intrecciandole tra loro possiamo dare luogo a trasformazioni unitarie non-abeliane proprio come l'esempio di Figura 5.13. Ogni volta che si scambia una quasiparticle si ha una trasformazione unitaria sul sistema: l'intera sequenza di scambi può essere pensata come un singolo operatore (gate) unitario  $U$ .

Se fossimo in grado di realizzare abbastanza trasformazioni unitarie con scambi multipli, potremmo eseguire del QC grazie ad essi. Perché sarebbe molto interessante poter costruire computer quantistici basati su questo funzionamento? Questi dispositivi sarebbero molto robusti e fault-tolerant perché il rumore o altri disturbi locali andrebbero ad

<sup>xiii</sup>Ne consideriamo quattro perché in questi modelli le quasiparticle vengono prodotte in coppia.

<sup>xiv</sup>Non nello spazio tridimensionale, perché in 3D un doppio scambio deve essere banale per via della topologia, cosicché un singolo scambio possa dare solo  $\pm 1$  (bosoni o fermioni).

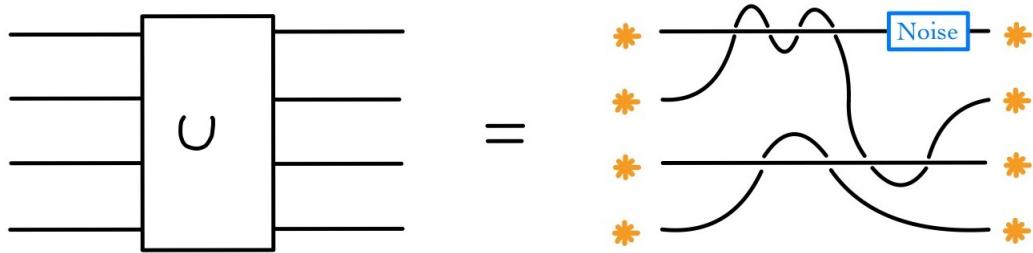


Figura 5.13: Implementazione in QC di un circuito utilizzando un array di quasiparticle. Si suppone che i fili del circuito possano essere sostituiti dalle particelle, le quali possono essere spostate tra loro. Il rumore può intervenire unicamente su un singolo intreccio: per cambiare l'intero  $U$  dovrebbe annullare ogni singolo intreccio!

agire solo localmente sulla linea delle quasiparticle. Affinché il disturbo causato dall'ambiente possa essere in grado di cambiare l'intero  $U$ , esso dovrebbe poter annullare tutte le singole trasformazioni.

I tipi più comuni di anyons (non-abeliani) sono:

- **Ising Anyons:** non sono universali nel senso del QC, ma appaiono teoricamente in molti sistemi della materia condensata:
  - Effetto Hall quantistico frazionario ( $\nu = 5/2$ ;  $SU(2)_2$  nel contesto della TQFT);
  - Majorana zero-mode in superconduttori topologici bidimensionali (generalizzano il più semplice modello monodimensionale chiamato catena di Kitaev).
- **Fibonacci Anyons:** sono universali, sono stati sviluppati nella teoria dei modelli che generalizzano il toric code e si suppone che appaiano nell'effetto Hall quantistico frazionario ( $\nu = 12/5$ ;  $SU(2)_3$  nel contesto della TQFT).

Due figure di spicco che proposero e diedero inizio al campo del topological quantum computing sono:

- Alexei Kitaev, il quale propose nel 1997 un topological quantum computing basato sugli anyons;
- Michael Freedman, vincitore nel 1986 della medaglia Fields per aver risolto la congettura di Poincaré in dimensione 4. Era interessato a calcolare degli invarianti della teoria dei nodi noti come polinomi di Jones, un problema di difficoltà esponenziale dal punto di vista del CC, quando scoprì che in QC in realtà può essere risolto in un tempo polinomiale. Attualmente dirige il gruppo di Microsoft Station Q a Santa Barbara per lo sviluppo del topological quantum computing. Nel 2018 il gruppo annunciò di aver realizzato sperimentalmente i Majorana zero-mode, ma nel 2021 l'articolo fu ritirato.

# Capitolo 6

## Realizzazione fisica dei qubit

### 6.1 Introduzione

Nella parte introduttiva del primo capitolo abbiamo visto che esistono moltissimi modi per poter realizzare fisicamente un qubit, dato che, dal punto di vista della QM, si tratta di un qualsiasi sistema quantistico a due livelli. Lasciando stare il discorso sulla realizzazione dei qubit nell'ambito della topological quantum computing, i più semplici da realizzare sono basati su:

- Sistemi costituiti da particelle con **Spin 1/2**; le particelle possono essere semplicemente controllate attraverso un campo magnetico  $\vec{B}$ , in quanto l'hamiltoniana che descrive questo tipo di interazione con lo spin è

$$\hat{H} = -\mu \hat{\vec{S}} \cdot \vec{B},$$

dove  $\mu$  è il momento magnetico.

- Sistemi che sfruttano la **polarizzazione dei fotoni**; sono in generale più difficili da gestire rispetto ai precedenti, tuttavia possono essere opportunamente controllati attraverso filtri polarizzatori (ad esempio un prisma per controllare i cambi di fase), beam splitters, ecc.

Altre realizzazioni fisiche, alcune delle quali approfondiremo nelle prossime sezioni, riguardano i qubit superconduttori<sup>i</sup>, i qubit basati sulla risonanza magnetica nucleare<sup>ii</sup>, i qubit a trappola ionica<sup>iii</sup>, ecc. Spendiamo alcune parole sui qubit realizzati mediante sistemi basati sulla trappola ionica e sulla superconduttività.

Nei primi dispositivi si vuole andare a creare un campo elettromagnetico che confini un insieme di ioni in una catena lineare lungo una direzione privilegiata (per convenzione è l'asse  $z$ ). Si veda la Figura 6.1 per una raffigurazione schematica.

L'idea è quella di raffreddare questo sistema fino allo stato fondamentale in maniera tale che l'unico grado di libertà rimanente a questi ioni riguardi piccole vibrazioni lungo l'asse  $z$ . In questo modo si può incorporare un qubit in ognuno di essi combinando due differenti tipi di sistemi a due livelli:

---

<sup>i</sup>Utilizzati da IBM e Google.

<sup>ii</sup>Nota meglio come NMRQC: Nuclear Magnetic Resonance Quantum Computing.

<sup>iii</sup>Utilizzata da IonQ.

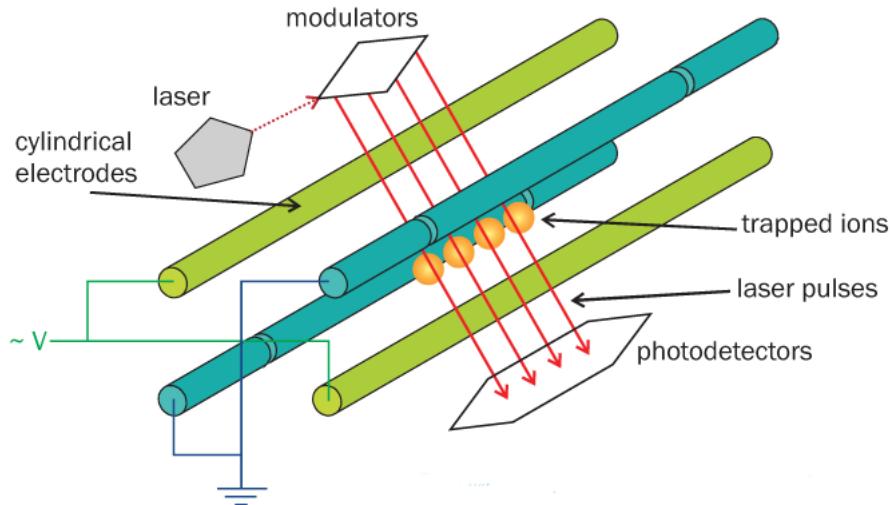


Figura 6.1: Rappresentazione schematica del sistema della trappola ionica.

- Ogni ione presenta una struttura iperfine nei livelli energetici, si avrà quindi uno stato fondamentale  $|0\rangle$  e uno stato eccitato  $|1\rangle$ , il quale è metastabile. Essi sono separati da un'energia pari a  $\hbar\omega_1$ .
- Ogni ione ha però al tempo stesso un modo vibrazionale, il quale è assimilabile a un oscillatore armonico. In termini di fisica della materia condensata, ogni **fonone** ha quindi due stati energetici separati da un'energia pari a  $\hbar\omega_2$ .

Perciò è possibile costruire due qubit identificando lo stato con la notazione  $|nm\rangle$ , dove  $n$  indica il primo sistema a due livelli (livelli iperfini dello ione) ed  $m$  il secondo sistema a due livelli (modi del fonone), proprio come mostrato in Figura 6.2. Utilizzando infine degli impulsi generati da laser, si può andare a interagire e a manipolare questo sistema (si pensi alla Figura 6.1).

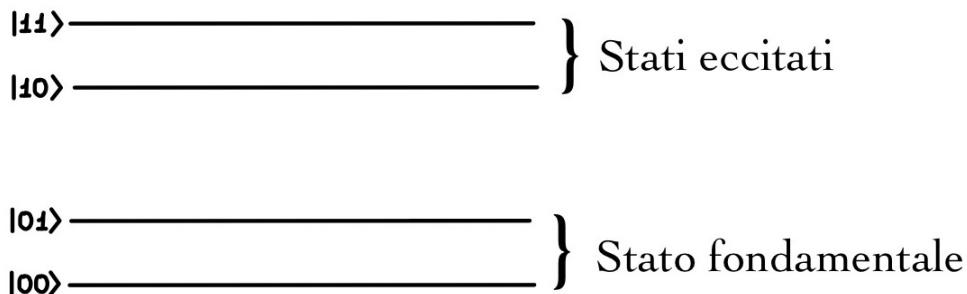


Figura 6.2: Sistema doppio a due livelli che coinvolge gli stati energetici degli ioni e i modi vibrazionali dei fononi. Notare che la differenza energetica tra gli stati fondamentali e gli stati eccitati è maggiore rispetto alla differenza energetica dovuta ai modi vibrazionali.

Per quanto riguarda invece i sistemi superconduttori l'idea che sta alla base è quella di realizzare un semplice circuito LC. Risolvendo le equazioni di Kirchhoff è possibile mostrare che il comportamento di tale circuito sia quello di un oscillatore armonico, il quale può essere facilmente quantizzato attraverso la quantizzazione canonica. Si parla di supercondutività poiché si cerca di lavorare con elementi che non presentano alcuna resistenza a bassa temperatura.

Il problema, che ribadiremo più volte, è che questo circuito LC per come è fatto non è molto adatto a descrivere un sistema a due livelli, dunque bisogna fare in modo che il comportamento dell'oscillatore risulti anarmonico: solitamente lo si fa introducendo la cosiddetta **giunzione Josephson**, per mezzo della quale si passa da un sistema a livelli equispaziati a un sistema con livelli non più equidistanti e che presentano dell'anarmonicità. Per interagire con questi sistemi è poi quindi necessario introdurre un generatore di impulsi a microonde mentre per ottenere informazioni sui qubit si utilizzano delle cavità elettromagnetiche. La differenza sostanziale tra i due dispositivi sta nel campo elettromagnetico, in quanto nel primo è classico mentre nel secondo è quantizzato. Si veda la Figura 6.3 per una rappresentazione schematica.

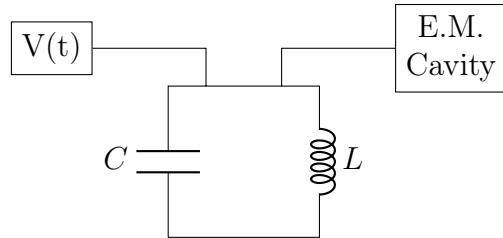


Figura 6.3: Circuito LC con generatore di microonde e cavità elettromagnetica.

## 6.2 Oscillatore armonico quantistico

Prima di poter descrivere accuratamente un modello fisico completo per un computer quantistico realizzabile, richiamiamo alcune nozioni su un sistema fisico molto elementare: l'oscillatore armonico quantistico<sup>iv</sup>. Supponiamo di avere un sistema che oscilla con una frequenza pari a  $\omega$ . Il suo moto sarà descritto dall'equazione del moto

$$\frac{d^2x}{dt^2} + \omega^2 x = 0, \quad (6.2.1)$$

le cui soluzioni sono del tipo  $x(t) = e^{\pm i\omega t}$ . L'hamiltoniana associata a questo sistema risulta quindi in

$$H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2. \quad (6.2.2)$$

Per passare ad una descrizione quantomeccanica si procede con la quantizzazione canonica identificando le osservabili posizione e momento lineare con i rispettivi operatori hermitiani  $\hat{x}$  e  $\hat{p}$ ; inoltre introduciamo la regola di commutazione  $[\hat{x}, \hat{p}] = i\hbar$ . In questo modo l'hamiltoniana (6.2.2) può essere scritta immediatamente come

$$\hat{H} = \frac{\hat{p}^2}{2m} + \frac{1}{2}m\omega^2 \hat{x}^2,$$

oppure

$$\hat{H} = \hbar\omega \left( \hat{a}^\dagger \hat{a} + \frac{1}{2} \right) = \hbar\omega \left( \hat{n} + \frac{1}{2} \right), \quad (6.2.3)$$

---

<sup>iv</sup>Non ci dilunghiamo molto su questo argomento perché è stato già trattato in maniera sufficientemente approfondita nel corso di MQ.

dove in quest'ultima equazione abbiamo introdotto tre nuovi operatori

$$\text{Operatore di creazione:} \quad \hat{a}^\dagger = \frac{1}{\sqrt{2m\hbar\omega}}(m\omega\hat{x} - i\hat{p}),$$

$$\text{Operatore di distruzione:} \quad \hat{a} = \frac{1}{\sqrt{2m\hbar\omega}}(m\omega\hat{x} + i\hat{p}),$$

$$\text{Operatore numero:} \quad \hat{n} = \hat{a}^\dagger \hat{a}.$$

Dalla relazione di commutazione precedente avremo  $[\hat{a}, \hat{a}^\dagger] = 1$ . Con queste definizioni, possiamo anche riscrivere  $\hat{x}$  e  $\hat{p}$  in funzione dei primi due nuovi operatori

$$\hat{x} = \sqrt{\frac{\hbar}{2m\omega}}(\hat{a} + \hat{a}^\dagger), \quad (6.2.4)$$

$$\hat{p} = -i\sqrt{\frac{m\omega\hbar}{2}}(\hat{a} - \hat{a}^\dagger). \quad (6.2.5)$$

Con queste nuove definizioni avremo che gli autostati dell'hamiltoniana (6.2.3) sono gli stessi dell'operatore numero  $\hat{n}$ , quindi possiamo considerare una base comune di autostati  $|n\rangle$  tale per cui  $\hat{n}|n\rangle = n|n\rangle$ . Esplicitamente avremo

$$\hat{H}|n\rangle = \hbar\omega\left(n + \frac{1}{2}\right)|n\rangle, \quad \text{dove } n \in \mathbb{N}.$$

La cosa importante da sottolineare è che gli operatori  $\hat{a}^\dagger$  e  $\hat{a}$  non a caso sono chiamati operatori di creazione e distruzione, perché a partire dallo stato fondamentale  $|0\rangle$ , che ha energia  $\frac{\hbar\omega}{2}$ , possiamo costruire tutti gli altri livelli. L'azione su un autostato  $|n\rangle$  non è altro che

$$\begin{aligned} \hat{a}^\dagger|n\rangle &= \sqrt{n+1}|n+1\rangle, \\ \hat{a}|n\rangle &= \sqrt{n}|n-1\rangle. \end{aligned} \quad (6.2.6)$$

Pertanto, per costruire il livello  $n$ -esimo, sarà sufficiente applicare la definizione sul ground state  $|0\rangle$ :

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}|0\rangle.$$

Se ora andassimo a rappresentare graficamente il potenziale armonico

$$V(x) = \frac{1}{2}m\omega^2x^2,$$

con le varie funzioni d'onda (*polinomi di Hermite*), potremmo osservare l'andamento rappresentato in Figura 6.4. Dal momento che tutti i livelli sono equispaziati, ciascun livello differisce dal precedente e dal successivo per un termine  $\hbar\omega$ : l'idea, per realizzare un sistema a due livelli, è quindi quella di considerare i livelli  $n = 0$  e  $n = 1$ , che identifichiamo con  $|0\rangle$  e  $|1\rangle$ , come stati del nostro qubit. Allo stesso tempo però dobbiamo essere in grado di controllare il passaggio dallo stato fondamentale  $|0\rangle$  allo stato eccitato  $|1\rangle$  e questo può essere facilmente realizzato attraverso un impulso laser. Tuttavia è possibile che il nostro sistema si trovi già in uno stato eccitato e mediante un altro impulso laser passi a un livello eccitato che si trova al di fuori del nostro sistema a due livelli, ad esempio si può verificare

$$|1\rangle \longrightarrow |2\rangle,$$

$$|2\rangle \longrightarrow |3\rangle,$$

$$\vdots \longrightarrow \vdots$$

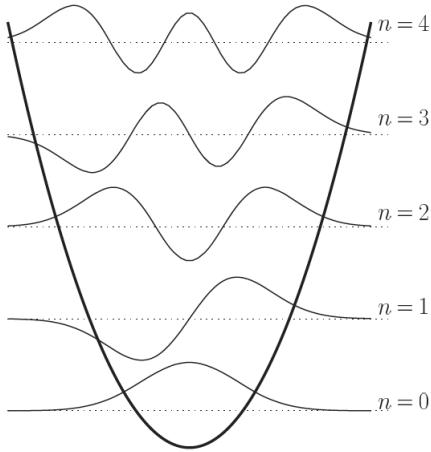


Figura 6.4: Potenziale armonico con le funzioni d'onda associate. I livelli energetici sono chiaramente equidistanti dal punto di vista energetico, quindi è molto difficile interagire con dei livelli a piacere mediante l'utilizzo della radiazione.

Per cui la descrizione dell'oscillatore armonico quantistico è sì utile per la realizzazione di sistemi a due livelli, però presenta dei difetti correlati al fatto che i livelli energetici siano equidistanti. Vedremo nelle sezioni successive come si può intervenire per ovviare a questo inconveniente.

Sebbene quest'ultimo aspetto sia spesso visto come un problema per la realizzazione di un qubit, l'oscillatore armonico quantistico può essere utilizzato per realizzare alcuni gate non banali. Vediamo il seguente esempio accademico.

**Esempio 6.1 (Codifica del CNOT gate.).** *Supponiamo di voler eseguire un calcolo quantistico che faccia uso di un CNOT-gate costruito con l'oscillatore armonico quantistico descritto sopra. Che cosa possiamo fare? La scelta più naturale per la rappresentazione dei qubit sono gli autostati energetici  $|n\rangle$ . Questa scelta ci permette di eseguire un CNOT-gate nel seguente modo: codifichiamo i seguenti 4 qubit logici utilizzando l'identificazione*

$$\begin{aligned} |00\rangle_L &= |0\rangle, & |01\rangle_L &= |2\rangle, \\ |10\rangle_L &= \frac{|4\rangle + |1\rangle}{\sqrt{2}}, & |11\rangle_L &= \frac{|4\rangle - |1\rangle}{\sqrt{2}}, \end{aligned} \quad (6.2.7)$$

dove il pedice  $L$  è usato per distinguere chiaramente gli stati logici in contrasto con gli autostati dell'hamiltoniana dell'oscillatore armonico. Dal punto di vista concettuale, il fatto che stiamo utilizzando stati energetici come  $|2\rangle$  e  $|4\rangle$  sarà presto chiaro.

La manipolazione dei qubit, come abbiamo visto all'inizio, può essere effettuata, ad esempio, tramite l'applicazione di un campo magnetico nel caso di un sistema con degli spin: in generale può essere necessario sottoporre il sistema a delle perturbazioni esterne. In questo caso possiamo semplicemente sfruttare l'evoluzione temporale degli stati: assumiamo di aver preparato il sistema in uno stato  $|n\rangle$  e decidiamo di lasciarlo evolvere nel tempo, quindi

$$|n\rangle \rightarrow \hat{U}(t)|n\rangle = e^{-\frac{i}{\hbar}\hat{H}t}|n\rangle = e^{-\frac{i}{\hbar}E_n t}|n\rangle;$$

lo stato finale rimane nello stato di partenza acquisendo tuttavia una fase: il punto importante che ci permette di costruire un CNOT-gate è che l'evoluzione temporale non crea una sovrapposizione di stati, ma mantiene bensì un singolo stato stazionario. Ricordando

che i livelli energetici sono dati da

$$E_n = \hbar\omega \left( n + \frac{1}{2} \right),$$

allora, trascurando il fattore  $1/2$  perché fase comune a tutti i livelli, possiamo procedere nell'applicare l'operatore di evoluzione temporale agli stati logici in (6.2.7)

$$\begin{aligned} |00\rangle_L &= |0\rangle, & |01\rangle_L &= e^{-2i\omega t} |2\rangle, \\ |10\rangle_L &= \frac{e^{-4i\omega t} |4\rangle + e^{-i\omega t} |1\rangle}{\sqrt{2}}, & |11\rangle_L &= \frac{e^{-4i\omega t} |4\rangle - e^{-i\omega t} |1\rangle}{\sqrt{2}}. \end{aligned}$$

Se scegliamo un valore di tempo particolare, come ad esempio  $t = \pi/\omega$ , l'evoluzione temporale porterà allora a

$$\begin{aligned} |00\rangle_L \rightarrow |0\rangle &\equiv |00\rangle_L, & |01\rangle_L \rightarrow |2\rangle &\equiv |01\rangle_L, \\ |10\rangle_L \rightarrow \frac{|4\rangle - |1\rangle}{\sqrt{2}} &\equiv |11\rangle_L, & |11\rangle_L \rightarrow \frac{|4\rangle + |1\rangle}{\sqrt{2}} &\equiv |10\rangle_L. \end{aligned}$$

Abbiamo ottenuto esattamente l'azione di un **CNOT-gate** utilizzando semplicemente l'evoluzione temporale del sistema!

Perché non è possibile utilizzare fisicamente un CNOT-gate così costruito? Perché ogni conto in QC è basato sul calcolo quantistico, non sul calcolo analogico: per usare i qubit ottenuti è necessario intervenire mediante l'utilizzo della radiazione, ma così ritorniamo al problema originale dei livelli energetici equispaziati! È semplice costruire un CNOT-gate, ma purtroppo è molto difficile controllare un tale sistema.

LEZIONE 16 - 29/11/2021

### 6.3 Campo elettromagnetico quantizzato

Per capire come il campo elettromagnetico può interagire con un sistema a due livelli dobbiamo prima di tutto studiare come si quantizza la radiazione elettromagnetica. L'idea che sta alla base è quella di considerare, come per la radiazione di corpo nero in fisica classica, il campo elettromagnetico nel vuoto come un'infinita collezione di oscillatori armonici.

Consideriamo la nota formulazione dei campi elettromagnetici in termini del potenziale vettore  $\vec{A}$ :

$$\vec{E} = -\frac{\partial \vec{A}}{\partial t}, \quad \vec{B} = \nabla \times \vec{A}. \quad (6.3.1)$$

Imponendo il **gauge di Coulomb**<sup>v</sup>  $\nabla \cdot \vec{A} = 0$  sulle equazioni di Maxwell in termini di  $\vec{A}$  è possibile ottenere facilmente l'equazione delle onde

$$\frac{1}{c^2} \frac{\partial^2 \vec{A}}{\partial t^2} - \nabla^2 \vec{A} = 0; \quad (6.3.2)$$

---

<sup>v</sup>Noto anche come *gauge trasversale* o *gauge di radiazione*.

chiaramente la scelta del gauge non cambia la fisica, infatti senza la condizione  $\nabla \cdot \vec{A} = 0$  è possibile dimostrare che si ottiene nuovamente la (6.3.2) con un extra termine a RHS dovuto alla presenza di una sorgente. Generiche soluzioni della (6.3.2) sono, ad esempio, le onde piane

$$\vec{A} = \vec{A}_{\vec{k}} e^{i(\vec{k} \cdot \vec{x} - \omega t)} + \vec{A}_{\vec{k}}^* e^{-i(\vec{k} \cdot \vec{x} - \omega t)}, \quad (6.3.3)$$

dove  $\vec{A}_{\vec{k}}$  è un generico coefficiente vettoriale complesso che specifica la polarizzazione dell'onda piana e  $\vec{k}$  il vettore d'onda che ne individua la direzione di propagazione. Si noti che abbiamo sommato al primo termine il suo complesso coniugato per assicurare che la soluzione sia reale.

L'informazione fisica che si ottiene inserendo la soluzione precedente nell'equazione delle onde è la **relazione di dispersione**  $\omega = c|\vec{k}|$ , quindi d'ora in avanti  $\omega$  non è più indipendente da  $\vec{k}$ ; similmente, imponendo la condizione di gauge avremo  $\vec{k} \cdot \vec{A}_{\vec{k}} = 0$ , perciò il vettore d'onda (direzione della propagazione dell'onda) è perpendicolare rispetto al vettore della polarizzazione. Nel piano perpendicolare a  $\vec{k}$  è sempre possibile scegliere una base di vettori di polarizzazione di modulo unitario ( $|\vec{\varepsilon}_i| = 1$ ) tali che

$$\vec{A}_{\vec{k}} = A_{k,1} \vec{\varepsilon}_1 + A_{k,2} \vec{\varepsilon}_2.$$

Dato che l'equazione (6.3.2) è lineare, allora una combinazione lineare di soluzioni è anch'essa soluzione, quindi possiamo scrivere la generica soluzione di onde piane come la seguente sovrapposizione

$$\vec{A}(\vec{x}, t) = \sum_{\vec{k}} \sum_{i=1}^2 \left( A_{k,i} \vec{\varepsilon}_i e^{i(\vec{k} \cdot \vec{x} - \omega t)} + \text{c.c.} \right) \Big|_{\omega=c|\vec{k}|}, \quad (6.3.4)$$

dove "c.c." sta per complesso coniugato. Notiamo che abbiamo considerato una sovrapposizione di onde con diverso  $\vec{k}$  (nel caso infinito si rimpiazza  $\sum_{\vec{k}} \rightarrow \int d\vec{k}$ ) e, per ognuno di essi, abbiamo scelto una base su cui scrivere il vettore della polarizzazione. La relazione precedente è la più generale soluzione del campo elettromagnetico nel vuoto.

La somma precedente è costituita nient'altro che da oscillatori perché ogni parentesi è un oscillatore: se scriviamo infatti

$$\mathcal{A}_{\vec{k}}(\vec{x}, t) \equiv \left( A_{k,i} e^{i\vec{k} \cdot \vec{x}} \right) e^{-i\omega_k t},$$

allora  $\mathcal{A}_{\vec{k}}(\vec{x}, t)$  soddisfa l'equazione del moto (6.2.1) di un oscillatore armonico di frequenza  $\omega_k$  (pedice  $k$  per ricordare che la frequenza soddisfa una relazione di dispersione)

$$\ddot{\mathcal{A}}_{\vec{k},i} + \omega_k^2 \mathcal{A}_{\vec{k},i} = 0.$$

Dunque  $\vec{A}(\vec{x}, t)$  in (6.3.4) costituisce un'infinita collezione di oscillatori armonici disaccoppiati.

Per quantizzare un tale sistema è necessario utilizzare una procedura analoga alla quantizzazione dell'oscillatore armonico: così come si quantizza l'equazione (6.2.1) introducendo l'operatore (6.2.4), dobbiamo riscrivere l'ampiezza  $\mathcal{A}_{\vec{k},i}$  in funzione degli operatori  $(a_{\vec{k},i}, a_{\vec{k},i}^\dagger)$ . Nonostante ciò, già sappiamo che l'hamiltoniana dell'oscillatore armonico quantistico in termini di  $(a, a^\dagger)$  è la (6.2.3), dunque possiamo facilmente generalizzare tale scrittura per un'**hamiltoniana del campo elettromagnetico**, ossia

$$H = \sum_{\vec{k},i} \hbar \omega_{\vec{k}} \left( a_{\vec{k},i}^\dagger a_{\vec{k},i} + \frac{1}{2} \right). \quad (6.3.5)$$

Che tipologia di spettro avrà un sistema di questo tipo? Per ogni oscillatore possiamo introdurre un operatore numero  $\hat{n}_{\vec{k}}$  tale che

$$a_{\vec{k},i}^\dagger a_{\vec{k},i}^{\phantom\dagger} \left| n_{\vec{k},i} \right\rangle = n_{\vec{k},i} \left| n_{\vec{k},i} \right\rangle ;$$

in questo modo ciascun oscillatore presenterà livelli energetici equispaziati come in Figura 6.4, dove la differenza energetica è data  $\hbar\omega_{\vec{k}}$ .

Dato che la (6.3.5) è una somma, allora lo spazio di Hilbert totale è costituito da un'infinità di spazi di Hilbert disaccoppiati (uno per ciascun oscillatore), dunque è come se si trattasse di un sistema costituito da un'infinità di sottosistemi: lo spazio di Hilbert totale è chiamato **spazio di Fock** ed è dato dal prodotto tensoriale di tutti i singoli spazi degli oscillatori

$$\mathcal{H} = \bigotimes_{\vec{k},i} \mathcal{H}_{\vec{k},i} .$$

Qual è l'interpretazione degli stati  $|n_{\vec{k},i}\rangle$ ? Ogni stato  $|n_{\vec{k},i}\rangle$  è costituito da  $n_{\vec{k},i}$  fotoni di momento  $\vec{p} = \hbar\vec{k}$  e polarizzazione associata ai vettori  $\vec{\varepsilon}_i$ . Una particella (fotone) nello spazio di Fock corrisponde ad una particolare eccitazione dello stato fondamentale: i vari modi identificano un numero d'onda (lunghezza d'onda e frequenza precise) e ognuno di essi può essere eccitato numerose volte. Se identifichiamo lo stato  $|0\rangle$  con un modo non eccitato che non presenta fotoni, allora, per esempio, per gli stati eccitati possiamo scrivere

$$\begin{aligned} E_{|1\rangle} - E_{|0\rangle} &= \hbar\omega_{\vec{k}} & \Rightarrow & |1\rangle = 1 \text{ fotone con energia } \hbar\omega_{\vec{k}}, \\ E_{|2\rangle} - E_{|0\rangle} &= 2\hbar\omega_{\vec{k}} & \Rightarrow & |2\rangle = 2 \text{ fotoni con energia } \hbar\omega_{\vec{k}} \text{ ciascuno.} \end{aligned}$$

È importante sottolineare che nello stato  $|2\rangle$  (così come  $|3\rangle, |4\rangle, \dots$ ), tutti i fotoni presenti hanno la medesima energia ( $\hbar\omega_{\vec{k}}$ ) perché presentano lo stesso momento e la stessa polarizzazione.

Qual è l'interpretazione dell'**energia di punto zero** della (6.3.5)? Dato che siamo sempre interessati a differenze di energia (solamente queste sono finite), possiamo sempre ridefinire a piacimento l'energia dello stato fondamentale. Per tale motivo possiamo trascurare questo termine costante e riscrivere la (6.3.5) come

$$H = \sum_{\vec{k},i} \hbar\omega_{\vec{k}} \left( a_{\vec{k},i}^\dagger a_{\vec{k},i}^{\phantom\dagger} \right) .$$

Ricordando dalle (6.2.6) l'azione di  $(a, a^\dagger)$  sugli stati dell'oscillatore armonico, possiamo interpretare gli operatori  $(a_{\vec{k},i}, a_{\vec{k},i}^\dagger)$  di distruzione e creazione alla luce delle particelle del campo elettromagnetico:

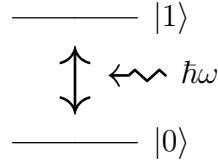
$a_{\vec{k},i}^\dagger$  = Operatore che crea un fotone di momento  $\vec{k}$  e polarizzazione  $\vec{\varepsilon}_i$ ,

$a_{\vec{k},i}$  = Operatore che distrugge un fotone di momento  $\vec{k}$  e polarizzazione  $\vec{\varepsilon}_i$ .

Per tale ragione il generico stato

$$\left| n_{\vec{k}_1,i_1}, n_{\vec{k}_2,i_2}, n_{\vec{k}_3,i_3}, \dots \right\rangle$$

dello spazio di Fock del campo elettromagnetico rappresenta un insieme di  $n_{\vec{k}_j,ij}$  fotoni con momenti  $\vec{p}_j = \hbar\vec{k}_j$  e polarizzazioni  $\vec{\epsilon}_j$ . Si noti che ognuno degli stati dati da  $n_{\vec{k}_j,ij}$  può avere in generale un differente numero di fotoni con momenti e polarizzazioni differenti. Nel contesto del QC siamo interessati a fotoni con momenti e frequenze ben precise perché, come sottolineato all'inizio del capitolo, l'idea è quella di utilizzare la radiazione per controllare i qubit: si invia un fotone di energia  $E = \hbar\omega$ , la quale è proprio identica (o circa uguale) alla differenza in energia dei due livelli energetici del qubit



Tipicamente solo un singolo fotone con un ben preciso momento, polarizzazione e direzione è sufficiente per eccitare un sistema come questo. Per questo motivo siamo interessati solamente ad un singolo modo del campo elettromagnetico: la fisica si riduce a ciò che abbiamo ripassato sull'oscillatore armonico quantistico! L'hamiltoniana del campo elettromagnetico risulterà quindi semplicemente nella (6.2.3), dove un particolare fotone è descritto da un singolo oscillatore armonico: gli stati  $|n\rangle$  rappresenteranno quindi situazioni con  $n$  fotoni con la medesima energia.

A seguito della procedura di quantizzazione precedente, il campo elettromagnetico viene promosso dalla semplice ampiezza (6.3.3) ad un operatore (similmente a  $x \rightarrow \hat{x}(a, a^\dagger)$  in (6.2.4)). Avremo quindi

$$\hat{A} = A_0 a e^{i(\vec{k} \cdot \vec{x} - \omega t)} + A_0^* a^\dagger e^{-i(\vec{k} \cdot \vec{x} - \omega t)}.$$

Non utilizziamo in questo contesto tutti i tecnicismi della QM perché stiamo utilizzando la rappresentazione di Heisenberg<sup>vi</sup>: il vantaggio di tale rappresentazione risiede nel fatto che è proprio l'operatore appena definito a soddisfare l'equazione del moto (6.3.2). Analogamente, anche i campi elettrici e magnetici sono promossi ad operatori. Ad esempio, dalle (6.3.1), l'operatore campo elettrico è dato da

$$\hat{E} = i\hat{a}\omega A_0 e^{i(\vec{k} \cdot \vec{x} - \omega t)} - i\hat{a}^\dagger \omega A_0^* e^{-i(\vec{k} \cdot \vec{x} - \omega t)};$$

chiaramente la parte operatoriale risiede negli operatori  $a$  e  $a^\dagger$ .

A seconda della scelta che si può fare su  $A_0$ , si utilizzano differenti convenzioni:

- Se  $A_0 \in \mathbb{R}$  allora si scrive

$$\hat{E} = iE_0 \left( \hat{a} e^{i(\vec{k} \cdot \vec{x} - \omega t)} - \hat{a}^\dagger e^{-i(\vec{k} \cdot \vec{x} - \omega t)} \right), \quad \text{con} \quad E_0 = \omega A_0.$$

- Quando invece  $A_0$  è puramente immaginario si pone

$$\hat{E} = \tilde{E}_0 \left( \hat{a} e^{i(\vec{k} \cdot \vec{x} - \omega t)} + \hat{a}^\dagger e^{-i(\vec{k} \cdot \vec{x} - \omega t)} \right), \quad \text{con} \quad \tilde{E}_0 = i\omega A_0.$$

<sup>vi</sup>A differenza della rappresentazione di Schrödinger, per la quale sono gli stati ad evolvere nel tempo, in quella di Heisenberg sono gli operatori a dipendere dal tempo. Si pone  $\hat{O}_H(t) = e^{i\hat{H}t} \hat{O}_S e^{-i\hat{H}t}$ , dove  $\hat{O}_S$  è il corrispondente operatore indipendente dal tempo nella rappresentazione di Schrödinger.

## 6.4 Accoppiamento qubit - campo e.m. classico

Cominciamo ora a studiare l'accoppiamento di un qubit con un campo elettromagnetico classico esterno; successivamente affronteremo l'analogo caso di accoppiamento con il campo elettromagnetico quantizzato. In generale la differenza tra le due situazioni dipende da ciò che si sta considerando e da ciò che si intende fare con il qubit. Ad esempio, se si considera una sorgente laser esterna allora si può svolgere una trattazione con entrambi gli accoppiamenti (il caso classico risulta però più semplice), invece quando si devono affrontare situazioni con cavità è necessario considerare solamente il caso quantizzato.

Sia nel caso dell'accoppiamento classico sia in quello dell'accoppiamento con il campo quantizzato, quando il qubit è posto in un campo elettromagnetico comincia ad oscillare con la medesima frequenza del campo: si tratta di un tipico modo per controllare a piacimento un qubit.

Supponiamo di considerare un singolo qubit: come possiamo controllarlo e manipolarlo in maniera tale che diventi qualcos'altro? In termini della sfera di Bloch, ricordiamo, si tratta di muovere questo sistema lungo la superficie della sfera. Un modo di farlo è quello di accoppiarlo ad un campo elettromagnetico classico esterno: ad esempio per un sistema di spin sappiamo che, a meno di costanti,  $H = \vec{S} \cdot \vec{B}$ , quindi basta regolare il campo magnetico per decidere la direzione dello spin. In una tale situazione sorge spontanea un'idea molto semplice: l'evoluzione temporale sarà data da

$$\hat{U} = e^{-\frac{i}{\hbar} \hat{H} t} = e^{-\frac{i}{\hbar} \vec{S} \cdot \vec{B} t},$$

ma l'operatore di spin  $\vec{S}$  è costituito dalle matrici di Pauli! Questo significa che l'evoluzione temporale è proprio regolata dall'operatore  $R_{\vec{n}}(\gamma)$  della (1.5.3), il quale implementa una rotazione di angolo  $\gamma$  attorno alla direzione individuata da  $\vec{n}$ : utilizzando l'accoppiamento  $H = \vec{S} \cdot \vec{B}$  (quasi universale) e regolando il campo magnetico è quindi possibile realizzare l'operatore  $R_{\vec{n}}(\gamma)$  mediante la sola evoluzione temporale.

Discutiamo l'interazione degli stati  $|0\rangle$  e  $|1\rangle$  di un sistema a due livelli con un campo elettromagnetico esterno. Se immaginiamo che tale sistema sia costituito da un atomo, allora esso interagisce con il campo tramite un'interazione di dipolo del tipo  $H = -\vec{d} \cdot \vec{E}$ : se l'atomo assorbe radiazione di energia  $\hbar\omega$  allora può subire la transizione energetica  $|0\rangle \rightarrow |1\rangle$ . Facciamo due assunzioni:

- **La dipendenza spaziale del campo  $\vec{E}$  è irrilevante.** Questo è dovuto al fatto che nella maggior parte delle situazioni la lunghezza d'onda della radiazione è molto più grande rispetto alle dimensioni del qubit (comparabili alle dimensioni atomiche,  $r_0 \sim 10^{-10}$  m): ad esempio, nello spettro del visibile  $\lambda \sim 10^{-6}$  m, mentre per le microonde  $\lambda \sim \text{cm/m}$ , quindi la differenza è persino maggiore. Il campo esterno è praticamente costante sul qubit e possiamo trascurare la sua dipendenza spaziale. Per tale ragione assumeremo

$$\vec{E} = \vec{E}_0 \cos(\omega_d t + \phi_0),$$

dove  $\omega_d$  è detta **frequenza di drive**<sup>vii</sup>.

- La radiazione interagisce con il dipolo dell'atomo, dove il dipolo non è altro che  $\vec{d} = e\vec{x}$ , quindi è lineare nella posizione. Siamo interessati solamente a due livelli

---

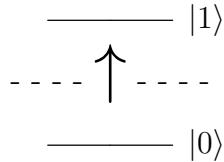
<sup>vii</sup>Poiché grazie a questa si andrà a guidare l'interazione del campo con il qubit.

atomici, dunque calcoleremo sempre elementi di matrice della forma  $\langle \omega | H | \omega' \rangle$ , dove  $\omega, \omega' = 0, 1$ . In tal caso  $\langle \omega | H | \omega' \rangle \sim \langle \omega | \hat{d} | \omega' \rangle \sim \langle \omega | \hat{x} | \omega' \rangle$ , ma non vogliamo calcolare elementi di matrice di questo tipo perché dipendono da molti fattori (direzione del campo, tipo di radiazione, regole di selezione in QM, ecc.). In generale  $\langle \omega | \hat{x} | \omega' \rangle$  **può essere il più generico elemento di una matrice**  $2 \times 2$ . Per questa ragione l'hamiltoniana a cui siamo interessati descrive un'interazione molto generica, scrivibile nella forma

$$H_{\text{couple}} = - \left( a\mathbb{I} + \vec{b} \cdot \vec{\sigma} \right) \cos(\omega_d t + \phi_0); \quad (6.4.1)$$

si noti che l'hamiltoniana precedente non è solamente applicabile all'interazione di un atomo con la radiazione perché, per esempio, per un sistema di spin si ha  $H = -\mu \vec{S} \cdot \vec{B}$ , che può essere scritta nella forma precedente.

Chiamiamo  $H_0$  l'hamiltoniana del qubit imperturbato. D'ora in avanti definiamo  $E_1 - E_0 = \hbar\omega_q$ <sup>viii</sup> la differenza di energia tra i due livelli del qubit (assumiamo sempre che  $E_1 > E_0$ , quindi  $|1\rangle$  è lo stato eccitato). Per convenzione si misura l'energia dal livello energetico intermedio tra i due stati:



quindi per simmetria  $E_1 = \hbar\frac{\omega_q}{2}$  e  $E_0 = -\hbar\frac{\omega_q}{2}$ . In questo modo possiamo scrivere

$$H_0 = -\frac{\hbar}{2}\omega_q\sigma_3,$$

cosicché  $H_0|0\rangle = E_0|0\rangle$  e  $H_0|1\rangle = E_1|1\rangle$ . Per semplificare la scrittura porremo nel seguito  $\hbar = 1$ . Perciò l'hamiltoniana generale sarà

$$H = -\frac{\hbar}{2}\omega_q\sigma_3 - \left( a\mathbb{I} + \vec{b} \cdot \vec{\sigma} \right) \cos(\omega_d t + \phi_0). \quad (6.4.2)$$

Come evidente, le situazioni in cui si considerano  $\mathbb{I}$  e  $\sigma_3$  nel secondo termine sono immediate da studiare, quindi senza perdita di generalità assumiamo  $a = b_3 = 0$ ; il caso interessante riguarda infatti situazioni in cui la perturbazione è trasversale al qubit, quindi lungo  $x$  o  $y$ . Per convenzione si pone  $b_1 + ib_2 = Ae^{-i\phi_1}$  in maniera tale che

$$(b_1\sigma_1 + b_2\sigma_2)\cos(\omega_d t + \phi_0) = \begin{pmatrix} 0 & Ae^{i\phi_1} \\ Ae^{-i\phi_1} & 0 \end{pmatrix} \cos(\omega_d t + \phi_0),$$

dove  $\phi_1$  contiene informazioni sull'orientazione del campo esterno rispetto al dipolo con cui esso interagisce. Se introduciamo

$$\sigma_+ = \frac{\sigma_1 + i\sigma_2}{2} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \sigma_- = \frac{\sigma_1 - i\sigma_2}{2} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad (6.4.3)$$

i quali non sono altro che gli operatori  $J_+$  e  $J_-$  del momento angolare in QM, allora possiamo infine riscrivere la (6.4.2) come

$$H = -\frac{\omega_q}{2}\sigma_3 - (Ae^{i\phi_1}\sigma_+ + Ae^{-i\phi_1}\sigma_-) \cos(\omega_d t + \phi_0); \quad (6.4.4)$$

---

<sup>viii</sup>Chiamiamo  $\omega_q$  la frequenza associata al sistema qubit.

Il termine di interazione dell'hamiltoniana (6.4.4) è la più generale matrice hermitiana non diagonale che descrive l'accoppiamento con un campo elettromagnetico classico oscillante. Purtroppo se si vuole risolvere il problema dell'evoluzione temporale di questa hamiltoniana si è costretti a svolgere delle approssimazioni perché non esiste alcuna soluzione analitica semplice. L'approssimazione che usiamo è la cosiddetta **Rotating Waves Approximation** (RWA). Come prima cosa, tramite un cambio di base, vogliamo riscrivere lo stato quantistico in un sistema di riferimento rotante:

$$|\psi(t)\rangle \rightarrow |\tilde{\psi}(t)\rangle = U(t)|\psi(t)\rangle , \quad (6.4.5)$$

dove l'operatore  $U(t)$  è peculiare perché unitario ( $U(t)U^\dagger(t) = \mathbb{I}$ ) e dipendente dal tempo. Si noti che, nonostante la notazione,  $U(t)$  non è l'operatore di evoluzione temporale (in alcuni casi particolari, come nella rappresentazione di interazione, si pone  $U(t) = e^{\frac{i}{\hbar}H_0 t}$ ). Essendo  $U(t)$  unitario, la probabilità sarà conservata a seguito di questo cambio di base. Cosa succede esplicitamente alla (6.4.4)? Dato che lo stato non ruotato risolve l'equazione di Schrödinger

$$i\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle ,$$

allora

$$\begin{aligned} i\frac{d}{dt}|\tilde{\psi}(t)\rangle &= U(t)i\frac{d}{dt}|\psi(t)\rangle + i\dot{U}(t)|\psi(t)\rangle \\ &= U(t)H|\psi(t)\rangle + i\dot{U}(t)|\psi(t)\rangle \\ &= UHU^\dagger|\tilde{\psi}(t)\rangle + i\dot{U}U^\dagger|\tilde{\psi}(t)\rangle . \end{aligned}$$

Questo significa che anche lo stato ruotato risolve l'equazione di Schrödinger

$$i\frac{d}{dt}|\tilde{\psi}(t)\rangle = \tilde{H}|\tilde{\psi}(t)\rangle , \quad \text{dove } \tilde{H} = UHU^\dagger + i\dot{U}U^\dagger . \quad (6.4.6)$$

Per riscrivere l'hamiltoniana (6.4.4) come nella (6.4.6) è necessario dimostrare il seguente lemma:

**Lemma 6.1.** *Dati due operatori  $A$  e  $T$  tali che  $[T, A] = \alpha A$ , allora*

$$e^{iT}Ae^{-iT} = e^{i\alpha}A . \quad (6.4.7)$$

*Dimostrazione.* Definiamo  $A(t) = e^{itT}Ae^{-itT}$ . Perciò

$$\dot{A}(t) = ie^{itT}TAe^{-itT} - ie^{itT}ATE^{-itT} = ie^{itT}[T, A]e^{-itT} = i\alpha A(t) .$$

La precedente è un'equazione differenziale lineare per  $A(t)$  che può essere facilmente risolta scrivendo  $A(t) = A(0)e^{i\alpha t} = Ae^{i\alpha t}$ . Scegliendo  $t = 1$  otteniamo la tesi.  $\square$

Scriviamo l'hamiltoniana in questo nuovo sistema ruotato: ruotiamo lo stato con una rotazione unitaria dipendente dal tempo scegliendo

$$U(t) = e^{-\frac{i}{2}\omega_d\sigma_3 t} ,$$

ossia andiamo ad un sistema di riferimento che ruota alla stessa frequenza del campo esterno. Per il primo termine di  $\tilde{H}$  (coniugazione con  $U$ ) avremo 3 contributi da (6.4.4):

$$\begin{aligned} UHU^\dagger &\propto U\sigma_3U^\dagger + U\sigma_+U^\dagger + U\sigma_-U^\dagger \\ &\propto \sigma_3 + e^{-i\omega_d t}\sigma_+ + e^{i\omega_d t}\sigma_- , \end{aligned}$$

dove per gli ultimi due termini abbiamo usato la (6.4.7) con  $[\sigma_3, \sigma_{\pm}] = \pm 2\sigma_{\pm}$  (formula semplice da dimostrare con le definizioni di  $\sigma_{\pm}$ ). Dato che il secondo termine di  $\tilde{H}$  in (6.4.6) è semplicemente

$$i\dot{U}U^{\dagger} = \frac{\omega_d}{2}\sigma_3,$$

allora, unendo i pezzi in (6.4.6), avremo

$$\begin{aligned}\tilde{H} &= -\frac{\omega_q}{2}\sigma_3 - (Ae^{i\phi_1}e^{-i\omega_dt}\sigma_+ + Ae^{-i\phi_1}e^{i\omega_dt}\sigma_-)\cos(\omega_dt + \phi_0) + \frac{\omega_d}{2}\sigma_3 \\ &= -\frac{(\omega_q - \omega_d)}{2}\sigma_3 - (Ae^{-i(\omega_dt - \phi_1)}\sigma_+ + Ae^{i(\omega_dt - \phi_1)}\sigma_-)\frac{e^{i(\omega_dt + \phi_0)} + e^{-i(\omega_dt + \phi_0)}}{2}.\end{aligned}$$

Come anticipato sopra, non esiste alcun modo di estrarre una soluzione analitica esatta dell'hamiltoniana precedente (per adesso abbiamo solo riscritto la  $H$  di partenza in un sistema di riferimento differente senza fare alcuna approssimazione). Qui entra in gioco la RWA: scriviamo i 4 termini che si originano dal secondo prodotto di  $\tilde{H}$

$$Ae^{i(\phi_0 + \phi_1)}\sigma_+ + Ae^{-2i\omega_dt}e^{i(\phi_1 - \phi_0)}\sigma_+ + Ae^{2i\omega_dt}e^{-i(\phi_1 - \phi_0)}\sigma_- + Ae^{-i(\phi_0 + \phi_1)}\sigma_-;$$

abbiamo quindi 2 termini dipendenti dal tempo e 2 indipendenti: nella RWA trascuriamo i termini dipendenti dal tempo perché assumiamo di guardare il sistema per grandi  $t$ . Come possiamo giustificare tale assunto? La fisica è dominata dalla risonanza, quindi solamente le frequenze vicino alla risonanza contribuiranno significativamente al processo. Questa stima può essere calcolata in teoria delle perturbazioni<sup>ix</sup>, dove si ottengono dei denominatori  $\frac{1}{E_t - E_1 \pm \hbar\omega}$ : considerare solo i casi in cui il denominatore si annulla (o quasi) è lo stesso che trascurare i termini dipendenti da  $t$  nell'espressione precedente.

Tenendo quindi conto della RWA,  $\tilde{H}$  può essere riscritta come un'hamiltoniana indipendente dal tempo

$$\tilde{H} = -\frac{\Delta}{2}\sigma_3 - \left( \frac{A}{2}e^{i\phi}\sigma_+ + \frac{A}{2}e^{-i\phi}\sigma_- \right), \quad (6.4.8)$$

dove  $\phi = \phi_0 + \phi_1$  e  $\Delta = \omega_q - \omega_d$ . La frequenza  $\Delta$  è detta **frequenza di detuning** e dice quanto siamo lontani dalla risonanza, la quale corrisponde ovviamente al caso  $\Delta = 0$ . Dato che il segno tra le fasi in  $\phi$  è  $+$ , possiamo essenzialmente riassorbire a piacimento tutte la fasi del campo esterno nella direzione in cui si sta prendendo l'elemento di matrice  $\langle \omega | \hat{x} | \omega' \rangle$  o viceversa (nei termini trascurabili dalla RWA c'è al contrario un  $-$ ). Tenendo quindi conto della (6.4.8), l'evoluzione temporale è descritta da un'hamiltoniana indipendente dal tempo, perciò l'operatore che la descrive è proprio  $e^{-i\tilde{H}t} \equiv R_{\vec{n}}(\gamma)$ : l'evoluzione temporale può quindi essere utilizzata per controllare il singolo qubit e muoverlo sulla sfera di Bloch.

LEZIONE 17 - 04/12/2021

Riprendiamo il discorso che stavamo affrontando la volta scorsa. L'hamiltoniana  $\tilde{H}$  in RWA è indipendente dal tempo, perciò l'evoluzione temporale dello stato generico ruotato è molto semplice

$$|\tilde{\psi}(t)\rangle = e^{-i\tilde{H}t} |\tilde{\psi}(0)\rangle. \quad (6.4.9)$$

---

<sup>ix</sup>Per vedere esplicitamente perché i termini dipendenti dal tempo sono trascurabili per grandi  $t$  è necessario fare un conto completo in teoria delle perturbazioni.

In realtà avremmo potuto fin dall'inizio scrivere l'evoluzione temporale dello stato  $|\psi(t)\rangle$  non ruotato, utilizzando l'hamiltoniana (6.4.4): abbiamo deciso di non intraprendere quella strada poiché l'espressione dell'operatore unitario che descrive l'evoluzione temporale per  $H$  dipendenti dal tempo è abbastanza complicata.

Dato che ci serve nella (6.4.9) l'esponenziazione di  $\tilde{H}$ , esplicitiamo in (6.4.8) le matrici  $\sigma_1$  e  $\sigma_2$  (da  $\sigma_+$  e  $\sigma_-$ ) e riscriviamo gli esponenziali in termini di seno e coseno: in questo modo otteniamo la seguente combinazione lineare di matrici di Pauli

$$\tilde{H} = -\frac{1}{2} (\Delta \sigma_3 + A \cos \phi \sigma_1 - A \sin \phi \sigma_2) \equiv -\frac{\Omega}{2} \vec{n} \cdot \vec{\sigma},$$

dove

$$\vec{n} = \frac{1}{\Omega} (A \cos \phi, -A \sin \phi, \Delta) \quad \text{con} \quad \Omega = \sqrt{A^2 + \Delta^2}; \quad (6.4.10)$$

si noti che  $\vec{n}$  è correttamente normalizzato dimodoché  $|\vec{n}| = 1$ . La frequenza  $\Omega$  è chiamata **frequenza di Rabi**<sup>x</sup> e controlla l'oscillazione del qubit. Quindi l'operatore di evoluzione temporale diventa

$$e^{-i\tilde{H}t} = e^{i\frac{\Omega}{2}\vec{n}\cdot\vec{\sigma}t}; \quad (6.4.11)$$

(la presenza del fattore  $1/2$  è comune quando sono presenti le matrici di Pauli). La relazione precedente è esattamente analoga all'operatore (1.5.3), introdotto nella Sezione 1.5 riguardante i gate agenti su singoli qubit: la più generale matrice unitaria  $2 \times 2$  (a meno di una fase globale) può essere infatti scritta proprio come l'operatore  $R_{\vec{n}}(\gamma)$ , ossia

$$R_{\vec{n}}(\gamma) = e^{-i\frac{\gamma}{2}(\vec{n}\cdot\vec{\sigma})}.$$

Questo operatore va interpretato come una rotazione del qubit lungo la sfera di Bloch: l'evoluzione temporale  $R_{\vec{n}}(-\Omega t)$  effettua una rotazione di angolo  $-\Omega t$  attorno alla direzione individuata dal vettore  $\vec{n}$  scritto in precedenza. È bene notare che la direzione attorno a cui avviene questa precessione è specificata dai parametri che individuano i dettagli dell'interazione con la radiazione esterna oscillante, come  $\omega_d$ ,  $A$  e  $\phi$ , ma anche dalla frequenza di oscillazione del qubit stesso ( $\omega_q$ ).

Prima di dare uno sguardo concreto alla sfera di Bloch, ricordiamo che per scrivere l'esponenziale di una combinazione lineare di matrici di Pauli è possibile usare la seguente formula:

$$R_{\vec{n}}(\gamma) = e^{-i\frac{\gamma}{2}(\vec{n}\cdot\vec{\sigma})} = \mathbb{I} \cos\left(\frac{\gamma}{2}\right) - i \sin\left(\frac{\gamma}{2}\right) (\vec{\sigma} \cdot \vec{n}). \quad (6.4.12)$$

*Dimostrazione.* Ricordando la serie dell'esponenziale, la proprietà  $(\vec{\sigma} \cdot \vec{n})^2 = \mathbb{I}$  e la serie di seno e coseno avremo:

$$\begin{aligned} R_{\vec{n}}(\gamma) &= \sum_{k=0}^{\infty} \frac{1}{k!} \left( -\frac{i}{2} \gamma \vec{n} \cdot \vec{\sigma} \right)^k \\ &= \sum_{k=0}^{\infty} \frac{1}{(2k)!} \left( -\frac{i}{2} \gamma \vec{n} \cdot \vec{\sigma} \right)^{2k} + \sum_{k=0}^{\infty} \frac{1}{(2k+1)!} \left( -\frac{i}{2} \gamma \vec{n} \cdot \vec{\sigma} \right)^{2k+1} \\ &= \mathbb{I} \sum_{k=0}^{\infty} \frac{(i)^{2k}}{(2k)!} \left( \frac{\gamma}{2} \right)^{2k} - i(\vec{n} \cdot \vec{\sigma}) \sum_{k=0}^{\infty} \frac{(i)^{2k}}{(2k+1)!} \left( \frac{\gamma}{2} \right)^{2k+1} \\ &= \mathbb{I} \cos\left(\frac{\gamma}{2}\right) - i \sin\left(\frac{\gamma}{2}\right) (\vec{\sigma} \cdot \vec{n}). \end{aligned}$$

□

---

<sup>x</sup>Molti libri usano differenti convenzioni sul significato di tale frequenza. Indipendentemente da ciò, la cosa importante è che l'oscillazione del qubit è controllata da  $\Omega$ .

La (6.4.12) è molto utile quando si vogliono affrontare dei conti esplicativi. Vediamo per esempio un caso di un esercizio molto semplice in QM:

**Esempio 6.2 (Oscillazioni di Rabi).** Supponiamo che il sistema si trovi nello stato iniziale  $|\tilde{\psi}(0)\rangle = |0\rangle$  e calcoliamo la probabilità che al tempo  $t$  il qubit subisca una transizione  $|0\rangle \rightarrow |1\rangle$ . Ricordando l'espressione (6.4.11) e la formula appena dimostrata avremo

$$P(t)_{0 \rightarrow 1} = \left| \langle 1 | e^{-i\tilde{H}t} | 0 \rangle \right|^2 = \left| \langle 1 | \cos\left(\frac{\Omega}{2}t\right) + i \sin\left(\frac{\Omega}{2}t\right) \vec{\sigma} \cdot \vec{n} | 0 \rangle \right|^2;$$

il primo termine è nullo, mentre il secondo, ricordando che  $\sigma_1 |0\rangle = |1\rangle$  e  $\sigma_2 |0\rangle = i|1\rangle$ , riceve contributi solamente da  $\sigma_1$  e  $\sigma_2$ . In questo modo possiamo scrivere

$$\begin{aligned} P(t)_{0 \rightarrow 1} &= \left| i \sin\left(\frac{\Omega}{2}t\right) (n_1 + i n_2) \right|^2 \\ &= \left| i \sin\left(\frac{\Omega}{2}t\right) \frac{A}{\Omega} e^{-i\phi} \right|^2 \\ &= \frac{A^2}{\Omega^2} \sin^2\left(\frac{\Omega}{2}t\right), \end{aligned}$$

dove nella seconda riga abbiamo usato le componenti di  $\vec{n}$  in (6.4.10). Inserendo infine l'espressione di  $\Omega$  otteniamo la cosiddetta **formula di Rabi**

$$P(t)_{0 \rightarrow 1} = \frac{A^2}{A^2 + \Delta^2} \sin^2\left(\frac{\sqrt{A^2 + \Delta^2}}{2}t\right). \quad (6.4.13)$$

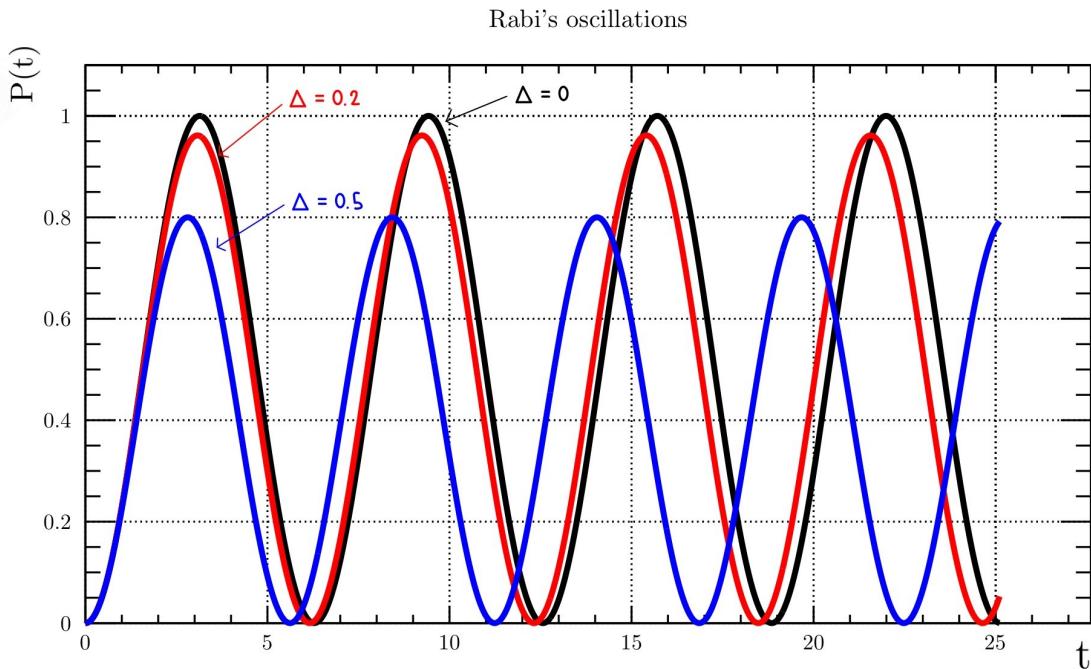


Figura 6.5: Oscillazioni di Rabi per  $A = 1$ . È evidente come la probabilità del sistema oscilli allo scorrere del tempo. Più il sistema è vicino alla risonanza ( $\Delta = 0$ ), più vicino ad 1 saranno i picchi e quindi maggiore sarà la probabilità di trovare il sistema in  $|1\rangle$ .

Ricapitolando, la (6.4.13) ci fornisce la probabilità al tempo  $t$  che applicando una perturbazione esterna oscillante con frequenza  $\omega_d$ , ampiezza  $A$  e detuning  $\Delta$  avvenga una transizione  $|0\rangle \rightarrow |1\rangle$ . Si tratta di un risultato molto importante e spesso presente in diversi rami della fisica.

Facendo un grafico della probabilità (6.4.13) in funzione del tempo si ottiene la Figura 6.5.

Cerchiamo ora di visualizzare che cosa accade dal punto di vista della sfera di Bloch. Ricordando la (6.4.5) possiamo scrivere lo stato non ruotato come

$$|\psi(t)\rangle = U^\dagger(t) |\tilde{\psi}(t)\rangle, \quad \text{dove} \quad U^\dagger(t) = e^{\frac{i}{2}\omega_d\sigma_3 t},$$

in questo modo, inserendo anche la (6.4.9), possiamo scrivere l'evoluzione temporale dello stato non ruotato

$$|\psi(t)\rangle = e^{\frac{i}{2}\omega_d\sigma_3 t} R_{\vec{n}}(-\Omega t) |\tilde{\psi}(0)\rangle. \quad (6.4.14)$$

Come già anticipato (vedi Figura 6.6a), l'operatore  $R_{\vec{n}}(-\Omega t)$  implementa una rotazione di angolo  $-\Omega t$  attorno alla direzione di  $\vec{n}$ . Per esempio

**Esempio 6.3 (Rotazione attorno a  $z$ ).** Supponiamo una rotazione lungo  $z$  implementata dall'operatore  $R_z(\gamma) = e^{-\frac{i}{2}\sigma_3\gamma}$ . Ricordando la generica parametrizzazione del qubit in (1.1.2) avremo

$$\begin{aligned} R_z(\gamma) |\psi\rangle &= \cos\left(\frac{\theta}{2}\right) e^{-\frac{i}{2}\gamma} |0\rangle + \sin\left(\frac{\theta}{2}\right) e^{\frac{i}{2}\gamma} e^{i\phi} |1\rangle \\ &= e^{-\frac{i}{2}\gamma} \left[ \cos\left(\frac{\theta}{2}\right) |0\rangle + \sin\left(\frac{\theta}{2}\right) e^{i(\phi+\gamma)} |1\rangle \right]; \end{aligned}$$

riassorbendo la fase globale abbiamo effettivamente ottenuto che l'operatore  $R_{\vec{n}}(\gamma)$  produce una rotazione lungo  $z$  perché il qubit finale è dello stesso tipo di quello iniziale con  $\theta \rightarrow \theta$  e  $\phi \rightarrow \phi + \gamma$ .

Che cosa accade per una rotazione lungo una generica direzione  $\vec{n}$ ? La direzione dipende da  $(A, \Omega, \phi)$ , quindi per rilevarla sperimentalmente basta variare questi parametri.

La situazione in cui  $A = 0$  (assenza di una perturbazione esterna) è abbastanza curiosa: in una tale situazione si potrebbe pensare  $R_{\vec{n}}(-\Omega t) = \mathbb{I}$ , quindi sembrerebbe dalla (6.4.14) che rimanga un termine  $e^{\frac{i}{2}\omega_d\sigma_3 t}$  di rotazione lungo  $z$ . In realtà questo risultato è sbagliato perché, quando non c'è alcun campo oscillante, è necessario porre  $\omega_d = 0$ : dalla (6.4.10) il vettore  $\vec{n}$  non è zero, ma bensì  $\vec{n} = (0, 0, \Delta/\Omega)$ , perciò

$$R_{\vec{n}}(-\Omega t) = e^{\frac{i}{2}\Delta\sigma_3 t} = e^{\frac{i}{2}(\omega_q - \omega_d)\sigma_3 t};$$

questo significa che lo stato continua a subire una precessione

$$|\psi(t)\rangle = e^{\frac{i}{2}\omega_d\sigma_3 t} e^{\frac{i}{2}(\omega_q - \omega_d)\sigma_3 t} |\tilde{\psi}(0)\rangle = e^{\frac{i}{2}\omega_q\sigma_3 t} |\tilde{\psi}(0)\rangle.$$

Esiste sempre una precessione lungo  $z$  con la frequenza naturale del qubit! Delle volte è utile sbarazzarsi di questa precessione cambiando sistema di coordinate: ad esempio possiamo andare in un sistema di riferimento che ruota come il qubit scegliendo  $U(t) = e^{iH_0 t}$ ; in questo modo è possibile tenere solamente la parte non banale dell'evoluzione

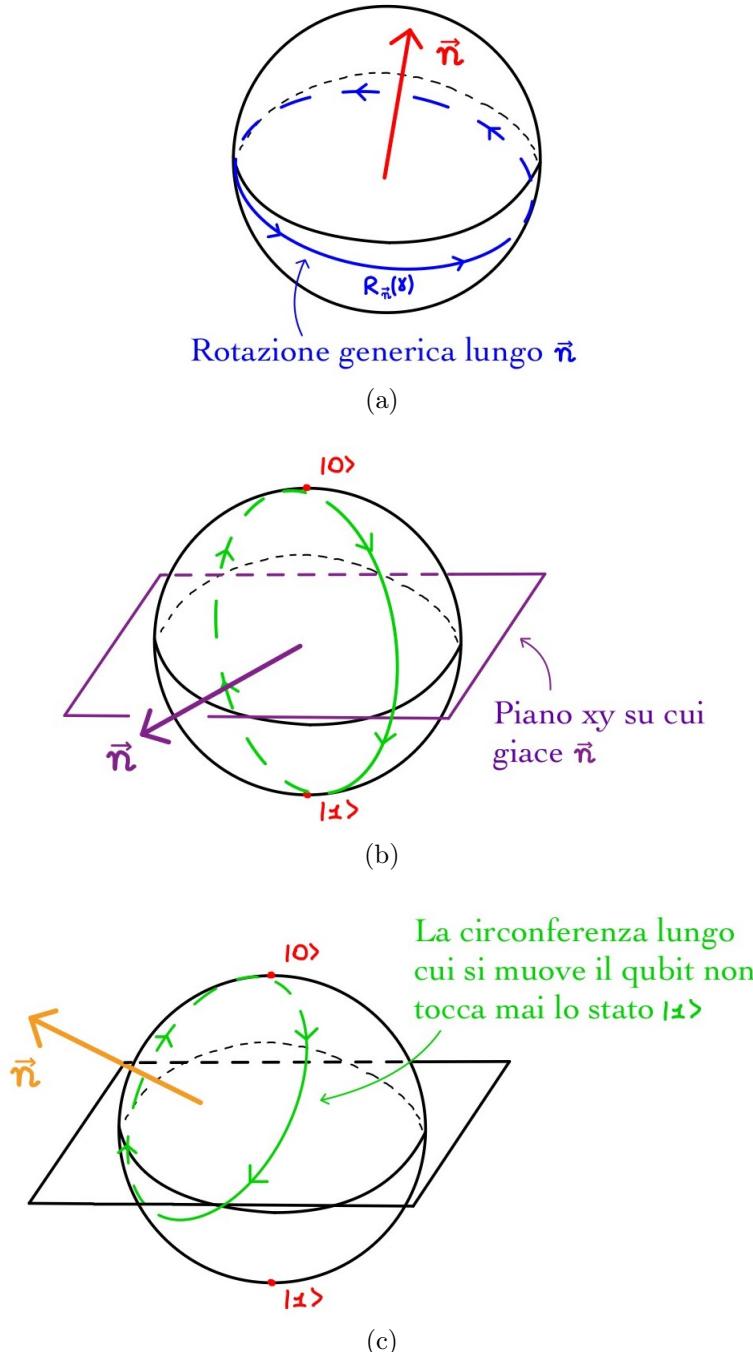


Figura 6.6: (6.6a) L'operatore  $R_{\vec{n}}(\gamma)$  implementa una generica rotazione attorno ad  $\vec{n}$  lungo la superficie della sfera di Bloch. (6.6b) Alla risonanza,  $\vec{n}$  giace nel piano  $xy$ , quindi per determinati tempi vi è la certezza che il qubit si trovi in  $|1\rangle$ . (6.6c) Per  $\vec{n}$  generico non si ha mai la certezza che il qubit si trovi in  $|1\rangle$ .

temporale eliminando questo effetto di precessione. Spesso il sistema di riferimento scelto dipende da ciò che si vuole fare.

Per capire meglio il significato della rotazione di Figura 6.6a immaginiamo che il qubit parta nello stato  $|0\rangle$ . In regime di risonanza ( $\Delta = 0$ ) avremo  $\vec{n} = (\cos \phi, -\sin \phi, 0)$ , perciò l'asse di rotazione giace nel piano  $xy$  (si consideri la Figura 6.6b): geometricamente, il qubit ruota con frequenza  $\Omega$  lungo la circonferenza evidenziata in verde, ossia nel piano perpendicolare ad  $\vec{n}$ , andando continuamente avanti e indietro da  $|0\rangle$  ad  $|1\rangle$  (si pensi alla

probabilità di Figura 6.5). Ci saranno tempi particolari in cui il qubit si troverà con certezza in  $|1\rangle$ .

Per quale ragione invece per  $\Delta \neq 0$  la probabilità non è mai 1? Dalle relazioni (6.4.10), il vettore  $\vec{n}$  presenta 3 componenti non nulle per  $\Delta \neq 0$  quindi, partendo da  $|0\rangle$ , la circonferenza lungo la quale il qubit si muove non raggiunge mai  $|1\rangle$ ! (si pensi alla Figura 6.6c). Ovviamente dalle leggi della QM sappiamo che ci sarà sempre della probabilità che la misura restituisca  $|1\rangle$ , tuttavia per nessun tempo si avrà la certezza che il qubit si trovi in quello stato. Dal punto di vista pratico è possibile utilizzare questa perturbazione esterna oscillante per muovere arbitrariamente il qubit sulla sfera di Bloch e invertire lo stato dimodoché oscilli continuamente  $|0\rangle \leftrightarrow |1\rangle$ .

Cosa succede quando la perturbazione non è periodica? Una tale situazione è parametrizzata da un campo esterno proporzionale a  $f(t) \cos(\omega_d t + \phi_0)$ , dove  $f(t)$  è un'opportuna funzione dipendente dal tempo. Per svolgere dei conti esplicativi è necessario utilizzare il formalismo della teoria delle perturbazioni dipendenti dal tempo: il punto fondamentale è che la fisica rimane la stessa! L'oscillazione è modulata da  $f(t)$  perciò è sempre possibile scegliere opportunamente questa funzione e le frequenze in maniera tale che si abbia una situazione in cui, per un dato tempo  $t$ , il qubit si ritrovi con certezza in  $|1\rangle$ ; in questo modo il tempo può essere scelto arbitrariamente per manipolare il qubit a piacimento.

## 6.5 Accoppiamento qubit - cavità QED

L'accoppiamento di un qubit con un campo elettromagnetico (classico) esterno oscillante può essere essenzialmente utilizzato per creare tutti i gate agenti sui singoli qubit. I gate agenti su più qubit (quelli che creano entanglement tra stati), invece, sono più complessi da realizzare: alcuni di essi possono essere costruiti a partire da situazioni simili a quelle studiate nella scorsa sezione, tuttavia la maggior parte sono realizzati tramite l'accoppiamento di un qubit con un campo elettromagnetico quantizzato. Cerchiamo di approfondire questo discorso.

L'elettrodinamica quantistica della cavità (**Cavity QED**) è un campo di studio che si focalizza su un regime che coinvolge l'accoppiamento di singoli atomi con solo alcuni (pochi) modi ottici. Sperimentalmente, ciò è reso possibile collocando singoli atomi all'interno di cavità ottiche. Poiché all'interno della cavità esistono solo uno o due modi elettromagnetici, e ciascuno di questi ha un'intensità di campo elettrico molto elevata, l'accoppiamento tra il dipolo dell'atomo e il campo è molto intenso. I due principali componenti sperimentali di un sistema QED a cavità sono la cavità elettromagnetica e l'atomo; quest'ultimo, il quale modellizza il qubit, interagisce con alcuni fotoni della cavità, perciò è evidente che dobbiamo considerare un'hamiltoniana che coinvolge una radiazione quantizzata.

Nel contesto dell'ottica quantistica si costruisce un tale sistema considerando una cavità Fabry-Perot costituita da una serie di specchi che permettono di intrappolare dei fotoni: il campo elettromagnetico che si genera dalle riflessioni dei fotoni sugli specchi è molto intenso, ma si riescono a selezionare alcuni modi di frequenza  $\omega_c$  (pedice  $c$  per cavità) ben precisi (o multipli di tale frequenza). Un sistema di questo tipo diventa molto simile alla radiazione di corpo nero perché l'atomo (qubit) nella cavità QED può scambiare e riassorbire fotoni se la frequenza del qubit è simile a quella della cavità, ossia  $\omega_q \sim \omega_c$ . In generale se i fotoni non possono uscire e l'atomo assorbe alcuni di essi con frequenze ben precise, allora il sistema necessita una completa trattazione in QM. Ovviamente i fotoni

possono uscire attraverso delle emissioni spontanee (ricordiamo che c'è sempre qualche perdita e decoerenza).

L'hamiltoniana totale del sistema, il quale è costituito dal qubit e dalla cavità, sarà descritta da

$$\hat{H}_0 = -\frac{1}{2}\omega_q \hat{\sigma}_3 + \omega_c \left( \hat{a}^\dagger \hat{a} + \frac{1}{2} \right), \quad (6.5.1)$$

dove in questo caso, nel secondo termine, stiamo descrivendo un solo modo ottico perché nella maggior parte delle situazioni se ne riescono ad eccitare molto pochi; avendo un unico modo del campo e.m. allora, nella trattazione che segue, assumeremo che l'eccitazione dei fotoni coinvolgerà sempre fotoni dello stesso modo ottico dato dagli operatori  $\hat{a}$  e  $\hat{a}^\dagger$ . L'hamiltoniana precedente non è nient'altro che l'hamiltoniana libera che descrive contemporaneamente e indipendentemente il qubit e la cavità. Per descrivere la parte interagente del sistema assumiamo un'interazione con il dipolo dell'atomo, quindi introduciamo l'hamiltoniana

$$\hat{H}_I = \vec{d} \cdot \vec{E}, \quad (6.5.2)$$

dove  $\vec{d}$  dipende dalle interazioni concrete che hanno luogo<sup>xi</sup>, ma allo stesso tempo fornisce i generici elementi di matrice per le transizioni  $|0\rangle \rightarrow |1\rangle$  e  $|1\rangle \rightarrow |0\rangle$ ;  $\vec{E}$  è ovviamente il campo elettrico. Dato che il campo è quantizzato possiamo utilizzare il risultato ottenuto alla fine della Sezione 6.3, cioè

$$\hat{\vec{E}} = \vec{E}_0 \left( \hat{a} e^{i\vec{k} \cdot \vec{x} - i\omega t} + \hat{a}^\dagger e^{-i\vec{k} \cdot \vec{x} + i\omega t} \right). \quad (6.5.3)$$

Diamo uno sguardo alla relazione (6.5.3), in particolar modo alla dipendenza spaziale e temporale. Per quanto riguarda la prima, usando l'approssimazione di dipolo, se consideriamo per i fotoni lunghezze d'onda grandi<sup>xii</sup> rispetto alle dimensioni atomiche del sistema, possiamo trascurare la dipendenza spaziale. Un discorso analogo può essere fatto anche per la dipendenza temporale: nel momento in cui si va a quantizzare il campo e.m. di un sistema che assumiamo isolato, l'hamiltoniana che si realizza è solitamente indipendente dal tempo e quindi può essere costruita rispetto a un certo riferimento temporale che, per semplicità, facciamo coincidere con  $t = 0$ . Sotto queste due assunzioni, la (6.5.3) può essere riscritta come

$$\hat{\vec{E}} = \vec{E}_0 (\hat{a} + \hat{a}^\dagger).$$

Inserendo questo risultato nella (6.5.2) avremo che

$$\hat{H}_I = g \hat{\sigma}_1 (\hat{a} + \hat{a}^\dagger), \quad (6.5.4)$$

dove  $g$  è la costante di accoppiamento dell'interazione tra il qubit e la radiazione e, anziché prendere gli elementi di matrice dell'operatore  $\vec{d}$  tra gli stati del qubit (dipendono da molti fattori, come ad esempio i livelli energetici che scegliamo dalle regole di selezione), consideriamo una generica matrice hermitana  $2 \times 2$  che, come sappiamo, può essere scritta in termini di una combinazione lineare delle matrici di Pauli. Tra tutte le possibili scelte

<sup>xi</sup>Questo vettore è la posizione se il qubit è costruito da un atomo, altrimenti è lo spin se il qubit è realizzato da un sistema con spin. Similmente, il campo è elettrico nel primo caso, altrimenti è magnetico per l'accoppiamento con lo spin.

<sup>xii</sup>Tipicamente la lunghezza d'onda dei fotoni non è così lontana dalla lunghezza d'onda di risonanza del qubit, la quale rimane comunque molto più grande delle dimensioni atomiche.

prendiamo, senza perdita in generalità,  $\hat{\sigma}_1$ . Ovviamente possiamo fare scelte diverse, come ad esempio  $\hat{\sigma}_2$ , ma ogni opzione darà sempre un risultato fisico simile.

A questo punto possiamo mettere insieme la (6.5.1) e la (6.5.4) per scrivere l'hamiltoniana completa del sistema

$$\hat{H} = -\frac{1}{2}\omega_q \hat{\sigma}_3 + \omega_c \left( \hat{a}^\dagger \hat{a} + \frac{1}{2} \right) + g \hat{\sigma}_1 (\hat{a} + \hat{a}^\dagger) ; \quad (6.5.5)$$

sottolineiamo nuovamente che la differenza principale rispetto al caso della sezione precedente è che qui il campo elettrico è quantizzato, cosa che si riflette con la presenza degli operatori  $\hat{a}$  e  $\hat{a}^\dagger$ .

Ancora una volta, scriviamo  $\hat{\sigma}_1$  usando le definizioni di  $\hat{\sigma}_+$  e  $\hat{\sigma}_-$  in (6.4.3): è evidente che  $\hat{\sigma}_+ |1\rangle = |0\rangle$  e  $\hat{\sigma}_- |0\rangle = |1\rangle$ , quindi la prima matrice agisce come operatore di abbassamento sullo stato del qubit, ossia  $|1\rangle \rightarrow |0\rangle$ , mentre la seconda come operatore di innalzamento  $|0\rangle \rightarrow |1\rangle$ . Se scriviamo  $\hat{\sigma}_1 = \hat{\sigma}_+ + \hat{\sigma}_-$  e ci concentriamo sul solo termine di interazione, avremo quindi

$$\hat{H}_I = g \left( \underbrace{\hat{\sigma}_+ \hat{a}^\dagger}_1 + \underbrace{\hat{\sigma}_- \hat{a}}_2 + \underbrace{\hat{\sigma}_+ \hat{a}}_3 + \underbrace{\hat{\sigma}_- \hat{a}^\dagger}_4 \right); \quad (6.5.6)$$

quale è l'interpretazione di ciascuno di questi 4 termini sottolineati? Tenendo presente che  $\hat{a}$  distrugge un fotone,  $\hat{a}^\dagger$  crea un fotone e che abbiamo posto  $\hbar\omega_q = E_1 - E_0$ , il loro significato sarà:

1. Il qubit emette un fotone e di conseguenza lo stato energetico si dissecita;
2. Il qubit assorbe un fotone e di conseguenza lo stato energetico si eccita;
3. Assorbimento di un fotone e dissecitazione del qubit: viene fornita energia  $2\omega_q$ ;
4. Emissione di un fotone ed eccitazione del qubit: viene rimossa energia  $-2\omega_q$ .

Gli ultimi due processi sono abbastanza insoliti, anche se potrebbero verificarsi se il sistema possiede energia a sufficienza. In teoria delle perturbazioni al primo ordine solamente i primi due processi sono permessi, mentre gli ultimi due sono vietati dalla regola d'oro di Fermi, perciò, anche in una trattazione esatta, hanno una probabilità molto piccola di verificarsi. Possiamo quindi assumere che i primi due termini siano permessi (più probabili) quando siamo vicini alla risonanza, mentre gli ultimi sono soppressi in teoria delle perturbazioni perché hanno una piccola probabilità che accadano: dunque, a meno che  $\omega_c$  e  $\omega_q$  non siano troppo lontani tra loro, possiamo trascurare gli ultimi due processi.

Verifichiamo quanto detto, ancora una volta, con la RWA, ma questa volta prendiamo una strada leggermente diversa perché è più conveniente scegliere

$$\hat{U}(t) = e^{i\hat{H}_0 t},$$

dove  $\hat{H}_0$  non è nient'altro che l'hamiltoniana della (6.5.1) (questa è nota come *rappresentazione di interazione* in teoria delle perturbazioni). Vediamo come cambia la nuova hamiltoniana a seguito dell'azione  $\hat{U}$ : se usiamo la (6.4.6) allora è facile vedere che la scelta precedente ci permette di cancellare il termine libero, infatti

$$\hat{\tilde{H}} = \hat{U} \hat{H} \hat{U}^\dagger + i \dot{\hat{U}} \hat{U}^\dagger = \hat{H}_0 + \hat{U} \hat{H}_I \hat{U}^\dagger - \hat{H}_0 = \hat{U} \hat{H}_I \hat{U}^\dagger.$$

Per calcolare la coniugazione dell'hamiltoniana (6.5.6) è necessario fare uso del Lemma 6.1. Ricordando le seguenti regole di commutazione

$$\begin{aligned} \left[ \hat{H}_0, \hat{a}^\dagger \right] &= \omega_c \hat{a}^\dagger, & \left[ \hat{H}_0, \hat{\sigma}_+ \right] &= -\omega_q \hat{\sigma}_+, \\ \left[ \hat{H}_0, \hat{a} \right] &= -\omega_c \hat{a}, & \left[ \hat{H}_0, \hat{\sigma}_- \right] &= \omega_q \hat{\sigma}_-, \end{aligned}$$

possiamo facilmente scrivere che

$$\begin{aligned} e^{i\hat{H}_0 t} \hat{a}^\dagger e^{-i\hat{H}_0 t} &= e^{i\omega_c t} \hat{a}^\dagger, & e^{i\hat{H}_0 t} \hat{\sigma}_+ e^{-i\hat{H}_0 t} &= e^{-i\omega_q t} \hat{\sigma}_+, \\ e^{i\hat{H}_0 t} \hat{a} e^{-i\hat{H}_0 t} &= e^{-i\omega_c t} \hat{a}, & e^{i\hat{H}_0 t} \hat{\sigma}_- e^{-i\hat{H}_0 t} &= e^{i\omega_q t} \hat{\sigma}_-; \end{aligned} \quad (6.5.7)$$

in questo modo la coniugazione completa diventa

$$\hat{H} = g \left( \underbrace{e^{i(\omega_c - \omega_q)t} \hat{\sigma}_+ \hat{a}^\dagger}_{\sim 1} + \underbrace{e^{-i(\omega_c - \omega_q)t} \hat{\sigma}_- \hat{a}}_{\sim 1} + \underbrace{e^{-i(\omega_c + \omega_q)t} \hat{\sigma}_+ \hat{a}}_{\sim e^{-2i\omega_q t}} + \underbrace{e^{i(\omega_c + \omega_q)t} \hat{\sigma}_- \hat{a}^\dagger}_{\sim e^{2i\omega_q t}} \right)$$

dove abbiamo supposto il regime di risonanza  $\omega_c \sim \omega_q$ . Gli ultimi due termini, dal momento che presentano delle rapide oscillazioni, sono soppressi in teoria delle perturbazioni e possiamo quindi trascurarli nella RWA, proprio come avevamo discusso nella sezione precedente.

Ritornando infine all'hamiltoniana (6.5.5) nel sistema di riferimento non ruotato, possiamo trascurare gli ultimi due termini della (6.5.6) e scrivere quindi la cosiddetta **hamiltoniana di Jaynes-Cummings**:

$$\hat{H} = -\frac{\omega_q}{2} \hat{\sigma}_3 + \omega_c \left( \hat{a}^\dagger \hat{a} + \frac{1}{2} \right) + g (\hat{\sigma}_+ \hat{a}^\dagger + \hat{\sigma}_- \hat{a}). \quad (6.5.8)$$

Si tratta dell'hamiltoniana che descrive il sistema della cavity QED, ossia un qubit interagente con delle oscillazioni descrivibili dal punto di vista quantistico (non necessariamente fotoni). Nelle sezioni successive, quando verrà trattato il sistema della trappola ionica, considereremo dei fononi, ma l'hamiltoniana rimarrà comunque della stessa forma. Di solito anche per i qubit superconduttori si utilizzano hamiltoniane di questo tipo.

LEZIONE 18 - 10/12/2021

Abbiamo visto come la CQED<sup>xiii</sup> modellizzi l'interazione tra un qubit e il campo elettromagnetico quantizzato generato all'interno di una cavità o un risonatore. L'hamiltoniana di Jaynes-Cummings (6.5.8) fu studiata per la prima volta nel contesto dell'ottica quantistica: non appare solo in questo caso particolare, ma in tutti quei casi in cui un qubit interagisce con uno dei modi quantizzati del campo elettromagnetico, ossia descrive tutte quelle interazioni della forma  $\vec{d} \cdot \vec{E}$ ,  $\vec{\mu} \cdot \vec{B}$ , ecc.

Giunti a questo punto vogliamo discutere il significato fisico che si trova dietro a questa hamiltoniana, in particolare vedremo qualche semplice esempio di codifica di un qubit in un modello CQED. Innanzitutto notiamo che l'hamiltoniana originale non approssimata della relazione (6.5.5) non poteva essere risolta esattamente, tuttavia grazie alla RWA può essere invece diagonalizzata!

---

<sup>xiii</sup> Abbreviazione per Cavity Quantum Electrodynamics.

Dal punto di vista della QM, l'hamiltoniana (6.5.8) costituisce un semplice problema di accoppiamento tra spin e oscillatore armonico (le eccitazioni di questo oscillatore sono fotoni). Lo spazio di Hilbert totale è infinito dimensionale in quanto è frutto del prodotto  $\mathcal{H}_c \otimes \mathcal{H}_q$ , dove  $\dim \mathcal{H}_c = \infty$  (infiniti oscillatori). Nonostante ciò, l'hamiltoniana sopra è diagonalizzabile perché è una matrice diagonale a blocchi; per tale ragione suddividiamo gli stati utilizzando la seguente notazione:

$$\begin{aligned} |0\rangle &\equiv |g\rangle & \Rightarrow & \text{Stato fondamentale del qubit.} \\ |1\rangle &\equiv |e\rangle & \Rightarrow & \text{Stato eccitato del qubit.} \\ |n\rangle &= |0\rangle, |1\rangle, |2\rangle, \dots & \Rightarrow & \text{Numero di fotoni campo elettromagnetico.} \end{aligned}$$

La struttura a blocchi è evidente notando che  $|e, n\rangle \leftrightarrow |g, n+1\rangle$ , ossia sono trasformati l'uno nell'altro dai termini dell'interazione: infatti

$$\begin{aligned} \hat{a}^\dagger \hat{\sigma}_+ |e, n\rangle &= \sqrt{n+1} |g, n+1\rangle, \\ \hat{a} \hat{\sigma}_- |g, n+1\rangle &= \sqrt{n+1} |e, n\rangle, \end{aligned}$$

perché nel primo caso dissecchiamo lo stato del qubit e creiamo un fotone di dissecitazione (lo stato finale è lo stato fondamentale con un fotone in più), mentre nel secondo caso distruggiamo un fotone della cavità, il quale viene assorbito dallo stato fondamentale, che sarà poi eccitato. Alla luce di questa osservazione possiamo suddividere lo spazio di Hilbert totale  $\mathcal{H}$  in

$$\{|g, 0\rangle\}, \quad \{|e, n\rangle, |g, n+1\rangle\}; \quad (6.5.9)$$

decomponendo  $\mathcal{H}$  in questo modo, ogni qualvolta che si agisce con i termini di interazione in (6.5.8) si rimane sempre nello stesso sottospazio. Tenendo presente che  $\hat{H}_0$  è diagonale, mentre  $\hat{H}_I$  è off-diagonal, allora in forma matriciale l'hamiltoniana diventa

$$\hat{H} = \frac{1}{2}\omega_c \mathbb{I} + \begin{pmatrix} -\frac{\omega_q}{2} & & & & |g, 0\rangle \\ & \left( \begin{matrix} \omega_c - \frac{\omega_q}{2} & g \\ g & \omega_c + \frac{\omega_q}{2} \end{matrix} \right) & & & |g, 1\rangle \\ & & \ddots & & |e, 0\rangle \\ & & & \left( \begin{matrix} \omega_c(n+1) - \frac{\omega_q}{2} & g\sqrt{n+1} \\ g\sqrt{n+1} & \omega_c n + \frac{\omega_q}{2} \end{matrix} \right) & |g, n+1\rangle \\ & & & & |e, n\rangle \end{pmatrix},$$

dove il termine iniziale rappresenta l'energia di punto zero, detta **ZPE** ("Zero Point Energy"). (Gli stati a destra sono per ricordare ciò a cui fanno riferimento i blocchi di questa matrice). Ricordando che il **detuning** è definito come  $\Delta = \omega_q - \omega_c$  e tenendo conto della ZPE, possiamo allora riscrivere il blocco generico (ultimo elemento) della matrice precedente come

$$\left( \begin{matrix} (n+1)\omega_c - \frac{\Delta}{2} & \sqrt{n+1}g \\ \sqrt{n+1}g & (n+1)\omega_c + \frac{\Delta}{2} \end{matrix} \right);$$

diagonalizzando questo blocco, lo spettro dell'hamiltoniana è dato dai seguenti autovalori e autostati

$$\begin{aligned} E_+ &= (n+1)\omega_c + \frac{1}{2}\sqrt{\Delta^2 + 4g^2(n+1)}, & |n_+\rangle &= \sin \theta_n |g, n+1\rangle + \cos \theta_n |e, n\rangle, \\ E_- &= (n+1)\omega_c - \frac{1}{2}\sqrt{\Delta^2 + 4g^2(n+1)}, & |n_-\rangle &= \cos \theta_n |g, n+1\rangle - \sin \theta_n |e, n\rangle; \end{aligned}$$

ad essi si aggiunge il singolo stato  $|g, 0\rangle$  con energia  $E_0 = -\frac{\Delta}{2}$ . Gli stati  $|n_-\rangle$  e  $|n_+\rangle$  prendono il nome di **dressed states** e l'angolo  $\theta_n$  risulta essere definito come

$$\tan 2\theta_n = \frac{2g\sqrt{n+1}}{\Delta}.$$

Che cosa succede ad un sistema come questo? L'evoluzione temporale, che ricordiamo essere data da  $e^{-i\hat{H}t}$  (hamiltoniana indipendente dal tempo), realizza delle **oscillazioni di Rabi** sulla coppia dei **dressed states**: ogni stato si comporta come un sistema a due livelli che oscilla coerentemente in cicli di assorbimento ed emissione di fotoni in maniera tale che gli stati in (6.5.9) si trasformino continuamente l'uno nell'altro, ossia  $|g, n+1\rangle \leftrightarrow |e, n\rangle$ . Confrontando con il caso dei campi esterni, qui abbiamo due accoppiamenti: l'interazione è quantificata da  $g$ , la forza dell'accoppiamento tra i due sistemi, alla quale si aggiunge però  $n$ , ovvero il numero dei fotoni. La frequenza di Rabi delle oscillazioni risulta quindi essere data da  $\sqrt{\Delta^2 + 4g^2(n+1)}$ : maggiore è il numero di fotoni, più grande sarà la frequenza di oscillazione del qubit.

In ottica quantistica si è spesso interessati a guardare a situazioni in cui si ha una sovrapposizione di differenti stati con numero di fotoni fissato. In questi contesti l'oscillazione generale è più complicata: ogni insieme di fotoni si accoppia in blocchi di 2 cosicché ogni blocco oscilli a coppie. Il punto fondamentale è che la sovrapposizione di oscillazioni crea una situazione in cui non ci sono oscillazioni! Talvolta è possibile aspettare del tempo a sufficienza fino a quando si ritorna ad osservare un pattern di oscillazioni: tipicamente, quando si sovrappongono molti sistemi oscillatori, si ha interferenza, quindi se si aspetta un tempo sufficiente si possono di nuovo osservare delle oscillazioni (rilevate sperimentalmente).

Nel caso invece del qubit è possibile "giocare" con  $g$ ,  $n$  e  $\Delta$  per osservare questo pattern di oscillazioni. Nella scorsa sezione abbiamo visto che in una situazione di risonanza esatta ( $\Delta = 0$ ) vi era certezza che ad un certo punto il qubit avesse subito una transizione  $|0\rangle \rightarrow |1\rangle$ . Come vedremo tra poco, in altre situazioni può essere utile considerare il cosiddetto **regime dispersivo**, ossia  $\Delta \neq 0$ . Consideriamo l'energia dei **dressed states** come funzione del **detuning**: la differenza in energia con lo stato fondamentale non è altro che

$$E_{\pm} - E_0 = (n+1)\omega_c \pm \frac{1}{2}\sqrt{\Delta^2 + 4g^2(n+1)} + \frac{\Delta}{2};$$

se disegniamo un plot in funzione di  $\frac{\Delta}{g}$  otteniamo la Figura 6.7. I due regimi particolarmente interessanti sono:

- **Regime di risonanza**, quindi  $\Delta = 0$  ( $\omega_c = \omega_q$ ): in questo caso  $\theta_n = \frac{\pi}{4}$ , per cui  $\cos \theta_n = \sin \theta_n = \frac{1}{\sqrt{2}}$ . Si dice che vi è un'**ibridizzazione massima** degli stati poiché

$$|n_{\pm}\rangle = \frac{|g, n+1\rangle \pm |e, n\rangle}{\sqrt{2}};$$

essi prendono il nome di **polarons**. La differenza in energia qui è la minima possibile e dipende da  $n$ :

$$E_{\pm} = (n+1)\omega_c \pm g\sqrt{n+1}.$$

In generale è una situazione abbastanza simile alle oscillazioni di Rabi della Figura 6.5.

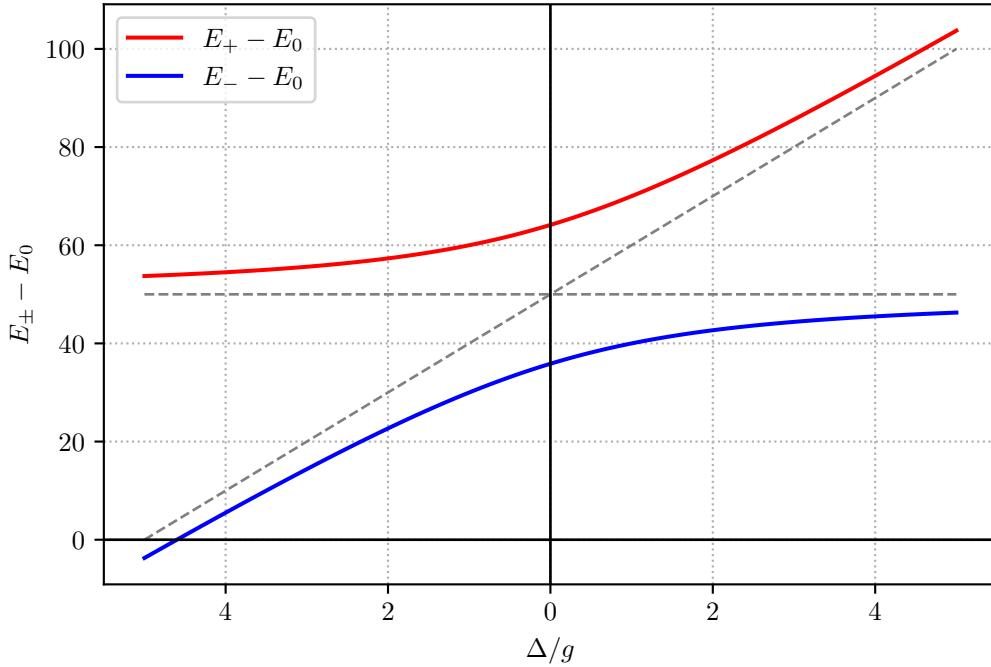


Figura 6.7: Differenza in energia dei dressed states con lo stato fondamentale in funzione del detuning. Si noti che la minima differenza di energia tra  $E_+$  e  $E_-$  si trova in corrispondenza di  $\Delta = 0$ , mentre la maggior differenza è data quando  $\Delta$  diverge. L'asintoto orizzontale si trova in corrispondenza dei limiti:  $\lim_{\Delta \rightarrow -\infty} (E_+ - E_0) = \lim_{\Delta \rightarrow +\infty} (E_- - E_0) = (n + 1)\omega_c$ . In questo caso si sono impostati i seguenti valori  $\omega_c = 25$ ,  $g = 10$ ,  $n = 1$ .

- **Regime dispersivo**, tale che  $\Delta \gg g$ : qui  $\theta_n \ll 1$  e gli stati originali rimangono pressoché invariati a meno di piccole correzioni

$$\begin{aligned}|n_-\rangle &= |g, n+1\rangle + \dots, \\|n_+\rangle &= |e, n\rangle + \dots;\end{aligned}$$

notiamo che questo comportamento è previsto dato che  $\frac{\Delta}{g} \rightarrow \infty$  significa equivalentemente che  $\Delta = \text{cost}$  e  $g \simeq 0$ : siamo vicini al caso libero in cui il qubit e la radiazione e.m. sono quasi disaccoppiati.

Questo regime è interessante per diverse ragioni: ad esempio può essere utile tenere le piccole correzioni negli stati  $|n_+\rangle$  e  $|n_-\rangle$ . Sviluppando la radice in  $\frac{g^2}{\Delta^2}$  si ha

$$\begin{aligned}E_\pm &= (n + 1)\omega_c \pm \frac{1}{2}\sqrt{\Delta^2 + 4g^2(n + 1)} \\&= (n + 1)\omega_c \pm \frac{\Delta}{2}\sqrt{1 + \frac{4g^2}{\Delta^2}(n + 1)} \\&= (n + 1)\omega_c \pm \frac{\Delta}{2}\left(1 + \frac{2g^2}{\Delta^2}(n + 1) + \dots\right) \\&= (n + 1)\omega_c \pm \left(\frac{\Delta}{2} + \frac{g^2}{\Delta}(n + 1) + \dots\right);\end{aligned}$$

Osserviamo che possiamo ricavare le medesime energie dando una descrizione efficace del sistema con la seguente hamiltoniana

$$\hat{H}^{(2)} = \omega_c \left( \hat{a}^\dagger \hat{a} + \frac{1}{2} \right) - \frac{\omega_q}{2} \hat{\sigma}_3 - \frac{g^2}{\Delta} \left( \hat{a}^\dagger \hat{a} + \frac{1}{2} \right) \hat{\sigma}_3 + \frac{g^2}{2\Delta} \mathbb{I}_{2 \times 2}, \quad (6.5.10)$$

infatti

$$\begin{aligned} \hat{H}^{(2)} |g, n+1\rangle &= \omega_c \left( n+1 + \frac{1}{2} \right) - \frac{\omega_q}{2} - \frac{g^2}{\Delta} (n+1) \\ &= \omega_c (n+1) - \frac{\Delta}{2} - \frac{g^2}{\Delta} (n+1) \equiv E_-, \\ \hat{H}^{(2)} |e, n\rangle &= \omega_c \left( n + \frac{1}{2} \right) + \frac{\omega_q}{2} + \frac{g^2}{\Delta} \left( n + \frac{1}{2} \right) + \frac{g^2}{2\Delta} \\ &= \omega_c (n+1) + \frac{\Delta}{2} + \frac{g^2}{\Delta} (n+1) \equiv E_+. \end{aligned}$$

Dunque possiamo dire che l'hamiltoniana efficace  $\hat{H}^{(2)}$  descrive la fisica del sistema nel regime dispersivo. Sui libri si trovano spesso hamiltoniane più complicate: questa hamiltoniana è un esempio della cosiddetta **trasformazione di Schrieffer-Wolff**. Si tratta di scegliere l'operatore  $\hat{U}$  della (6.4.6) indipendente dal tempo e della forma

$$\hat{U} = e^{\hat{S}}, \quad \text{dove} \quad S^\dagger = -S.$$

L'operatore  $\hat{S}$  è scelto in maniera tale che si possa effettuare un'espansione in teoria delle perturbazioni su un opportuno parametro. Se l'hamiltoniana si scrive come  $\hat{H} = \hat{H}_0 + \hat{H}_I$ , allora si sceglie un  $\hat{S}$  tale che  $[\hat{S}, \hat{H}_0] = -\hat{H}_I$ . Con un po' di algebra si dimostra che

$$\hat{U} \hat{H} \hat{U}^\dagger = \hat{H}_0 + \frac{1}{2} [\hat{S}, \hat{H}_I] + \mathcal{O}(S^3).$$

Nel nostro caso, l'espressione di  $\hat{H}^{(2)}$  si ottiene dall'espansione fino a  $\mathcal{O}(g^2/\Delta^2)$  nel sistema ruotato dall'operatore

$$\hat{U} = e^{-\frac{g}{\Delta} (\hat{\sigma}_+ \hat{a}^\dagger - \hat{\sigma}_- \hat{a})}.$$

Riscriviamo l'hamiltoniana (6.5.10) senza i termini costanti:

$$\hat{H}^{(2)} = \omega_c \hat{a}^\dagger \hat{a} - \frac{\omega_q}{2} \hat{\sigma}_3 - \frac{g^2}{\Delta} \left( \hat{a}^\dagger \hat{a} + \frac{1}{2} \right) \hat{\sigma}_3.$$

A seconda di ciò che si sta facendo è utile raggruppare gli operatori interni a questa espressione in due modi:

- Possiamo raggruppare scrivendo

$$\hat{H}^{(2)} = (\omega_c - \chi \hat{\sigma}_3) \hat{a}^\dagger \hat{a} - \frac{\tilde{\omega}_q}{2} \hat{\sigma}_3,$$

dove  $\chi = g^2/\Delta$  e  $\tilde{\omega}_q = \omega_q + g^2/\Delta$ . È evidente che l'energia della cavità dipenderà da una frequenza che risulta shiftata di una costante  $\chi$  dipendente dallo stato del qubit; similmente  $\omega_q$  è ridefinito a seguito dell'interazione con il

campo elettromagnetico (si parla infatti di **Lamb shift**, in onore dell'analogo in fisica atomica). Per tale ragione questa situazione può essere utilizzata per realizzare una **quantum nondemolition measurement**: possiamo stabilire lo stato in cui si trova il qubit misurando la frequenza della cavità! Si noti che questo non viola le leggi della QM.

- Un modo equivalente è quello di raggruppare tutte le matrici  $\hat{\sigma}_3$  scrivendo

$$\hat{H}^{(2)} = \omega_c \hat{a}^\dagger \hat{a} - \frac{\hat{\sigma}_3}{2} \left( \omega_q + \frac{g^2}{\Delta} + \frac{2g^2}{\Delta} \hat{a}^\dagger \hat{a} \right);$$

in questa visione la frequenza del qubit è ridefinita a seguito di due fattori: il Lamb shift (secondo termine della parentesi) e il cosiddetto **AC - Stark Effect** (ultimo termine), il quale indica il numero di fotoni che creano rumore nella frequenza dei qubit; quindi in questo caso anche il numero di fotoni influenza la frequenza del qubit.

### 6.5.1 Operazioni su 2 qubit

Il regime dispersivo nel sistema qubit-cavità può essere utilizzato per codificare delle operazioni (gate) che coinvolgono due qubit. Ricordiamo che nella sezione precedente abbiamo visto che le operazioni sui **singoli** qubit sono realizzate abbastanza semplicemente per mezzo delle oscillazioni di Rabi. Qui il trucco è quello introdurre uno stato addizionale, che chiamiamo  $|\gamma\rangle$ , al fuori della cavità risonante (in cui sono presenti gli stati  $|g\rangle$  e  $|e\rangle$  che interagiscono con i fotoni):

$$\begin{array}{c} |e\rangle \\ |g\rangle \end{array} \xrightarrow{\quad} |\gamma\rangle$$

Precisiamo che  $|e\rangle$  e  $|g\rangle$  sono accoppiati con la cavità, mentre  $|\gamma\rangle$  è disaccoppiato dal sistema qubit-cavità. L'idea è quella di codificare un qubit con gli stati  $(|g\rangle, |\gamma\rangle)$  e uno con gli stati  $(|0\rangle, |1\rangle)$  dei fotoni, cosicché lo spazio di Hilbert totale contenga gli stati seguenti

$$\mathcal{H} = \{|\gamma 0\rangle, |\gamma 1\rangle, |g 0\rangle, |g 1\rangle\}.$$

L'interazione sarà descritta dall'hamiltoniana (6.5.10): lo stato  $|e\rangle$  è irrilevante in questa descrizione, mentre l'accoppiamento qubit-cavità è dato dagli ultimi due termini interagenti (quelli con  $g$ ). Consideriamo l'evoluzione temporale del sistema del qubit: gli operatori  $\hat{\sigma}_3$  e  $\mathbb{I}$  agiscono solamente su  $|e\rangle$  e  $|g\rangle$  perché  $|\gamma\rangle$  è disaccoppiato. Per tale motivo, dal momento che  $\hat{\sigma}_3 |\gamma\rangle = \mathbb{I} |\gamma\rangle = 0$  e  $\hat{\sigma}_3 |g\rangle = |g\rangle$ , la parte interagente di  $\hat{H}$  agisce come

$$e^{-i\hat{H}_I t} = e^{i\frac{g^2}{\Delta} \hat{a}^\dagger \hat{a} \hat{\sigma}_3 t + i\frac{g^2}{2\Delta} (\hat{\sigma}_3 - \mathbb{I}_{2 \times 2}) t} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{i\frac{g^2}{\Delta} t} \end{pmatrix} \begin{array}{c} |\gamma 0\rangle \\ |\gamma 1\rangle \\ |g 0\rangle \\ |g 1\rangle \end{array}.$$

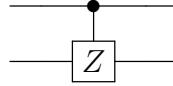
(come in precedenza sono scritti gli stati sulla destra per ricordare l'origine degli elementi di matrice). Il gate risultante è detto **QPG**, ossia **Quantum Phase Gate**, poiché è della forma

$$Q_\eta = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{i\eta} \end{pmatrix}.$$

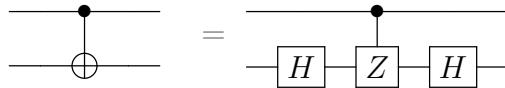
Questa tipologia di gate include il caso  $\eta = \pi$ , ovvero

$$Q_\pi = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix};$$

il gate precedente potrebbe sembrare banale ma non lo è perché, usando operazioni a singolo gate su  $|\gamma\rangle$ ,  $|g\rangle$ , può essere convertito in un **CZ-gate** (Controlled-Z)



ma sappiamo che quest'ultimo è legato al **CNOT-gate** attraverso l'applicazione di due **H-gate**



Questo significa che con delle singole operazioni possiamo trasformare un QPG in un **CNOT-gate**, che sappiamo molto bene che agisce su due qubit contemporaneamente.

Cosa succede invece ai termini non interagenti in (6.5.10)? Anche loro permettono di implementare delle trasformazioni sui qubit: l'evoluzione temporale dell'hamiltoniana libera è disaccoppiata poiché  $\hat{H}_0^{(2)}$  è somma delle hamiltoniane del qubit e della cavità. Perciò questa evoluzione può sempre essere fattorizzata come

$$e^{-i\omega_c(\hat{a}^\dagger\hat{a}+\frac{1}{2})t+i\frac{\omega_q}{2}\hat{\sigma}_3t} = e^{-i\omega_c(\hat{a}^\dagger\hat{a}+\frac{1}{2})t}e^{i\frac{\omega_q}{2}\hat{\sigma}_3t} = e^{-i\frac{\omega_c}{2}t} \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\omega_q}{2}t} \end{pmatrix}}_{\{|g\rangle, |\gamma\rangle\}} \otimes \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & e^{i\omega_ct} \end{pmatrix}}_{\{|0\rangle, |1\rangle\}}.$$

Questo è un fatto generale: l'evoluzione libera descrive sempre l'evoluzione del singolo qubit perché  $\hat{H}_0^{(2)}$  è fattorizzata.

Nelle prossime sezioni vedremo alcuni esempi esplicativi, come qubit superconduttori e trappole ioniche, che metteranno in pratica i concetti che abbiamo studiato nel corso delle ultime due sezioni. In generale non è così difficile creare i gate, ma la difficoltà spesso risiede nel controllarli; spesso le idee funzionanti sono frutto di intuizioni creative e geniali legate al trovare la corretta evoluzione temporale del sistema.

LEZIONE 19 - 13/12/2021

## 6.6 Sistemi a trappola ionica

A partire da questa sezione focalizzeremo la nostra attenzione sullo studio del controllo e della realizzazione fisica (pratica) di sistemi costituiti da qubit e gate.

I sistemi basati sulle cosiddette **trappole di ioni** sono una tecnologia sperimentale sviluppatisi nel corso degli anni '80. Come già introdotto all'inizio del capitolo, queste apparecchiature sono costituite da un campo elettromagnetico generato da una serie di

elettrodi cilindrici che intrappola al proprio interno un gruppo di ioni (solitamente ioni di berillio). Si faccia riferimento alla Figura 6.1 di Pagina 118 per una rappresentazione schematica. A causa della loro particolare disposizione, gli elettrodi generano un potenziale<sup>xiv</sup> indipendente dal tempo e uno variabile:

$$\begin{aligned}\phi_{\text{dc}} &= kU_0(z^2 - x^2 - y^2) , \\ \phi_{\text{rf}} &= (V_0 \cos(\Omega t) + U_0) \left( 1 - \frac{x^2 - y^2}{R^2} \right) .\end{aligned}$$

È possibile mostrare che l'effetto di questi potenziali è quello di creare un'hamiltoniana con il seguente potenziale armonico

$$H = \sum_{i=1}^N \frac{M}{2} (\omega_x^2 x_i^2 + \omega_y^2 y_i^2 + \omega_z^2 z_i^2) + \sum_{j>i} \frac{e^2}{4\pi\varepsilon_0 |\vec{x}_i - \vec{x}_j|} ,$$

dove  $N$  è il numero di ioni intrappolati dal campo e  $M$  la loro massa (il secondo termine è repulsivo). Per realizzare un tale setup si sceglie una direzione privilegiata (per convenzione  $z$ ) tale per cui  $\omega_x, \omega_y \gg \omega_z$ , in questo modo l'effetto che si ottiene è che gli ioni cercano di allinearsi solamente lungo  $z$ , ossia la direzione in cui sono "accesi" i modi vibrazionali (lungo  $x$  e  $y$  sono soppressi). Diagonalizzando esplicitamente un'hamiltoniana della forma precedente si ricava che la frequenza minore è associata al moto del centro di massa del sistema: la frequenza minima corrisponde quindi al movimento rigido degli ioni lungo  $z$ .

Per gli scopi del QC vorremmo essere in grado di indirizzare e manipolare a piacimento gli stati quantistici del sistema. Innanzitutto è necessario lavorare a temperature molto basse, ossia  $kT \ll \hbar\omega_z$  (molto più piccole del primo stato eccitato), perché nessuno dei modi vibrazionali lungo  $x$  o  $y$  deve essere eccitato. Non entriamo nei dettagli<sup>xv</sup>, tuttavia ci limitiamo a sottolineare che questa procedura di raffreddamento viene attuata per mezzo di opportuni laser. In aggiunta ai laser è necessario costruire le cosiddette **sidebands**: si eccitano i livelli energetici interni degli stati degli ioni in modo tale che si possano etichettare gli stati utilizzando anche i modi vibrazionali. In generale entrambe queste procedure possono essere realizzate sperimentalmente con il seguente risultato: il primo stato eccitato quantistico corrisponde all'oscillazione del centro di massa del sistema lungo  $z$  con frequenza  $\omega_z$ .

Spesso i modi vibrazionali che possono essere eccitati sono comunemente detti **fononi**. Il moto (oscillazione) del centro di massa è il primo elemento su cui si basano i sistemi a trappola ionica e può essere descritto in maniera del tutto analoga ad un oscillatore armonico: come nella (6.2.4), la quantizzazione è effettuata promuovendo la coordinata spaziale ad operatore

$$\hat{z} = z_0(\hat{a} + \hat{a}^\dagger) , \quad \text{dove} \quad z_0 = \sqrt{\frac{\hbar}{2\omega MN}} .$$

Il secondo ingrediente che si aggiunge ai modi vibrazionali sono gli stati atomici degli ioni: solitamente si scelgono opportunamente gli ioni in maniera tale che si riescano a isolare

<sup>xiv</sup>I pedici **dc** e **rf** significano rispettivamente *direct current* e *radio frequency*.

<sup>xv</sup>Ad esempio viene effettuato il cosiddetto **Doppler cooling**, il quale sfrutta il fatto che, per effetto Doppler, la frequenza degli ioni in movimento rispetto al laser cambia a seconda del verso del moto. In questo modo solamente gli ioni che si dirigono verso il laser possono assorbire fotoni, al contrario invece di quelli che si muovono in direzione contraria.

esplícitamente due livelli energetici dello spettro rispetto a tutti gli altri; in questo modo è possibile codificare in questi livelli un qubit, ma soprattutto, essendo gli stati separati dal resto dello spettro, sono facilmente controllabili dai laser. Per ridurre al minimo la probabilità di transizione  $|1\rangle \rightarrow |0\rangle$  a seguito dell'emissione spontanea si cercano degli stati eccitati che presentano una vita media molto lunga, come ad esempio alcuni ioni con stati eccitati metastabili. Un'altra scelta è quella di sfruttare la struttura iperfine dei livelli energetici degli ioni (dovuta all'interazione tra gli spin dei nucleoni e degli elettroni esterni): visto che l'ampiezza di decadimento per emissione spontanea è  $\Gamma \sim \omega^3$ , questi livelli molto più stabili di altri livelli energetici atomici.

Come già mostrato nella Figura 6.2, per gli scopi del QC i qubit sono codificati in ciascuno degli ioni (si ottiene un array di qubit) utilizzando entrambi gli stati precedenti: un generico stato è quindi descritto da entrambi i modi, quelli vibrazionali (fononi) e quelli energetici. Per quanto riguarda i fononi si utilizzano due livelli:  $|0\rangle$ , ossia nessun fonone, e il suo stato eccitato  $|1\rangle$ , un fonone; vedremo a breve che utilizzando questi stati è possibile codificare un qubit extra, detto **bus qubit**.

Per interagire con un sistema così generato si utilizzano delle opportune radiazioni elettromagnetiche generate da laser. Queste radiazioni presentano un comportamento classico, quindi consideriamo l'accoppiamento tra qubit e campo esterno classico oscillante della Sezione 6.4 (notare che gli operatori  $\hat{a}$  e  $\hat{a}^\dagger$  fanno riferimento ai modi vibrazionali, non al campo quantizzato). Consideriamo un solo ione: l'interazione con il campo è descritta dall'accoppiamento  $\vec{d} \cdot \vec{E}$ , quindi l'hamiltoniana non è altro che la (6.4.1), ossia

$$\hat{H} = \Omega \hat{\sigma}_1 \cos(kz - \omega t + \phi). \quad (6.6.1)$$

In questo contesto  $kz \simeq kz_0 = 2\pi \frac{z_0}{\lambda}$  e  $kz_0 \equiv \eta$  è detto **parametro di Lamb-Dicke**, il quale misura il rapporto tra l'ampiezza dell'oscillazione dei modi vibrazionali del qubit e la lunghezza d'onda della radiazione. Per assicurare che  $kz$  sia circa costante sul qubit dobbiamo stare attenti alle due scale del problema:

1. Dato che la grandezza dei qubit è quella degli ioni allora vorremmo che la lunghezza d'onda dei laser ( $\lambda$ ) sia molto più grande delle scale atomiche.
2. Per la presenza dei modi vibrazionali lungo  $z$  dobbiamo richiedere che  $\lambda$  sia molto più grande delle oscillazioni lungo  $z$ .

Quando le precedenti sono verificate possiamo assumere che  $kz \ll 1$ , ma non completamente trascurabile, in modo tale da poter effettuare un'espansione perturbativa della (6.6.1):

$$\hat{H} = \Omega \hat{\sigma}_1 \cos(-\omega t + \phi) - \Omega kz \hat{\sigma}_1 \sin(-\omega t + \phi) + \mathcal{O}((kz)^2);$$

inserendo gli operatori e trascurando i termini di ordine superiore avremo

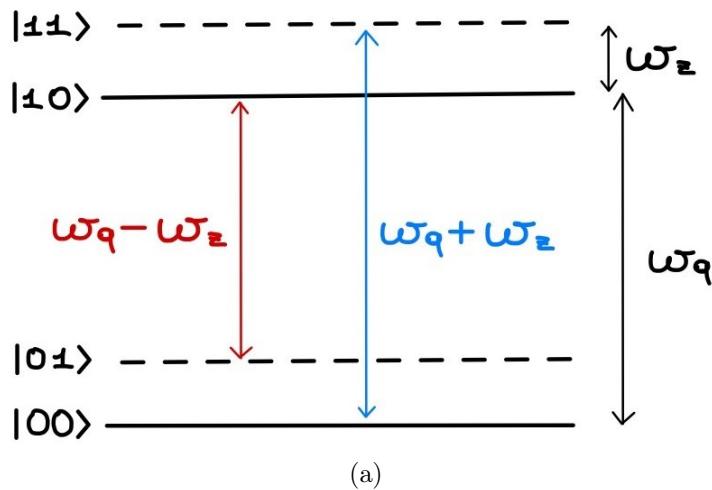
$$\begin{aligned} \hat{H} &= \underbrace{\frac{\Omega}{2}(\hat{\sigma}_+ + \hat{\sigma}_-) (e^{-i(\omega t - \phi)} + e^{i(\omega t - \phi)})}_{\hat{H}_{(I)}} + \\ &\quad + \underbrace{i \frac{\Omega}{2} \eta (\hat{\sigma}_+ + \hat{\sigma}_-) (\hat{a} + \hat{a}^\dagger) (e^{-i(\omega t - \phi)} - e^{i(\omega t - \phi)})}_{\hat{H}_{(II)}}, \end{aligned} \quad (6.6.2)$$

dove abbiamo distinto i due termini di  $\hat{H}$  perché tra poco vedremo che contribuiranno in modo differente. Assumiamo di lavorare in un regime in cui la frequenza del laser

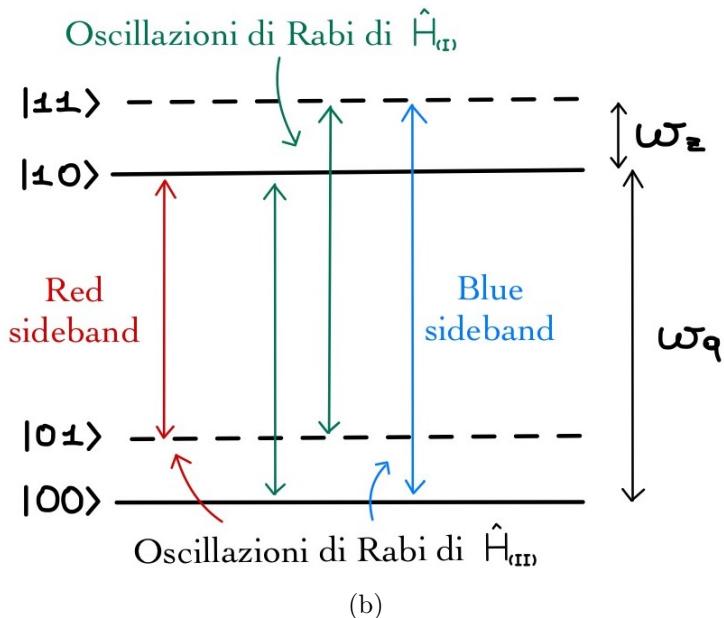
sia sintonizzata su entrambe le frequenze in gioco, ossia quella della differenza in energia dei livelli del qubit e la frequenza dei modi vibrazionali. Per questo possiamo utilizzare nuovamente la RWA perché sappiamo che solo i termini in risonanza contribuiscono. Innanzitutto, l'hamiltoniana libera e l'operatore  $\hat{U}$  con cui effettuiamo la rotazione saranno ( $\hbar = 1$ )

$$\hat{H}_0 = -\frac{\omega_q}{2}\hat{\sigma}_3 + \omega_z(\hat{a}^\dagger\hat{a}), \quad \Rightarrow \quad \hat{U} = e^{i\hat{H}_0 t};$$

facendo uso delle (6.5.7) (chiaramente in questo contesto  $\omega_c \equiv \omega_z$ ) possiamo facilmente scrivere l'hamiltoniana ruotata della (6.4.6): come sappiamo ogni operatore ottiene un fattore di fase e l'idea è quella di tenere solamente i termini in risonanza e trascurare tutti gli altri per tempi molto lunghi.



(a)



(b)

Figura 6.8: (6.8a) Suddivisione dei livelli energetici degli ioni in un sistema a trappola ionica. Le frequenze  $\omega_q - \omega_z$  e  $\omega_q + \omega_z$  sono dette **red sideband** e **blue sideband** rispettivamente. (6.8b) Oscillazioni di Rabi prodotte dai termini delle hamiltoniane  $\hat{H}_{(I)}$  e  $\hat{H}_{(II)}$ . Notare che per la red sideband contribuiscono gli operatori  $\hat{\sigma}_-\hat{a}$  ( $|01\rangle \rightarrow |10\rangle$ ) e  $\hat{\sigma}_+\hat{a}^\dagger$  ( $|10\rangle \rightarrow |01\rangle$ ); mentre per la blue sideband contribuiscono  $\hat{\sigma}_+\hat{a}$  ( $|11\rangle \rightarrow |00\rangle$ ) e  $\hat{\sigma}_-\hat{a}^\dagger$  ( $|00\rangle \rightarrow |11\rangle$ ).

Ci sono molti termini che possono contribuire a seconda della frequenza del laser. L'idea nei sistemi a trappola ionica è quella di utilizzare una radiazione che possa accomodare 4 differenti frequenze. Innanzitutto etichettiamo gli stati del sistema con la notazione  $|nm\rangle$ , dove  $n$  è il livello energetico del qubit e  $m$  il modo di oscillazione vibrazionale (fonone). Tenendo conto della Figura 6.8a vorremmo utilizzare le 4 frequenze  $\pm\omega_q \pm \omega_z$  e  $\pm\omega_q$  (quest'ultimo permette le oscillazioni  $|0m\rangle \leftrightarrow |1m\rangle$ ).

Scriviamo i termini che "sopravvivono" dalla RWA nelle due hamiltoniane  $\hat{H}_{(I)}$  e  $\hat{H}_{(II)}$ :

$$\hat{H}_{(I)} = \frac{\Omega}{2} (\hat{\sigma}_+ e^{i(\omega t - \phi)} + \hat{\sigma}_- e^{-i(\omega t - \phi)}) \quad (6.6.3)$$

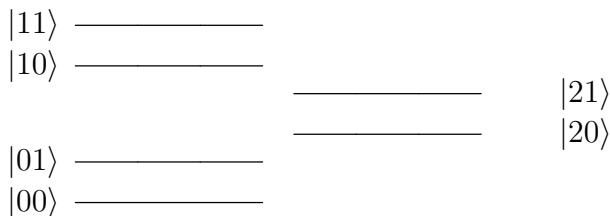
$$\begin{aligned} \hat{H}_{(II)} = & i \frac{\eta\Omega}{2} (-\hat{\sigma}_+ \hat{a}^\dagger e^{i(\omega t - \phi)} + \hat{\sigma}_- \hat{a} e^{-i(\omega t - \phi)}) + \\ & + i \frac{\eta\Omega}{2} (-\hat{\sigma}_+ \hat{a} e^{i(\omega t - \phi)} + \hat{\sigma}_- \hat{a}^\dagger e^{-i(\omega t - \phi)}), \end{aligned} \quad (6.6.4)$$

dove nella (6.6.3) abbiamo assunto  $\omega \sim \omega_q$  e nella (6.6.4) si ha  $\omega \sim \omega_q - \omega_z$  nella prima riga e  $\omega \sim \omega_q + \omega_z$  nella seconda (notare che  $\omega$  in queste due righe è scelto appositamente per annullare le fasi derivanti dalla (6.5.7)). Come evidente dal disegno in Figura 6.8b,  $\hat{H}_{(I)}$  genera oscillazioni di Rabi tra  $|0m\rangle \leftrightarrow |1m\rangle$  se si utilizza un laser con frequenza  $\omega \sim \omega_q$ ; similmente, le due righe di  $\hat{H}_{(II)}$  hanno un comportamento analogo perché la blue sideband (seconda riga) genera oscillazioni di Rabi tra  $|11\rangle \leftrightarrow |00\rangle$  e la red sideband (prima riga) produce oscillazioni di Rabi tra  $|01\rangle \leftrightarrow |10\rangle$  (si faccia sempre riferimento alla Figura 6.8b tenendo presente l'azione di  $\hat{\sigma}_\pm$  sui livelli del qubit).

La logica è quindi quella di utilizzare le oscillazioni di  $\hat{H}_{(I)}$  per muovere il qubit lungo la sfera di Bloch (implementare gate agenti su singoli qubit) e le oscillazioni di  $\hat{H}_{(II)}$  per codificare delle operazioni agenti contemporaneamente su due tipi differenti di qubit. Vediamo il più semplice esempio di costruzione di un tale gate.

### 6.6.1 Cirac-Zoller gate

Il **Cirac-Zoller gate** costituisce un esempio di realizzazione pratica di un CNOT-gate. Immaginiamo di considerare, in aggiunta ai livelli energetici nella Figura 6.8, un livello extra, che chiamiamo  $|2m\rangle$ , del sistema atomico:



Chiamiamo  $E_{10} - E_{20} = \omega_{\text{aux}}$  (aux per ausiliaria) e chiaramente poniamo come prima  $E_{10} - E_{00} = \omega_q$ . L'idea è quella di utilizzare un laser sintonizzato ad una frequenza  $\omega = \omega_{\text{aux}} + \omega_z$  per produrre transizioni tra gli stati  $|20\rangle \leftrightarrow |11\rangle$ . Le oscillazioni di Rabi così prodotte, regolando opportunamente l'ampiezza, la fase e la frequenza del laser, possono essere parametrizzate come al solito dall'operatore in (6.4.12)

$$R_{\vec{n}}(\gamma) = e^{-\frac{i}{2}\gamma(\vec{\sigma} \cdot \vec{n})} = \mathbb{I} \cos\left(\frac{\gamma}{2}\right) - i(\vec{\sigma} \cdot \vec{n}) \sin\left(\frac{\gamma}{2}\right);$$

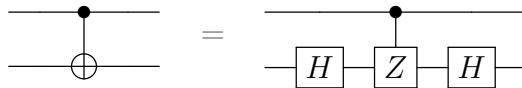
se scegliamo di ruotare con angolo  $2\pi$  attorno ad  $x$  allora

$$R_x(2\pi) = e^{-\frac{i}{2}2\pi\sigma_x} = \mathbb{I} \cos \pi - i \sin \pi \sigma_x = -\mathbb{I},$$

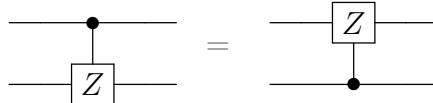
quindi una rotazione spaziale di  $360^\circ$  agisce in maniera non banale sui fermioni! (Si noti che questo è vero per qualsiasi direzione  $\vec{n}$ ). Quindi se si scelgono dei laser opportuni che implementano trasformazioni  $R_x(2\pi)$  e si aspetta del tempo a sufficienza, allora possiamo realizzare questa operazione sugli stati precedenti:  $|11\rangle \rightarrow -|11\rangle$  e  $|20\rangle \rightarrow -|20\rangle$ . Se ci dimentichiamo dello stato ausiliario  $|20\rangle$  (l'informazione è codificata negli stati  $|nm\rangle$ ), allora l'effetto netto sul sistema non è altro che un CZ-gate

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix} \begin{pmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{pmatrix} = \begin{cases} |00\rangle \rightarrow |00\rangle \\ |01\rangle \rightarrow |01\rangle \\ |10\rangle \rightarrow |10\rangle \\ |11\rangle \rightarrow -|11\rangle \end{cases} = \begin{array}{c} \text{---} \bullet \text{---} \\ \text{---} \square Z \text{---} \end{array}$$

perché l'operatore  $Z$  viene applicato sul secondo qubit solamente quando il primo si trova in  $|1\rangle$ . Come già anticipato al termine della Sezione 6.5, è molto semplice passare da un CZ-gate ad un CNOT-gate:



In generale è abbastanza semplice realizzare un CZ-gate sui qubit, ma è invece meno banale realizzare questa operazione sugli stati costruiti con i modi vibrazionali. Nonostante ciò, si può ovviare a questo problema ricordando che questo gate ha la proprietà



perché il risultato è analogo a quello sopra anche se  $Z$  agisce sul primo qubit quando il secondo è in  $|1\rangle$ : non importa dove è posto  $Z$  perché si può equivalentemente applicare questo gate sul qubit (più semplice) o sui modi vibrazionali!

Questi risultati relativi alla realizzazione di operazioni su un insieme di due qubit furono un grande traguardo negli anni '90, tuttavia al giorno d'oggi si vorrebbe costruire un QC con  $\sim 100$  qubit, quindi sarebbe veramente poco pratico creare un sistema entangled tra ioni e modi vibrazionali. Dato che nella trappole ioniche si allinea facilmente un array di qubit in cui essi sono creati separatamente, si vorrebbe codificare l'informazione solamente nei qubit realizzati dagli ioni e non in quelli ottenuti dai modi vibrazionali. Questo scopo può essere raggiunto sfruttando i modi vibrazionali come **bus**, ossia modi ausiliari, che muovono l'informazione da ione a ione.

Immaginiamo un generico array di qubit: vorremmo poter indirizzare operazioni a due qubit su due qubit ben precisi dell'array utilizzando in qualche modo i modi vibrazionali come step intermedio. Ciò può essere fatto per mezzo dei fononi e utilizzando il cosiddetto SWAP-gate, ossia un gate che scambia informazioni da un qubit ai modi vibrazionali e successivamente da questi ultimi ad un altro qubit.

Immaginiamo ad esempio di voler scambiare gli stati  $|01\rangle \leftrightarrow |10\rangle$ : questo può essere fatto per mezzo della matrice

$$\begin{pmatrix} 1 & & & \\ & 0 & 1 & \\ & -1 & 0 & \\ & & & 1 \end{pmatrix} \begin{pmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{pmatrix} = \begin{pmatrix} |00\rangle \\ |10\rangle \\ |01\rangle \\ |11\rangle \end{pmatrix},$$

ma il blocco interno non è altro che una rotazione di Rabi di angolo  $\pi$  lungo  $y$ :

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = i\sigma_2 = \cos\left(\frac{\pi}{2}\right) + i \sin\left(\frac{\pi}{2}\right) \sigma_2 = e^{\frac{i}{2}\pi\sigma_2} = R_y(-\pi).$$

Riusciamo a codificare in qualche modo un'oscillazione di Rabi che operi con  $R_y(-\pi)$  su  $|01\rangle$  e  $|10\rangle$ ? La risposta è affermativa perché possiamo utilizzare una delle frequenze di sideband dell'hamiltoniana in (6.6.4): ad esempio possiamo impiegare la red sideband (prima riga) per implementare tutti i possibili operatori  $R_{\vec{n}}(\gamma)$  agenti sul sottospazio  $\{|01\rangle, |10\rangle\}$ . Come funziona questo **SWAP-gate**? Immaginiamo di partire in uno stato dato dal prodotto tensoriale di un modo senza fononi e un qubit arbitrario dell'array di ioni:

$$(a|0\rangle + b|1\rangle) \otimes |0\rangle = a|00\rangle + b|10\rangle \xrightarrow{\text{SWAP}} a|00\rangle + b|01\rangle = |0\rangle \otimes (a|0\rangle + b|1\rangle),$$

è quindi possibile scambiare informazioni che erano codificate nel qubit con lo stato del modo vibrazionale. Successivamente si agisce con un altro **SWAP-gate** e si sceglie un altro ione nel quale trasferire l'informazione acquisita.

Più esplicitamente, etichettiamo gli ioni dell'array con  $j, k = 1, 2, 3, 4, \dots$ ; ora mostriamo che è possibile costruire un gate  $\text{CZ}_{(i)}$  per ogni ione (gate che coinvolge il sistema combinato fononi-ioni) e poi agire con un **SWAP-gate** su ciascun ione per trasferire l'informazione e utilizzare quindi i modi vibrazionali come **bus**.

**Esempio 6.4 (CZ-gate e CNOT-gate tra ioni).** Supponiamo di voler realizzare un **CZ-gate** tra due ioni generici  $j$  e  $k$ , dove quest'ultimo agisce come control-qubit sul primo. Possiamo agire con  $\text{SWAP}_k$  per muovere l'informazione da  $k$  ai fononi, applicare  $\text{CZ}_j$  tra i fononi e lo ione  $j$  e infine ritornare allo ione  $k$  con  $\text{SWAP}_k^{-1}$ : in ordine significa applicare le operazioni

$$\text{SWAP}_k^{-1} \text{CZ}_j \text{SWAP}_k.$$

La stessa procedura può essere applicata per l'implementazione di un **CNOT-gate** con l'unica differenza che è necessario aggiungere due **H-gate** prima e dopo:

$$H_k \text{SWAP}_k^{-1} \text{CZ}_j \text{SWAP}_k H_k.$$

Storicamente questa procedura per costruire un 2-qubit gate fu importante perché fu il primo esempio di implementazione di operazioni agenti su due qubit contemporaneamente in una trappola ionica. Oggigiorno è considerato un esempio per lo più di importanza storica e non pratica, perché per far sì che lo scambio dell'informazione con lo **SWAP-gate** avvenga è necessario partire con un sistema senza fononi, cosa che è raggiunta senza non poche difficoltà raffreddandolo con dei laser.

Sarebbe decisamente più conveniente poter lavorare con dei gate che funzionino con un numero arbitrario di fononi. Questo è il caso del seguente esempio.

## 6.6.2 Mølmer-Sørensen gate

Non entriamo nel dettaglio della discussione di questo gate, tuttavia ci limitiamo a notare che si tratta di un'altra situazione in cui si necessita risolvere un ingegnoso esercizio in QM. L'idea peculiare è quella di considerare un laser bicromatico (irradia con 2 frequenze differenti) che possa indirizzare 2 o più ioni simultaneamente, i quali possono avere stati intermedi con  $n - 1$ ,  $n$  e  $n + 1$  fononi. Denotando come al solito con  $|e\rangle, |g\rangle$  gli stati

del qubit e con  $|n\rangle$  i modi vibrazionali dei fononi, facciamo riferimento alla Figura 6.9a. Supponiamo che esistano alcuni stati intermedi tra  $|ggn\rangle$  e  $|een\rangle$ : è possibile utilizzare un laser con una frequenza leggermente desintonizzata di un fattore  $\delta$  per mandare lo stato  $|ggn\rangle$  alla sovrapposizione di stati immediatamente prima di  $|eg n+1\rangle$ ; successivamente si sceglie la seconda frequenza del laser bicromatico in maniera tale che permetta poi la transizione fino a  $|een\rangle$  (vedi frecce rosse). Ovviamente la stessa cosa può essere fatta invertendo le frequenze del laser (vedi frecce blu). Esplicitamente le due frequenze del laser bicromatico sono  $\omega = \omega_q \pm (\omega_z - \delta)$ .

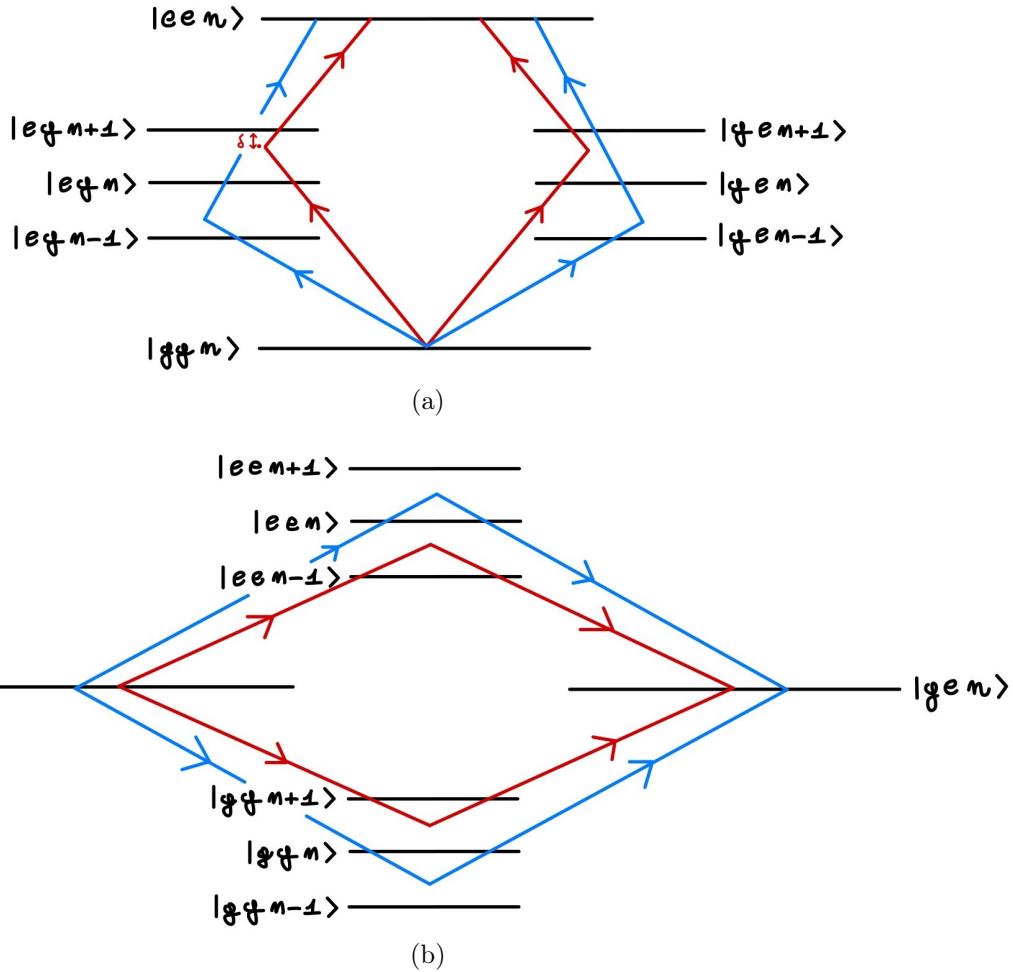


Figura 6.9: (6.9a) Oscillazioni di Rabi che connettono gli stati  $|ggn\rangle \leftrightarrow |een\rangle$  nel Mølmer-Sørensen gate. (6.9b) Caso analogo al precedente in cui sono connessi gli stati  $|egn\rangle \leftrightarrow |gen\rangle$ .

Come mostrato in Figura 6.9b, lo stesso setup può essere utilizzato per connettere gli stati  $|egn\rangle \leftrightarrow |gen\rangle$ : è quindi possibile, in generale, creare oscillazioni di Rabi tra gli stati  $|ggn\rangle \leftrightarrow |een\rangle$  e  $|egn\rangle \leftrightarrow |gen\rangle$ .

Questa tipologia di trasformazioni sono al secondo ordine in teoria delle perturbazioni: gli stati intermedi non sono mai realmente popolati perché per poter effettuare operazioni sui qubit per mezzo delle oscillazioni di Rabi è necessario lavorare alla risonanza. In generale questo non è del tutto ovvio, tuttavia la cosa molto ingegnosa sta nel fatto che le oscillazioni di Rabi risultanti sono del tutto indipendenti dal numero  $n$  di fononi! Dunque non è più necessario raffreddare il sistema.

Per mostrarlo rigorosamente è necessario svolgere un conto completo in teoria delle perturbazioni dipendenti dal tempo. Intuitivamente si può notare che, dato che  $\hat{H}_{\text{int}} \sim (\hat{a} + \hat{a}^\dagger)$ ,

allora negli stati dei modi vibrazionali si possono avere solamente un fonone in più o un fonone in meno rispetto allo stato di partenza, quindi  $|m\rangle = |n+1\rangle$  oppure  $|m\rangle = |n-1\rangle$ ; ciò è dato dal fatto che solamente gli elementi di matrice di questi stati intermedi sono diversi da zero, ossia  $\langle n|\hat{a}|n+1\rangle = \sqrt{n+1}$  e  $\langle n|a^\dagger|n-1\rangle = \sqrt{n}$ . Per questo motivo, un calcolo in teoria delle perturbazioni per campo debole produce un'ampiezza di Rabi indipendente da  $n$ :

$$\text{Ampiezza di Rabi} \sim \sum_m \frac{\langle een|\hat{H}_{\text{int}}|m\rangle \langle m|\hat{H}_{\text{int}}|ggn\rangle}{E_m - E_{ggn} - \omega} \sim \frac{(n+1)}{\delta} + \frac{n}{-\delta} \sim \frac{1}{\delta}.$$

Un conto più completo in approssimazione RWA consente di calcolare esattamente l'operatore di evoluzione temporale che ha la forma

$$\hat{U}(t) \sim e^{\alpha(t)\hat{a} + \alpha^*(t)\hat{a}^\dagger + iS_y^2\beta(t)}, \quad \text{dove } S_y = \sigma_1^{(1)} + \sigma_y^{(2)},$$

dove  $\alpha(t)$  e  $\beta(t)$  sono due funzioni del tempo calcolabili. Scegliendo i valori del tempo che risolvono l'equazione  $\alpha(t) = 0$ , l'operatore di evoluzione temporale diventa indipendente dagli oscillatori associati ai fononi e produce un gate universale che realizza l'entanglement tra due qubit.

LEZIONE 20 - 17/12/2021

## 6.7 Sistemi superconduttori

Dopo aver studiato e analizzato i sistemi a trappola ionica, diamo uno sguardo, in maniera del tutto generale, a un altro modo, molto diffuso e utilizzato, di andare a realizzare sistemi a due livelli: i **sistemi superconduttori**. Spesso vengono anche definiti come **circuiti QED (cQED)** in analogia proprio con le cavità QED (CQED). Negli esempi analizzati nel caso della CQED si sfruttava il fatto che un semplice modello possa essere utilizzato per descrivere l'interazione di un atomo con una cavità ottica oppure anche per spiegare l'accoppiamento di un qubit con un risonatore a microonde: questo modello include il numero di fotoni nella cavità/risonatore, lo stato dell'atomo/qubit e l'interazione del dipolo elettrico tra l'atomo/qubit e la cavità/risonatore.

Invece, come suggerisce il nome, la fisica che sta dietro ai sistemi superconduttori sfrutta il fenomeno della superconduttività. Per una trattazione completa sarebbe richiesto un corso intero, per cui, nel nostro studio, ci limitiamo a riportare i risultati generali che serviranno a descrivere questo tipo di sistemi.

### 6.7.1 Cenni di superconduttività

L'idea alla base della realizzazione fisica dei qubit è abbastanza semplice, tuttavia la fisica che ci sta dietro è abbastanza complessa perché coinvolge il concetto della **superconduttività**. Prima di vedere come si realizza la costruzione dei qubit e dei gate, facciamo alcuni cenni su questo importante argomento.

Che cos'è la superconduttività? In corrispondenza di temperature sufficientemente basse, elementi metallici ed alcuni semiconduttori vanno incontro ad una transizione di fase. Al di sotto di una particolare temperatura, detta temperatura critica  $T_C$ , essi acquistano

notevoli proprietà fisiche; la loro resistività diventa bruscamente nulla, perciò in questi materiali diventa possibile, in assenza di campi esterni, misurare correnti che non decadono nel tempo. L'assenza di effetti dissipativi nel meccanismo di conduzione, assieme ad altri fenomeni correlati, sono indicati sinteticamente con il termine **superconduttività**. Nel 1957 J. Bardeen, L. N. Cooper e J. R. Schrieffer, formularono la prima teoria microscopica della superconduttività (**teoria BCS**) utilizzando la meccanica quantistica, che valse loro il Nobel nel 1972. Tale teoria è in grado di dare una spiegazione del fenomeno della superconduzione (capacità predittiva e base per le applicazioni).

Il fenomeno della superconduttività consiste nella creazione, per mezzo dello scambio di fononi nel metallo e a temperatura sufficientemente bassa, di stati legati costituiti da coppie di elettroni ( $e^-, e^-$ ), chiamate **coppie di Cooper**. Questi oggetti sono ovviamente bosoni e costituiscono un particolare condensato di Bose-Einstein.

In questa configurazione, mentre i fermioni, a causa del principio di esclusione di Pauli, sono disposti in maniera tale da non avere lo stesso set di numeri quantici, i bosoni, a basse temperature, sono tutti situati nello stato fondamentale. In un metallo regolare se gli elettroni vengono messi in moto, tipicamente, per via della presenza di impurezze o reticolati di cristallo con cui gli elettroni fanno scattering, vi è una resistenza. La stessa situazione vale per i bosoni, ma vi è una interazione di scambio: è energicamente favorevole mettere i bosoni nello stesso stato (stesso set di numeri quantici), in particolare nello stato fondamentale perché per spostare uno di questi bosoni è richiesta una grande quantità di energia. La corrente che si viene a originare è un flusso di bosoni, tutti con la stessa velocità e dato che è richiesta energia per rimuovere un bosone dallo stato in cui si trovano tutti gli altri, hanno tutti una bassa resistenza. Un esempio di spettro energetico a basse temperature di un materiale superconduttivo è dato dalla Figura 6.10.

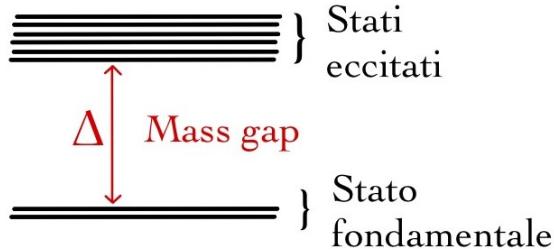


Figura 6.10: Spettro energetico di un materiale superconduttivo. La differenza tra lo stato fondamentale e gli stati eccitati è noto come **mass gap**  $\Delta$ .

### 6.7.2 cQED

L'idea è quella di realizzare dei qubit con dei piccoli circuiti superconduttori (non si tratta più di un sistema atomico o di spin). Un tale sistema sembrerebbe a prima vista macroscopico, tuttavia, come vedremo, grazie alla presenza del fenomeno della superconduttività è davvero quantistico.

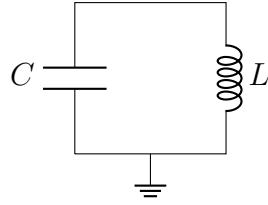


Figura 6.11: Circuito LC.

Ancora una volta si utilizza un oscillatore armonico: affinché si possa utilizzare come un sistema a due livelli è necessario introdurre dell'anarmonicità nei livelli energetici così da poter distinguere lo stato fondamentale dal primo eccitato senza preoccuparsi degli altri livelli. Il nostro punto di partenza è un semplice **circuito LC**, come mostrato in Figura 6.11.

Vediamo il motivo per cui un tale circuito presenta un comportamento oscillatorio. Innanzitutto, ricordiamo che ciascun elemento mette in relazione la carica o la corrente con il potenziale; in particolare le relazioni costitutive della capacità e dell'induttanza risultano:

$$\begin{array}{ll} \text{Capacità:} & Q = CV, \\ \text{Induttanza:} & V = L \frac{dI}{dt}. \end{array}$$

Per svolgere questo tipo di trattazione può tornare utile riscrivere la corrente come  $I = \frac{dQ}{dt}$  e introdurre il *flusso* definito come

$$\Phi(t) = \int_{-\infty}^t dt' V(t');$$

a questo punto, la relazione sull'induttanza può, ad esempio, essere riscritta in termini di flusso integrando entrambi i membri

$$\Phi = LI.$$

Note le relazioni tra carica/corrente e potenziale, possiamo andare a valutare le energie associate a ciascun elemento del circuito. A partire da

$$E(t) = \int_{-\infty}^t dt' V(t') I(t') \quad (\text{da } \delta E = V \delta Q), \quad (6.7.1)$$

assumendo che tutte le quantità in gioco si annullino a  $t = -\infty$ , ricaviamo

$$\begin{array}{ll} \text{Capacità:} & E = \int_{-\infty}^t dt' V C \frac{dV}{dt'} = \frac{C}{2} V^2 = \frac{Q^2}{2C}, \\ \text{Induttanza:} & E = \int_{-\infty}^t dt' L \frac{dI}{dt'} I = \frac{L}{2} I^2 \equiv \frac{\Phi^2}{2L}. \end{array}$$

In una trattazione classica possiamo interpretare il termine relativo alla capacità come un'**energia cinetica** mentre quello relativo all'induttanza come **energia potenziale**. In questo contesto possiamo andare a scrivere la lagrangiana classica del sistema nel seguente modo

$$\mathcal{L} = E_k - E_p = \frac{Q^2}{2C} - \frac{\Phi^2}{2L} = \frac{C}{2} V^2 - \frac{\Phi^2}{2L} = \frac{C}{2} \dot{\Phi}^2 - \frac{\Phi^2}{2L},$$

dove abbiamo inserito il fatto che  $V = \frac{d\Phi}{dt}$ . Applicando le equazioni di Eulero-Lagrange

$$\frac{d}{dt} \left( \frac{\partial \mathcal{L}}{\partial \dot{\Phi}} \right) - \frac{\partial \mathcal{L}}{\partial \Phi} = 0,$$

si ottiene l'equazione del moto

$$C\ddot{\Phi} + \frac{\Phi}{L} = 0,$$

che possiamo riscrivere sotto forma di equazione del moto di un oscillatore armonico nel seguente modo

$$\ddot{\Phi} + \omega^2 \Phi = 0, \quad \text{con} \quad \omega = \frac{1}{\sqrt{LC}}.$$

Per passare ad una descrizione quantistica del sistema dobbiamo riscrivere la fisica nel formalismo hamiltoniano. Calcoliamo il *momento coniugato*

$$\Pi = \frac{\delta \mathcal{L}}{\delta \dot{\Phi}} = C\dot{\Phi} = CV = Q,$$

cosicché possiamo calcolarci la *trasformata di Legendre* della lagrangiana precedente

$$H = \Pi \dot{\Phi} - \mathcal{L} = Q \frac{Q}{C} - \left( \frac{Q^2}{2C} - \frac{\Phi^2}{2L} \right) = \frac{Q^2}{2C} + \frac{\Phi^2}{2L}; \quad (6.7.2)$$

è evidente che l'hamiltoniana corrisponde proprio alla somma dell'energia cinetica e dell'energia potenziale.

Supponiamo ora di considerare il medesimo sistema, ma di volerne dare una descrizione quantistica. In Tabella 6.1 sono riportate le relative identificazioni con il nuovo sistema quantistico.

Oscillatore armonico	Circuito LC
$H = \frac{\hat{p}^2}{2m} + \frac{m\omega^2}{2}\hat{x}^2$	$H = \frac{Q^2}{2C} + \frac{C\omega^2}{2}\Phi^2$
$\hat{x}$	$\Phi$
$\hat{p}$	$Q$
$m$	$C$

Tabella 6.1: Identificazioni tra quantità fisiche e operatori dell'oscillatore armonico quantistico e le grandezze fisiche di un circuito LC. Si ricordi che per il circuito LC la frequenza è  $\omega = \frac{1}{\sqrt{LC}}$ .

Possiamo quindi mappare un circuito LC con un oscillatore armonico e imporre la quantizzazione canonica per quantizzare un tale sistema. Possiamo promuovere  $(\Phi, Q) \rightarrow (\hat{\Phi}, \hat{Q})$  ad operatori e scriverli in funzioni degli operatori di creazione e distruzione

$$\hat{\Phi} = \sqrt{\frac{\hbar}{2C\omega}} (\hat{a} + \hat{a}^\dagger), \quad \hat{Q} = \frac{\sqrt{2C\omega\hbar}}{2i} (\hat{a} - \hat{a}^\dagger); \quad (6.7.3)$$

in questo modo imponiamo le seguenti regole di commutazione

$$[\hat{\Phi}, \hat{Q}] = i\hbar, \quad \Leftrightarrow \quad [\hat{a}, \hat{a}^\dagger] = 1.$$

È dunque evidente che la procedura di quantizzazione è immediata, tuttavia è abbastanza insolito pensare di svolgere una trattazione quantistica di un sistema macroscopico. Se supponiamo invece di considerare un sistema superconduttivo, possiamo utilizzare alcuni risultati della teoria BCS per riscrivere l'hamiltoniana della relazione (6.7.2) nel seguente modo

$$\hat{H} = 4E_C \hat{n}^2 + \frac{E_L}{2} \hat{\phi}^2, \quad \text{con} \quad \hbar\omega = \sqrt{8E_L E_C}, \quad (6.7.4)$$

dove

- $\hat{n} = \frac{Q}{2e}$  è l'operatore che indica il numero di coppie di Cooper;
- $\hat{\phi} = \frac{2\pi}{\Phi_0} \Phi$  è l'operatore del flusso ridotto ( $\Phi_0 = \frac{h}{2e}$  è il *quanto di flusso*);
- $E_C = \frac{e^2}{2C}$  è l'energia necessaria per aggiungere un elettrone extra alla capacità del circuito;
- $E_L = \left(\frac{\Phi_0}{2\pi}\right)^2 \frac{1}{L}$  è l'energia associata all'induttanza.

L'altro fatto fondamentale, accanto all'utilizzo di materiali superconduttori, che rende il sistema adatto ad una descrizione quantistica è che in realtà non andiamo a utilizzare un circuito LC generico (il quale presenta infiniti livelli energetici equidistanti), ma uno in cui si introduce una cosiddetta **giunzione Josephson** (Figura 6.12a). Quest'ultima produce il cosiddetto **effetto Josephson** (Figura 6.12b), introducendo quindi dell'anarmonicità.

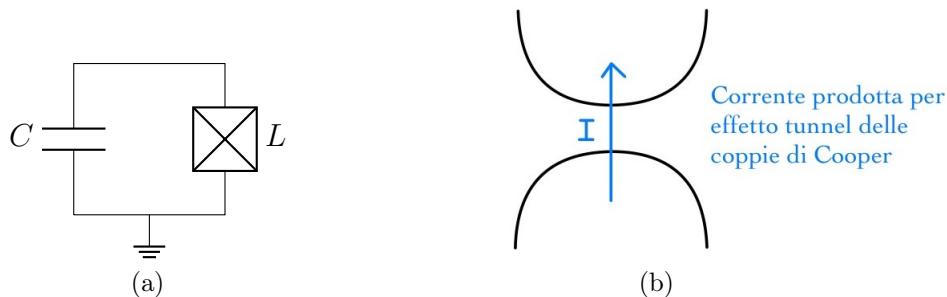


Figura 6.12: (6.12a) Circuito LC con giunzione Josephson (la giunzione è caratterizzata da una propria capacità  $C_J$  e induttanza  $L_J$ ). D'ora in avanti indicheremo nei circuiti una giunzione Josephson con la notazione di questo circuito. (6.12b) Effetto tunnel della coppia di Cooper tra due elettrodi metallici superconduttori sufficientemente vicini e separati da una sottile barriera di ossido.

L'effetto Josephson può essere riassunto nei seguenti due risultati:

1. La corrente prodotta per effetto tunnel delle coppie di Cooper segue la **prima legge di Josephson**

$$I = I_C \sin \phi, \quad (6.7.5)$$

dove  $I_C$  è detta **corrente critica**;

2. Applicando una differenza di potenziale ai capi degli elettrodi scorrerà un'altra corrente, la quale segue la **seconda legge di Josephson**

$$V = \frac{d\Phi}{dt} = \frac{\hbar}{2e} \frac{d\phi}{dt}. \quad (6.7.6)$$

Se si costruisce un circuito LC inserendo questa giunzione è possibile ricalcolare l'energia potenziale associata al circuito sfruttando la relazione in (6.7.1)

$$E = \int_{-\infty}^t dt' V(t') I(t') = \frac{\hbar}{2e} I_C \int_{-\infty}^t dt' \frac{d\phi}{dt'} \sin \phi = -E_J \cos \phi, \quad (6.7.7)$$

dove abbiamo indicato l'**energia Josephson** con  $E_J = \frac{\hbar I_C}{2e}$ . In questo modo l'hamiltoniana di un sistema di questo tipo risulta in

$$\hat{H} = 4E_C \hat{n}^2 - E_J \cos \hat{\phi}, \quad (6.7.8)$$

che differisce dalla (6.7.4) per la presenza di un potenziale periodico anarmonico. In Figura 6.13 si può osservare lo spettro energetico dell'hamiltoniana che descrive un circuito LC con giunzione Josephson. L'obiettivo è quello di utilizzare per la costruzione di un qubit i livelli energetici evidenziati in figura: il punto fondamentale è stato l'introduzione della giunzione Josephson, la quale non solo rende il sistema veramente quantistico, ma soprattutto introduce dell'anarmonicità nello spettro dell'oscillatore.

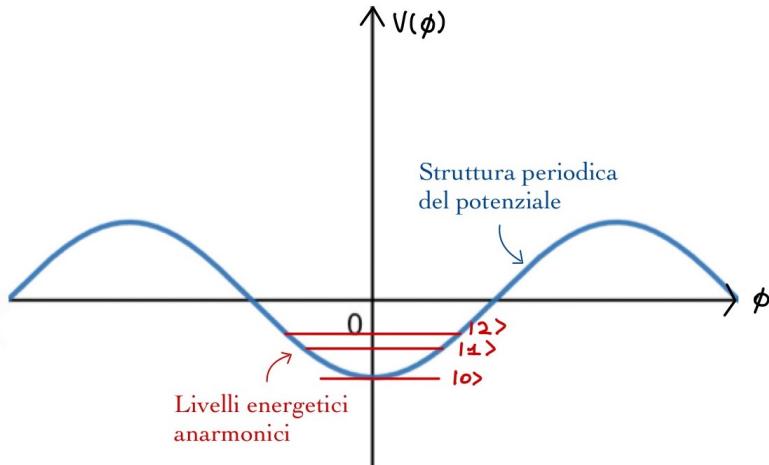


Figura 6.13: Spettro energetico dell'hamiltoniana in (6.7.8). Per piccoli  $\phi$  possiamo approssimare lo spettro come dei livelli energetici dell'oscillatore armonico più piccole correzioni anarmoniche.

### 6.7.3 Interpretazione dell'effetto Josephson

Per parlare in maniera del tutto completa ed esaustiva dell'effetto Josephson sarebbe necessaria una lezione completa, pertanto per approfondimenti e chiarimenti rimandiamo a corsi sulla supercondutività.

L'idea che seguiamo è quella di procedere attraverso una trattazione schematica dell'effetto Josephson dovuta a Feynman. Il punto di partenza è la differenza nello spettro energetico che c'è tra un metallo normale, dove possiamo avere bande che sono riempite da un mare di elettroni (Figura 6.14a) e un superconduttore, in cui vi è una netta separazione tra lo stato fondamentale e gli stati eccitati (Figura 6.14b).

Nel momento in cui andiamo a considerare una giunzione metallica come in basso in Figura 6.14a, costituita da due elettrodi ciascuno con il proprio mare di elettroni riempito fino all'energia di Fermi  $\varepsilon_F$ , e supponiamo che tra i due vi sia una differenza di potenziale  $V$ , allora possiamo osservare una corrente  $I$  che scorre tra i due terminali dovuta al fatto

che gli elettronni possano fare tunneling da un elettrodo a un altro. Questa corrente  $I$  sarà proporzionale alla tensione applicata  $V$  e il coefficiente di proporzionalità è dato dall'inverso della resistenza  $R$  del sistema. Supponiamo invece di considerare due metalli superconduttori, che indichiamo con (L) left e (R) right, ciascuno caratterizzato da un mass-gap  $\Delta$ : a basse temperature, dove la fisica della supercondutività è rilevante, quello che succede è che gli stati fondamentali di entrambi saranno occupati da un certo numero di coppie di Cooper  $N_L$  e  $N_R$ ; in tale situazione il tunneling è dovuto alle coppie di Cooper, da sinistra verso destra e viceversa.

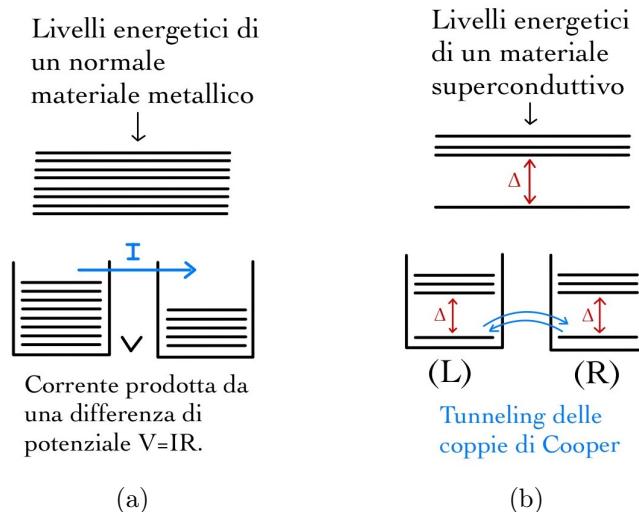


Figura 6.14: (6.14a) Livelli energetici di un metallo caratterizzato da un mare di elettronni e sistema di due elettrodi in cui avviene il fenomeno del tunneling di elettronni da un elettrodo all'altro. (6.14b) Livelli energetici di un metallo superconduttivo caratterizzato, a basse temperature, da uno stato fondamentale in cui si trovano tutte le coppie di Cooper e i livelli eccitati separati da un mass-gap  $\Delta$  e sistema di due elettrodi superconduttori in cui avviene il fenomeno del tunneling di coppie di Cooper da un elettrodo all'altro.

Dal punto di vista della QM, se la temperatura è sufficientemente bassa a tal punto da non considerare gli stati eccitati, ciò che conta è il numero quantico che identifica quanti bosoni sono nello stato fondamentale. Nel nostro caso, il sistema dei due elettrodi superconduttori è descritto da due interi  $N_L$  e  $N_R$  (numero di coppie di Cooper nello stato fondamentale presenti rispettivamente nell'elettrodo di sinistra e nell'elettrodo di destra). Passare da un elettrodo all'altro significa quindi andare a incrementare e diminuire il numero di bosoni di entrambi gli elettrodi: ad esempio

$$\text{Tunneling di un bosone da : } |N_L, N_R\rangle \longrightarrow |N_L - 1, N_R + 1\rangle$$

Dal momento che il numero totale di bosoni dei due elettrodi è fissato, è sufficiente analizzare solamente uno di questi due numeri, ad esempio  $N_L$  e lo andiamo a identificare con  $m$  e il corrispondente stato con  $|m\rangle$ , cioè il numero di coppie di Cooper nel primo metallo. L'idea di Feynman è quella di andare a modellizzare il tunneling tramite un'hamiltoniana di interazione che non è altro che una matrice  $2 \times 2$ :

$$\hat{H} = -\frac{E_J}{2} \sum_m \left( \underbrace{|m\rangle\langle m+1|}_{\substack{\text{Operatore che} \\ \text{riduce il numero} \\ \text{di coppie} \\ \text{di Cooper.}}} + \underbrace{|m+1\rangle\langle m|}_{\substack{\text{Operatore che} \\ \text{incrementa il} \\ \text{numero di coppie} \\ \text{di Cooper.}}} \right).$$

Questa hamiltoniana è caratterizzata da due operatori che non fanno altro che eseguire il tunneling di una coppia di Cooper da un metallo superconduttivo all'altro. Da questa definizione si possono ottenere vari risultati che ci limitiamo a citare, ma che possono essere verificati con semplici conti di QM:

1. Gli autostati dell'hamiltoniana precedente sono del tipo

$$|\varphi\rangle = \sum_{m=-\infty}^{+\infty} e^{im\varphi} |m\rangle , \quad \text{con } \varphi \in [0, 2\pi) ,$$

e gli autovalori sono dati dall'energia nella (6.7.7)

$$\hat{H} |\varphi\rangle = -E_J \cos \varphi |\varphi\rangle ,$$

dove si vede che il flusso ridotto  $\phi$  può essere identificato con la fase  $\varphi$  degli autostati.

2. Definendo un operatore numero  $\hat{n}$  che indica il numero di coppie di Cooper trasferite attraverso la giunzione

$$\hat{n} = \sum_m m |m\rangle \langle m| ,$$

cioè tale che

$$\hat{n} |m\rangle = m |m\rangle ;$$

e definendo inoltre un operatore corrente  $\hat{I}$  tale che

$$\hat{I} = 2e \frac{d\hat{n}}{dt} = \frac{2ie}{\hbar} [\hat{H}, \hat{n}] - i \frac{e}{\hbar} E_J \sum_m |m\rangle \langle m+1| - |m+1\rangle \langle m| ,$$

allora è possibile ottenere la prima legge di Josephson della (6.7.5)

$$\hat{I} |\varphi\rangle = \underbrace{\frac{2eE_J}{\hbar}}_{I_C} \sin \varphi |\varphi\rangle = I_C \sin \varphi |\varphi\rangle .$$

3. Cosa succede quando si applica una differenza di potenziale tra gli elettrodi dei metalli? Pensiamo alla situazione in cui un campo elettrico esterno viene applicato e mantenuto in modo tale che vi sia una caduta di tensione fissa  $V$  attraverso il tunnel della giunzione. Questo modifica l'hamiltoniana nel seguente modo

$$\hat{H} \longrightarrow \hat{H} - (2e)V\hat{n} ;$$

si tratta di un esercizio di QM dimostrare che l'evoluzione temporale dello stato a seguito dell'equazione di Schrödinger non è altro che

$$|\psi(t)\rangle = \exp \left\{ \frac{i}{\hbar} E_J \int_0^t d\tau \cos \left( \varphi(0) + \frac{2e}{\hbar} V\tau \right) \right\} \left| \varphi_0 + \frac{2e}{\hbar} Vt \right\rangle .$$

Dunque partendo al tempo  $t = 0$  dallo stato  $|\psi(0)\rangle = |\varphi_0\rangle$ , allora al tempo  $t$  si ottiene una fase globale e lo stato evolve linearmente nel tempo risultando shiftato di  $\varphi_0 \rightarrow \varphi_0 + \frac{2eV}{\hbar} t$ . Questo significa che riotteniamo la seconda legge di Josephson della (6.7.6) usando ancora  $\varphi = \phi$

$$\frac{d\phi}{dt} = \frac{2eV}{\hbar} , \quad \Rightarrow \quad V = \frac{\hbar}{2e} \frac{d\phi}{dt} .$$

Per riassumere, ciò di cui abbiamo bisogno sono le seguenti informazioni: la natura quantistica del sistema è data dallo stato fondamentale, il quale è l'unico che importa nella supercondutività; la corrente che si origina è dovuta al tunneling delle coppie di Cooper, le quali sono frutto di una particolare condensazione di bosoni; l'oscillatore risultante è quantistico, ma non armonico perché l'hamiltoniana associata è data dalla relazione (6.7.8).

### 6.7.4 Transmon qubit

Discutiamo come codificare un qubit in un circuito come quello di Figura 6.12b. Tra tutte le varie tipologie di qubit superconduttori, quello più popolare e largamente utilizzato è il regime del cosiddetto **transmon qubit**. Consideriamo l'hamiltoniana ottenuta in (6.7.8) a cui aggiungiamo un termine costante  $E_J$  (questo porta a una variazione nei livelli energetici, ma non sulla dinamica del sistema)

$$\hat{H} = 4E_C \hat{n}^2 + E_J(1 - \cos \hat{\phi}) .$$

I transmon qubit si hanno nel limite in cui  $E_J/E_C \gg 1$ , ossia quando  $\phi \sim 0$ . Questo limite ci permette di sviluppare il potenziale attraverso un'espansione con il polinomio di Taylor

$$\hat{V}(\hat{\phi}) = E_J(1 - \cos \hat{\phi}) = \frac{E_J}{2!} \hat{\phi}^2 - \frac{E_J}{4!} \hat{\phi}^4 + \frac{E_J}{6!} \hat{\phi}^6 + \mathcal{O}(\hat{\phi}^8) ;$$

si noti che il primo termine genera il potenziale armonico. Per capire il peso relativo di ciascun termine è utile normalizzare il primo introducendo il cambio di variabili  $\hat{x} = \sqrt{E_J} \hat{\phi}$ :

$$\hat{V}(\hat{\phi}) = \frac{\hat{x}^2}{2} - \frac{\hat{x}^4}{4!E_J} + \frac{\hat{x}^6}{6!E_J^2} + \mathcal{O}(\hat{x}^8) ;$$

i vari termini sono soppressi da potenze di  $E_J$ . Se tronchiamo l'espansione al termine di ordine  $\hat{x}^4$ , l'hamiltoniana del transmon qubit risultante sarà

$$\hat{H} = \underbrace{4E_C \hat{n}^2}_{\hat{H}_0} + \underbrace{\frac{E_J \hat{\phi}^2}{2}}_{\text{correzione}} - \underbrace{\frac{E_J \hat{\phi}^4}{24}}_{\text{correzione}}, \quad (6.7.9)$$

dove si è indicato con  $\hat{H}_0$  la corrispondente hamiltoniana di oscillatore armonico. In Figura 6.15 sono riportate le differenze nello spettro di un oscillatore armonico (Figura 6.15a) e un oscillatore anarmonico con **accoppiamento quartico** (Figura 6.15b), dovuto al termine chiamato *correzione*.

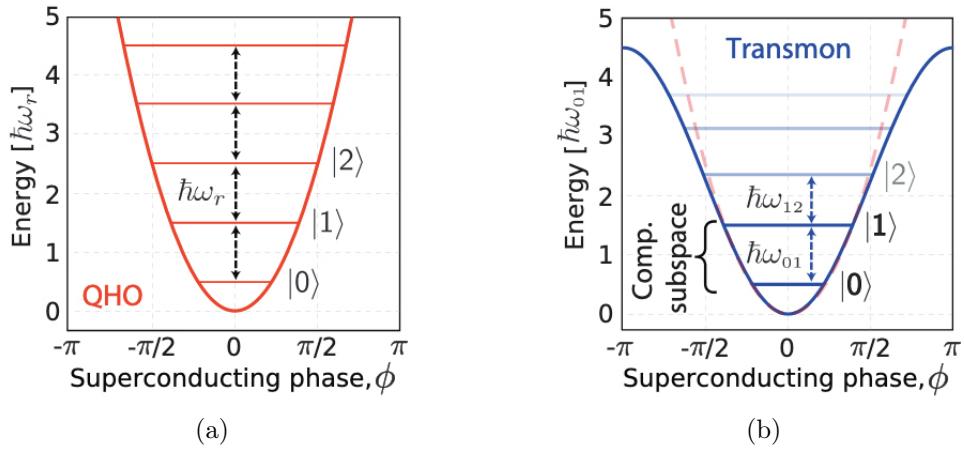


Figura 6.15: (6.15a) Spettro energetico del QHO, dove i livelli di energia sono equidistanti l’uno dall’altro. (6.15b) La giunzione Josephson rimodella il potenziale energetico quadratico (tratteggiato in rosso) in sinusoidale (blu fisso), il quale non presenta più livelli energetici equispaziati. Si noti che questo potenziale è una buona approssimazione solamente nel limite  $\phi \simeq 0$ .

In questa nuova configurazione gli autovalori non sono più equidistanziati: in Figura 6.16 possiamo notare che gli stati  $|0\rangle$  e  $|1\rangle$  sono separati da un’energia  $\hbar\omega$ , mentre gli stati  $|1\rangle$  e  $|2\rangle$  da un’energia  $\hbar\omega + \alpha$  con  $\alpha < 0$ . (Si veda la discussione che segue per capire perché in figura è indicata la frequenza “ $\tilde{\omega}$ ”, non “ $\omega$ ”).

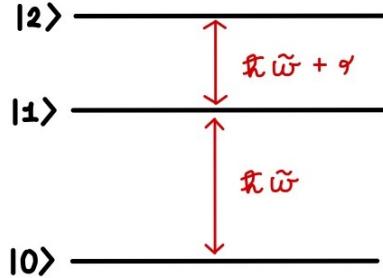


Figura 6.16: Differenza energetica tra i livelli  $|0\rangle$ ,  $|1\rangle$  e  $|2\rangle$ .

Se  $\hbar\omega$  è ragionevolmente grande possiamo pensare di utilizzare gli stati  $|0\rangle$  e  $|1\rangle$  per codificare il qubit e usare degli impulsi laser esterni di frequenza  $\sim \omega$  per mandare solamente  $|0\rangle \leftrightarrow |1\rangle$ , dato che questi livelli non sono in risonanza con tutti gli altri. In particolare, nel caso dei transmon qubit, si lavora con  $\omega \sim 3 - 4$  GHz mentre  $\alpha \sim 300$  MHz, quindi  $E_J/E_C \sim 40$ . Tuttavia, a volte, per misure di precisione, si necessita l’utilizzo del livello  $|2\rangle$ , quindi non lo si tiene molto distante energeticamente dagli altri livelli.

Per vedere esplicitamente come avviene la codifica del qubit, usiamo la definizione di  $\hat{\phi}$  e esplicitiamo gli oscillatori delle relazioni (6.7.3)

$$\hat{\phi} = \frac{2\pi}{\Phi_0}\Phi = \frac{2e}{\hbar}\Phi = \frac{2e}{\hbar}\sqrt{\frac{\hbar}{2C\omega}}(\hat{a} + \hat{a}^\dagger) = 2\left(\frac{E_C}{8E_J}\right)^{\frac{1}{4}}(\hat{a} + \hat{a}^\dagger);$$

(abbiamo utilizzato le definizioni di  $E_C$  e  $E_J$ ). Inserendo questo risultato all'interno dell'hamiltoniana in (6.7.9) otteniamo

$$\hat{H} = \underbrace{\hbar\omega \left( \hat{a}^\dagger \hat{a} + \frac{1}{2} \right)}_{\hat{H}_0} - \frac{E_C}{12} (\hat{a} + \hat{a}^\dagger)^4. \quad (6.7.10)$$

Questa è un'hamiltoniana di un oscillatore anarmonico con potenziale quartico che non presenta alcuna soluzione analitica. Come al solito, per semplificare la situazione, consideriamo l'hamiltoniana libera, ci mettiamo in un sistema ruotato e teniamo solamente i termini dell'interazione che evolvono lentamente nel tempo. L'operatore che effettua la rotazione è quindi

$$\hat{U} = e^{i\hat{H}_0 t},$$

che applicato agli operatori di creazione e distruzione genera una fase dipendente dal tempo (si vedano le relazioni in (6.5.7))

$$\hat{a} \longrightarrow e^{-i\omega t} \hat{a} \quad \hat{a}^\dagger \longrightarrow e^{i\omega t} \hat{a}^\dagger.$$

Questo significa che tutti i termini che hanno un differente numero di  $\hat{a}$  e  $\hat{a}^\dagger$  in  $(\hat{a} + \hat{a}^\dagger)^4$  sono mediamente nulli; soltanto i termini con un ugual numero sopravvivono, ovvero

$$(\hat{a} + \hat{a}^\dagger)^4 = \hat{a}\hat{a}\hat{a}^\dagger\hat{a}^\dagger + \hat{a}\hat{a}^\dagger\hat{a}\hat{a}^\dagger + \hat{a}\hat{a}^\dagger\hat{a}^\dagger\hat{a} + \hat{a}^\dagger\hat{a}^\dagger\hat{a}\hat{a} + \hat{a}^\dagger\hat{a}\hat{a}\hat{a}^\dagger + \hat{a}^\dagger\hat{a}^\dagger\hat{a}\hat{a};$$

ricordando che  $[\hat{a}, \hat{a}^\dagger] = 1$  possiamo portare tutti gli  $\hat{a}^\dagger$  sulla sinistra e scrivere i termini in *normal ordering*

$$(\hat{a} + \hat{a}^\dagger)^4 = c_1 \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} + c_2 \hat{a}^\dagger \hat{a} + c_3,$$

dove  $c_1 = 6$ ,  $c_2 = 12$  e  $c_3 = 3$ . Nella nostra trattazione non consideriamo  $c_3$  perché comporta solamente una ridefinizione dell'energia di punto zero; il fatto che  $c_2$  sia uguale a 12, come vedremo ora, è importante. Tenendo conto di questo risultato e non considerando i termini costanti, l'hamiltoniana in (6.7.10) si scrive

$$\begin{aligned} \hat{H} &= \hbar\omega \hat{a}^\dagger \hat{a} - \frac{E_C}{2} \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} - E_C \hat{a}^\dagger \hat{a} \\ \Rightarrow \quad \hat{H} &= \hbar\tilde{\omega} \hat{a}^\dagger \hat{a} + \frac{\alpha}{2} \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a}, \end{aligned} \quad (6.7.11)$$

dove abbiamo posto  $\hbar\tilde{\omega} = \hbar\omega - E_C$  lo shift in frequenza del qubit e  $\alpha = -E_C$  l'energia del termine quartico. Ricordando come al solito l'azione di  $\hat{a}$  e  $\hat{a}^\dagger$  su  $|n\rangle$  dalle relazioni in (6.2.6), questa nuova hamiltoniana presenta i seguenti livelli energetici

$$\begin{aligned} \hat{H} |0\rangle &= 0, \\ \hat{H} |1\rangle &= \hbar\tilde{\omega} |1\rangle, \\ \hat{H} |2\rangle &= (2\hbar\tilde{\omega} + \alpha) |2\rangle; \end{aligned}$$

è evidente quindi, come nella Figura 6.16, che  $E_1 - E_0 = \hbar\tilde{\omega}$  e  $E_2 - E_1 = \hbar\tilde{\omega} + \alpha$ . Si noti, in particolare, che  $|2\rangle$  è ancora autostato, infatti

$$\begin{aligned} \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} |2\rangle &= \hat{a}^\dagger \hat{a}^\dagger \hat{a} \sqrt{2} |1\rangle = \hat{a}^\dagger \hat{a}^\dagger \sqrt{1} \sqrt{2} |0\rangle \\ &= \hat{a}^\dagger \sqrt{1} \sqrt{1} \sqrt{2} |1\rangle = \sqrt{2} \sqrt{1} \sqrt{1} \sqrt{2} |2\rangle = 2 |2\rangle. \end{aligned}$$

Vediamo alcune grandezze tipiche: se il rapporto  $E_J/E_C \sim 40$  e  $\hbar\omega = \sqrt{8E_C E_J} \sim 10E_C$  allora la differenza energetica  $\alpha$  è circa del 10%.

Ricapitolando, per codificare il qubit l'idea è quella di considerare gli stati  $|0\rangle$  e  $|1\rangle$  e trascurare  $|2\rangle$  (se non utilizzarlo per le considerazioni viste precedentemente). Consideriamo i seguenti stati

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

allora in forma matriciale

$$\hat{a}^\dagger \hat{a} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = -\frac{\hat{\sigma}_3}{2} + \frac{\mathbb{I}}{2};$$

trascurando nuovamente il termine costante si ottiene l'hamiltoniana standard di un sistema a due livelli:

$$\hat{H} = -\frac{\hbar}{2}\tilde{\omega}\hat{\sigma}_3. \quad (6.7.12)$$

Il termine quartico  $\hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a}$  è nullo su  $|0\rangle$  e  $|1\rangle$ , ma è necessario tenerlo in considerazione quando si vuole includere correzioni dovute allo stato eccitato  $|2\rangle$ . In un contesto di oscillatore armonico lo spazio di Hilbert considera solamente

$$\begin{aligned} \hat{a}|0\rangle &= 0 & \hat{a}^\dagger|0\rangle &= |1\rangle \\ \hat{a}|1\rangle &= |0\rangle & \hat{a}^\dagger|1\rangle &= \sqrt{2}|2\rangle \stackrel{!}{=} 0, \end{aligned}$$

perché nell'ultimo caso abbiamo troncato lo spazio di Hilbert. Le definizioni matriciali degli operatori di creazione e distruzione possono essere facilmente dedotte dalla forma vettoriale di  $|0\rangle$  e  $|1\rangle$ :

$$\hat{a} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \equiv \hat{\sigma}_+, \quad \hat{a}^\dagger = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \equiv \hat{\sigma}_- \quad (6.7.13)$$

In maniera del tutto simile possiamo anche notare che

$$\hat{\sigma}_1 = (\hat{a} + \hat{a}^\dagger), \quad \hat{\sigma}_2 = -i(\hat{a} - \hat{a}^\dagger). \quad (6.7.14)$$

Precisiamo che vi sono altre tipologie di transmon qubit: ad esempio, molto diffusi, sono quelli in cui si aggiungono nel circuito di Figura 6.12b due giunzioni Josephson in maniera tale che  $\tilde{\omega}$  possa essere regolata sperimentalmente mediante una variazione di un flusso magnetico esterno  $\phi_e$ . Una rappresentazione schematica di questo tipo di qubit è data dalla Figura 6.17.

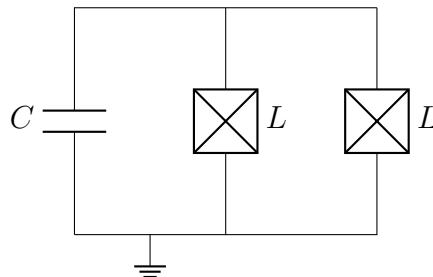


Figura 6.17: Transmon qubit caratterizzato da due giunzioni Josephson. La frequenza del qubit è regolata attraverso la variazione di un campo magnetico esterno  $\phi_e$ .

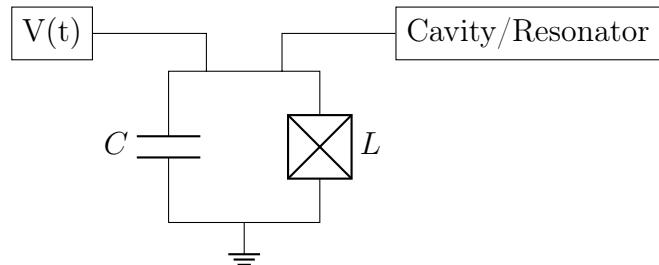
LEZIONE 21 - 20/12/2021

Vediamo alcuni esempi di gate che possono essere realizzati a partire da sistemi superconduttori. Prima di farlo, riassumiamo velocemente i risultati ottenuti nel corso di questa Sezione.

L'idea è quella di codificare un qubit nei livelli energetici ( $|0\rangle$ ,  $|1\rangle$ ) di un circuito superconduttivo che presenta una giunzione Josephson (Figura 6.12b): quest'ultima permette di dare una descrizione quantistica al sistema e introduce dell'anarmonicità nello spettro energetico (vedi Figura 6.16); l'hamiltoniana del sistema risultante è riportata nella (6.7.11). Trascurando il livello energetico  $|2\rangle$  ci si riduce alla nota all'hamiltoniana in (6.7.12), tipica di un sistema a due livelli; la rappresentazione matriciale degli operatori sugli stati del sistema è riportata nelle relazioni in (6.7.13) e (6.7.14).

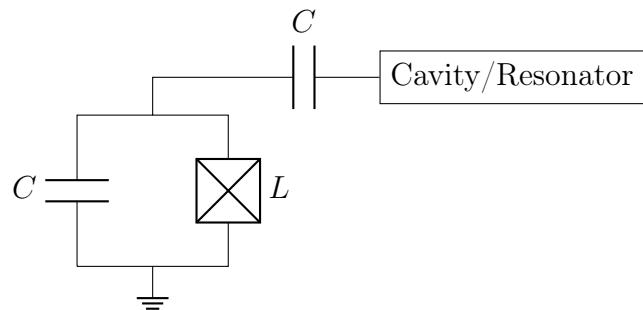
Vediamo come possiamo esplicitamente realizzare su un sistema superconduttivo le tipiche operazioni di un qubit: *misura del sistema*, *codifica di gate agenti su singoli qubit con le oscillazioni di Rabi* e *codifica di gate agenti su più qubit*.

Per effettuare questo tipo di operazioni è necessario in generale applicare al circuito dei segnali esterni  $V(t)$  (tipicamente dell'ordine del GHz) e dei risonatori del tipo CQED, come nel circuito seguente



### Misura su un qubit

Supponiamo ad esempio di partire con un transmon qubit di frequenza  $\omega_q$ : una tipica misurazione viene effettuata con un risonatore di frequenza  $\omega_r$  in un apparato della forma seguente



Dato che la fisica del qubit risulta in questo caso accoppiata alla CQED, sappiamo che l'hamiltoniana del sistema risultante è descritta dall'hamiltoniana di Jaynes-Cummings in (6.5.8)

$$\hat{H} = -\frac{\omega_q}{2}\hat{\sigma}_3 + \omega_r \left( \hat{a}_r^\dagger \hat{a}_r + \frac{1}{2} \right) + g (\hat{a}_r \hat{\sigma}_+ + \hat{a}_r^\dagger \hat{\sigma}_-) ;$$

come già visto nella Sezione 6.5, la misura può essere effettuata nel regime dispersivo dove  $\frac{g}{\Delta} \ll 1$  ( $\Delta = \omega_q - \omega_r$ ): in tal caso l'hamiltoniana precedente viene modificata in

$$\hat{H} = -\frac{\tilde{\omega}_q}{2}\hat{\sigma}_3 + (\omega_r - \chi\hat{\sigma}_3)\hat{a}_r^\dagger\hat{a}_r, \quad (6.7.15)$$

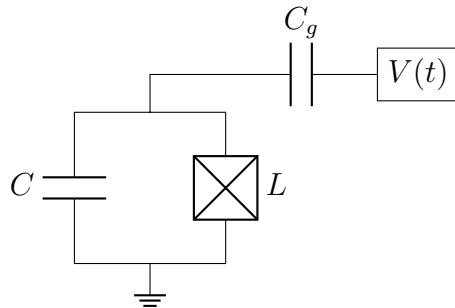
dove la frequenza del qubit è shiftata in  $\tilde{\omega}_q$  a seguito del **Lamb shift** e  $\chi = \frac{g^2}{\Delta}$ . Cosa succede nel caso di un qubit superconduttivo? Nell'approssimazione che abbiamo considerato si trascurava il livello energetico  $|2\rangle$ : dato che il suo peso relativo rispetto a  $\hbar\tilde{\omega}_q$  è del 10% circa, per svolgere una trattazione più precisa e completa è necessario considerare l'intera hamiltoniana in (6.7.11) accoppiata alla CQED. L'inclusione di queste correzioni si traduce nella seguente modifica di  $\chi$

$$\chi = \frac{g^2}{\Delta(1 + \frac{\Delta}{\alpha})};$$

dato che vi è un esplicita dipendenza da  $\alpha$ , se quest'ultimo non è grande a tal punto da rendere la correzione trascurabile allora è necessario includerlo nella trattazione. Dalla (6.7.15) è evidente che la frequenza della cavità viene modificata dallo stato in cui si trova il qubit! Per misurare il qubit basta quindi misurare la frequenza del risonatore.

### Controllare lo stato di un singolo qubit

Per ottenere questo scopo è necessario accoppiare il qubit ad un campo elettromagnetico esterno oscillante nel tempo e "guidarlo" mediante le oscillazioni di Rabi (si veda la Sezione 6.4). Esistono diversi modi: ad esempio si può costruire il circuito



dove la sorgente  $V(t)$  fornisce un segnale e.m. oscillante dipendente dal tempo e con frequenza circa uguale a quella del qubit. Come funziona questo apparato? I gradi di libertà del circuito (carica, corrente, ecc.) sono legati al comportamento dell'oscillatore (vedi Tabella 6.1), il quale è controllato dagli operatori  $\hat{a}$ ,  $\hat{a}^\dagger$  e  $\hat{\sigma}_i$ . Questo significa che l'energia del circuito è regolata dalle differenze di potenziale delle due differenti componenti del circuito:  $E_C = \frac{1}{2}CV^2 \rightarrow C_gV_1V_2$  dove  $V_1 = \frac{Q}{C}$  e  $V_2 = V(t)$ ; ma allora

$$E_C = \frac{C_g}{C}QV(t);$$

dal punto di vista del qubit le identificazioni da fare sono

$$\begin{aligned} \hat{x} &\longleftrightarrow \hat{\Phi} \sim (\hat{a} + \hat{a}^\dagger) \sim \hat{\sigma}_1, \\ \hat{p} &\longleftrightarrow \hat{Q} \sim -i(\hat{a} - \hat{a}^\dagger) \sim \hat{\sigma}_2; \end{aligned} \quad (6.7.16)$$

quindi l'hamiltoniana del sistema diventa

$$\hat{H} = -\frac{\omega_q}{2}\hat{\sigma}_3 - ig(\hat{a} - \hat{a}^\dagger)V(t) = -\frac{\omega_q}{2}\hat{\sigma}_3 + g\hat{\sigma}_2V(t),$$

dove il potenziale oscillante controlla il qubit con una frequenza esterna  $\omega_d$ , ed è quindi della forma

$$V(t) = V_0 \cos(\omega_d t + \phi_0).$$

Questo non è altro che il problema delle oscillazioni di Rabi affrontato nella Sezione 6.4. Come ben sappiamo, dopo la rotazione l'hamiltoniana è scrivibile come

$$\hat{H} = -\frac{1}{2}(\Delta\hat{\sigma}_3 + A\cos(\phi)\hat{\sigma}_1 - A\sin(\phi)\hat{\sigma}_2),$$

dove  $\Delta = \omega_q - \omega_d$  e  $\phi = \phi_0 + \phi_1$ . Se poniamo  $Ae^{-i\phi_1} \equiv -igV_0$  allora otteniamo che  $A = gV_0$  e  $\phi_1 = \frac{\pi}{2}$ . Con una tale hamiltoniana possiamo agire con l'evoluzione temporale

$$\hat{U}_{\text{ev}}(t) = e^{-i\hat{H}t};$$

la miglior situazione possibile accade in corrispondenza della risonanza ( $\Delta = 0$ ): scegliendo  $\phi = 0$  sopravvive solamente il contributo di  $\hat{\sigma}_1$ , perciò l'evoluzione temporale non è altro che una tipica trasformazione agente sulla sfera di Bloch

$$\hat{U}_{\text{ev}}(t) = e^{\frac{i}{2}A\hat{\sigma}_1 t} = R_x(-At);$$

similmente per  $\phi = -\frac{\pi}{2}$

$$\hat{U}_{\text{ev}}(t) = e^{-\frac{i}{2}A\hat{\sigma}_2 t} = R_y(At).$$

Scegliendo opportunamente  $t$  è quindi possibile ottenere qualsiasi matrice di  $SU(2)$ , ossia qualsiasi gate agente su singoli qubit.

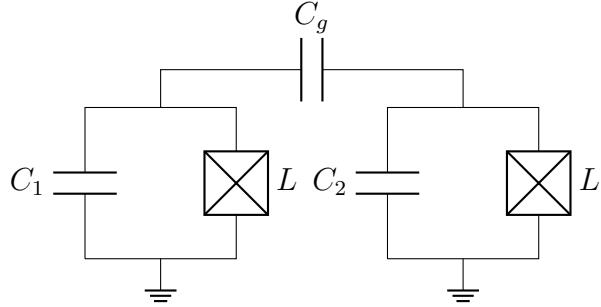
In realtà bisogna prestare attenzione: come già mostrato nella Figura 6.6b, partendo da  $|0\rangle$ , se si vuole avere la certezza che ad un certo istante ci si ritroverà in  $|1\rangle$  è necessario effettuare una rotazione lungo l'asse  $x$ ; in realtà questo è vero solamente se l'hamiltoniana del sistema superconduttivo non è approssimata e considera anche lo stato  $|2\rangle$ . Il motivo è dato dal fatto che nelle realizzazioni pratiche la differenza tra  $E_2 - E_1$  non è così più piccola rispetto a  $E_1 - E_0$ ! Questo vuol dire che sperimentalmente è necessario ricalcolare l'oscillazione di Rabi includendo l'effetto di  $|2\rangle$  e in seguito rimpiazzare l'ampiezza  $A$  della perturbazione con un'opportuna funzione dipendente dal tempo scelta appositamente per avere la certezza di raggiungere lo stato  $|1\rangle$ .

### Creare entanglement tra due qubit

Nella Sezione 3.2 abbiamo visto che è necessario possedere almeno un gate agente su due qubit (che produce entanglement) per poter costruire un qualsiasi gate. Utilizzare un CNOT-gate sarebbe perfetto, tuttavia non è l'unica scelta possibile perché, come vedremo tra poco, utilizzando un sistema superconduttivo è possibile realizzare un cosiddetto iSWAP-gate.

Innanzitutto, per mettere in contatto tra loro differenti qubit superconduttori esistono diversi modi:

- Il primo modo è quello di combinare due circuiti superconduttori con un extra capacità  $C_g$ , come ad esempio nel circuito

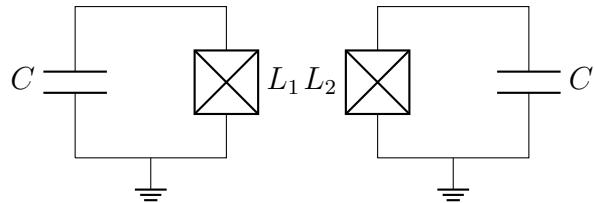


In tal caso notiamo che le due componenti del circuito presentano due capacità  $C_1$  e  $C_2$ : utilizzando l'identificazione in (6.7.16) e gli operatori in (6.7.14), possiamo scrivere l'hamiltoniana di un tale sistema come

$$\hat{H}_{\text{int}} = C_g V_1 V_2 = \frac{C_g}{C_1 C_2} \hat{Q}_1 \hat{Q}_2 \sim (\hat{a}_1 - \hat{a}_1^\dagger) (\hat{a}_2 - \hat{a}_2^\dagger) \sim \hat{\sigma}_2^{(1)} \otimes \hat{\sigma}_2^{(2)}, \quad (6.7.17)$$

dove gli apici " $(j)$ " indicano il qubit  $j$ -esimo.

- Nel secondo caso possiamo combinare due circuiti tramite l'induttanza, ossia utilizzando due giunzioni Josephson tali che si possano scambiare la corrente prodotta dalle coppie di Cooper:

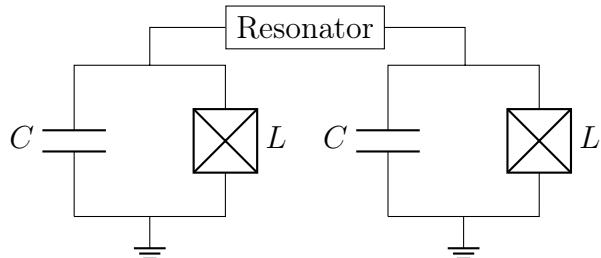


È un caso molto simile al precedente in cui bisogna tenere in considerazione il fatto che questa volta l'hamiltoniana si scrive a partire dalle correnti nei due circuiti:

$$\hat{H}_{\text{int}} = M_{12} I_1 I_2 = \frac{M_{12}}{L_1 L_2} \hat{\Phi}_1 \hat{\Phi}_2 \sim (\hat{a}_1 + \hat{a}_1^\dagger) (\hat{a}_2 + \hat{a}_2^\dagger) \sim \hat{\sigma}_1^{(1)} \otimes \hat{\sigma}_1^{(2)},$$

dove  $M_{12}$  è il coefficiente di mutua induzione.

- L'ultima opzione è quella di mediare l'interazione dei circuiti con una cavità/risonatore:



A differenza dei casi precedenti, questa situazione è più complessa perché l'accoppiamento coinvolge un'hamiltoniana di Jaynes-Cummings (i pedici " $r$ " stanno per "risonatore")

$$\hat{H}_{\text{int}} = \omega_r \left( \hat{a}_r^\dagger \hat{a}_r + \frac{1}{2} \right) + g_1 \left( \hat{a}_r \hat{\sigma}_+^{(1)} + \hat{a}_r^\dagger \hat{\sigma}_-^{(1)} \right) + g_2 \left( \hat{a}_r \hat{\sigma}_+^{(2)} + \hat{a}_r^\dagger \hat{\sigma}_-^{(2)} \right);$$

si noti che i due qubit interagiscono l'uno con l'altro per mezzo dei modi di oscillazione nel risonatore.

I diversi gate che si trovano in letteratura possono essere costruiti con delle opportune combinazioni dei circuiti precedenti. Discutiamo brevemente i casi più semplici, ossia le situazioni rappresentate nei primi due circuiti: gli operatori  $\hat{\sigma}_1$  e  $\hat{\sigma}_2$  sono detti **trasversi** perché al contrario  $\hat{\sigma}_3$  è utilizzato per fissare la frequenza del qubit.

Consideriamo il circuito del primo caso (accoppiamento dato dalla capacità) e vediamo come può essere esplicitamente costruito un **iSWAP-gate** (la  $i$  perché l'output è moltiplicato per l'unità immaginaria). Chiamiamo  $\omega_q^{(1)}$  e  $\omega_q^{(2)}$  le frequenze proprie dei due qubit: assumiamo che possiamo arbitrariamente variare queste frequenze usando transmon a frequenza regolabile<sup>xvi</sup>. Innanzitutto è bene notare che dobbiamo stare attenti alla forma dell'interazione in (6.7.17) perché abbiamo omesso numerosi termini: infatti in un sistema di riferimento ruotato mediante l'operatore  $\hat{U}(t) = e^{i\hat{H}_0 t}$ , sono gli operatori  $\hat{\sigma}_\pm^{(j)}$  a trasformare prendendo una singola "fase", e non  $\hat{\sigma}_{1,2}^{(j)}$ :

$$\hat{\sigma}_\pm^{(j)} \longrightarrow \hat{\sigma}_\pm^{(j)} e^{\mp i\omega_q^{(j)} t};$$

scriviamo quindi esplicitamente l'interazione (6.7.17) in un frame ruotato:

$$\begin{aligned} \hat{\sigma}_2^{(1)} \otimes \hat{\sigma}_2^{(2)} &= - \left( \hat{\sigma}_+^{(1)} - \hat{\sigma}_-^{(1)} \right) \otimes \left( \hat{\sigma}_+^{(2)} - \hat{\sigma}_-^{(2)} \right) \\ &\xrightarrow{\hat{U}(t)} \hat{\sigma}_+^{(1)} \hat{\sigma}_-^{(2)} e^{-i(\omega_q^{(1)} - \omega_q^{(2)})t} + \hat{\sigma}_-^{(1)} \hat{\sigma}_+^{(2)} e^{i(\omega_q^{(1)} - \omega_q^{(2)})t} - \\ &\quad - \hat{\sigma}_+^{(1)} \hat{\sigma}_+^{(2)} e^{-i(\omega_q^{(1)} + \omega_q^{(2)})t} - \hat{\sigma}_-^{(1)} \hat{\sigma}_-^{(2)} e^{i(\omega_q^{(1)} + \omega_q^{(2)})t}; \end{aligned}$$

di solito nelle applicazioni sperimentali si preferisce lavorare in regime di risonanza dei due circuiti, quindi assumiamo che  $\omega_q^{(1)} = \omega_q^{(2)}$  e utilizziamo la RWA:

$$\hat{\sigma}_2^{(1)} \otimes \hat{\sigma}_2^{(2)} \xrightarrow{\hat{U}(t)} \hat{\sigma}_+^{(1)} \hat{\sigma}_-^{(2)} + \hat{\sigma}_-^{(1)} \hat{\sigma}_+^{(2)};$$

quest'ultima è proprio l'interazione che darà origine al gate, detta **accoppiamento trasverso in RWA**. Con questo accoppiamento possiamo scrivere, nel frame ruotato, la seguente hamiltoniana di interazione efficace

$$\hat{H}_{\text{int}} = g \left( \hat{\sigma}_+^{(1)} \hat{\sigma}_-^{(2)} + \hat{\sigma}_-^{(1)} \hat{\sigma}_+^{(2)} \right) = g \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

---

<sup>xvi</sup>Si ricordi che questo scopo può essere raggiunto grazie all'inserimento di un'ulteriore giunzione Josephson (vedi Figura 6.17) e alla variazione di un opportuno flusso magnetico esterno.

dove nell'ultimo passaggio abbiamo fatto uso del prodotto di Kronecker della definizione 1.5 (è omesso il simbolo " $\otimes$ " tra le due matrici dei due termini in parentesi). Il blocco centrale non è altro che la matrice  $\sigma_1$ , ricordando quindi che

$$e^{-igt\sigma_1} = R_x(2gt) = \cos(gt) - i\sigma_1 \sin(gt) = \begin{pmatrix} \cos(gt) & -i \sin(gt) \\ -i \sin(gt) & \cos(gt) \end{pmatrix}, \quad (6.7.18)$$

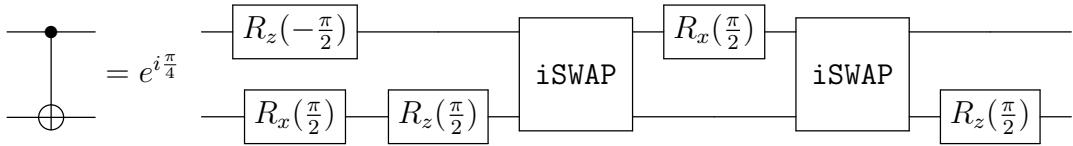
possiamo facilmente scrivere l'operatore di evoluzione temporale

$$\hat{U}_{\text{ev}}(t) = e^{-i\hat{H}_{\text{int}}t} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(gt) & -i \sin(gt) & 0 \\ 0 & -i \sin(gt) & \cos(gt) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array}.$$

Perciò l'evoluzione temporale del sistema ruota automaticamente gli stati  $|01\rangle$  e  $|10\rangle$ . Scegliendo il tempo  $t = \frac{3\pi}{2g}$  otteniamo esattamente un **iSWAP-gate**

$$\hat{U}_{\text{ev}}\left(\frac{3\pi}{2g}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \equiv \text{iSWAP}.$$

Come accennato sopra, è possibile dimostrare che l'**iSWAP-gate** e i gate agenti sui singoli qubit formano un insieme universale di gate: la seguente combinazione permette infatti di ricostruire, a meno di una fase globale, un **CNOT-gate**



È importante sottolineare che per la presenza di due **iSWAP-gate**, un **CNOT-gate** così costruito non risulta in realtà molto efficiente: si preferirebbe lavorare con un singolo **iSWAP-gate**.

Per costruire gate agenti su più qubit in maniera più efficiente si può anche sfruttare il fatto che esistono degli stati eccitati nel transmon: una volta costruito un qubit superconduttivo con frequenza regolabile e una volta identificati i livelli energetici ( $|0\rangle, |1\rangle, |2\rangle$ ), è possibile dimostrare che esiste una situazione in cui gli stati eccitati ( $|11\rangle, |20\rangle$ ) sono indistinguibili (coincidenti) per un opportuno valore di  $\Delta = \omega_q^{(1)} - \omega_q^{(2)}$  (per  $\Delta = 0$  sono distinguibili). Una volta trovato tale valore si possono effettuare delle oscillazioni di Rabi per mandare  $|11\rangle \rightarrow -|11\rangle$  e  $|20\rangle \rightarrow |20\rangle$ .

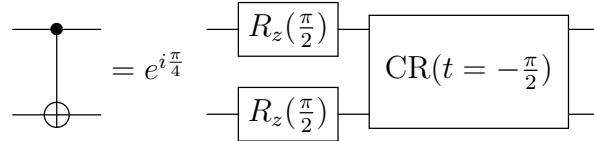
Nella situazione appena analizzata abbiamo impiegato un accoppiamento trasverso della forma in (6.7.17), la cui evoluzione temporale produceva un **iSWAP-gate**. In realtà sarebbe meglio se potessimo usare un'interazione della forma

$$\hat{H}_{\text{int}} = \frac{g}{2} \hat{\sigma}_3^{(1)} \otimes \hat{\sigma}_1^{(2)} = \frac{g}{2} \begin{pmatrix} \sigma_1 & 0 \\ 0 & -\sigma_1 \end{pmatrix} = \frac{g}{2} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}; \quad (6.7.19)$$

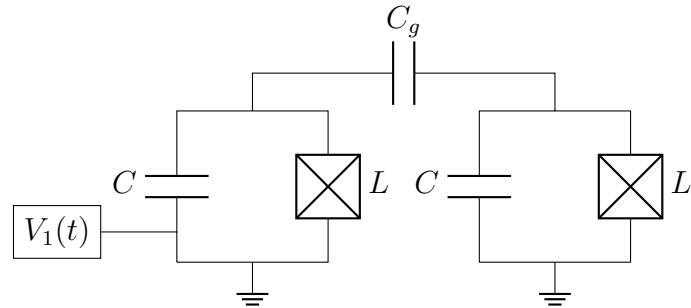
il motivo è dato dal fatto che la sua evoluzione temporale produce il cosiddetto **Cross-Resonant gate (CR-gate)**

$$\hat{U}_{\text{ev}}(t) = e^{-i\hat{H}_{\text{int}}t} = \begin{pmatrix} \cos\left(\frac{gt}{2}\right) & -i\sin\left(\frac{gt}{2}\right) & 0 & 0 \\ -i\sin\left(\frac{gt}{2}\right) & \cos\left(\frac{gt}{2}\right) & 0 & 0 \\ 0 & 0 & \cos\left(\frac{gt}{2}\right) & i\sin\left(\frac{gt}{2}\right) \\ 0 & 0 & i\sin\left(\frac{gt}{2}\right) & \cos\left(\frac{gt}{2}\right) \end{pmatrix} \equiv \text{CR-gate},$$

dove abbiamo fatto uso due volte della (6.7.18) nell'esponenziazione. Il motivo per cui tale gate è in un certo senso migliore dell'iSWAP-gate è dato dal fatto che permetta di costruire un CNOT-gate più efficientemente mediante un solo impiego:



Chiaramente può sorgere spontanea la domanda: come si realizza un'interazione della forma in (6.7.19)? Si tratta di un modo con cui IBM costruisce i propri computer quantistici superconduttori. Questo può essere fatto mediante il seguente trucco: si realizza un circuito



dove si regola la frequenza di drive del primo circuito (mediante  $V_1(t)$ ) utilizzando esattamente la frequenza propria del secondo qubit, ossia  $\omega_d = \omega_q^{(2)}$ . In una tale situazione è possibile dimostrare che per  $\Delta = \omega_q^{(1)} - \omega_q^{(2)} \gg g$  l'unico contributo che sopravvive nell'interazione è della forma desiderata, ossia come in (6.7.19).



# Bibliografia

## Corso

- [1] Zaffaroni, A. (2021). [Teoria della informazione e della computazione quantistica](#). Università degli Studi di Milano - Bicocca.

## Libri

- [2] Nielsen, M. A., Chuang, I. L. (2000). Quantum Computation and Quantum Information. Cambridge University Press.
- [3] Mermin, N. (2007). Quantum Computer Science: An Introduction. Cambridge University Press.

## Lezioni

- [4] Aaronson, S. (2018). [Introduction to Quantum Information Science Lecture Notes](#). University of Texas at Austin.
- [5] Preskill, J. (1997-2020). [Course Information for Physics and Computer Science on Quantum Computation](#). California Institute of Technology.

## Articoli

- [6] Fowler, A., Mariantoni, M., Martinis, J., & Cleland, A. (2012). Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, 86(3).
- [7] Haffner, H., Roos, C., & Blatt, R. (2008). Quantum computing with trapped ions. *Physics Reports*, 469(4), 155–203.
- [8] Bruzewicz, C., Chiaverini, J., McConnell, R., & Sage, J. (2019). Trapped-ion quantum computing: Progress and challenges. *Applied Physics Reviews*, 6(2), 021314.
- [9] Sørensen, A., & Mølmer, K. (2000). Entanglement and quantum computation with ions in thermal motion. *Physical Review A*, 62(2).

- [10] Mølmer, K., & Sørensen, A. (1999). Multiparticle Entanglement of Hot Trapped Ions. *Physical Review Letters*, 82(9), 1835–1838.
- [11] Krantz, P., Kjaergaard, M., Yan, F., Orlando, T., Gustavsson, S., & Oliver, W. (2019). A quantum engineer’s guide to superconducting qubits. *Applied Physics Reviews*, 6(2), 021318.
- [12] Kwon, S., Tomonaga, A., Lakshmi Bhai, G., Devitt, S., & Tsai, J.S. (2021). Gate-based superconducting quantum computing. *Journal of Applied Physics*, 129(4), 041102.
- [13] Girvin, S. M. (2012). Circuit QED: Superconducting Qubits Coupled to Microwave Photons.