Alma Mater Studiorum · Università di Bologna

**Scuola di Scienze**
**Dipartimento di Fisica e Astronomia**
**Corso di Laurea in Fisica**

# I codici di correzione degli errori quantistici

**Relatore:**
**Prof.ssa Elisa Ercolessi**

**Presentata da:**
**Virginio Miroglio**

Anno Accademico 2023/2024

*A nonna Franci*

# Abstract

Il tema fondamentale di questo elaborato è la correzione degli errori quantistici, uno dei campi principali della computazione quantistica. È necessario introdurre la trattazione attraverso le basi del calcolo quantistico, in quanto particolarmente utili per descrivere correttamente la correzione degli errori. Per una comprensione ottimale risulta conveniente porre queste nozioni in corrispondenza con la computazione classica. Utilizzando i canali e le operazioni quantistiche viene definito il concetto di errore e le varie forme che esso può assumere. La correzione degli errori viene sviluppata a partire da questo aspetto essenziale fino alla descrizione di codici di correzione basilari come i CSS e gli Stabilizers. L'ultima sezione è dedicata alla descrizione di particolari tipologie di codici quali Surface codes, LDPC codes e BB codes. Questi esempi permettono di avere una visione completa del processo di correzione; confrontandoli è infatti possibile capire a fondo le proprietà della correzione degli errori quantistici.

# Indice

# Introduzione

Il formalismo teorico della meccanica quantistica era conosciuto nella sua interezza già alla fine degli anni '30 del secolo scorso grazie al lavoro di fisici come Paul Dirac e Erwin Schrödinger; fu tuttavia necessario attendere il 1982 per poter assistere alla comparsa del concetto di computazione quantistica. In quell'anno si tenne la famosa conferenza di Richard Feynman in cui il fisico statunitense presentò i possibili vantaggi che sarebbero stati introdotti attraverso la realizzazione di computer mediante oggetti quantistici [6]. La computazione quantistica è infatti caratterizzata da una diminuzione esponenziale del tempo di simulazione rispetto alla controparte classica; ciò è possibile grazie alle proprietà della meccanica quantistica come la sovrapposizione di stati e l'entanglement. L'elemento fondamentale della computazione quantistica è il qubit che, rispetto al bit classico che può assumere solo i valori 0 e 1, può trovarsi in una sovrapposizione continua di stati che permette una maggiore efficienza di calcolo data la possibilità di lavorare su più stati contemporaneamente.

Nel 1985 fu la volta di David Deutsch, il fisico britannico presentò l'idea di un computer quantistico universale in grado di simulare qualunque sistema fisico [4]. Da lì in avanti gli sviluppi a livello teorico sono stati molti, tra questi fu di particolare importanza l'algoritmo di Shor del 1994 [13] che permise di fattorizzare grandi numeri con un'efficienza molto maggiore degli algoritmi classici. Per la realizzazione di un effettivo computer quantistico è stato necessario attendere il 1997, anno in cui l'azienda statunitense IBM produsse il primo prototipo di computer quantistico, in cui i qubit erano nuclei atomici o particolari molecole di cui era possibile modificare e misurare lo spin. La stessa IBM nel 2001 ha presentato il primo elaboratore quantistico a 7 qubit in grado di implementare l'algoritmo di Shor. Nel 2019 Google ha realizzato un computer quantistico in grado di eseguire le funzioni richieste meglio e più velocemente di un computer classico, in quel momento si è raggiunta la cosiddetta supremazia quantistica. Nel 2022 la IBM ha realizzato un computer quantistico formato da 433 qubit, avvicinandosi alla risoluzione di problemi tuttora ritenuti irrisolti.

Uno dei principali ostacoli che è necessario superare nella realizzazione di un computer quantistico consiste nella fragilità dell'informazione contenuta all'interno dei qubit. La quantum error correction corrisponde alla branca della computazione quantistica che si occupa di creare codici quantistici in grado di individuare, e successivamente correggere,

gli errori in grado di alterare lo stato di un qubit. Le cause dell'errore possono essere molteplici, tra queste imperfezioni nei qubit, nei materiali utilizzati, nella preparazione degli stati quantistici e nella loro misura ma anche interferenze con campi magnetici esterni e raggi cosmici in grado di interagire con lo stato quantistico. La correzione degli errori risulta quindi essere di fondamentale importanza all'interno della computazione quantistica. L'idea alla base di questo campo consiste nell'utilizzo dell'entanglement per delocalizzare l'informazione in modo ridondante, in modo che il singolo errore non possa corromperla completamente e la correzione sia possibile.

Alcuni tra i codici maggiormente utilizzati attualmente per la quantum error correction sono i Surface codes, proposti per la prima volta da Daniel Gottesman nel 2002 [3]. Questi particolari codici sfruttano le proprietà geometriche del reticolo formato dai qubit per identificare gli errori che occorrono durante la computazione. Tuttavia, i surface codes risultano essere poco performanti rispetto, ad esempio, ad alcuni codici appartenenti alla famiglia degli LDPC codes come, ad esempio, i BB codes, un'importante famiglia presentata nel 2024 proprio da IBM [1]. Gli obiettivi principali per il futuro della computazione quantistica corrispondono alla creazione di computer a larga scala tolleranti agli errori. Alcuni dei principali temi di ricerca atti allo sviluppo dei computer quantistici corrispondono al miglioramento della scalabilità dei codici in modo da aumentare il numero di qubit, alla diminuzione del numero di componenti necessarie per svolgere le operazioni quantistiche e alla creazione di porte logiche tolleranti agli errori.

Lo studio di questi temi è stato sviluppato in questo elaborato all'interno di tre capitoli: nel primo vengono presentate le basi della computazione quantistica e il loro rapporto con la meccanica quantistica; viene definito il qubit ma anche le principali operazioni che possono essere eseguite su di esso. Il secondo capitolo è invece dedicato alla descrizione degli errori e, in particolare, alla loro correzione; partendo dalle basi di questa branca della computazione quantistica si arriva a descrivere importanti famiglie di codici come i CSS e gli Stabilizers. Nel terzo capitolo è invece presente una discussione su Surface codes e LDPC codes; in particolare, attraverso l'esempio dei BB codes, si è studiato come gli LDPC costituiscano un grande vantaggio operativo rispetto ai Surface codes.

# Capitolo 1

# La computazione quantistica

*All'interno di questo capitolo vengono riportati principali concetti utili allo studio e alla comprensione degli errori quantistici e della loro correzione. Risulta dunque necessario richiamare i concetti base della meccanica quantistica e definire i fondamenti matematici della computazione quantistica per poter effettuare una trattazione completa ed esaustiva nei successivi capitoli.* [10, 11].

## 1.1 Brevi richiami di meccanica quantistica

Prima di introdurre i principali concetti riguardanti la computazione quantistica è necessario richiamare gli elementi fondanti della meccanica quantistica; questa disciplina si fonda sui seguenti postulati:

1. ***Stati*** Uno stato corrisponde alla completa descrizione di un sistema fisico isolato. Possiamo associare ad ogni sistema uno spazio vettoriale dotato di prodotto interno (spazio di Hilbert), uno stato è quindi rappresentato da un raggio (classe di vettori che differiscono per una costante scalare moltiplicativa) di questo spazio. I vettori appartenenti a questo spazio sono denominati $|\psi\rangle$ e il prodotto interno tra due vettori $\langle\psi|\phi\rangle$, è una mappa tra lo spazio di Hilbert e l'insieme dei numeri complessi $\mathbb{C}$ che presenta le seguenti proprietà:
   - È definita positiva: $\langle\psi|\psi\rangle > 0$ se $|\psi\rangle \neq 0$;
   - È lineare: $\langle\phi| (a|\psi_1\rangle + b|\psi_2\rangle) = a\langle\phi|\psi_1\rangle + b\langle\phi|\psi_2\rangle$;
   - È antisimmetrica: $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$.
2. ***Osservabili*** Un osservabile è una proprietà di un sistema fisico che può essere misurata, in meccanica quantistica è definito da un operatore $A : |\psi\rangle \to A|\psi\rangle$, tale che $A = A^\dagger$ (autoaggiunto).

3. ***Misure*** Una misura è un processo in cui si acquisisce conoscenza riguardo lo stato del sistema studiato; in meccanica quantistica essa è descritta da una collezione di operatori di misura $M_m$, tali che $\sum_m M_m M_m^\dagger = I$. La misura di un osservabile $M$ fa collassare il sistema in un certo autostato $M$ e l'osservatore è in grado di acquisire il valore dell'autovalore $m$ corrispondente.

   La probabilità di ottenere un determinato autovalore è data da

$$p(m) = ||M|\psi\rangle||^2 = \langle\psi|M^\dagger M|\psi\rangle\,, \tag{1.1}$$

   mentre $M|\psi\rangle / ||M|\psi\rangle||$ è lo stato normalizzato in cui si trova il sistema dopo la misura.

4. ***Dinamica*** L'evoluzione temporale di un sistema quantistico chiuso è descritta da operatori unitari, ovvero gli operatori $U$ tali che $UU^\dagger = U^\dagger U = I$. Il vettore $|\psi'\rangle$ al tempo t' è legato quindi al vettore $|\psi\rangle$ al tempo t da un operatore $U$ che dipende soltanto da t e t'

$$|\psi'\rangle = U|\psi\rangle\,. \tag{1.2}$$

5. ***Sistemi composti*** Dati gli spazi di Hilbert $\mathcal{H}_A$ e $\mathcal{H}_B$ corrispondenti ai sistemi $A$ e $B$, allora lo spazio corrispondente al sistema $AB$ è $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, ovvero il prodotto esterno dei due. Se i sistemi $A$ e $B$ sono preparati negli stati $|\psi\rangle_A$ e $|\phi\rangle_B$ rispettivamente, allora $|\psi\rangle_A \otimes |\phi\rangle_B$ rappresenta lo stato del sistema composto.

Tornando al concetto di misura, è possibile approfondire quanto annunciato in precedenza introducendo una classe speciale di misure note come misure proiettive. Una misura proiettiva è descritta da un osservabile $M$, un operatore hermitiano che presenta la seguente scomposizione spettrale:

$$M = \sum_m m P_m, \tag{1.3}$$

dove i $P_m$ sono i proiettori sugli autostati di $M$ con autovalori $m$, che corrispondono ai possibili esiti della misura. Essendo i proiettori idempotenti ($P_m^2 = P_m$) e hermitiani ($P^\dagger = P$), la probabilità di misurare il singolo autovalore è

$$p(m) = \langle\psi|P_m|\psi\rangle\,. \tag{1.4}$$

Risulta dunque immediato calcolare il valore medio di un osservabile:

$$E(M) = \sum_m m p(m) = \langle\psi|M|\psi\rangle\,. \tag{1.5}$$

## 1.2 Il Qubit

Per comprendere al meglio le basi della computazione quantistica, risulta utile descriverla partendo dai concetti di quella classica: così come il bit è l'elemento fondante della computazione classica, presentiamo la controparte quantistica introducendo il concetto di qubit. Nella trattazione che seguirà verrà fatto riferimento al bit quantistico come oggetto puramente matematico, la sua realizzazione fisica esula dagli argomenti trattati. Mentre il bit classico può assumere solamente i valori 0 o 1, il qubit è descritto da un vettore in uno spazio bi-dimensionale complesso dotato di prodotto interno. È possibile creare una base ortonormale di questo spazio attraverso i due elementi $|0\rangle$ e $|1\rangle$ detti stati della base computazionale. Lo stato generico di un qubit può essere quindi espresso come:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad |\alpha|^2 + |\beta|^2 = 1, \tag{1.6}$$

dove $|\alpha|^2$ e $|\beta|^2$ rappresentano le probabilità di trovare gli stati $|0\rangle$ e $|1\rangle$ una volta effettuata una misura dello stato del qubit, che generalmente non si trova in uno dei due stati, ma ne è la sovrapposizione quantistica. La misura di uno stato può essere tuttavia effettuata su una qualunque base dello spazio di Hilbert ad esso corrispondente, la differenza sta nel fatto che lo stato del qubit collasserà su uno dei due vettori di base e non su quelli della base computazionale $|0\rangle$ e $|1\rangle$.

È possibile a questo punto creare una rappresentazione geometrica di un qubit attraverso la cosiddetta Sfera di Bloch, esprimendo lo stato generico come:

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\,, \tag{1.7}$$

dove $\theta$ e $\psi$ definiscono un punto sulla sfera unitaria tridimensionale in coordinate polari. Nella descrizione del qubit è presente una fase relativa tra i due stati in quanto questa è l'unica fisicamente significativa; una fase globale non è infatti misurabile e può essere dunque trascurata.

### 1.2.1 Stati di due qubit

Gli assiomi della meccanica quantistica possono essere utilizzati per la descrizione di un sistema chiuso, il quale non interagisce con l'ambiente circostante. Per studiare i qubit è tuttavia necessario considerare dei sistemi aperti, in cui le misure non sono proiezioni ortogonali e le evoluzioni non sono unitarie. Il modo migliore per avvicinarsi alla trattazione dei sistemi aperti è quello di considerare il sistema formato da due qubit $A$ e $B$; le basi dei due spazi ad essi corrispondenti sono $\{|0\rangle_A\,, |1\rangle_A\}$ e $\{|0\rangle_B\,, |1\rangle_B\}$. Attraverso il quinto postulato siamo in grado di descrivere lo stato del sistema come stato prodotto:

$$|\psi\rangle_{AB} = (\alpha\,|0\rangle_A + \beta\,|1\rangle_A) \otimes (\alpha'\,|0\rangle_B + \beta'\,|1\rangle_B), \tag{1.8}$$

dove $\alpha$, $\beta$, $\alpha'$ e $\beta'$ sono costanti di normalizzazione. È inoltre possibile scrivere il prodotto esterno di due vettori come $|a\rangle \otimes |b\rangle = |ab\rangle$; in questo modo possiamo scrivere le basi computazionali come: $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$.

Si consideri ora il seguente stato quantistico:

$$|\psi\rangle_{AB} = \alpha(|0\rangle_A \otimes |0\rangle_B) + \beta(|1\rangle_A \otimes |1\rangle_B) \tag{1.9}$$

e si supponga di misurare il qubit $A$ nella base $\{|0\rangle_A, |1\rangle_A\}$. Se l'esito della misura è $|0\rangle_A$, allora sappiamo che il sistema totale è collassato nello stato $(|0\rangle_A \otimes |0\rangle_B)$ mentre se si ottiene come risultato $|1\rangle_A$, esso è collassato in $(|1\rangle_A \otimes |1\rangle_B)$. Si dice quindi che i qubit $A$ e $B$ sono correlati in quanto la misura dello stato di $A$ fornisce automaticamente la misura dello stato di B. Questa correlazione, chiamata entanglement, sarà approfondita nei capitoli successivi.

Vogliamo ora capire quale sia il risultato di una misura generica effettuata solo sul qubit $A$, che, in termini operatoriali, è esprimibile come $M_A \otimes I_B$, dove $M_A$ è un operatore autoaggiunto che agisce su $A$ mentre $I_B$ è l'operatore identità che agisce su $B$. Possiamo esprimere il valore di aspettazione di $M_A$ come:

$$\langle M_A \rangle = \mathrm{Tr}(M_A \rho_A), \quad \rho_A = |\alpha|^2 |0\rangle \langle 0| + |\beta|^2 |1\rangle \langle 1|, \tag{1.10}$$

dove $\mathrm{Tr}(\cdot)$ è la traccia e $\rho_A$ è l'operatore densità per il qubit $A$; esso rappresenta un ensemble di possibili stati quantistici $|\psi\rangle$ i quali occorrono con una specifica probabilità $p_i$ tale che $0 \leq p_i \leq 1$ e $\sum_i p_i = 1$. L'operatore densità risulta quindi essere autoaggiunto, definito positivo e idempotente, inoltre presenta traccia e norma unitarie; di conseguenza può essere diagonalizzato in una base ortonormale con autovalori positivi e di somma uno. Quanto appena detto può essere riassunto nel seguente teorema per la cui dimostrazione si fa riferimento a [10].

**Teorema 1.1** *Caratterizzazione dell'operatore densità*
Un operatore autoaggiunto $\rho$ è l'operatore densità associato ad un ensemble $\{p_i, |\psi_i\rangle\}$, se e solo se soddisfa le seguenti condizioni:

- ha traccia uguale a uno;
- è definito positivo.

Se consideriamo un sistema quantistico più ampio, possiamo voler conoscere un suo sottosistema che può non essere noto a priori ma comunque rappresentato da una matrice densità. Un sistema quantistico del quale si conosce perfettamente lo stato $|\psi\rangle$, è detto in uno stato puro, altrimenti lo stato è misto in quanto è l'insieme di più stati puri nell'ensemble di $\rho$. Se lo stato di $A$ è puro, allora l'operatore densità $\rho_A = |\psi\rangle \langle\psi|$ è la proiezione sullo stato uno-dimensionale generato da $|\psi\rangle_A$. È inoltre possibile dimostrare che $\mathrm{Tr}(\rho^2) = 1$ per quanto riguarda uno stato puro mentre $\mathrm{Tr}(\rho^2) < 1$ per gli stati misti.

È possibile ora analizzare l'operatore densità di un generico sistema bipartito di due qubit $|\psi\rangle_{AB}$. Possiamo scrivere il corrispondente spazio di Hilbert come $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, ovvero il prodotto esterno degli spazi corrispondenti alle due parti. La base ortonormale ad esso associata sarà quindi $\{|i\rangle_A \otimes |\mu\rangle_B\}$ dove $|i\rangle_A$ e $|\mu\rangle_B$ sono i vettori di base dei due spazi. Per un sistema di questo tipo è utile introdurre il concetto di operatore di densità ridotto: considerato l'operatore densità totale $\rho_{AB}$, l'operatore di densità ridotto per il sistema $A$ è definito da

$$\rho_A = tr_B(\rho_{AB}), \tag{1.11}$$

dove $tr_B(\cdot)$ è una mappa tra operatori detta traccia parziale sul sistema $B$ definita come

$$tr_B(|\psi\rangle_{AB} \langle\psi|_{AB}) = tr_B(|i_1\rangle \langle i_2| \otimes |\mu_1\rangle \langle\mu_2|) = |i_1\rangle \langle i_2| \operatorname{Tr}(|\mu_1\rangle \langle\mu_2|). \tag{1.12}$$

### 1.2.2 Entanglement

**Teorema 1.2** *Decomposizione di Schmidt*
Detto $|\psi\rangle_{AB}$ lo stato puro del sistema composto $AB$, allora esiste una base ortonormale $\{|i\rangle_A\}$ di $A$ e una $\{|\mu\rangle_B\}$ di $B$ tali che

$$|\psi\rangle_{AB} = \sum_j \lambda_j |i\rangle_A \otimes |\mu\rangle_B , \tag{1.13}$$

dove $\lambda_i$ sono numeri reali non negativi noti come coefficienti di Schmidt.

Applicando la decomposizione di Schmidt ad uno stato puro di un sistema composto otteniamo $\rho_A = \sum_i \lambda_i^2 |i\rangle_A \langle i|_A$ e $\rho_B = \sum_i \lambda_i^2 |\mu\rangle_B \langle\mu|_B$, ciò significa che i due operatori di densità ridotti hanno gli stessi autovalori non nulli $\lambda_i^2$. Se $\mathcal{H}_A$ e $\mathcal{H}_B$ non hanno la stessa dimensione, il numero di autovalori nulli sarà differente. Possiamo dunque associare allo stato bipartito $|\psi\rangle_{AB}$, il numero di Schmidt, ovvero il numero di autovalori non nulli di $\rho_A$ ($\rho_B$). Risulta ora immediato fornire la definizione di stato entangled, ovvero uno stato bipartito con un numero di Schmidt maggiore di uno, in caso contrario lo stato è detto separabile. Il numero di Schmidt quantifica dunque la quantità di entanglement tra due sistemi $A$ e $B$. Uno stato separabile può essere quindi espresso come $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$ e le corrispondenti matrici di densità ridotte $\rho_A$ e $\rho_B$ hanno le stesse proprietà di quelle corrispondenti a stati puri. Se lo stato non può essere espresso come prodotto dei due sottostati è detto entangled e le matrici sono equivalenti a quelle degli stati misti. È possibile ora servirsi dei cosiddetti stati di Bell per approfondire ulteriormente questo concetto. I quattro stati sono:

$$|\phi^{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \quad |\psi^{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}. \tag{1.14}$$

Utilizziamo solamente lo stato $|\phi^+\rangle$ e calcoliamo il suo operatore densità:

$$\rho = (\frac{|00\rangle + |11\rangle}{\sqrt{2}})(\frac{\langle 00| \pm \langle 11|}{\sqrt{2}}) = \frac{|00\rangle \langle 00| + |11\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 11|}{2}. \tag{1.15}$$

È possibile ora trovare l'operatore ridotto per il primo qubit applicando la traccia parziale sul secondo:

$$\begin{aligned}\rho_A &= tr_B(\rho) \\ &= \frac{tr_B(|00\rangle\langle 00|) + tr_B(|11\rangle\langle 00|) + tr_B(|00\rangle\langle 11|) + tr_B(|11\rangle\langle 11|)}{2} \\ &= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2},\end{aligned} \tag{1.16}$$

dove con $I$ si intende l'operatore identità. È immediato dimostrare che quello ottenuto è uno stato misto: $\mathrm{Tr}(\rho_A^2) = \mathrm{Tr}((I/2)^2) = 1/2 < 1$. La possibilità di conoscere lo stato congiunto puro ma non i sottostati misti è una definizione alternativa di entanglement; è possibile dimostrare la coerenza di questa affermazione con la precedente, infatti il numero di Schmidt per entrambi gli operatori di densità ridotti è 2, questo significa che i due stati sono massimamente entangled.

### 1.2.3 Misure generalizzate e misure POVM

Dopo aver descritto l'entanglement possiamo ora introdurre il concetto di misure generalizzate, ovvero quelle misure che non sono necessariamente una proiezione ortogonale agente sul sistema. Quando vogliamo misurare un osservabile $M$, modifichiamo l'Hamiltoniana del sistema facendo interagire l'osservabile con un'altra variabile che rappresenta l'apparato detta puntatore. È conveniente in questo caso descrivere la misura espandendo il sistema entangled di stato e puntatore nella base in cui è misurato il puntatore. Consideriamo il caso in cui il puntatore è n dimensionale e la sua misura proietta sulla base ortonormale $\{|b\rangle\}$. Possiamo assumere che inizialmente lo stato A, oggetto della misura e il puntatore $B$ (preparato nello stato "bianco" $|0\rangle_B$) si trovino in uno stato prodotto ma che vengano messi in correlazione attraverso un operatore unitario $U$, che viene successivamente espanso in una base di $B$.

$$U : |\psi\rangle_A \otimes |0\rangle_B \to \sum_b M_b |\psi\rangle_A \otimes |b\rangle_B . \tag{1.17}$$

Data l'unitarietà di $U$ (preserva la norma) otteniamo per ogni $|\psi\rangle$:

$$1 = || \sum_b M_b |\psi\rangle_A \otimes |b\rangle_B ||^2 = \sum_{b,b'} \langle\psi| M_{b'}^\dagger M_b |\psi\rangle \langle b'|b\rangle , \tag{1.18}$$

da cui ricaviamo:

$$\sum_b M_b^\dagger M_b = I. \tag{1.19}$$

Una misura ortogonale completa proiettiva sulla base del puntatore equivale quindi ad una misura incompleta su $AB$ eseguita mediante il proiettore $\{I \otimes |b\rangle\langle b|\}$. Questi risultati sono di particolare rilevanza in quanto, sebbene la relazione di completezza appena

trovata ci assicuri che la probabilità totale sia 1, gli stati ottenuti dopo la misura non sono necessariamente ortogonali e la misura non è necessariamente ripetibile.

Possiamo ora introdurre un nuovo concetto di misura che attribuisca un valore probabilistico alla singola misura, senza fornire informazioni sullo stato del sistema dopo il procedimento. Questa descrizione giustifica la possibilità di scartare lo stato ottenuto e crearne un altro da zero dopo aver effettuato la misura. A questo proposito in meccanica quantistica si usa il formalismo POVM (Positive Operator-Valued Measure), che può essere visto come una conseguenza del terzo postulato. Rifacendoci al paragrafo precedente, definiamo quindi l'operatore

$$E_a = M_a^\dagger M_a \tag{1.20}$$

associato ad ogni possibile esito della misura $a$. La probabilità di misurare $a$, dato l'operatore di densità del sistema iniziale sarà quindi:

$$p(a) = \mathrm{Tr}(\rho E_a). \tag{1.21}$$

Il nuovo operatore $E_a$ presenta le seguenti proprietà:

- È hermitiano ($E_a = E_a^\dagger$);
- È definito positivo ($\langle\psi|E_a|\psi\rangle \geq 1$);
- Rispetta la relazione di completezza $\sum_a E_a = I$.

$E_a$ è detto elemento POVM associato alla misura in quanto l'insieme degli operatori $E_a$ è sufficiente per determinare la probabilità dei diversi risultati della misura. Vogliamo ora dimostrare che esiste un insieme di operatori $M_a$ in grado di operare la misura descritta da un generico elemento POVM. Un operatore hermitiano non negativo ha sempre una radice quadrata non negativa; di conseguenza possiamo definire la decomposizione polare dell'operatore $M_a$ come:

$$M_a = U_a \sqrt{E_a}, \tag{1.22}$$

dove $U_a$ è un generico operatore unitario, in modo che sia verificata la (1.20). Si ha una decomposizione polare quando si può scomporre un operatore $A$ nel prodotto di un fattore Hermitiano e uno unitario. Dopo aver effettuato la misura, lo stato risultante $|\psi\rangle_a$ è:

$$|\psi\rangle_a = U_a \left( \frac{\sqrt{E_a}\,|\psi\rangle}{||\sqrt{E_a}\,|\psi\rangle\,||} \right). \tag{1.23}$$

È facile verificare che in una misura proiettiva gli elementi POVM sono gli stessi operatori di misura $E_a = P_a^\dagger P_a = P_a$.

Per fornire un esempio supponiamo che ci venga fornito un qubit preparato in uno dei due stati $|\psi_1\rangle = |0\rangle$ e $|\psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ e che vogliamo conoscerne lo stato con una

singola misura. È possibile dimostrare che, dati due stati non ortonormali, non esiste alcuna misura in grado di distinguerli sempre; tuttavia, utilizzando una specifica misura POVM, è possibile conoscere lo stato del qubit che ci viene fornito almeno alcune volte. Consideriamo il POVM$\{E_1, E_2, E_3\}$ formato dai seguenti elementi:

$$\begin{aligned} E_1 &= \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle \langle 1| ; \\ E_2 &= \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2}; \\ E_3 &= I - E_1 - E_2. \end{aligned} \tag{1.24}$$

Nel caso in cui ricevessimo lo stato $|\psi_1\rangle$, la probabilità di ottenere $E_1$ come esito della misura sarebbe $p(|\psi_1\rangle) = \langle\psi_1|E_1|\psi_1\rangle = 0$. Misurando $E_1$ saremmo quindi certi di aver ricevuto lo stato $|\psi_2\rangle$, così come avremmo la certezza di aver lavorato su $|\psi_1\rangle$ dopo aver misurato $E_2$. Nel caso in cui l'esito della misura fosse l'elemento $E_3$, non avremmo alcuna informazione sul sistema, tuttavia saremmo in grado di non incorrere mai in errori di scambio dei due stati.

## 1.3 Operazioni sui qubit

### 1.3.1 Porte logiche quantistiche

Rientra nell'analogia tra computer classico e quantistico anche il concetto di porta logica, possiamo dunque trovare il corrispettivo quantistico delle principali porte classiche. La porta classica più semplice è il NOT, che cambia lo stato di un bit da 0 a 1 e viceversa; la sua controparte quantistica esegue lo stesso procedimento anche su stati formati dalla sovrapposizione degli stati di base $|0\rangle$ e $|1\rangle$. Il quantum NOT agisce quindi linearmente sul generico stato $\alpha|0\rangle + \beta|1\rangle$ trasformandolo in $\alpha|1\rangle + \beta|0\rangle$; essa può essere rappresentata matematicamente come la matrice X di Pauli:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{1.25}$$

Generalizzando, è possibile intuire che tutte le porte logiche quantistiche che agiscono su un singolo qubit possono essere espresse come matrici 2x2. Per la conservazione del prodotto scalare, la matrice $U$ per rappresentare una porta logica quantistica deve essere unitaria $U^\dagger U = I$; questa richiesta è ovviamente verificata per $X$.

Altre importanti porte logiche sono rappresentate dalla $Z$ di Pauli, che inverte il segno dello stato $|1\rangle$ e, di conseguenza, la fase relativa:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{1.26}$$

e da altre tre particolari porte, l'Hadamard ($H$) e le porte $S$ e $T$:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad S = \begin{bmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}, \quad T = \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{bmatrix}. \tag{1.27}$$

$H = \frac{1}{\sqrt{2}}(X+Z)$ rappresenta la radice quadrata di una porta NOT che opera una rotazione di $90^o$ sulla sfera di Bloch attorno all'asse $\hat{x} + \hat{z}$; il risultato consiste nella trasformazione di $|0\rangle$ e $|1\rangle$ rispettivamente in $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ e $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Bisogna sottolineare che applicando due volte l'Hadamard, non si ottiene una porta NOT, sebbene corrisponda alla sua radice quadrata, ma l'identità $H^2 = I$. $S = exp(-i\frac{\pi}{4}Z)$ e $T = exp(-i\frac{\pi}{8}Z)$ rappresentano invece rotazioni di 90 e $45^o$ attorno all'asse $\hat{z}$. La porta Y non è altro che una sovrapposizione di X e Z.

Possiamo ora trattare le porte logiche a due qubit, il cui prototipo è il cosiddetto control-NOT (CNOT), il quale necessita come input, un qubit di controllo e un qubit bersaglio. Il funzionamento è basato sullo stato del qubit di controllo: se è $|0\rangle$, allora lo stato del qubit bersaglio rimane invariato, altrimenti ad esso viene applicata una porta NOT. La forma matriciale del CNOT è (l'ordine considerato è $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$):

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{1.28}$$

Il CNOT può essere espresso come la controparte quantistica della porta XOR classica, infatti l'effetto su due stati $A$ e $B$ può essere visto come $|A, B\rangle \rightarrow |A, A \oplus B\rangle$, la sua rappresentazione grafica risulta esser quella riportata in Figura 1.1.

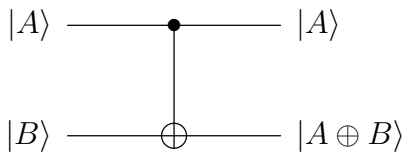



**Figura 1.1:** *Schema del circuito corrispondente ad una porta CNOT*

La differenza sostanziale tra la porta classica e quella quantistica consiste nella reversibilità del CNOT, che è infatti rappresentato in forma matriciale come una matrice unitaria (l'inversa di una matrice unitaria è unitaria); questo significa che applicando un $C^\dagger$ è possibile tornare allo stato iniziale senza alcuna perdita di informazione. Questa porta è inoltre particolarmente importante in quanto fornisce un modo semplice di creare stati entangled partendo da stati separati. Risulta essere di particolare importanza il

caso degli stati di Bell, definiti in precedenza come:

$$|\phi^{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}} \quad |\psi^{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}} \tag{1.29}$$

Essi possono essere infatti ricavati utilizzando un circuito formato da una porta Hadamard e un CNOT; dato infatti lo stato di partenza $|\alpha\beta\rangle$, si ricava lo stato di Bell $|B_{\alpha\beta}\rangle$ attraverso la seguente equazione:

$$|B_{\alpha\beta}\rangle = \frac{|0,\beta\rangle + (-1)^{\alpha}|1,\bar{\beta}\rangle}{\sqrt{2}} \tag{1.30}$$

Nel caso in cui lo stato iniziale dei due qubit corrisponda a $|10\rangle$, l'Hadamard lo trasformerà in $(|0\rangle - |1\rangle)|0\rangle/\sqrt{2}$ mentre attraverso l'applicazione del CNOT risulta immediato verificare la creazione dello stato massimamente entangled $|\phi^{-}\rangle$, come mostrato in Figura 1.2:

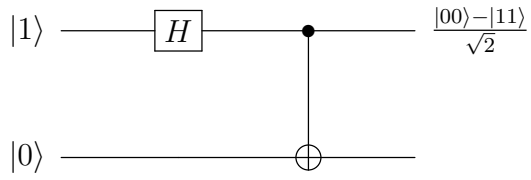



**Figura 1.2:** *Circuito che rappresenta l'effetto di una porta Hadamard e di un CNOT. Lo stato in uscita è completamente entangled e quindi condiviso tra i due qubit.*

### 1.3.2 Porte quantistiche universali

Immaginiamo che il nostro circuito abbia un insieme finito di porte logiche quantistiche $\mathcal{G} = \{U_1, U_2, ..., U_m\}$ le quali possono essere combinate arbitrariamente ai qubit desiderati attraverso delle porte SWAP ovvero porte logiche formate da tre CNOT in grado di scambiare lo stato di due qubit, come si può vedere nel circuito riportato in Figura 1.3.

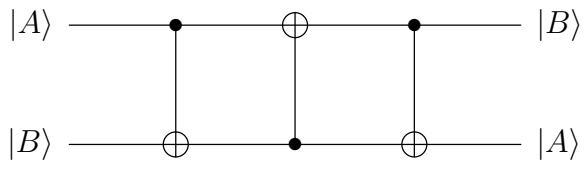



**Figura 1.3:** *Schema di un circuito corrispondente ad una porta SWAP.*

Vogliamo capire se attraverso un insieme finito di porte è possibile ricreare una qualunque porta logica arbitraria, ovvero se questo insieme è universale. Diremo che l'insieme $\mathcal{G}$

è universale se le trasformazioni unitarie che possono essere costruite attraverso questo insieme sono dense in $U(2^n)$ a meno di una fase globale. Sia dunque $V \in U(2^n)$ e $\delta > 0$, allora esiste un $\tilde{V}$ unitario creato da una combinazione finita delle porte logiche in $\mathcal{G}$ tale che, per una certa fase $e^{i\phi}$,

$$||\tilde{V} - e^{i\phi}V||_{sup} < \delta. \tag{1.31}$$

È possibile tuttavia fornire una definizione meno stringente, ovvero quella di universalità codificata che si verifica quando il nostro circuito è denso in un sottoinsieme $U(N)$ di $U(2^n)$, in cui $N$ è esponenziale in $n$.

Possiamo ora introdurre alcuni esempi di universalità esatta, ovvero quella che occorre quando è possibile riprodurre esattamente una certa trasformazione unitaria. È possibile dimostrare che un qualsiasi elemento di $U(2^n)$ può essere espresso come un circuito finito di porte logiche di due qubit, ovvero che data una generica trasformazione U esistono matrici unitarie a due livelli $U_1, U_2, ..., U_n$ tali che $U_n...U_2U_1U = I$ e che quindi $U = U_1^\dagger U_2^\dagger ...U_n^\dagger$ (le inverse di matrici unitarie a due livelli sono sempre unitarie a due livelli). Un altro esempio di insieme di porte esattamente universali è quello composto dalle porte a singolo qubit e dal CNOT, il quale può essere sostituito da una qualunque porta a due qubit "entangling" (ovvero una porta che mappa uno stato prodotto in uno non scomponibile). Le uniche porte non entangling sono lo SWAP e la porta logica $V = A \otimes B$, ovvero quella che genera il prodotto unitario dei due stati. Il CNOT tuttavia ricopre una posizione preferenziale in quanto attraverso di esso e le porte ad un qubit è possibile ricreare tutte le porte a due qubit esistenti che operano sullo stato formato da $n$ qubit.

### 1.3.3 Teorema di Solovay-Kitaev

È necessario ora comprendere l'importanza della dimensione dei circuiti utilizzati per approssimare una porta logica arbitraria, questa proprietà è fornita dal teorema di Solvay-Kitaev, prima di enunciarlo bisogna tuttavia fornire alcune definizioni. Richiediamo innanzitutto che $\mathcal{G}$, l'insieme finito di elementi di $SU(2)$, contenga il suo stesso inverso, ovvero che se $U \in \mathcal{G}$, allora $U^\dagger \in \mathcal{G}$. Definiamo inoltre una parola di lunghezza $l$ in $\mathcal{G}$ come il prodotto $g_1g_2...g_l \in SU(2)$, tale che $g_i \in \mathcal{G}$ per ogni $i$. Facendo riferimento a $\mathcal{G}_l$ si intende invece l'insieme di tutte le parole di lunghezza massima $l$ mentre $\langle\mathcal{G}\rangle$ è l'insieme di tutte le parole di lunghezza finita appartenenti a $\mathcal{G}$. Possiamo infine definire il concetto di "$\epsilon$-net": un insieme finito di trasformazioni unitarie $\mathcal{R}$ è un $\epsilon$-net in U(N) se ogni elemento di U(N) è ad una distanza minore di $\epsilon$ da un elemento di $\mathcal{R}$ (nella norma dichiarata in precedenza). È ora possibile enunciare il teorema.

**Teorema 1.3** *Solovay-Kitaev*

Sia $\mathcal{G}$ un insieme finito di elementi in SU(2) che contiene il suo stesso inverso, tale che $\langle\mathcal{G}\rangle$ sia denso in SU(2) e sia $\epsilon > 0$. Allora $\mathcal{G}_l$ è un $\epsilon$-net in SU(2) per $l = O(log^c(1/\epsilon))$ per $c \approx 2$.

Dall'enunciato del teorema è possibile comprendere quanto veloce $\mathcal{G}_l$ ricopra SU(2) al crescere di $l$, ovvero di quanto migliori l'accuratezza della nostra approssimazione in funzione del numero di porte utilizzate. La dimostrazione del teorema è riportata in [10].

### 1.3.4 Canali quantistici

Prima di parlare in modo approfondito degli errori nei computer quantistici è necessario introdurre il concetto di canale quantistico, ovvero una mappa lineare del tipo $\mathcal{E}(\rho) = \sum_a M_a^\dagger \rho M_a$, dove $\mathcal{E}$ agisce su un qualunque operatore densità e le $\{M_a\}$ rispettano la condizione completezza $\sum_a M_a^\dagger M_a = I$. Il canale quantistico rappresenta i cambiamenti dinamici che subisce un sistema, il quale passa da uno stato $\rho$ ad uno $\mathcal{E}(\rho)$; altri nomi con cui è indicato sono superoperatore e Trace-preserving completely positive map (mappa TPCP). Una canale quantistico mappa linearmente operatori densità in altri operatori densità preservando l'hermiticità, la positività e la traccia, attraverso gli operatori $\{M_a\}$ detti di Kraus.

I canali quantistici permettono di rappresentare matematicamente la decoerenza, ovvero l'evoluzione di uno stato puro in uno stato misto, molto importante nella trattazione degli errori. Studiamo ora singolarmente le proprietà:

- Reversibilità: È possibile dimostrare che ogni operatore di Kraus è proporzionale ad una singola matrice unitaria, quindi anche $\mathcal{E}$ risulta essere una mappa unitaria e di conseguenza reversibile. La decoerenza è invece irreversibile; una volta che il sistema $A$ è entangled con B, non possiamo tornare al punto di partenza senza avere accesso a B.

- Linearità: Un'evoluzione non lineare sarebbe incompatibile con l'interpretazione dell'operatore densità come un ensemble di possibili stati.

- Completa positività: Il canale rimane positivo anche quando lo consideriamo agire su una parte di un sistema più grande. Se il canale $\mathcal{E}$ mappa operatori lineari in operatori lineari tra gli spazi di Hilbert $\mathcal{H}_A$ e $\mathcal{H}_{A'}$, possiamo estendere lo spazio iniziale rendendolo del tipo $\mathcal{H}_A \otimes \mathcal{H}_B$ e considerare il canale esteso $\mathcal{E} \otimes I$ definito come una mappa tra $\mathcal{H}_A \otimes \mathcal{H}_B$ e $\mathcal{H}_{A'} \otimes \mathcal{H}_B$. Diciamo che $\mathcal{E}$ è completamente positivo se ogni sua estensione risulta essere positiva; in questo caso il canale esteso viene infatti rappresentato come $M_a \otimes I$ rispettando le condizioni necessarie.

#### Analisi dei canali quantistici

Andiamo ora ad analizzare i canali quantistici da tre punti di vista differenti: come interazioni tra il sistema e l'ambiente, introducendo una rappresentazione nota come a somma di operatori e fornendo un insieme di postulati derivanti dalla meccanica quantistica.

Partendo dal primo punto assumiamo che il sistema iniziale sia uno stato prodotto tra lo stato principale e l'ambiente $\rho \otimes \rho_{env}$. Dopo l'azione dell'operatore $U$, supponiamo che il sistema non interagisca più con l'ambiente in modo da ricavare lo stato ridotto del sistema principale attraverso la traccia parziale:

$$\mathcal{E}(\rho) = tr_{env}[U^\dagger(\rho \otimes \rho_{env})U]. \tag{1.32}$$

Questa equazione corrisponde alla prima definizione di operazione quantistica (consideriamo infatti i canali quantistici e le misure generalizzate come esempi particolarmente rilevanti di operazioni quantistiche). Sebbene la richiesta di stato prodotto è abbastanza stringente in quanto un sistema interagisce costantemente con l'ambiente esterno, è un'approssimazione in molti casi ragionevole per la nostra trattazione. Dato che l'ambiente ha infiniti gradi di libertà supponiamo inoltre che, se lo spazio di Hilbert $\mathcal{H}$ dello spazio principale ha dimensione $d$, allora possiamo modellare l'ambiente in modo da avere uno spazio complessivo di dimensione $d^2$.

La rappresentazione a somma di operatori è invece una riformulazione dell'equazione precedente in termini operatoriali. Definisco $|e_k\rangle$ come una base ortonormale per lo spazio degli stati dell'ambiente, il quale avrà stato iniziale $\rho_{env} = |e_0\rangle \langle e_o|$ (possiamo introdurlo in uno stato puro in quanto siamo in grado di purificarlo). Posso quindi riscrivere l'equazione precedente come:

$$\mathcal{E}(\rho) = \sum_k \langle e_k| U^\dagger(\rho \otimes |e_0\rangle \langle e_0|)U |e_k\rangle = \sum_k E_k^\dagger \rho E_k, \tag{1.33}$$

dove $E_k = \langle e_k|U|e_0\rangle$ è un operatore nello spazio degli stati del sistema principale, nonché l'operatore di Kraus definito precedentemente. È tuttavia possibile definire delle operazioni quantistiche che non preservano la traccia, esse descrivono infatti il caso in cui venga effettuata una misura sullo stato di sistema e ambiente dopo l'interazione unitaria in modo ottenere informazioni sullo stato stesso. Le mappe $\mathcal{E}$ della forma (1.32), e che soddisfano la relazione $\sum_k = E_k^\dagger E_k \leq 1$ forniscono la seconda definizione di operazioni quantistiche, più generale della precedente in quanto considera il caso in cui non viene preservata la traccia. Questa rappresentazione permette di conoscere l'evoluzione del sistema ignorando le proprietà dell'ambiente. In definitiva l'azione dell'operazione quantistica è equivalente a sostituire randomicamente lo stato $\rho$ con $E_k^\dagger \rho E_k / \mathrm{Tr}(E_k^\dagger \rho E_k)$ con probabilità $\mathrm{Tr}(E_k^\dagger \rho E_k)$ (molto simile al concetto di errore classico). È importante sottolineare che questa rappresentazione non è unica, infatti differenti processi fisici possono produrre la medesima dinamica del sistema come dichiarato dal teorema seguente:

**Teorema 1.4** *Libertà unitaria della rappresentazione a somma di operatori*

Presi $\{E_1, ..., E_m\}$ e $\{F_1, ..., F_n\}$ siano gli operatori di Kraus che formano le operazioni $\mathcal{E}$ e $\mathcal{F}$. Si aggiungano operatori nulli alla lista più corta in modo da ottenere $m = n$. Allora $\mathcal{E} = \mathcal{F}$ se e solo se esistono dei numeri complessi $u_{ij}$ tale che $E_i = \sum_j u_{ij} F_j$ e $u_{ij}$ è una matrice $m \times m$.

Come già accennato in precedenza, il terzo modo di analizzare le operazioni quantistiche è attraverso l'utilizzo di alcuni assiomi fisicamente validi. Definiamo quindi $\mathcal{E}$ come una mappa dall'insieme di operatori densità del sistema $Q_1$ a quello del sistema $Q_2$ con le seguenti proprietà assiomatiche:

- $tr[\mathcal{E}(\rho)]$ è la probabilità che avvenga il processo rappresentato da $\mathcal{E}$, essendo $\rho$ lo stato iniziale.
- $\mathcal{E}$ è una mappa lineare convessa sull'insieme delle matrici densità; per le probabilità $\{p_i\}$:
$$\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}(\rho_i). \tag{1.34}$$
- $\mathcal{E}$ è una mappa completamente positiva.

Possiamo collegarci ai due punti precedenti attraverso il seguente teorema.

**Teorema 1.5** La mappa $\mathcal{E}$ soddisfa i tre assiomi sopracitati se e solo se
$$\mathcal{E}(\rho) = \sum_k E_k^\dagger \rho E_k \tag{1.35}$$
per un certo insieme di operatori $\{E_i\}$, tali che $\sum_k = E_k^\dagger E_k \leq 1$.

### 1.3.5 Nuovi postulati

Possiamo concludere il capitolo riadattando i postulati della meccanica quantistica alla base delle nuove definizioni fornite.

- ***Stati*** Uno stato è un operatore densità, ovvero un operatore non negativo hermitiano a traccia unitaria su uno spazio di Hilbert.
- ***Misure*** Una misura è una POVM, la partizione di un'unità fatta da operatori non negativi. Quando la misura $\{E_a\}$ è applicata allo stato $\rho$, si ottiene il risultato a con probabilità $\mathrm{Tr}(E_a \rho)$
- ***Dinamica*** L'evoluzione del sistema è descritta da una mappa TPCP.

# Capitolo 2

# Gli errori quantistici e la QECC

*In questo secondo capitolo viene trattato in modo approfondito il concetto di errore quantistico. Sono dunque introdotte le principali regole di correzione e riportati alcuni esempi di codici. La parte finale del capitolo è dedicata alla descrizione degli stabilizers codes, utili per introdurre la trattazione del terzo capitolo. I riferimenti presenti in questo capitolo sono tratti da* [10–12].

## 2.1 Errori quantistici

Prima di dedicarci alla correzione degli errori quantistici è necessario introdurre alcuni esempi di canali particolarmente rilevanti, attraverso i quali è possibile spiegare il quantum noise, ovvero quell'insieme di interazioni tra il sistema e l'ambiente che modifica l'informazione quantistica. Il nostro interesse ricade dunque su capire come ciò avviene per cercare di limitarlo ed eventualmente correggerlo. Per ora vedremo canali che agiscono solamente sul singolo qubit in cui il canale $\mathcal{E}$ rappresenta la trasmissione di informazione con una non certa sicurezza.

Prima di affrontare i singoli esempi è necessario definire la rappresentazione di Bloch, in cui il generico operatore densità è espresso come:

$$\rho(\vec{r}) = \frac{1}{2}(I + \vec{r} \cdot \vec{\sigma}), \tag{2.1}$$

dove $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ è il vettore di Pauli, mentre $\vec{r}$ è la cosiddetta "polarizzazione di spin" del qubit, ovvero un vettore a tre componenti reali. L'equazione precedente può dunque essere riscritta nel seguente modo:

$$\rho(\vec{r}) = \frac{1}{2}\begin{bmatrix} 1 + r_z & r_x - ir_y \\ r_x + ir_y & 1 - r_z \end{bmatrix}. \tag{2.2}$$

Possiamo dunque rappresentare in modo esplicito un'arbitraria operazione quantistica come:

$$\vec{r} \xrightarrow{\mathcal{E}} \vec{r'} = M\vec{r} + \vec{c}, \tag{2.3}$$

dove M è una matrice reale e $\vec{c}$ è un vettore costante; $\mathcal{E}$ è quindi una mappa affine essendo un'applicazione dalla sfera di Bloch in se stessa.

Possiamo interpretare l'effetto della mappa affine attraverso la rappresentazione polare di $M$, ovvero $M = UJ$ dove $U$ è una matrice unitaria mentre $J$ è Hermitiana. Dato che $M$ è una matrice reale, allora sia $U$ che $J$ sono reali e possiamo quindi scrivere $U = O$ in quanto matrice ortogonale con det = 1, che corrisponde ad una rotazione, e $J = S$ data la sua simmetria. In questo modo è possibile intuitivamente capire come la (2.3) non sia altro che una deformazione della sfera di Bloch lungo l'asse determinato da $S$, seguita da una rotazione causata da O e una traslazione di $\vec{c}$.

### 2.1.1 Canale depolarizzante

Il canale depolarizzante è un modello di decoerenza con particolari proprietà di simmetria. Immaginiamo infatti di avere un qubit che è soggetto ad un errore (si depolarizza) con una certa probabilità $p$. Un canale depolarizzante può provocare tre tipi differenti di errore:

- **Bit flip**: $|\psi\rangle \to \sigma_x |\psi\rangle$ scambia i vettori della base computazionale con probabilità p. Per un singolo qubit abbiamo che $\mathrm{Tr}(\rho^2) = (1 + |r|^2)/2$ dove $|r|$ è la norma del vettore di Bloch; sappiamo inoltre che la matrice $\sigma_x$ provoca una contrazione della sfera, perciò $\mathrm{Tr}(\rho^2)$ non può che diminuire sotto l'effetto di un bit flip. Si può quindi perdere la purezza dello stato in cui ci si trova.

- **Phase flip**: $|\psi\rangle \to \sigma_z |\psi\rangle$ inverte il segno del vettore $|1\rangle$ della base computazionale con probabilità p. Geometricamente è rappresentato come una proiezione del vettore di Bloch lungo l'asse $\hat{z}$, vi è dunque una contrazioni delle componenti $\hat{x}$ e $\hat{y}$.

- **Bit-Phase flip**: $|\psi\rangle \to \sigma_y |\psi\rangle$ è la combinazione di un bit flip e di un phase flip in quanto $\sigma_y = i\sigma_x\sigma_z$.

Il canale depolarizzante mappa quindi un qubit $A$ in se stesso ed è realizzato attraverso un'isometria tra $A$ e $A \otimes E$ dove $E$ è lo spazio di Hilbert quadridimensionale legato all'ambiente:

$$\begin{aligned} U_{A\to A\otimes E} : |\psi\rangle_A \to & \sqrt{1-p}\,|\psi\rangle_A \otimes |0\rangle_E + \\ & \sqrt{\frac{p}{3}}(\sigma_x |\psi\rangle_A \otimes |1\rangle_E + \sigma_y |\psi\rangle_A \otimes |2\rangle_E + \sigma_z |\psi\rangle_A \otimes |3\rangle_E) \end{aligned} \tag{2.4}$$

L'ambiente evolve quindi uno dei quattro stati ortogonali, per cui se fossimo in grado misurare il suo stato nella base $\{|a\rangle_E\} = |0\rangle_E, |1\rangle_E, |2\rangle_E, |3\rangle_E$, potremmo sapere con certezza quale errore si è verificato.

Possiamo esprimere il canale nella rappresentazione a somma di operatori applicando la traccia parziale sull'ambiente nella base $\{|a\rangle_E\}$ e ottenendo $M_a = {}_{\mathrm{E}}\langle a|\, U$ dove $U$ è un operatore generico. Si ottiene dunque:

$$M_0 = \sqrt{1-p}I, \quad M_1 = \sqrt{\frac{p}{3}}\sigma_x, \quad M_2 = \sqrt{\frac{p}{3}}\sigma_y, \quad M_3 = \sqrt{\frac{p}{3}}\sigma_z. \tag{2.5}$$

Possiamo facilmente verificare la condizione di normalizzazione sapendo che il quadrato delle matrici di Pauli è l'identità:

$$\sum_a M_a^\dagger M_a = \left[(1-p) + 3\frac{p}{3}\right] I = I, \tag{2.6}$$

mentre l'evoluzione del generico operatore densità è descritta da

$$\rho \to \rho' = (1-p)\rho + \frac{p}{3}(\sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z), \tag{2.7}$$

in questo caso la somma viene fatta sui possibili quattro stati finali dell'ambiente che sono teoricamente distinguibili.

Per capire fino in fondo l'importanza di questo canale possiamo rifarci agli stati di Bell. Scelta infatti una coppia di qubit $R$ e $A$ nello stato $|\phi^+\rangle$ consideriamo il caso in cui il canale agisce soltanto su $A$:

$$|\phi^+\rangle\langle\phi^+| \to (1-p)\,|\phi^+\rangle\langle\phi^+| + \frac{p}{3}(|\psi^+\rangle\langle\psi^+| + |\psi^-\rangle\langle\psi^-| + |\phi^-\rangle\langle\phi^-|). \tag{2.8}$$

Possiamo ora prendere in esame il caso in cui $p = 3/4$ per cui il sistema considerato diventa:

$$|\phi^+\rangle\langle\phi^+| \to \frac{1}{4}(|\phi^+\rangle\langle\phi^+| + |\psi^+\rangle\langle\psi^+| + |\psi^-\rangle\langle\psi^-| + |\phi^-\rangle\langle\phi^-|) = \frac{I}{4}. \tag{2.9}$$

Come si può vedere dal valore dell'operatore densità si ottiene uno stato totalmente misto. Possiamo eseguire i medesimi calcoli per uno stato puro di $A$ ed eseguire la traccia parziale su R per ottenere:

$$\rho_A \to {}_R\langle\psi^*|\, 2\left(\frac{1}{4}I_{RA}\right)|\psi^*\rangle_R = \frac{1}{2}I_A, \tag{2.10}$$

dove il fattore due è utilizzato per la normalizzazione. Si ottiene dunque che un qubit viene mappato per p=3/4 in uno stato massimamente misto, qualunque sia il suo stato iniziale. L'informazione contenuta nel qubit è quindi compromessa.

Possiamo esprimere l'evoluzione di uno stato massimamente entangled in un secondo modo:

$$\rho \to \left(1 - \frac{4}{3}p\right)\rho + \frac{4}{3}p\left(\frac{1}{4}I_{RA}\right). \tag{2.11}$$

In questo caso abbiamo una diversa definizione di errore, esso infatti occorre con probabilità $4/3p$ e il suo effetto è quello di randomizzare completamente il sistema. Se applico questo errore così definito ad un sistema quantistico di dimensione arbitraria d ottengo una nuova definizione di canale depolarizzante:

$$\rho \to \left(1 - \frac{4}{3}p\right)\rho + \frac{4}{3}p\left(\frac{1}{d}I\right). \tag{2.12}$$

Siamo inoltre in grado di sapere quanto il canale abbia modificato il sistema quantistico attraverso la "entanglement fidelity" $F_e$ che quantifica quanto l'operatore densità finale sia vicino allo stato massimamente entangled originale $|\phi^+\rangle$: $F_e = \langle\phi^+|\rho'|\phi^+\rangle$. In questo caso si ha $F_e = 1-p$; la fidelity può essere quindi interpretata come la probabilità che l'errore non si sia verificato.

In ultima analisi possiamo considerare l'effetto del canale depolarizzate in termini geometrici applicando le trasformazioni descritte in precedenza al generico operatore densità sulla sfera di Bloch:

$$\begin{aligned}\rho'(\vec{r}) &= \left(1 - \frac{4}{3}p\right)\left[\frac{1}{2}(I + \vec{r}\cdot\vec{\sigma})\right] + \frac{4}{3}p\left(\frac{I}{2}\right) \\ &= \frac{1}{2}\left[I + \left(1 - \frac{4}{3}p\right)\vec{r}\cdot\vec{\sigma}\right] = \rho(\vec{r'}),\end{aligned} \tag{2.13}$$

dove è stata utilizzata l'importante relazione:

$$\vec{r'} = \left(1 - \frac{4}{3}p\right)\vec{r}. \tag{2.14}$$

Essa esplica come la sfera si contragga sotto l'effetto del canale e lo spin di polarizzazione sia riscalato di un fattore $1 - 4/3p$, per questo motivo il canale è detto depolarizzante (ovviamente ciò vale per $p \leq 3/4$).

È interessante notare come questo canale non sia invertibile, infatti per decontrarre la sfera bisognerebbe passare ad un $|\vec{r}| > 1$ e questo porterebbe l'operatore densità ad avere autovalori negativi.

### 2.1.2 Canale di phase damping

Possiamo ora dedicarci alla trattazione di un esempio di rumore puramente quantistico, il canale di attenuazione di fase. Gli autostati di un sistema non cambiano in funzione

del tempo, tuttavia si accumula una fase proporzionale agli autovalori, la quale comporta che, dopo un certo periodo di tempo, una parte dell'informazione legata alla fase sia irrimediabilmente perduta. È possibile dunque descrivere il canale attraverso una rappresentazione isometrica del tipo:

$$\begin{aligned} |0\rangle_A &\to \sqrt{1-p}\,|0\rangle_A \otimes |0\rangle_E + \sqrt{p}\,|0\rangle_A \otimes |1\rangle_E\,, \\ |1\rangle_A &\to \sqrt{1-p}\,|1\rangle_A \otimes |0\rangle_E + \sqrt{p}\,|1\rangle_A \otimes |2\rangle_E\,, \end{aligned} \tag{2.15}$$

in cui è facile notare come gli autostati di $A$ non siano sottoposti a nessun cambiamento nella base computazionale, mentre avviene invece la cosiddetta phase kick, per cui l'ambiente transisce con probabilità $p$ nello stato $|1\rangle_E$ se $A$ si trova in $|0\rangle$ e nello stato $|2\rangle_E$ se si trova in $|1\rangle$. La base computazione è dunque una base privilegiata per questo canale quantistico in quanto è l'unica che non subisce variazioni sotto l'effetto del canale.

Applicando la traccia parziale su $E$ è possibile ottenere gli operatori di Kraus:

$$M_0 = \sqrt{1-p}I, \quad M_1 = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad M_2 = \sqrt{p}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}. \tag{2.16}$$

Tuttavia siamo in grado di esprimere l'operazione solamente attraverso due operatori:

$$M_1 = \frac{\sqrt{p}}{2}(I + \sigma_z), \quad M_2 = \frac{\sqrt{p}}{2}(I - \sigma_z) \tag{2.17}$$

che rispettano ovviamente la relazione di completezza e da cui è possibile ricavare:

$$\mathcal{E}(\rho) = \sum_a M_a \rho M_a = (1 - \frac{1}{2}p)\rho + \frac{1}{2}p\sigma_z\rho\sigma_z \tag{2.18}$$

e risulta quindi intuitivo identificare l'azione del canale come l'applicazione di $\sigma_z$ con probabilità $1/2$. L'effetto può essere spiegato attraverso la rappresentazione matriciale di $\rho$:

$$\mathcal{E}\begin{bmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{bmatrix} = \begin{bmatrix} \rho_{00} & (1-p)\rho_{01} \\ (1-p)\rho_{10} & \rho_{11} \end{bmatrix}, \tag{2.19}$$

dove rimangono invarianti i termini sulla diagonale come già accennato in precedenza.

Possiamo ora prendere in considerazione il caso in cui il canale non è discreto, ovvero presenta una probabilità dipendente dal tempo $\Gamma$, poniamo quindi $p = \Gamma\Delta t \ll 1$ per un $\Delta t$ piccolo. Se tuttavia esaminiamo la generica evoluzione per un certo $t = n\Delta t$, il canale quantistico risultante diventa $\mathcal{E}^n$ e ciò, considerando il limite $n \to \infty$, provoca una soppressione dei termini non diagonali dell'ordine di

$$(1-p)^n = (1 - \Gamma t/n)^n \to e^{-\Gamma t}. \tag{2.20}$$

L'operatore densità del generico stato $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ è soggetto alla seguente evoluzione per $t \gg \Gamma^{-1}$:

$$\begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix} \to \begin{bmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix}. \tag{2.21}$$

Si ha dunque una decoerenza dello stato nella base computazionale, questo decadimento esponenziale è tipico del phase damping.

Come abbiamo già visto per il canale di phase flip un generico vettore di Bloch subisce una deformazione del tipo:

$$\vec{r} = (r_x, r_y, r_z) \to ((1-p)r_x, (1-p)r_y, r_z) = \vec{r'}, \tag{2.22}$$

ovvero si ha una contrazione della sfera lungo gli assi $\hat{x}$ e $\hat{y}$. Per grandi $\Gamma t$ la sfera si riduce al solo asse $\hat{z}$; si ottiene ovviamente, come in ogni caso di decoerenza, uno stato misto. La principale differenza con il phase flip, che rende questo canale particolarmente interessante, è la sua continuità. Può essere importante sottolineare che non esiste alcun canale quantistico in grado di sopprimere una sola componente del vettore di Bloch. Non esiste infatti alcuna mappa completamente positiva che associa alla sfera iniziale uno sferoide tangente ad essa lungo l'equatore. Geometricamente non è infatti possibile deformare un oggetto piatto in una sfera tridimensionale mantenendo le distanze tra i punti.

Siamo ora in grado di mostrare cosa succede sottoponendo ad un canale di questo tipo un singolo atomo preparato nel ground state $|0\rangle$ o nel suo stato eccitato $|1\rangle$, i quali hanno una differenza energetica di $\hbar\omega$. Senza considerare la decoerenza, lo stato dell'atomo al tempo $t$ sarebbe:

$$|\psi(t)\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{-i\omega t}|1\rangle), \tag{2.23}$$

mentre l'effetto di un canale di phase damping modificherebbe l'operatore densità nel modo seguente:

$$\rho(t) = \frac{1}{2}\begin{bmatrix} 1 & e^{i\omega t}e^{-\Gamma t} \\ e^{-i\omega t}e^{-\Gamma t} & 1 \end{bmatrix}. \tag{2.24}$$

L'effetto corrisponde, come descritto in precedenza, al decadimento esponenziale dei termini non diagonali della matrice. Lo stato risultante dopo un certo tempo $t \gg \Gamma^{-1}$ è dunque:

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle). \tag{2.25}$$

Appare quindi immediato calcolare la probabilità di misurare lo stato $|+\rangle$ al tempo $t$:

$$p(|+\rangle, t) = \langle +|\rho|+\rangle = \frac{1}{4}[2 + e^{-\Gamma t}(e^{i\omega t} + e^{-i\omega t}) = \frac{1}{2}(1 + e^{-\Gamma t}\cos\omega t). \tag{2.26}$$

Il valore di $\Gamma$ risulta quindi essere una proprietà del sistema che può essere misurata variando il tempo $t$ tra la preparazione e la misura dello stesso, fittando poi la visibilità decrescente delle oscillazioni coerenti della probabilità come una funzione esponenziale del tempo.

### 2.1.3 Canale di amplitude damping

Passiamo ora allo studio di un terzo canale particolarmente rilevante in quanto descrivente la dissipazione di energia di uno stato quantistico, come quella di un atomo che emette spontaneamente un fotone. Effettuando una POVM sul fotone possiamo ottenere informazioni su sullo stato iniziale dell'atomo.

Bisogna innanzitutto definire il ground state $|0\rangle_A$ e lo stato eccitato $|1\rangle_A$ e si assume che l'ambiente sia il campo elettromagnetico del vuoto nello stato $|0\rangle_E$. Si avrà dunque una probabilità $p$ che dopo un certo tempo $t$ l'atomo emetta un fotone modificando lo stato dell'ambiente in $|1\rangle_E$. L'evoluzione complessiva risulta quindi essere:

$$\begin{aligned} &|0\rangle_A \otimes |0\rangle_E \to |0\rangle_A \otimes |0\rangle_E \,, \\ &|1\rangle_A \otimes |0\rangle_E \to \sqrt{1-p}\,|1\rangle_A \otimes |0\rangle_E + \sqrt{p}\,|0\rangle_A \otimes |1\rangle_E \,. \end{aligned} \tag{2.27}$$

Come descritto in precedenza possiamo trovare gli operatori di Kraus operando una traccia parziale sull'ambiente e ottenendo:

$$M_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{bmatrix}, \quad M_1 = \begin{bmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{bmatrix}, \tag{2.28}$$

dove $M_0$ descrive il caso in cui non si verifica l'emissione mentre $M_1$ quello in cui occorre il salto quantistico; è facile infine verificare che gli operatori sopracitati rispettano la condizione di completezza $M_0^\dagger M_0 + M_1^\dagger M_1 = I$. L'operazione quantistica risultante è descritta come segue:

$$\begin{aligned} \rho \to \mathcal{E}(\rho) &= M_0 \rho M_0^\dagger + M_1 \rho M_1^\dagger \\ &= \begin{bmatrix} \rho_{00} & \sqrt{1-p}\rho_{01} \\ \sqrt{1-p}\rho_{10} & (1-p)\rho_{11} \end{bmatrix} + \begin{bmatrix} p\rho_{11} & 0 \\ 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} \rho_{00} + p\rho_{11} & \sqrt{1-p}\rho_{01} \\ \sqrt{1-p}\rho_{10} & (1-p)\rho_{11} \end{bmatrix}. \end{aligned} \tag{2.29}$$

Come prima possiamo analizzare il caso dipendente dal tempo con rate di decadimento $\Gamma$ tale che $\Gamma \Delta t \ll 1$ per un piccolo intervallo di tempo. Consideriamo quindi un tempo $t = n\Delta t$ su cui possiamo basarci per creare l'operatore densità a cui viene applicato $n$ volte il canale quantistico in modo da ottenere $(1-p)^n = (1 - \Gamma t/n)^n \to e^{-\Gamma t}$.

L'operatore da noi cercato corrisponde quindi a:

$$\rho(t) = \begin{bmatrix} \rho_{00} + (1 - e^{-\Gamma t})\rho_{11} & e^{-\Gamma t/2}\rho_{01} \\ e^{-\Gamma t/2}\rho_{10} & e^{-\Gamma t}\rho_{11} \end{bmatrix}. \tag{2.30}$$

È interessante vedere come il tempo di decadenza della popolazione nello stato eccitato $T_1$, e quello dei termini diagonali dell'operatore $T_2$ sono legati dalla relazione

$$T_2 = 2\Gamma^{-1} = 2T_1 \tag{2.31}$$

per cui un atomo si trova nello stato fondamentale con probabilità praticamente unitaria dopo un tempo $t \gg T_1$. L'effetto di questo canale dipendente dal tempo sulla sfera di Bloch risulta quindi essere il seguente:

$$\vec{r} = (r_x, r_y, r_z) \to (e^{-\Gamma t/2} r_x, e^{-\Gamma t/2} r_y, (1 - e^{-\Gamma t}) + e^{-\Gamma t} r_z) = \vec{r'}. \tag{2.32}$$

Per tempi lunghi rimane solamente il vettore $\vec{r'} = (0, 0, 1)$ e possiamo verificare che il risultato coincide con lo stato $|0\rangle$:

$$\rho(\vec{r'}) = \frac{1}{2}(I + Z) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}. \tag{2.33}$$

È tuttavia necessario ricordare che considerare il caso in cui lo stato $|0\rangle$ è lo stato fondamentale dell'atomo risulta essere una scelta totalmente arbitraria. Se anche questo stato fosse sottoposto a decoerenza ci troveremmo nel caso chiamato amplitude damping generalizzata.

Vogliamo ora tornare alla descrizione fatta all'inizio di questa sezione in cui si accennava alla possibilità di conoscere lo stato iniziale dell'atomo misurando l'ambiente (il fotone emesso). Consideriamo innanzitutto l'evoluzione di una sovrapposizione dei due stati dell'atomo:

$$(\alpha \left|0\right\rangle_A + \beta \left|1\right\rangle_A) \otimes \left|0\right\rangle_E \to (\alpha \left|0\right\rangle_A + \beta\sqrt{1-p} \left|1\right\rangle_A) \otimes \left|0\right\rangle_E + \beta\sqrt{p} \left|0\right\rangle_A \otimes \left|1\right\rangle_E. \tag{2.34}$$

Per studiarne l'evoluzione nel tempo possiamo applicare la mappa $n$ volte come in precedenza, richiedendo però che i fotoni emessi siano distinguibili e di conseguenza ortogonali. Queste assunzioni portano a considerare una misura POVM con $n+1$ operatori di Kraus che corrispondono allo stato del vuoto e agli n fotoni ortogonali. Le matrici, per $k = 1, 2, ..., n$, sono quindi esprimibili come:

$$M_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{(1-p)^n} \end{bmatrix}, \quad M_k = \begin{bmatrix} 0 & \sqrt{(1-p)^{k-1}p} \\ 0 & 0 \end{bmatrix}. \tag{2.35}$$

Questa trattazione porta alla conclusione per cui se viene rilevato un fotone si ha la certezza che lo stato si trovava in $|1\rangle_A$ e che ora sia decaduto in $|0\rangle_A$. Se invece il fotone non viene rilevato, vuol dire che è stata fatta una proiezione sullo stato vuoto dell'ambiente e, per grandi $n$, è stato quindi preparato lo stato:

$$M_0(\alpha |0\rangle_A + \beta |1\rangle_A) = \alpha |0\rangle_A + e^{-\Gamma t/2}\beta |1\rangle_A . \tag{2.36}$$

Nel limite di $t \to \infty$ la nostra misura POVM diventa ortogonale in quanto la rilevazione o meno di un fotone porta a conoscere con certezza in quale dei due stati della base computazionale si trovava il qubit.

## 2.2 La quantum error correction

Uno dei principali obiettivi nella realizzazione di un computer quantistico è quello di riuscire a codificare l'informazione in modo che sia il meno possibile soggetta ad errori. La codifica viene fatta aggiungendo qualche informazione ridondante al messaggio, il quale deve essere poi decodificato per recuperare l'informazione originale.

Dalla trattazione precedente è possibile cogliere le principali sfide che intercorrono nella correzione degli errori nei computer quantistici. Classicamente l'unico errore esistente è il bit flip che cambia lo stato di un bit da 0 a 1 e viceversa, questo tipo di errore è tuttavia facilmente controllabile: possiamo infatti misurare e di conseguenza clonare un singolo bit e correggere i flip servendoci della ridondanza. Nella correzione degli errori quantistici troviamo invece quattro ulteriori ostacoli da superare per la conservazione dell'informazione:

1. **Errori sulla fase** Come abbiamo già visto nel canale di phase damping;
2. **Errori continui** Esiste un continuo di errori che possono intaccare un singolo qubit, servirebbe quindi una precisione infinita;
3. **La misura disturba il sistema** Le osservazioni distruggono l'informazione quantistica;
4. **No-cloning** È impossibile clonare uno stato quantistico ignoto come conseguenza del Teorema di NO-cloning.

   **Teorema 2.1** *Teorema di No-cloning*

   Dato il sistema A nello stato $|\psi\rangle$ e il sistema B nello stato puro $|s\rangle$, non esiste alcuna trasformazione unitaria che trasforma lo stato di B in quello di A senza modificare quest'ultimo.

**Dim.** Lo stato iniziale della macchina copiatrice è $|\psi\rangle \otimes |s\rangle$ e supponiamo per assurdo che esista una trasformazione unitaria U in grado di copiare lo stato di A:

$$|\psi\rangle \otimes |s\rangle \rightarrow U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \,. \tag{2.37}$$

Supponiamo in particolare che la copia funzioni per due particolari stati puri $|\psi\rangle$ e $|\phi\rangle$, tale che:

$$\begin{aligned} U(|\psi\rangle \otimes |s\rangle) &= |\psi\rangle \otimes |\psi\rangle \,, \\ U(|\phi\rangle \otimes |s\rangle) &= |\phi\rangle \otimes |\phi\rangle \,. \end{aligned} \tag{2.38}$$

È possibile eseguire il prodotto interno delle due equazioni per ottenere:

$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2. \tag{2.39}$$

Risulta quindi immediato comprendere come $|\psi\rangle$ e $|\phi\rangle$ debbano essere uguali od ortogonali. Il fatto di poter clonare solamente lo stato ortogonale ad un altro rende impossibile la clonazione di uno stato ignoto.

### 2.2.1 I primi codici di correzione

Un quantum error correcting code (QECC) è una funzione che ha come dominio uno spazio di Hilbert di dimensione $2^k$, che corrisponde a $k$ qubit detti qubit logici, i quali vengono mappati in $n$ qubit, tale che $n > k$. I qubit logici contengono l'informazione che è nostro interesse preservare, mentre i rimanenti $n-k$ qubit sono utilizzati per realizzare la codifica.

Iniziamo la trattazione con il codice originale di Shor, che è in grado di proteggere un qubit logico ($k = 1$) dal bit flip utilizzandone $n = 3$. L'obiettivo è quello di correggere l'errore senza misurare direttamente lo stato dei qubit. Ci serviamo a questo punto degli stati logici:

$$\begin{aligned} |0\rangle &\rightarrow |\bar{0}\rangle \equiv |000\rangle \,, \\ |1\rangle &\rightarrow |\bar{1}\rangle \equiv |111\rangle \,, \end{aligned} \tag{2.40}$$

in modo da modificare la generica sovrapposizione di stati e ottenere:

$$\alpha\,|0\rangle + \beta\,|1\rangle \rightarrow \alpha\,|\bar{0}\rangle + \beta\,|\bar{1}\rangle \,. \tag{2.41}$$

Prima della codifica, lo spazio di Hilbert corrispondente al singolo qubit è di dimensione 2, infatti $|\psi\rangle \in \mathcal{H}_2 = span\{|0\rangle\,, |1\rangle\}$. Lo stato logico in questo caso fa parte di uno spazio 6-dimensionale (la base computazionale è formata da 8 vettori):

$$|\bar{\psi}\rangle \in \mathcal{H}_6 = span\{|000\rangle\,, |001\rangle\,, |010\rangle\,, |011\rangle\,, |100\rangle\,, |101\rangle\,, |110\rangle\,, |111\rangle\}. \tag{2.42}$$

Più precisamente lo stato logico è definito all'interno di un sottospazio bidimensionale di $\mathcal{H}_6$, chiamato spazio di codice $\mathcal{C}$:

$$|\bar{\psi}\rangle \in \mathcal{C} = span\{|000\rangle\,, |111\rangle\} \subset \mathcal{H}_6. \tag{2.43}$$

Per non distruggere lo stato del singolo qubit è necessario misurare osservabili che facciano riferimento ad almeno due qubit: dato infatti il sistema $|x, y, z\rangle$ potremo conoscere univocamente lo stato misurando i valori di $y \oplus z$ e $x \oplus z$. Per un singolo flip i due bit $(y \oplus z, x \oplus z)$ costituiscono la sindrome dell'errore e permettono di individuare, oltre alla presenza del flip, anche la sua posizione. È importante notare che la misura della sindrome non modifica lo stato del sistema in quanto si agisce soltanto su alcuni osservabili relativi tra i due qubit. In questo modo è possibile misurare la natura degli errori senza decodificare l'informazione. Supponiamo ora di assistere ad un flip del primo qubit:

$$\alpha |000\rangle + \beta |111\rangle \rightarrow \alpha |100\rangle + \beta |011\rangle , \tag{2.44}$$

la misura della sindrome corrisponderebbe a $(0, 1)$ che ci indica il numero del qubit su cui si è verificato l'errore in notazione binaria. L'effetto dell'errore sullo spazio di codice $\mathcal{C}$ consiste nella rotazione in un nuovo sottospazio:

$$X_1 |\bar{\psi}\rangle \in \mathcal{F}_1 \subset \mathcal{H}_8, \tag{2.45}$$

dove $\mathcal{F}_1 = span\{|100\rangle , |011\rangle\}$ è detto sottospazio d'errore. In questo particolare caso sono presenti tre sottospazi d'errore: oltre al già citato $\mathcal{F}_1$ esistono anche $\mathcal{F}_2 = span\{|010\rangle , |101\rangle\}$ e $\mathcal{F}_3 = span\{|001\rangle , |110\rangle\}$, che corrispondono agli spazi dove si trova lo stato logico dopo un flip del secondo e terzo qubit rispettivamente. Se lo stato logico non è soggetto ad errore, esso si trova nel sottospazio $\mathcal{C}$, se invece l'errore si verifica, fa parte di $\mathcal{F}$; i due sottospazi sono inoltre ortogonali. È dunque possibile distinguere in quale sottospazio si trovi il nostro stato logico attraverso una misura proiettiva senza compromettere l'informazione codificata. Queste misure sono dette stabilizzatrici.

Vogliamo ora dedicarci al caso in cui l'errore sia piccolo e che trasformi gli stati logici nel seguente modo:

$$\begin{aligned} |000\rangle &\rightarrow |000\rangle + \epsilon |100\rangle , \\ |111\rangle &\rightarrow |111\rangle - \epsilon |011\rangle . \end{aligned} \tag{2.46}$$

Possiamo tuttavia applicare lo stesso procedimento utilizzato in precedenza; la misura della sindrome $(y \oplus z, x \oplus z)$ proietta infatti lo stato in uno dei due autostati. Il risultato di questa proiezione risulta essere con probabilità $1 - |\epsilon|^2$ l'autostato originale, mentre, nel caso in cui si verificasse una proiezione su quello ortogonale, esso verrebbe corretto come in precedenza.

Il circuito legato alla codifica e all'estrazione della sindrome risulta quindi essere quello riportato in Figura 2.1, dove con E è indicato l'errore che avviene su uno dei tre qubit mentre $|0\rangle_{A1}$ e $|0\rangle_{A2}$ sono i qubit ancilla sui quali viene riportato il risultato della somma. Un qubit ancilla non è altro che un qubit ausiliario utilizzato per immagazzinare l'informazione derivante dalle misure dei qubit principali; la misura di questi qubit ausiliari fornisce la sindrome desiderata.

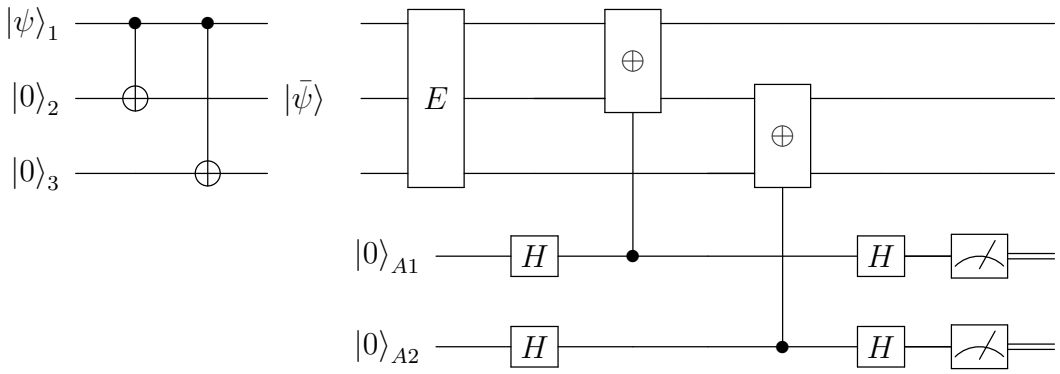



**Figura 2.1:** *Schema circuitale di codice a tre qubit. L'informazione $|\psi\rangle$ contenuta in un qubit viene prima codificata per creare lo stato logico $|\bar{\psi}\rangle$. Dopo l'effetto di un possibile errore E, vengono effettuare due operazioni sui tre qubit il cui risultato è riportato nelle ancillae $A_1$ e $A_2$ e successivamente misurato per ottenere la sindrome.*

Attraverso questa breve trattazione abbiamo già risolto tre dei quattro problemi citati in precedenza: l'informazione non è stata danneggiata dalla misura della sindrome, gli errori continui sono stati corretti semplicemente e per creare gli stati logici sono stati copiati degli stati noti e non è stato quindi violato il no-cloning.

Maggiore attenzione va dedicata dunque al primo errore citato precedentemente: il phase flip, per proteggere l'informazione da questo errore è infatti necessario un codice di 9 qubit formato dai seguenti stati logici:

$$\begin{aligned} |0\rangle \to |\bar{0}\rangle &\equiv \frac{1}{2^{3/2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle), \\ |1\rangle \to |\bar{1}\rangle &\equiv \frac{1}{2^{3/2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle). \end{aligned} \tag{2.47}$$

Entrambi consistono di tre cluster di tre qubit; supponiamo quindi che si verifichi un phase flip, ovvero un cambiamento del segno relativo all'interno di un cluster. La fase relativa di uno sarà quindi diversa da quella degli altri due, è dunque necessario misurare un osservabile di 6 qubit per poterli comparare e successivamente correggerli seguendo la maggioranza.

Data l'estrema semplicità di questi esempio, prima di addentrarci nella teoria, è necessario parlare di un altro QECC: il codice di Shor a nove qubit. Esso permette infatti di correggere un errore generico su un singolo qubit. Gli stati logici di base di questo codice sono:

$$\begin{aligned} |\bar{0}\rangle &= [\frac{1}{\sqrt{2}}\,|000\rangle + |111\rangle]^{\otimes 3}, \\ |\bar{1}\rangle &= [\frac{1}{\sqrt{2}}\,|000\rangle - |111\rangle]^{\otimes 3}. \end{aligned} \tag{2.48}$$

Risultano quindi identici a quelli del circuito di phase flip e possono essere distinti attraverso un osservabile $\sigma_x^{(1)} \otimes \sigma_x^{(2)} \otimes \sigma_x^{(3)}$, che d'ora in poi verrà denotato con $X_1X_2X_3$, in cui è sottinteso il prodotto esterno. Si noti che con gli indici $1, 2, 3$ presenti nelle due espressioni precedenti si fa riferimento al qubit su cui agiscono i singoli operatori. Gli stati $|\bar{0}\rangle$ e $|\bar{1}\rangle$ sono autostati di questo osservabile con autovalori 1 e $-1$ rispettivamente, non esiste tuttavia nessun modo di distinguerli osservando due qubit o meno.

Si consideri ora uno stato ignoto codificato come $\alpha |\bar{0}\rangle + \beta |\bar{1}\rangle$, l'obiettivo consiste ovviamente nel misurare e quindi correggere l'errore. Consideriamo un bit flip sul primo qubit; sappiamo per gli esempi precedenti che può essere localizzato misurando la sindrome $Z_1Z_2$, $Z_2Z_3$. Gli stati logici $|\bar{0}\rangle$ e $|\bar{1}\rangle$ sono autostati dei due operatori con autovalore 1; un flip trasforma tuttavia il valori dell'autovalore in $-1$. Se la nostra sindrome assume quindi la forma $(-1, 1)$, abbiamo la certezza che si è verificato un flip sul primo qubit e possiamo quindi correggerlo.

Supponiamo ora un errore di phase flip che agisce su uno dei due qubit, esso può essere diagnosticato misurando uno dei seguenti osservabili a 6 qubit:

$$\begin{aligned} &X_1X_2X_3X_4X_5X_6, \\ &X_4X_5X_6X_7X_8X_9. \end{aligned} \tag{2.49}$$

Un errore di fase modifica il valore di XXX in un determinato cluster rispetto agli altri due. Misurando i due osservabili esso può essere misurato e successivamente corretto.

Durante questa trattazione abbiamo sempre supposto che si verifichi un solo errore per volta, se ciò non dovesse avvenire e occorressero due errori uguali l'informazione sarebbe irrimediabilmente compromessa. Ad esempio l'effetto di due bit flip all'interno di un singolo cluster risulta essere un errore di fase sul qubit codificato:

$$X_1X_2X_3 : \alpha |\bar{0}\rangle + \beta |\bar{1}\rangle \to \alpha |\bar{0}\rangle - \beta |\bar{1}\rangle . \tag{2.50}$$

Problemi di questo tipo possono essere risolti assumendo che gli errori sono poco probabili e indipendenti sul singolo qubit. Ciò porta ad una maggiora probabilità di conservazione dell'informazione rispetto ad un computer sprovvisto di correzioni. Il codice di Shor è tuttavia in grado di correggere contemporaneamente errori di diversa tipologia, anche continui, come visto in precedenza.

### 2.2.2 Teoria e proprietà dei QECC

Vogliamo ora capire come implementare la quantum error correction in modo del tutto generico. Iniziamo considerando un errore generico su un singolo qubit: assumendo che l'ambiente si trovi nello stato puro $|0\rangle_E$ possiamo considerare la trasformazione unitaria:

$$\begin{aligned} U : |0\rangle \otimes |0\rangle_E \to |0\rangle \otimes |e_{00}\rangle_E + |1\rangle \otimes |e_{01}\rangle_E , \\ |1\rangle \otimes |0\rangle_E \to |0\rangle \otimes |e_{10}\rangle_E + |1\rangle \otimes |e_{11}\rangle_E , \end{aligned} \tag{2.51}$$

dove le $|e_{ij}\rangle_E$ sono gli stati dell'ambiente non necessariamente ortogonali. Se consideriamo uno stato generico $|\psi\rangle$, $U$ può essere espansa in termini delle matrici di Pauli $\{I, X, Y, Z\}$ in quanto quest'ultime sono una base dello spazio degli operatori $2 \times 2$. A livello fisico ciò comporta che esistono quattro possibilità per l'evoluzione di un qubit; tuttavia, a meno che gli stati della base dell'ambiente $\{|e_I\rangle, |e_X\rangle, |e_Y\rangle, |e_Z\rangle\}$ non siano tutti mutualmente ortogonali, in alcun modo è possibile effettuare una misura in grado di distinguere l'effetto delle quattro matrici. Ovviamente una matrice $2^n \times 2^n$ può essere allo stesso modo espansa in termini degli operatori $\{I, X, Y, Z\}^{\otimes n}$. Possiamo quindi esprime l'effetto di un operatore unitario su n qubit e l'ambiente come:

$$|\psi\rangle \otimes |0\rangle_E \rightarrow \sum_a E_a |\psi\rangle \otimes |e_a\rangle_E , \tag{2.52}$$

dove l'indice a copre un range di $2^{2n}$ valori e le $E_a$ sono operatori unitari in quanto corrispondono alle matrici di Pauli.

Il nostro obiettivo sarà dunque quello di effettuare una misura collettiva in grado di mostrare quali errori $E_a \in \mathcal{E}$ siano avvenuti, dove

$$\mathcal{E} \subseteq \{E_a\} = \{I, X, Y, Z\}^{\otimes n} \tag{2.53}$$

è un sottoinsieme di tutti gli operatori di Pauli. Consideriamo ora la base ortonormale per il sottospazio del codice $\{|\bar{i}\rangle\}$ (codeword); è dunque necessario che $\langle\bar{j}|E_b^\dagger E_a|\bar{i}\rangle = 0$ se $i \neq j$, altrimenti un errore potrebbe eliminare la distinguibilità di due stati ortogonali. Esiste tuttavia una condizione sufficiente, ovvero

$$\langle\bar{j}|E_b^\dagger E_a|\bar{i}\rangle = \delta_{ab}\delta_{ij}. \tag{2.54}$$

Gli stati quantistici sono codificati da un'operazione unitaria in un quantum error correcting code $\mathcal{C}$; gli operatori $E_a$ traspongono $\mathcal{C}$ in una serie di "sottospazi di errore"

$$\mathcal{H}_a = E_a\mathcal{C}. \tag{2.55}$$

Lo stato risultante di un errore agente su uno stato arbitrario $|\psi\rangle$ risulta quindi essere:

$$\sum_{E_a \in \mathcal{E}} E_a |\psi\rangle \otimes |e_a\rangle_E . \tag{2.56}$$

Effettuando una misura possiamo proiettarlo sul sottospazio di errore $\mathcal{H}_a$ in modo da ottenere $E_a |\psi\rangle \otimes |e_a\rangle_E$. A questo punto è possibile applicare l'operatore $E_a^\dagger$ per completare la procedura di recovery. Possiamo riassumere quanto detto in precedenza nel seguente teorema:

**Teorema 2.2** *Condizioni di correzione*
Sia $\mathcal{H}_C$ un codice quantistico e $\mathcal{E} = \{E_a\}$ l'insieme degli errori agenti su di esso. Una condizione necessaria e sufficiente affinché la recovery $\mathcal{R}$ sia possibile è:

$$\langle \bar{j}|E_b^\dagger E_a|\bar{i}\rangle = C_{ba}\delta_{ij}, \tag{2.57}$$

dove $E_a, E_b \in \mathcal{E}$ e le $C_{ba} = \langle \bar{i}|E_b^\dagger E_a|\bar{i}\rangle$ sono matrici hermitiane arbitrarie. Se è possibile effettuale la recovery diremo che $\{E_a\}$ è un insieme correggibile di errori.

Il vantaggio principale tra il risultato trovato e l'equazione (2.54) è che le $C_{ba}$ non dipendono da $i$, per cui questa condizione risulta essere più forte.

### Distanza

Passiamo ora, dopo aver analizzato le condizione di correzione, ad individuare le principali proprietà di un QECC. Oltre alla grandezza del blocco $n$ (qubit fisici) e al numero di qubit codificati $k$ (qubit logici), è necessario introdurre il concetto di distanza $d$, ovvero il peso minimo di un operatore di Pauli $E$ tale che:

$$\langle \bar{i}|E_a|\bar{j}\rangle \neq C_a\delta_{ij}. \tag{2.58}$$

Diremo che un codice è in grado di correggere $t$ errori se l'insieme $\mathcal{E}$ di $E_a$ sui quali è possibile effettuare una recovery, contiene tutti gli operatori di Pauli di peso t o minore. Il peso di un errore non è altro che il numero di termini all'interno del prodotto tensoriale che non è uguale all'identità. Il criterio per la correzione degli errori (2.57) risulta quindi essere soddisfatto solo per $E_a, E_b$ di peso $t$ o inferiore; ciò significa che $d \geq 2t+1$. Siamo giunti quindi alla conclusione che un codice di distanza $d = 2t + 1$ può correggere al massimo $t$ errori. D'ora in avanti definiremo i QECC attraverso la notazione $[[n, k, d]]$; ad esempio il codice di Shor visto in precedenza è un codice $[[9, 1, 3]]$, in quando codifica un qubit utilizzandone 9 e può correggere al massimo errori di peso 1.

Possiamo fare un'ulteriore precisazione in quanto un codice può proteggere da un numero maggiore di errori se questi agiscono in una posizione nota. In questo caso, attraverso una distanza $d = t + 1$, è infatti possibile correggere al massimo t errori; possiamo quindi dire che un QECC che corregge t errori in posizioni sconosciute, è in grado di correggerne 2t di posizione nota.

### Hamming bound

In questa sezione vogliamo fornire alcuni limiti al rapporto tra i valori $n$, $k$ e $d$, per capire quali siano i migliori codici per la correzione. Possiamo iniziare questa trattazione parlando del Quantum Hamming bound, il quale vale solo per codici non degeneri, ovvero quei codici che assegnano una distinta sindrome ad ogni possibile errore. Consideriamo quindi un codice che codifica $k$ qubit in $n$ in modo da correggere al massimo $t$ errori.

Su un dato qubit esistono soltanto tre errori linearmente indipendenti: $X$, $Y$ e $Z$ e supponiamo che si verifichino $j \leq t$ errori. Avendo a disposizione $\binom{n}{j}$ di distribuire gli errori sugli n qubit e tre possibili errori per ogni $j$ avremo che il numero totale di possibili combinazioni di peso massimo $t$ è:

$$N(t) = \sum_{j=0}^{t} 3^j \binom{n}{j} \tag{2.59}$$

Se codifichiamo $k$ qubit in uno modo non degenere, allora ognuno di questi errori deve corrispondere ad un sottospazio ortogonale di dimensione $2^k$. Allora la dimensione dello spazio di Hilbert $(2^n)$ deve essere abbastanza grande da contenere $N(t) \times 2^k$ vettori indipendenti. Si ottiene dunque il seguente risultato, ovvero il Quantum Hamming bound:

$$N(t) = \sum_{j=0}^{t} 3^j \binom{n}{j} \leq 2^{n-k} \tag{2.60}$$

Nel caso in cui volessimo codificare un solo qubit avremmo:

$$1 + 3n \leq 2^{n-1} \tag{2.61}$$

che è soddisfatto per $n \geq 5$. Un codice non degenere del tipo $[[5, 1, 3]]$ risulta quindi essere perfetto, non esiste un codice con $n < 5$ in grado di proteggere da tutti gli errori che possono verificarsi su un singolo qubit. Lo spazio di Hilbert di dimensione $2^5 = 32$ corrispondente ai 5 qubit è infatti utilizzato nella sua interezza per racchiudere tutti i possibili errori su un singolo qubit.

## 2.3 CSS codes

Per poter trattare la famiglia di QECC detta CSS (Calderbank-Shor-Steane) codes, è necessario introdurre qualche concetto relativo ai codici classici.

### I codici lineari classici

Un codice lineare $C$ codifica $k$ bit di informazione in uno spazio di codice formato da $n$ bit. All'interno dell'insieme formato dalle $2^n$ stringhe binarie di lunghezza $n$, prendiamo un sottospazio contenente $2^k$ stringhe, le codewords. $C$ risulta quindi essere un sottoinsieme dello spazio vettoriale binario $F_2^n$ il quale è un particolare tipo di spazio in cui i vettori sono costituiti da stringhe binarie, ovvero sequenze ordinate delle cifre binarie 0 e 1, e le operazioni di somma e prodotto per uno scalare sono definite secondo l'aritmetica del modulo 2. Ogni codice è specificato da una matrice generatrice $G$ $n \times k$ le cui entrate corrispondono sempre a 0 e 1; essa mappa i messaggi nel loro equivalente codificato.

Presa la codeword $x$, essa viene codificata in $Gx$, ovvero in una stringa di lunghezza $n$. Possiamo tuttavia definire il sottospazio di codice di $F_2^n$ utilizzando $n-k$ vincoli. La matrice di controllo parità $H$ è una matrice $(n-k)\times n$ tale che, presa una codeword $x$, si ha:

$$Hx = 0 \tag{2.62}$$

Il codice rappresenta quindi il nucleo di $H$, le cui righe sono $n-k$ vettori linearmente indipendenti ortogonali al sottospazio $C$. Si ha infine un'importante proprietà dei codici classici per cui:

$$HG^T = 0. \tag{2.63}$$

Risulta utile introdurre il concetto di codice duale, prendendo la trasposta dell'equazione (2.63) si ottiene $GH^T = 0$ possiamo interpretare la $H^T$ come la matrice generatrice e la $G^T$ come la matrice di controllo di parità del cosiddetto codice duale $C^\perp$. Il codice duale corrisponde al complemento ortogonale di C in $F_2^n$. Un codice è detto debolmente auto-duale se $C \subseteq C^\perp$, mentre è fortemente auto-duale se $C = C^\perp$ nel caso in cui $n = 2k$.

L'unico errore possibile per il codice classico è il bit flip, che corrisponde ad un vettore $e$ che presenta degli 1 nelle posizioni in cui esso occorre. Data una codeword $y$ si ottiene quindi $y' = y + e$. Per la condizione (2.62) si ha $Hy' = He$, dove $Hy'$ corrisponde alla sindrome e gli errori possono essere corretti soltanto se ognuno di essi corrisponde ad una diversa sindrome. La matrice di controllo di parità permette dunque di individuare e correggere gli errori. La distanza di un codice lineare corrisponde al peso minimo di un qualunque vettore $v \in C$, che in questo caso equivale il numero di 1. Un codice lineare di distanza $d = 2t+1$ può correggere al massimo $t$ errori.

### I CSS codes

Possiamo ora trattare i CSS codes che rappresentano la generalizzazione quantistica dei codici lineari classici. Siano $C_1$ e $C_2$ due codici lineari classici tali che $C_2 \subset C_1$ ($k_2 < k_1$), per cui la matrice di controllo di parità $H_2$ presenta le prime $n-k_1$ righe coincidenti a quelle di $H_1$ e $k_1 - k_2$ righe indipendenti. Possiamo definire il codice quantistico $\mathrm{CSS}(C_1, C_2)$ di tipo $[[n, k_1 - k_2]]$ in grado di correggere errori che occorrono su $t$ qubit. $C_2$ definisce una relazione di equivalenza in $C_1$, diremo che $x, y \in C_1$ sono equivalenti se esiste un vettore $w \in C_2$ tale che $x = y + w$. Le classi di equivalenza sono quindi i cosets di $C_2$ in $C_1$, dove con coset intendiamo l'insieme di tutte le codewords appartenenti a $C_1$ che possono essere ottenute aggiungendo ad una $x \in C_1$ ogni codeword di $C_2$, ovvero $x + C_2 = \{x + w | w \in C_2\}$. Dato che il nostro CSS quantistico associa una codeword ad ogni classe di equivalenza, presa la codeword $x \in C_1$ definiamo lo stato quantistico $|x + C_2\rangle$ come:

$$|x + C_2\rangle = \frac{1}{\sqrt{2^{k_2}}} \sum_{w \in C_2} |x + w\rangle \tag{2.64}$$

Lo spazio vettoriale corrispondente al CSS code è quindi generato dagli stati $|x + C_2\rangle$ per ogni $x \in C_1$. Dato che il numero di cosets corrisponde al rapporto tra le dimensioni di $C_1$ e $C_2$ , allora la dimensione di $\mathrm{CSS}(C_1, C_2)$ è $2^{k_1-k_2}$. Gli stati appartenenti a differenti cosets risultano essere ortogonali [10].

Supponiamo di avere due vettori $e_1$ e $e_2$ di $n$ bit che rappresentano rispettivamente bit e phase flip. Essi saranno dunque formati in modo da avere 1 nelle posizioni in cui si verifica l'errore e 0 altrove. Dato lo stato iniziale $|x + C_2\rangle$, l'effetto dei due errori può essere espresso come:

$$|x + C_2\rangle' = \frac{1}{\sqrt{2^{k_2}}} \sum_{w \in C_2} (-1)^{(x+w)\cdot e_2} |x + w + e_1\rangle \tag{2.65}$$

Applichiamo dunque la matrice di controllo di parità $H_1$ ad uno sistema formato dagli $n$ qubit nello stato precedente e da un qubit ancilla nello stato $|0\rangle$, ottenendo:

$$|x + w + e_1\rangle |0\rangle \to |x + w + e_1\rangle |H_1(x + w + e_1)\rangle = |x + w + e_1\rangle |H_1 e_1\rangle \tag{2.66}$$

È possibile trovare l'errore misurando il valore dell'ancilla, e correggerlo applicando una porta NOT ai qubit soggetti all'errore.

Nel caso di un phase flip applichiamo una porta Hadamard ad ogni qubit per ottenere lo stato:

$$H |x + C_2\rangle = \frac{1}{\sqrt{2^{k_2} \cdot 2^n}} \sum_z \sum_{w \in C_2} (-1)^{(x+w)\cdot(e_2+z)} |z\rangle \tag{2.67}$$

dove $z$ rappresenta tutti i valori per gli $n$ bit. Se definisco $z' = z + e_2$, allora il mio stato diventa:

$$\frac{1}{\sqrt{2^{k_2} \cdot 2^n}} \sum_z \sum_{w \in C_2} (-1)^{(x+w)\cdot z'} |z' + e_2\rangle \tag{2.68}$$

Se $z' \in C_2^\perp$, allora $\sum_{w \in C_2} (-1)^{w \cdot z'} = |C_2|$ (con $|C_2| = 2_2^k$ ne indichiamo la dimensione); mentre se $z' \notin C_2^\perp$, $\sum_{w \in C_2} (-1)^{w \cdot z'} = 0$. Per cui possiamo scrivere:

$$\frac{1}{\sqrt{2^n / 2^{k_2}}} \sum_{z' \in C_2^\perp} (-1)^{x \cdot z'} |z' + e_2\rangle \tag{2.69}$$

che corrisponde al caso del bit flip analizzato in precedenza. Per completare la correzione, dopo aver effettuato i procedimenti con il qubit ancilla, è necessario applicare un'altra porta Hadamard.

**Il codice di Steane**

Il più semplice dei CSS codes è il codice [[7,1,3]] di Steane che viene costruito attraverso il codice classico [7,4,3] di Hamming, la cui matrice di controllo di parità è:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \tag{2.70}$$

Se $C_1$ corrisponde a questo codice, allora $C_2$ deve essere uguale al suo duale. La matrice di controllo di parità di $C_2$ è quindi uguale alla matrice generatrice trasposta di $C_1$:

$$H_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{2.71}$$

per cui lo span delle righe di $H_2$ contiene lo span di quelle di $H = H_1$ per cui $C_2 \subset C_1$. Dato che $C_1$ e $C_2$ sono due codici classici di tipo [7,4] e [7,3] rispettivamente, allora otteniamo che il CSS corrispondente è di tipo [[7,1]]. Possiamo quindi scrivere gli stati logici come $|\bar{0}\rangle = |0 + C_2\rangle$ e $|\bar{1}\rangle = |1 + C_2\rangle$. Per ulteriori approfondimenti su questo particolare codice si rimanda a [11].

## 2.4 Stabilizers codes

Per poter trattare in modo completo la famiglia degli stabilizers codes e il formalismo necessario per descriverli è necessario introdurre il concetto di gruppo di Pauli, in quanto risulta particolarmente comodo espandere i superoperatori in termini degli operatori di Pauli agenti su $n$ qubit. Possiamo innanzitutto cambiare la notazione dell'operatore $Y$ in modo da avere soltanto matrici reali:

$$Y = ZX = i\sigma_y = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \tag{2.72}$$

la quale soddisfa $Y^2 = -I$. Abbiamo quindi il seguente gruppo di ordine 8: $\pm\{I, X, Y; Z\}$, tuttavia anche le $n$-uple di prodotti tensoriali a singolo qubit formano un gruppo

$$G_n = \pm\{I, X, Y, Z\}^{\otimes n} \tag{2.73}$$

di ordine $|G_n| = 2^{2n+1}$. Il gruppo $G_n$ è il gruppo di Pauli su $n$-qubit. Il gruppo di Pauli presenta le seguenti proprietà:

1. Ogni $M \in G_n$ è unitario ($M^{-1} = M^\dagger$);

2. Per ogni $M \in G_n$ si ha che $M^2 = \pm I = \pm I^{\otimes n}$. Inoltre $M^2 = I$ se il numero di $Y$ nel prodotto tensore è pari, $M^2 = -I$ se è dispari;

3. Se $M^2 = I$, allora M è hermitiana ($M = M^\dagger$), altrimenti è anti-hermitiana;

4. Presi due elementi $M, N \in G_n$, questi sono commutanti o anti-commutanti, per cui $NM = \pm MN$.

Prendiamo ora un sottogruppo abeliano $S$ (ovvero un sottogruppo in cui tutti gli elementi commutano tra di loro) di $G_n$, allora tutti gli elementi di $S$ agenti su $\mathcal{H}_{2^n}$ possono essere simultaneamente diagonalizzati, in quanto sono tutti commutanti ed esiste quindi una base simultanea di autovettori. Allora lo stabilizer code $\mathcal{H}_S \subset \mathcal{H}_{2^n}$ associato ad $S$ è l'autospazio simultaneo con autovalore 1 di tutti gli elementi di $S$, ovvero:

$$|\psi\rangle \in \mathcal{H}_S \quad se \quad M|\psi\rangle = \psi \quad \forall M \in S. \tag{2.74}$$

Il gruppo $S$ è quindi chiamato stabilizzatore in quanto preserva tutte le codewords. Possiamo quindi descrivere questo gruppo attraverso i suoi generatori, ovvero gli elementi $\{M_i\}$ indipendenti tali che ogni elemento di $S$ può essere espresso come prodotto degli elementi di $\{M_i\}$. Se $S$ ha $n-k$ generatori, è possibile dimostrare che lo spazio di codice $\mathcal{H}_S$ ha dimensione $2^k$, ovvero siamo in presenza di $k$ qubit codificati [11]. Utilizzare i generatori permette una descrizione compatta del gruppo. Possiamo pensare i generatori $M_1, ..., M_{n-k}$ come gli operatori di controllo del codice, ovvero quegli osservabili che vengono misurati per ottenere la sindrome. Se l'informazione codificata non è compromessa, allora otteniamo l'autovalore $+1$ per tutti i generatori. Se viene invece misurato un osservabile corrispondente all'autovalore $-1$ significa che lo stato è ortogonale allo spazio di codice, ciò indica la presenza di un errore.

Dato che un superoperatore di errore può essere espanso in termini degli elementi $E_a$ del gruppo di Pauli, allora un particolare $E_a$ può commutare o anti-commutare con un un generatore $M$. Se $E_a$ e $M$ commutano allora

$$ME_a|\psi\rangle = E_a M|\psi\rangle = E_a|\psi\rangle, \tag{2.75}$$

quindi l'errore preserva l'autovalore $+1$. Se invece i due sono anti-commutanti

$$ME_a|\psi\rangle = -E_a M|\psi\rangle = -E_a|\psi\rangle, \tag{2.76}$$

l'errore inverte il valore dell'autovalore e può essere identificato attraverso una misura di M. In generale, presi i generatori $M_i$ e l'errore $E_a$ si ha:

$$M_i E_a = (-1)^{s_{ia}} E_a M, \tag{2.77}$$

dove $s_{ia}$ costituisce la sindrome dell'errore analizzato, infatti $(-1)^{s_{ia}}$ è il risultato della misura di M dopo l'occorrenza dell'errore. Per un codice non degenere, la $s_{ia}$ risulta essere diversa per ogni $E_a \in \mathcal{E}$, quindi misurando gli $n-k$ generatori è possibile diagnosticare completamente ogni errore.

Vogliamo ora trovare una condizione generale per cui sia possibile la recovery. Per il Teorema (2.2), per ogni $E_a, E_b \in \mathcal{E}$, e data una $|\psi\rangle$ normalizzata nello spazio di codice, risulta esser sufficiente la condizione:

$$\langle\psi|E_a^\dagger E_b|\psi\rangle = C_{ab}, \tag{2.78}$$

dove $C_{ab}$ è indipendente da $|\psi\rangle$. È possibile dimostrare che quest'ultima risulta essere soddisfatta solo se si verifica una delle seguenti condizioni:

1. $E_a^\dagger E_b \in S$;
2. Esiste un $M \in S$ che anti-commuta con $E_a^\dagger E_b \in S$.

**Dim.** Possiamo analizzare separatamente i due casi:

1. $\langle\psi|E_a^\dagger E_b|\psi\rangle = \langle\psi|\psi\rangle = 1$ per $|\psi\rangle \in \mathcal{H}_S$;
2. Suppongo $M \in S$ e $ME_a^\dagger E_b = -E_a^\dagger E_b M$, allora:

$$\langle\psi|E_a^\dagger E_b|\psi\rangle = \langle\psi|E_a^\dagger E_b M|\psi\rangle = -\langle\psi|ME_a^\dagger E_b|\psi\rangle = -\langle\psi|E_a^\dagger E_b|\psi\rangle \tag{2.79}$$

   di conseguenza $\langle\psi|E_a^\dagger E_b|\psi\rangle = 0$.

Generalizzando, uno stabilizer code che corregge $\{\mathcal{E}\}$ è uno spazio $\mathcal{H}_S$ fissato da un sottogruppo abeliano $S$ del gruppo di Pauli per cui è soddisfatta una delle condizioni enunciate in precedenza per ogni $E_a^\dagger E_b$ con $E_{a,b} \in \mathcal{E}$.

È importante sottolineare che la recovery potrebbe fallire se un $E_a^\dagger E_b$ che commuta con lo stabilizzatore non ne fa parte, in quanto l'operatore potrebbe modificare l'informazione codificata preservando il sottospazio di codice $\mathcal{H}_S$. Presi $E_a|\psi\rangle$ e $E_b|\psi\rangle$ con la stessa sindrome, potremmo confonderli e applicare la recovery sbagliata in modo da ottenere $E_b^\dagger E_a$ che potrebbe causare dei danni al codice.

Uno stabilizer code con distanza d presenza la proprietà per cui ogni $E \in G_n$ dal peso minore di $d$, o fa parte dello stabilizzatore, o anti-commuta con alcuni dei suoi elementi. Il codice è invece non degenere se lo stabilizer non contiene alcun elemento dal peso minore di $d$.

### 2.4.1 Notazione simplettica

Lo stabilizer $S$ di un codice può essere visto come un sottospazio lineare chiuso dello spazio vettoriale binario $F_2^{2n}$ di dimensione $n-k$, auto-ortogonale rispetto ad un certo prodotto interno simplettico. Si noti come la definizione di $F_2^{2n}$ sia identica a quella riportata nella Sezione 2.3, con la differenza che in questo caso la dimensione risulta essere funzione di $2n$. Il centro di $G_n$, ovvero l'insieme degli elementi appartenenti al gruppo che commutano con tutti gli altri, è della forma $Z_2 = \{\pm I^{\otimes n}\}$. Siamo in grado di quozientare il centro per ottenere il gruppo $\bar{G}_n = G_n/Z_2$ il quale può essere visto come uno spazio vettoriale binario di dimensione $2^{2n}$. Il gruppo $\bar{G}_n$ è infatti isomorfo allo spazio $F_2^{2n}$, in quanto ogni elemento del gruppo di Pauli, al netto del segno, può essere espresso come prodotto di $Z$ e $X$. Possiamo quindi scrivere:

$$M = Z_M \cdot X_M, \tag{2.80}$$

dove $Z_M$ e $X_M$ sono prodotti tensoriali di $Z$ e $X$. Prese $\alpha$ e $\beta$ stringhe binarie di lunghezza $n$, ogni operatore di Pauli può essere scritto come:

$$(\alpha|\beta) = Z(\alpha)X(\beta) = \bigotimes_{i=1}^{n} Z^{\alpha_i} \cdot \bigotimes_{j=1}^{n} X^{\beta_j}. \tag{2.81}$$

Si avrà quindi l'azione dell'operatore $Y$ nei casi in cui $\alpha$ e $\beta$ collidono. La moltiplicazione in $G_n$ viene mappata nell'addizione in $F_2^{2n}$:

$$(\alpha|\beta)(\alpha'|\beta') = (-1)^{\alpha'\cdot\beta}(\alpha+\alpha'|\beta+\beta'). \tag{2.82}$$

Possiamo quindi esprimere la commutazione degli operatori di Pauli come:

$$(\alpha|\beta)(\alpha'|\beta') = (-1)^{\alpha\cdot\beta'+\alpha'\cdot\beta}(\alpha'|\beta')(\alpha|\beta). \tag{2.83}$$

Due operatori commutano se i vettori corrispondenti sono ortogonali rispetto al prodotto simplettico. Attraverso le proprietà dell'algebra lineare risulta possibile verificare tutte le proprietà degli stabilizers enunciate precedentemente. Possiamo esprimere gli $n-k$ generatori attraverso una matrice $(n-k)\times 2n$, detta $\tilde{H} = (H_Z|H_X)$, in cui ogni riga è un operatore di Pauli espresso nella notazione $(\alpha|\beta)$. La sindrome di un errore $E_a = (\alpha_a|\beta_a)$ è determinata da come questo commuta con i generatori $M_i = (\alpha_i'|\beta_i')$:

$$s_{ia} = (\alpha_a|\beta_a)\cdot(\alpha_i'|\beta_i') = \alpha_a\cdot\beta_i' + \alpha_i'\cdot\beta_a. \tag{2.84}$$

In caso di codice non degenere ogni errore presenta una diversa sindrome; se ad una stessa sindrome sono invece associati più errori, è necessario applicare tutti i $E_a^\dagger$.

Prima di concludere il capitolo con un breve esempio, è necessario parlare degli operatori logici di Pauli, ovvero quegli operatori per cui non è necessario decodificare e

ricodificare il codice per modificare gli stati logici. Il sottospazio ortogonale a $S$ rispetto al prodotto interno simplettico, è detto normalizzatore $S^{\perp}$ (il quale contiene $S$ in quanto tutti i vettori in quest'ultimo sono mutualmente ortogonali), e contiene $n+k$ generatori indipendenti. Esso è infatti formato da vettori che sono ortogonali agli $n-k$ presenti in $S$, per cui $2n-(n-k)=n+k$, di questi, $n-k$ possono essere presi come i generatori di $S$ stessi. I rimanenti $2k$ generatori preservano il sottospazio di codice in quanto commutano con lo stabilizer ma agiscono in modo non banale sui $k$ qubit codificati. Queste $2k$ operazioni possono essere scelte come gli operatori sui singoli qubit $X_{Li}$ e $Z_{Li}$ dove $i=1,2,...k$ indica il qubit codificato su cui agiscono. Scegliamo i $k$ operatori $Z_{L1},...,Z_{Lk}$ in modo da ottenere, sommandoli agli $n-k$, un insieme massimale di operatori commutanti. I restanti $k$ invece devono essere commutanti tra di loro e commutare con i generatori di S, ma non con i $\bar{Z}_i$ corrispondenti, possiamo quindi sceglierli in modo che ogni $\bar{Z}_i$ produca un flip dell'autovalore del $\bar{Z}_i$ corrispondente. Questa procedura corrisponde all'applicazione della porta $X$ sul qubit i-esimo e può essere espressa come:

$$Z_{Li}X_{Lj}=(-1)^{\delta_{ij}}X_{Lj}Z_{Li} \tag{2.85}$$

Possiamo infine sottolineare che la distanza di uno stabilizer è il più piccolo numero di qubit fisici che può formare un operatore logico non triviale.

### 2.4.2 I CSS come stabilizers

Possiamo analizzare brevemente come i CSS costituiscano una classe di stabilizers codes. Presi $C_1$ e $C_2$ codici classici lineari tali che $C_2 \subset C_1$ e $C_1$ e $C_2$ correggono entrambi $t$ errori. La matrice di controllo può essere definita come:

$$\tilde{H}=\left[\begin{array}{c|c} H(C_2^{\perp}) & 0 \\ 0 & H(C_1) \end{array}\right]. \tag{2.86}$$

È tuttavia necessario che le matrici soddisfino la relazione di commutazione $H(C_2^{\perp})H(C_1)^T=0$ che risulta essere verificata per la condizione $C_2 \subset C_1$.Se consideriamo il codice di Steane discusso in precedenza, gli operatori logici possono essere espressi come:

$$Z_L=Z_1Z_2Z_3Z_4Z_5Z_6Z_7Z_8Z_9, \quad X_L=X_1X_2X_3X_4X_5X_6X_7. \tag{2.87}$$

Passando ad un caso più generale, che tornerà utile nelle sezioni successive, consideriamo uno stabilizer i cui generatori possono essere espressi come soli prodotti di $Z$ o di $X$, per cui possono essere espressi come:

$$\tilde{H}=\left[\begin{array}{c|c} H_Z & 0 \\ 0 & H_X \end{array}\right]. \tag{2.88}$$

Per avere la relazione di commutazione desiderata è necessario che $Z$ e le $X$ collidano un numero pari di volte, per cui $H_ZH_X^T=0$ che corrisponde proprio alla relazione espressa in precedenza per i CSS, per cui sappiamo che $C_2=C_X^{\perp}\subseteq C_1=C_Z$.

### 2.4.3 Il codice a 5 qubit

Terminiamo questo capitolo attraverso un esempio in grado di chiarire i concetti riportati in questa sezione. Consideriamo quindi il codice non degenere [[5,1,3]]; i generatori dello stabilizzatore possono essere espressi come:

$$\begin{aligned} M_1 &= XZZXI, \\ M_2 &= IXZZX, \\ M_3 &= XIXZZ, \\ M_4 &= ZXIXZ. \end{aligned} \tag{2.89}$$

Dato che ogni $M_i$ non contiene nessuna $Y$, il suo quadrato è l'identità, inoltre tutti gli operatori sono commutanti in quanto, per ogni $M_iM_j$, ci sono due collisioni tra una $X$ e una $Z$. Infine ogni operatore di Pauli di peso 1 o 2 anti-commuta con i generatori, per cui la distanza del codice è uguale a 3. Possiamo notare che il codice in questione non fa parte della famiglia dei CSS, in quanto i suoi generatori dovrebbero essere prodotti di sole $Z$ e prodotti di sole $X$.

Nella notazione simplettica, possiamo rappresentare lo stabilizzatore come:

$$\tilde{H} = \left[\begin{array}{c|c} 01100 & 10010 \\ 00110 & 01001 \\ 00011 & 10100 \\ 10001 & 01010 \end{array}\right]. \tag{2.90}$$

Ogni colonna di questa matrice può essere vista come la sindrome di un errore a singolo qubit. Se si verifica ad esempio un qubit flip $X_j$; esso commuta con $M_i$ se questo presenta una $I$ o una $X$ nella posizione $j$-esima, anti-commuta se invece presenta una $Z$. Allo stesso modo la parte destra della matrice permette di individuare i phase flip, attraverso la somma delle due parti siamo in grado di valutare anche l'errore $Y$. Le 15 colonne così ottenute risultano essere tutte distinte, ciò rende il nostro codice completo. Specifichiamo infine che tutti gli elementi dello stabilizer hanno ovviamente peso 4.

Gli operatori logici che scegliamo sono:

$$\begin{aligned} Z_L &= ZZZZZ, \\ X_L &= XXXXX, \end{aligned} \tag{2.91}$$

in quanto commutano con ogni $M_i$, il loro quadrato è l'identità e anti-commutano tra di loro. Avendo peso 5, tuttavia, non sono contenuti all'interno di S. Possiamo conoscere il valore di $Z_L$ e $X_L$ misurando tre dei cinque qubit e studiando la parità del risultato, in quanto, dato che il codice ha distanza 3, esistono elementi di $S^{\perp}/S$ di peso tre.

Altre rappresentazioni di $Z_L$ e $X_L$ si ottengono moltiplicando gli operatori logici per elementi appartenenti allo stabilizer; in questo modo è possibile ottenere operatori logici

formati da tre soli operatori diversi dall'identità:

$$\begin{aligned} Z_L &= (ZZZZZ)(-ZYYZI) = -IXXIZ, \\ X_L &= (XXXXX)(-YXXYI) = -ZIIZX. \end{aligned} \tag{2.92}$$

.

### 2.4.4 Threshold

Nella quantum error correction, è possibile avere un calcolo quantistico arbitrariamente buono con porte logiche difettose, a condizione che la probabilità di errore sia al di sotto di una certa soglia costante, detta threshold. Il teorema di threshold per gli stabilizers codes afferma che aumentando la distanza di un codice si ottiene una riduzione del tasso dell'errore logico $P_L$, a condizione che il tasso di errore fisico $p$ dei singoli qubit sia inferiore a una certa soglia $p < p_{th}$. Con errore logico intendiamo l'errore che si manifesta sull'informazione codificata, ovvero gli stati logici. I QECC possono quindi essere utilizzati per sopprimere arbitrariamente il tasso di errori logici. Se abbiamo $p > p_{th}$, ovvero un tasso di errore fisico superiore alla soglia, la codifica risulta controproducente. La soglia rappresenta quindi un parametro sperimentale minimo per cui risulta fattibile la correzione degli errori; essa dipende dalla scelta del codice quantistico, dal circuito di misura della sindrome e dall'algoritmo di decodifica [10]. Questa proprietà risulta molto utile nella trattazione dei codici quantistici che verranno presentati nel prossimo capitolo, grazie ai quali sarà possibile osservare il comportamento teorico appena descritto.

# Capitolo 3

# I Quantum Surface e LDPC Codes

*In questo terzo e ultimo capitolo vengono descritte due famiglie di codici che stanno alla base moderna computazione quantistica: i surface codes e gli LDPC codes. Inoltre viene fatto un confronto tra le due tipologie per spiegare le differenze e i vantaggi degli LDPC rispetto ai surface codes. Per questo capitolo i riferimenti principali sono* [1, 2, 7].

## 3.1 Surface codes

Una delle sfide più grandi all'interno della computazione quantistica consiste nel trovare insiemi di stabilizers commutanti in grado di individuare gli errori senza compromettere lo stato codificato. I cosiddetti surface codes costituiscono la principale soluzione a questo problema. Essi fanno parte della famiglia dei "topological codes" ovvero di codici costruiti unendo insieme elementi ripetuti. I surface codes possono essere quindi riscalati conservando le proprietà di commutazione, il loro principale vantaggio a livello di implementazione consiste nel richiedere solo operazioni tra qubit vicini, in modo da evitare le operazioni a lungo raggio. Trattandosi di qubit fisici d'ora in poi faremo riferimento agli stati della base computazionale $|0\rangle$ e $|1\rangle$ come $|g\rangle$ e $|e\rangle$ rispettivamente; questi corrispondono infatti al ground state e ad uno stato eccitato del qubit fisico.

### 3.1.1 Il four-cycle

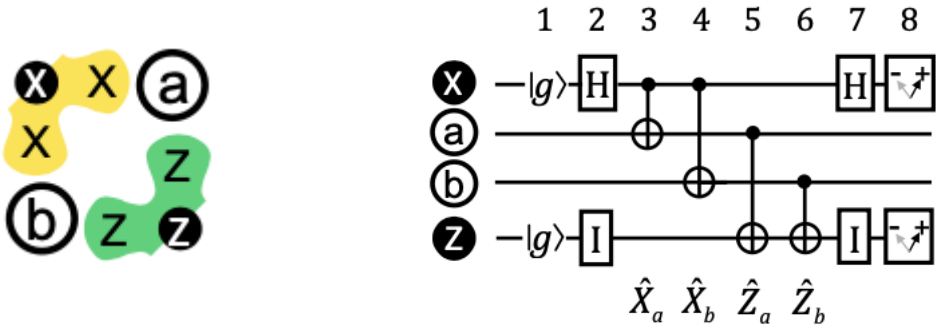
Prima di iniziare la trattazione sui surface codes è necessario richiamare alcuni concetti dai capitolo precedente. Sappiamo infatti che, preso uno stato formato da due qubit $a$ e $b$, i suoi stabilizers corrispondono agli operatori $X_aX_b$ e $Z_aZ_b$ i quali formano un insieme completo. È possibile dimostrare facilmente la commutazione:

$$[X_aX_b, Z_aZ_b] = X_aX_bZ_aZ_b - Z_aZ_bX_aX_b = X_aZ_aX_bZ_b - Z_aX_aZ_bX_b = 0, \tag{3.1}$$

come conseguenza dell'ovvia commutazione di operatori che agiscono su qubit diversi. Gli autostati corrispondenti agli operatori sopracitati risultano essere gli stati di Bell riportati nella (1.29).

I surface codes sono costruiti attraverso un array bidimensionale di qubit fisici. I qubit all'interno del reticolo possono essere di due tipologie: i data qubit in cui viene immagazzinata l'informazione e i qubit di misura. Tutti i qubit devono rispettare le regole della computazione quantistica: inizializzazione, rotazione di un singolo qubit ed esistenza di un CNOT a due qubit; risulta essere tuttavia necessario anche un modo per misurare $Z$. Esistono due tipi di qubit di misura: i measure-$Z$ (m-$Z$) e i measure-$X$ (m-$X$); ogni data qubit è connesso a due m-$Z$ e due m-$X$ e ogni qubit di misura è connesso a quattro data qubit.

Il primo esempio di surface code è il four-cycle, che corrisponde alla singola cella del reticolo come mostrato in Figura 3.1a.




**(a)** **(b)**

**Figura 3.1:** (a) *I data qubit a e b sono collegati a m-Z e m-X in modo da formare la cella unitaria nota come four-cycle.* (b) *Circuito che rappresenta l'effetto dei qubit di misura sui data qubit. I qubit di misura sono preparati nel ground state* $|g\rangle = |0\rangle$*; a m-X vengono applicate due porte Hadamard, mentre a m-Z due identità, che corrispondono ad "aspettare" che sia modificato lo stato sugli m-X. Le porte CNOT corrispondono ai passaggi 3-6, mentre all'indice 8 è associata l'operazione di misura* [7].

Il circuito è formato da due data qubit $a$ e $b$ stabilizzati da un m-$X$ e un m-$Z$, da questa semplificazione risulterà successivamente immediato ricavare le proprietà di un reticolo. Questo circuito stabilizza $a$ e $b$ negli autostati simultanei di $X_aX_b$ e $Z_aZ_b$, che corrispondono agli stati di Bell. Possiamo vedere come ciò accade utilizzando uno stato entangled qualsiasi come input che, sotto l'effetto dei CNOT (Figura 3.1b), si trasforma nello stato totalmente entangled $|\psi_X\psi_a\psi_b\psi_Z\rangle$. Possiamo quindi descrivere il comportamento del circuito:

1. I qubit di misura m-$X$ e m-$Z$ sono riportati allo stato $|g\rangle$, che corrisponde al loro ground state. I data qubit a e b si trovano nello stato $|\psi_{ab}\rangle = A\,|gg\rangle + B\,|ge\rangle +$

$C\,|eg\rangle + D\,|ee\rangle$, dove A, B, C e D sono coefficienti di normalizzazione complessi. Lo stato dell'intero circuito è quindi:

$$|\psi_1\rangle = A\,|gggg\rangle + B\,|ggeg\rangle + C\,|gegg\rangle + D\,|geeg\rangle\,. \tag{3.2}$$

2. Viene applicata una porta Hadamard al qubit m-$X$, il cui effetto risulta essere $|g\rangle \to |+\rangle = |g\rangle + |e\rangle$ e $|e\rangle \to |-\rangle = |g\rangle - |e\rangle$. L'identità lascia invece inalterato m-$Z$. Per cui lo stato totale dopo il secondo step risulta essere:

$$\begin{aligned}|\psi_2\rangle =& A\,|gggg\rangle + A\,|eggg\rangle + B\,|ggeg\rangle + B\,|egeg\rangle + \\ & C\,|gegg\rangle + C\,|eegg\rangle + D\,|geeg\rangle + D\,|eeeg\rangle\,.\end{aligned} \tag{3.3}$$

3. In questo passaggio consideriamo l'effetto dei due CNOT che hanno m-$X$ come qubit di controllo e come bersagli $a$ e $b$. L'effetto di questa porta è descritto dalla (1.28) e si ottiene:

$$\begin{aligned}|\psi_3\rangle =& A\,|gggg\rangle + A\,|eeeg\rangle + B\,|ggeg\rangle + B\,|eegg\rangle + \\ & C\,|gegg\rangle + C\,|egeg\rangle + D\,|geeg\rangle + D\,|eggg\rangle\,.\end{aligned} \tag{3.4}$$

4. Passiamo ora all'effetto che hanno le due porte CNOT controllate da $a$ e $b$ sul qubit m-$Z$:

$$\begin{aligned}|\psi_4\rangle =& A\,|gggg\rangle + A\,|eeeg\rangle + B\,|ggee\rangle + B\,|eege\rangle + \\ & C\,|gege\rangle + C\,|egee\rangle + D\,|geeg\rangle + D\,|eggg\rangle\,.\end{aligned} \tag{3.5}$$

5. A questo punto m-$X$ viene sottoposto nuovamente ad una porta Hadamard per cui si ottiene lo stato seguente:

$$\begin{aligned}|\psi_5\rangle =& (A+D)\,|g\rangle \otimes (|gg\rangle + |ee\rangle) \otimes |g\rangle + \\ & (A-D)\,|e\rangle \otimes (|gg\rangle - |ee\rangle) \otimes |g\rangle + \\ & (B+C)\,|g\rangle \otimes (|ge\rangle + |eg\rangle) \otimes |e\rangle + \\ & (B-C)\,|e\rangle \otimes (|ge\rangle - |eg\rangle) \otimes |e\rangle\,.\end{aligned} \tag{3.6}$$

6. Vengono ora effettuate due misure di $Z$ per i qubit m-$X$ e m-$Z$. Si hanno quindi quattro possibili combinazioni degli autovalori $\pm 1$, ognuna delle quali corrisponde ad un possibile stato finale:

$$\begin{aligned}&\{M_X, M_Z\} = \{+1, +1\}; \quad |\psi_{ab}\rangle = |gg\rangle + |ee\rangle\,, \\ &\{M_X, M_Z\} = \{-1, +1\}; \quad |\psi_{ab}\rangle = |gg\rangle - |ee\rangle\,, \\ &\{M_X, M_Z\} = \{+1, -1\}; \quad |\psi_{ab}\rangle = |ge\rangle + |eg\rangle\,, \\ &\{M_X, M_Z\} = \{-1, -1\}; \quad |\psi_{ab}\rangle = |ge\rangle - |eg\rangle\,.\end{aligned} \tag{3.7}$$

La probabilità di trovare un singolo stato è ovviamente data dal modulo quadrato dell'ampiezza.

Si è quindi giunti al risultato per cui per uno stato di input arbitrario, si ottiene sempre un autostato simultaneo di $X_aX_b$ e $Z_aZ_b$, ovvero uno stato di Bell. Inoltre, se lo stato di partenza è proprio uno stato di Bell, allora si otterrà lo stesso stato in uscita con probabilità unitaria, per cui il codice è in grado di mantenere il sistema sempre nello stesso stato e di fornire gli stessi risultati per le operazioni di misura.

**La rappresentazione di Heisenberg del CNOT**

Esiste tuttavia una notazione più veloce e compatta per studiare il comportamento di un four-cycle attraverso la rappresentazione di Heisenberg del CNOT. Consideriamo infatti una matrice $C$ della forma (1.28), questa è hermitiana e unitaria; possiamo studiare il suo comportamento quando viene applicata ad operatori agenti su due qubit. Fino ad ora abbiamo studiato soltanto la rappresentazione di Schrödinger in cui viene applicata ad una base di stati computazionali. È possibile dimostrare [7], che l'effetto di $C$ su queste porte è il seguente:

$$\begin{aligned} C^\dagger(I \otimes X)C &= I \otimes X, \\ C^\dagger(X \otimes I)C &= X \otimes X, \\ C^\dagger(I \otimes Z)C &= Z \otimes Z, \\ C^\dagger(Z \otimes I)C &= Z \otimes I. \end{aligned} \tag{3.8}$$

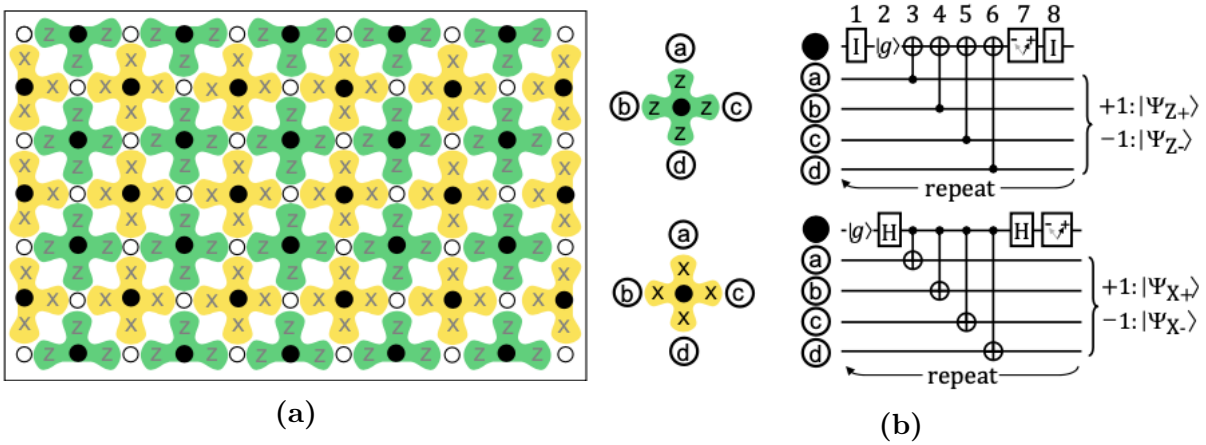
Le altre relazioni sono banali o combinazioni di queste riportate.

Possiamo ora trattare il four-cycle a livello operatoriale. Lo stato iniziale è dato dai due stabilizers $X_XI_aI_bI_Z$ e $I_XI_aI_bZ_Z$; il sistema è dunque autostato del prodotto di operatori. L'effetto dei primi due CNOT è quello di trasformare gli stabilizers in $X_XX_aX_bI_Z$ e $I_XI_aI_bZ_Z$; notiamo come questa operazione non modifichi il secondo prodotto di operatori. Possiamo quindi applicare le restanti due porte logiche per ottenere gli operatori $X_XX_aX_bI_Z$ e $I_XZ_aZ_bZ_Z$. Applicando una misura $X_X$ al qubit m-$X$ otteniamo il prodotto $X_aX_b$ dal primo stabilizer mentre il secondo rimane invariato in quanto commutante con $X_X$; al contrario applicando $Z_Z$ otteniamo il prodotto $Z_aZ_b$. Queste due misure identificano completamente lo stato dei due qubit.

### 3.1.2 Stati quiescenti ed errori su singolo qubit

Possiamo ora passare allo studio del reticolo completo, in cui i qubit di misura sono collegati ognuno a quattro data qubit come mostrato in Figura 3.2a. In analogia con quanto visto in precedenza, effettuando misure proiettive su m-$Z$ e m-$X$ si ottengono gli autostati degli operatori $Z_aZ_bZ_cZ_d$ e $X_aX_bX_cX_d$ tali che $Z_aZ_bZ_cZ_d\,|\psi\rangle = |\psi\rangle\, Z_{abcd}$ e $X_aX_bX_cX_d\,|\psi\rangle = |\psi\rangle\, X_{abcd}$ con $Z_{abcd} = \pm 1$ e $X_{abcd} = \pm 1$. A seguito delle misure il ciclo viene ripetuto da capo, come si vede in Figura 3.2b; inoltre, ogni step del ciclo deve essere completato su tutti i qubit dell'array prima dell'inizio di quello successivo.

Gli stabilizers codes non agiscono sul ground state del sistema ma sullo stato $|\psi\rangle$ che si ottiene dopo la misura proiettiva; quest'ultimo è chiamato stato quiescente. Lo stato quiescente viene selezionato randomicamente completando un intero ciclo in cui i data qubit e i qubit di misura si trovano tutti nello stato fondamentale $|g\rangle$.




**(a)** **(b)**

**Figura 3.2:** (a) *Implementazione 2D di un surface code. I data qubit sono indicati attraverso i cerchi vuoti, i qubit di misura attraverso quelli pieni. Lontano dai bordi, ogni data qubit è a contatto con quattro qubit di misura.* (b) *Sequenze geometriche e schemi dei circuiti che si riferiscono ad un singolo qubit di misura. In alto è riportato un m-Z mentre in basso un m-X. L'ordine delle operazioni è fondamentale per la commutazione degli stabilizers* [7].

In assenza di errori lo stato $|\psi\rangle$ viene conservato alla fine di ogni ciclo con $Z_{abcd}$ e $X_{abcd}$ che rimangono costanti nel tempo. Ciò accade in quanto due stabilizers che hanno qubit in comune ne condividono sempre esattamente due; presi quindi gli stabilizers $X$ e $Z$ che hanno in comune i qubit $a$ e $b$ si ha:

$$[X_aX_bX_cX_d, Z_aZ_bZ_eZ_f] = (X_aZ_a)(X_bZ_b)Q_{cdef} - (Z_aX_a)(Z_bX_b)Q_{cdef} = 0, \qquad (3.9)$$

dove $Q_{cdef} = X_cX_dZ_eZ_f$ in quanto gli operatori che riferiscono ad operatori diversi commutano sempre. Il numero di stati quiescenti è direttamente collegato al numero di qubit; per $n$ qubit esistono infatti $2^n$ stati.

Siamo allora in grado di affrontare il problema degli errori che agiscono su singolo qubit. Consideriamo ad esempio un errore del tipo $I_a + \epsilon Z_a$ che si verifica sul qubit a. La funzione d'onda subisce quindi una trasformazione del tipo $|\psi\rangle \to |\psi'\rangle = I_a + \epsilon Z_a |\psi\rangle$. Attraverso la misura proiettiva $|\psi'\rangle$ viene dunque proiettato su un autostato di $Z_aZ_bZ_cZ_d$ e $X_aX_bX_cX_d$. Questa operazione riconduce $|\psi'\rangle$ in $|\psi\rangle$ con probabilità quasi unitaria mentre si ottiene lo stato $Z_a |\psi\rangle$ con probabilità $|\epsilon|^2$. Nel primo caso il risultate della

misura è lo stesso di quella precedente, mentre nel secondo caso si ha un cambiamento degli autovalori corrispondenti ai due m-$X$ collegati al data qubit a:

$$X_a X_b X_c X_d (Z_a |\psi\rangle) = -Z_a (X_a X_b X_c X_d |\psi\rangle) = -X_{abcd} (Z_a |\psi\rangle) \tag{3.10}$$

$Z_a |\psi\rangle$ è quindi un autostato dello stabilizer ma con segno dell'autovalore opposto rispetto alle misure antecedenti e a quelle dei qubit vicini. L'errore in questione non modifica l'autovalore relativo all'operatore $Z_a Z_b Z_c Z_d$ in quanto questo commuta con $Z_a$. Applicare un secondo $Z_a$ permette di ritornare allo stato di partenza, senza tuttavia avere una fidelity completa; risulta infatti più sicuro ricordare su quale data qubit si è verificato l'errore e cambiare i segni dei risultati delle misure successive. Allo stesso modo è possibile identificare gli errori $X$ e $Y$: nel primo caso viene invertito il segno del risultato della misura sugli m-$Z$, nel secondo sono invertito tutti i segni in quanto $Y_a = Z_a X_a$; lo stato del sistema dopo un ciclo completo continua ad essere uno stato quiescente, diverso tuttavia da quello di partenza.

Se si verifica un errore durante la procedura di misura, esso può essere individuato confrontando il risultato con i valori precedenti e successivi che sono probabilisticamente corretti.

### 3.1.3 Operatori logici

Consideriamo il reticolo riportato in Figura 3.3, in esso sono presenti 41 data qubit, che corrispondono a $2 \times 41$ gradi di libertà, e 40 qubit di misura, ovvero $2 \times 40$ vincoli linearmente indipendenti (gli stabilizers agiscono su qubit diversi). Gli operatori logici $X_L$ e $Z_L$ sono dunque in grado di manipolare i due gradi di libertà rimanenti senza intaccare lo stato codificato. Dalle relazioni precedenti sappiamo che il prodotto di due operatori $X_a X_b$ commuta con un singolo stabilizer $Z$. Facendo quindi riferimento alla Figura 3.3 notiamo come l'effetto dell'operazione $X_1$ può essere identificato da un m-$Z$. Se applichiamo anche $X_2$, il nostro operatore $X_1 X_2$ commuta con il primo stabilizer, anche il risultato della misura è cambiato. Possiamo, iterando questo ragionamento, definire $X_L = X_1 X_2 X_3 X_4 X_5$ che connette i due bordi $X$ dell'array e, per costruzione, commuta con tutti gli stabilizers $Z$. L'effetto di $X_L$ su uno stato quiescente corrisponde a creare $|\psi_X\rangle = X_L |\psi\rangle$, dove $|\psi_X\rangle$ è a sua volta uno stato quiescente che presenta gli stessi risultati di $|\psi\rangle$ dopo una misura. Allo stesso modo possiamo definire $Z_L = Z_6 Z_7 Z_3 Z_8 Z_9$ che presenta tutte le proprietà di $X_L$. Rimane da dimostrare la proprietà di anticommutazione degli operatori logici:

$$\begin{aligned} X_L Z_L &= (X_1 X_2 X_3 X_4 X_5)(Z_6 Z_7 Z_3 Z_8 Z_9) = X_3 Z_3 (X_1 X_2 X_4 X_5)(Z_6 Z_7 Z_8 Z_9) \\ &= -Z_3 X_3 (Z_6 Z_7 Z_8 Z_9)(X_1 X_2 X_4 X_5) = -Z_L X_L \end{aligned} \tag{3.11}$$

Il risultato trovato risulta essere in perfetto accordo con il caso generale della (2.85).

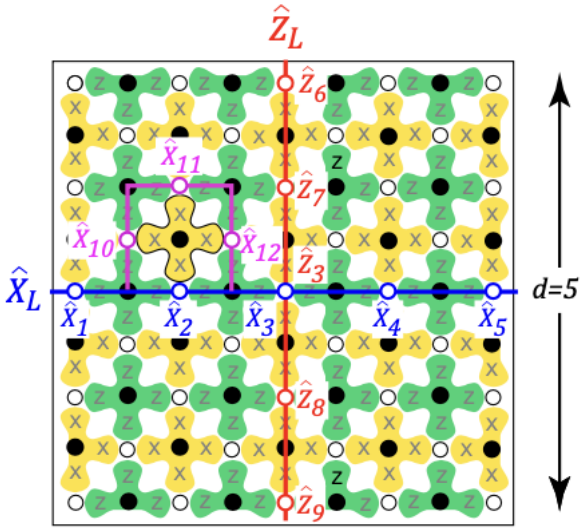



**Figura 3.3:** *Array 2D quadrato caratterizzato da bordi X a destra e sinistra (smooth boundaries) e bordi Z in alto e in basso (rough boundaries). Una catena prodotto $X_L$ (linea blu) connette due bordi X, mentre una $Z_L$ (linea rossa) connette due bordi Z. Con la linea rosa è invece segnata la differenza di percorso tra $X'_L$ e $X_L$* [7].

Consideriamo ora la catena $X'_L = X_1X_{10}X_{11}X_{12}X_3X_4X_5$, essa presenta tutte le proprietà di $X_L$ a cui è linearmente connessa:

$$\begin{aligned} X'_L &= X_1X_{10}X_{11}X_{12}X_3X_4X_5 = (X_2X_{10}X_{11}X_{12})(X_1X_2X_3X_4X_5) \\ &= (X_2X_{10}X_{11}X_{12})X_L \end{aligned} \tag{3.12}$$

Il prodotto di operatori $(X_2X_{10}X_{11}X_{12})$ non è altro che uno stabilizer, per cui giungiamo alla semplice relazione:

$$X'_L \left|\psi\right\rangle = X_{2,10,11,12}X_L \left|\psi\right\rangle = \pm X_L \left|\psi\right\rangle = \pm \left|\psi_X\right\rangle \tag{3.13}$$

Questo risultato illustra come ogni catena $X'_L$ che attraversa l'array può essere scritta come $X_L$ moltiplicato per il prodotto di stabilizers.

### 3.1.4 Error detection

Vogliamo ora estendere il concetto di errore considerato in precedenza passando agli errori su qubit fisici. Questo insieme è formato da errori su singolo qubit, errori di misura, errori di inizializzazione, errori sull'Hadamard e sul CNOT. Ovviamente i più comuni sono gli errori singoli ma possono verificarsi anche più errori all'interno di un ciclo, questi creano una error chain. È possibile correggere questi errori fino a quando

il surface code è in grado di identificarli, successivamente l'errore può essere tracciato e le misure seguenti possono essere corrette attraverso algoritmi classici. Un esempio di algoritmo classico è rappresentato dall'algoritmo di Edmonds per la corrispondenza perfetta a peso minimo il cui funzionamento è descritto in [5]; questo metodo funziona bene per errori radi ma fallisce all'aumentare della densità. Attraverso questo particolare algoritmo siamo in grado di eseguire delle simulazioni numeriche in grado di fornire delle stime riguardo alla tolleranza agli errori di un surface code. Gli errori randomici e non correlati considerati per le simulazioni sono:

- Si verifica un'operazione $X, Y, Z$ al posto dell'identità con probabilità $p/3$;
- Viene inizializzato un qubit in $|e\rangle$ invece che in $|g\rangle$ con probabilità $p$;
- Viene effettuata una $X, Y, Z$ al posto di un $H$ sui qubit di misura;
- Una misura fornisce il valore sbagliato e proietta su uno stato diverso con probabilità $p$;
- Al posto di un CNOT viene effettuata una qualunque operazione su due qubit con probabilità $p/15$.

La probabilità totale che si verifichi un errore in un ciclo risulta quindi essere $8p$. L'algoritmo mette in corrispondenza i cambiamenti rilevati negli autovalori degli stabilizers e gli errori che occorrono sui qubit fisici. Il suo tasso di errore, ovvero l'identificazione errata della sorgente dell'errore, è detto $P_L$ che rappresenta il numero di $X_L$ (o $Z_L$) che appaiono da qualche parte per ciclo di codice.

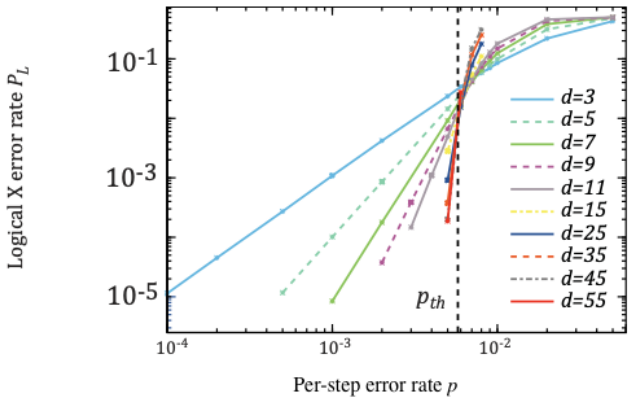



**Figura 3.4:** *Simulazione numerica del tasso di errore di un surface code. In scala doppiamente logaritmica, sull'asse delle ascisse sono riportati i valori di p, mentre sulle ordinate quelli di $P_L$. Attraverso una linea tratteggiata è indicato il valore di soglia $p_{th} = 0.57\%$, alla cui altezza avviene il cambiamento di regime. Questo valore corrisponde ad un tasso di errore del 4% per ogni ciclo di codice* [7].

Questo tasso può essere plottato in funzione del tasso di errore per step $p$, come mostrato in Figura 3.4. Il rapporto tra $P_L$ e $p$ dipende dalla distanza $d$ dell'array, ovvero il numero minimo di operatori necessario per definire un operatore logico. Nell'esempio riportato in Figura 3.3, la distanza risulta essere $d = 5$. Per $p$ piccolo, anche $P_L$ è piccolo e diminuisce all'aumentare di $d$, al contrario, per $p$ grande lo è anche $P_L$ e aumenta al decrescere di $d$. Il punto di incontro tra questi due regimi è il tasso di errore di threshold $p_{th}$: per $p < p_{th}$, il tasso di errore logico decade esponenzialmente con $d$, mentre per $p > p_{th}$ aumenta con la distanza. Nel regime $p < p_{th}$, il tasso di errore logico scala con $p$ come $P_L \sim p^{d_e}$ dove abbiamo $d_e = (d + 1)/2$ per $d$ dispari e $d_e = d/2$ per $d$ pari. Il comportamento della simulazione riproduce quindi perfettamente le nozioni teoriche riportate nella Sezione (2.4.4). Possiamo, in questo caso, approssimare il tasso di errore $P_L$ riportato in Figura 3.4 come $P_L = 0.03(p/p_{th})^{d_e}$.

### 3.1.5 Qubit logici

L'ultimo tassello necessario per completare la trattazione dei surface codes corrisponde ai qubit logici. Abbiamo visto che per creare degli operatori logici è necessario studiare i bordi dell'array, posiamo quindi creare nuovi bordi per modificare gli operatori logici. Creiamo quindi un buco all'interno del reticolo spegnendo uno o più qubit di misura. Consideriamo per semplicità solo il caso in cui viene spento un qubit m-$Z$, ovvero il caso chiamato "buca Z-cut", come mostrato in Figura 3.5. Spegnere un m-$Z$ significa non poter misurare il suo stabilizer e, di conseguenza, rimuovere due vincoli dal sistema. Possiamo manipolare questi due nuovi gradi di libertà definendo due nuovi operatori $X_L$ e $Z_L$ che anticommutano. Il qubit spento è detto "qubit a Z-cut singola" e la buca corrisponde al qubit logico.

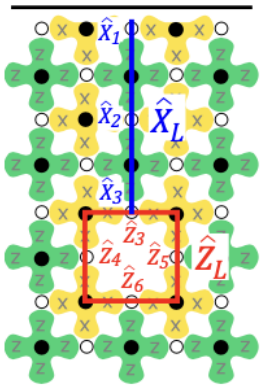



**Figura 3.5:** *Schema di un qubit a Z-cut singola. Il bordo X è indicato attraverso la linea nera in alto, gli altri tre lati non hanno rilevanza. Si noti che $X_L$ e $Z_L$ presentano un data qubit comune. Senza un bordo X, creare uno Z-cut non aggiungerebbe nessun grado di libertà* [7].

Posizionando il buco vicino ad un bordo $X$, siamo in grado di definire l'operatore $X_L = X_1X_2X_3$ che connette il bordo $X$ esterno a quello interno adiacente al buco; inoltre commuta con tutti gli stabilizers $Z$ nell'array. Possiamo introdurre anche $Z_L = Z_3Z_4Z_5Z_6$ formato dagli operatori $Z$ corrispondenti ai data qubit attorno al buco. $Z_L$ commuta con tutti gli stabilizers $X$ e anticommuta con $X_L$, come mostrato nella (3.11). Dato che $X_L^2 = Z_L^2 = I$ e $Y_L = Z_LX_L$ abbiamo creato un insieme di operatori logici anticommutanti, il qubit mancante è dunque un qubit logico.

La distanza di questo qubit è limitata al valore $d = 3$ da $X_L$ ; allontanando questo dal bordo $X$ si ottiene quindi un incremento di $d$. Tuttavia il valore massimo ammissibile è $d = 4$ a causa della dimensione di $Z_L$, questo valore non può essere aumentato senza creare buchi più grandi. A questo punto abbiamo elencato tutte le proprietà elementari dei surface codes, per ulteriori approfondimenti si fa riferimento al [7].

## 3.2 LDPC codes

I quantum LDPC (Low-density parity check) codes corrispondono ad una delle famiglie di codici maggiormente utilizzata all'interno della quantum error correction. In questa sezione vengono riportati alcuni dei principali traguardi ottenuti nella creazione di questi codici. Un QECC è un LDPC se ogni operatore di controllo agisce solo su alcuni qubit e ogni qubit partecipa a pochi controlli, da qui il nome. L'obiettivo principale nella realizzazione di codici di correzione è quello di riprodurre le proprietà dei codici classici per cui $k$ e $d$ scalano linearmente con $n$; inoltre, negli LDPC classici, il numero di bit che fanno parte di ogni controllo e il numero di controlli agenti sul singolo bit sono limitati superiormente da una costante per tutti i membri della famiglia di codici. È stato dimostrato che i codici LDPC quantistici con un tasso di codifica costante possono ridurre l'overhead della computazione quantistica tollerante agli errori ad un valore costante [8]. Per overhead intendiamo il costo aggiuntivo in termini di risorse computazionali, ridurlo equivale ad aumentare l'efficienza.

I surface codes, ampiamente discussi in precedenza, fanno quindi parte degli LDPC, tuttavia codificano un numero piccolo e costante di qubit e la distanza scala come $d \propto \sqrt{n}$ al massimo. I progressi recenti hanno portato ad incrementi notevoli di queste proprietà rispetto a quelle dei surface codes. Spesso non è conosciuta la relazione esatta tra i parametri, è quindi necessario introdurre alcune convenzioni di notazione. Prese due funzioni positive $f$ e $g$, abbiamo:

$$\begin{aligned} &f \in O(g) \text{ se } \limsup_{n\to\infty} f(n)/g(n) < \infty, \\ &f \in o(g) \text{ se } \lim_{n\to\infty} f(n)/g(n) = 0, \\ &f \in \Omega(g) \text{ se } \liminf_{n\to\infty} f(n)/g(n) > 0, \\ &f \in \Theta(g) \text{ se } f \in O(g) \text{ e } f \in \Omega(g). \end{aligned} \tag{3.14}$$

Con $f \in \Theta(g)$ si intende quindi che $f$ cresce esattamente come $g$ essendo rispettate sia $f \in O(g)$ che $f \in \Omega(g)$.

Per trattare gli LDPC riprendiamo il concetto di CSS codes (Sezioni 2.3 e 2.4.2), ovvero quei codici quantistici definiti da una coppia di codici classici $C_X, C_Z \subset F_2^n$, tali che $C_X \subset C_Z^{\perp}$. I due codici sono contraddistinti dalle rispettive matrici di controllo di parità $H_X$ e $H_Z$. Un CSS definisce uno stabilizer se il gruppo stabilizzatore è generato dagli stabilizers di controllo $X^c = \prod_{i=1}^n X_i^{c_i}$, dove $c$ è una riga di $H_X$, e $Z^d = \prod_{i=1}^n Z_i^{d_i}$, con $d$ riga di $H_Z$. La commutatività è data dalla condizione di ortogonalità e si traduce con $H_Z H_X^{\dagger} = 0$ in modulo 2. Gli LDPC sono quindi una famiglia di stabilizers codes per cui il numero di qubit che partecipano ad ogni operatore di controllo e il numero di stabilizers di controllo a cui ogni qubit partecipa sono limitati da una costante.

Vogliamo capire se esiste un buon LDPC code. Il termine buono deriva dalla computazione classica ed indica un codice per cui $k \in \Theta(n)$ e $d \in \Theta(n)$. Nel corso di questa sezione ne analizzeremo alcuni.

### Complessi di catene

Possiamo introdurre brevemente una descrizione omologica legata alla definizione di CSS codes. Un complesso di catene $C = (C, \partial^C)$ di spazi vettoriali appartenenti a $F_2^n$ è una collezione di spazi vettoriali $C_i$ e di mappe lineari $\partial_i^C$, dette operatori di bordo. Considero una catena di lunghezza $n+1$:

$$C = (C_n \xrightarrow{\partial_n} ... \xrightarrow{\partial_1} C_0), \tag{3.15}$$

che soddisfa la condizione $\partial_i \partial_{i+1} = 0$. Assumiamo inoltre che gli spazi $C_i$ siano dotati di base in modo da poter interpretare gli operatori come matrici. Le basi degli spazi vettoriali sono dette $i$-celle e i loro elementi $i$-catene. Gli $i$-cicli sono $i$-catene con bordi triviali, quindi elementi di $\ker(\partial_i)$ mentre un $i$-bordo è una $i$-catena nell'immagine di un operatore di bordo; appartiene quindi a $\mathrm{Im}(\partial_{i+1})$. La $i$-omologia di $C$ è lo spazio vettoriale degli $i$-cicli modulo gli $i$-bordi, ovvero $H_i(C) = \ker(\partial_i)/\mathrm{Im}(\partial_{i+1})$. Di tutti queste definizioni è possibile introdurre i duali, per ulteriori approfondimenti è possibile consultare [2].

Un CSS può essere rappresentato da un complesso di catene di lunghezza 3:

$$C = (C_2 \xrightarrow{\partial_2 = H_Z^{\dagger}} C_1 \xrightarrow{\partial_1 = H_X} C_0). \tag{3.16}$$

Attraverso questa corrispondenza, gli operatori $Z_L$ corrispondono al gruppo di omologia $H_1(C) = \ker(\partial_1)/\mathrm{Im}(\partial_2)$ mentre gli $X_L$ corrispondono al gruppo di coomologia $H^1(C) = \ker(\partial_1^{\dagger})/\mathrm{Im}(\partial_2^{\dagger})$. Il numero di qubit logici è $k = \dim H_1(C) = \dim H^1(C)$, mentre $d_Z$ e $d_X$ sono il peso minimo di tutte le classi non triviali di omologie e coomologie.

### 3.2.1 Costruzione geometrica

Il toric code è il più noto CSS quantum code ed è definito da una tassellatura di un toro con mattonelle quadrate, i cui bordi corrispondono a qubit fisici mentre gli stabilizers di controllo sono le facce ($Z$-checks) e i vertici ($X$-checks). Molti altri codici possono essere derivati dalla tassellatura di superfici o varietà; le proprietà di questi codici sono terminate dalla geometria dello spazio sottostante. I codici con un tasso di codifica finito $k/n \to R > 0$ per $n \to \infty$ si presentano su varietà di curvatura negativa, dette varietà iperboliche. Ciò deriva dal teorema di Gauß–Bonnet–Chern che lega la geometria della varietà alla topologia [9]. Il teorema afferma che per una varietà iperbolica di dimensione pari $D = 2i$, la dimensione del gruppo di omologia $H_i$ aumenta linearmente con il volume totale della varietà, si ha quindi un tasso di codifica lineare per il codice associato.

Consideriamo il caso degli Hyperbolic Surface codes, definito come il toric code ma su una varietà iperbolica. Per una tassellatura regolare basata su poligoni regolari con r lati e s poligoni regolari che si incontrano ad ogni vertice, si può dimostrare attraverso il teorema precedente che il numero di qubit logici è $k = (1 - 2/r - 2/s)n + 2$. Si ha inoltre che $r$ è il peso degli $Z$-checks e s quelle degli $X$-checks. La distanza cresce in modo logaritmico rispetto alla dimensione del codice, questo è sufficiente per affermare l'esistenza di una correzione al di sotto di un valore minimo di threshold. Per codici di questo tipo è possibile utilizzare codificatori come l'algoritmo di Edmonds visto in precedenza, ciò significa che la soppressione degli errori sui qubit logici per tasso di errore fisico scala in modo polinomiale al di sotto del valore di threshold. La geometria iperbolica è stata utilizzata da Freedman– Meyer–Luo per costruire una famiglia di codici quantistici del tipo $[[n, 2, \Omega(\sqrt[4]{\log(n)}\sqrt{n})]]$, questo codice, fino al 2020, è stato quello con la migliore scala di distanza. Tuttavia, la costruzione geometrica impone alcuni limiti ai parametri come quello sulla distanza introdotto da Delfosse: $kd^2 \leq O(\log^2(k)n)$.

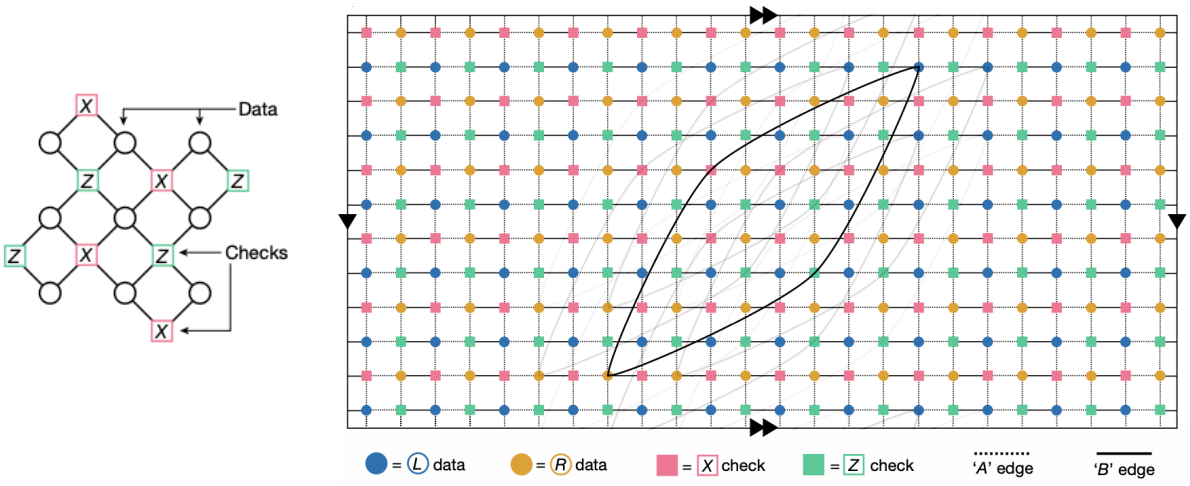
Esistono molti altri metodi di costruzione degli LDPC, i principali rientrano nelle costruzioni prodotto, che non tratteremo e che sono riportati in [2], questi codici sono in grado di proteggere dagli errori con un'alta efficienza di codifica, fattore cruciale rispetto ai surface codes.

## 3.3 BB codes

Abbiamo visto come sia difficile scalare un surface code a 100 o più qubit logici data la sua bassa efficienza di codifica; per sopperire a questo problema sono stati introdotti gli LDPC. Abbiamo visto che un buon LDPC presenta un tasso di codifica costante e una distanza che cresce linearmente con la dimensione, al contrario i surface codes hanno un tasso di codifica che tende a zero all'aumentare di n. La famiglia di LDPC più efficiente risulta essere quella dei codici a lunga distanza in cui vi è una netta diminuzione del tasso di errori logici.

Partendo proprio dagli LDPC, in quest'ultima sezione vogliamo concentrarci sui codici BB (bivariate-bicycle) in quanto basati sui polinomi bivariati; questi codici sono studiati in modo approfondito in [1]. Questi codici sono stabilizers del tipo CSS e possono essere descritti da una collezione di operatori di controllo di 6 qubit composti da $X$ e $Z$. I qubit fisici possono essere disposti su una griglia bidimensionale con condizioni al contorno periodiche, in modo che tutti gli operatori di controllo siano ottenuti da una singola coppia di $X$ e $Z$-checks applicando traslazioni orizzontali e verticali alla griglia.

Un Tanner graph è un grafico bipartito in cui i due insiemi di nodi corrispondono rispettivamente ai bit logici e ai controlli. I bit sono collegati ai controlli in cui compaiono. Descriviamo il codice in questione con un Tanner graph G, un vertice di controllo $i$ e un vertice data $j$ sono collegati da uno spigolo se l'$i$-esimo operatore di controllo agisce sul $j$-esimo data qubit.




**(a)** **(b)**

**Figura 3.6:** (a) *Tanner graph di un surface code.* (b) *Tanner graph di un BB code con parametri* [[144,12,12]]*, i data qubit associati ai registri q(L) e q(R) sono rappresentati attraverso cerchi blu e arancioni. Ogni vertice presenta sei spigoli, quattro a corto raggio e due a lungo raggio, dei quali ne vengono mostrati solo alcuni. Le linee tratteggiate e continue indicano i due sottografici planari* [1].

Il Tanner graph di qualsiasi codice BB, mostrato in Figura 3.6b ha un grado di vertici uguale a sei (ogni nodo è connesso ad altri sei nodi) e lo spessore del grafico uguale a due, può essere quindi decomposto in due grafici planari disgiunti per spigolo, ovvero che non si intersecano. In un BB code dividiamo gli n data qubit nei registri q(L) e q(R) in numero uguale a $n/2$ per ciascun registro. Sono poi presenti n qubit ancilla divisi nei registri n(X) e n(Z) che misurano le rispettive sindromi. La codifica si basa quindi su 2n qubit fisici e il tasso di codifica è $r = k/2n$. Prendendo l'esempio di un surface code

standard, come quello riportato in Figura 3.6a, si hanno $k = 1$ qubit logici codificati in $n = d^2$ data qubit, si utilizzano poi $n - 1$ qubit per la misura della sindrome. Il tasso di codifica è quindi $r \approx 1/(2d)^2$, che risulta essere molto scomodo in quanto si è obbligati a lavorare con ampie distanze per rimare sotto il valore di threshold.

Nel caso di un codice BB, si ha che il tasso di codifica è $r \gg 1/d^2$. prendiamo ad esempio il codice BB [[144,12,12]], questo ha buone proprietà in quanto combina una grande distanza e un alto tasso di codifica $r = 1/24$ (contro il tasso $r = 241$ di un surface code di distanza 11).

Possiamo ora vedere il circuito di misura della sindrome la quale deve essere misurata molto frequentemente per prevenire l'accumularsi degli errori. Il circuito di un BB code è mostrato in Figura 3.7, esso richiede soltanto sette strati di CNOT a prescindere dalla lunghezza del codice.

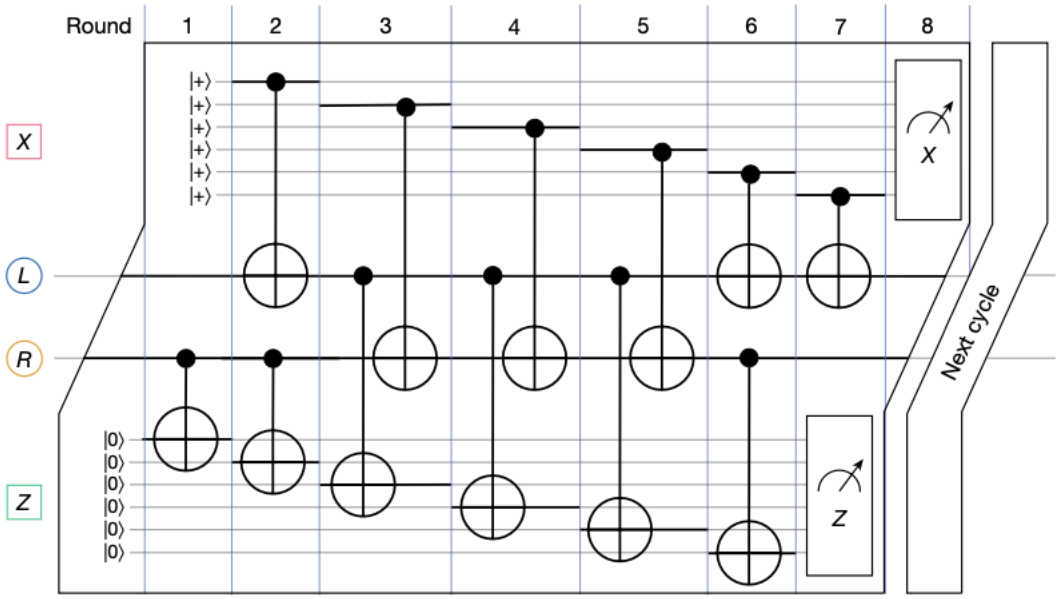
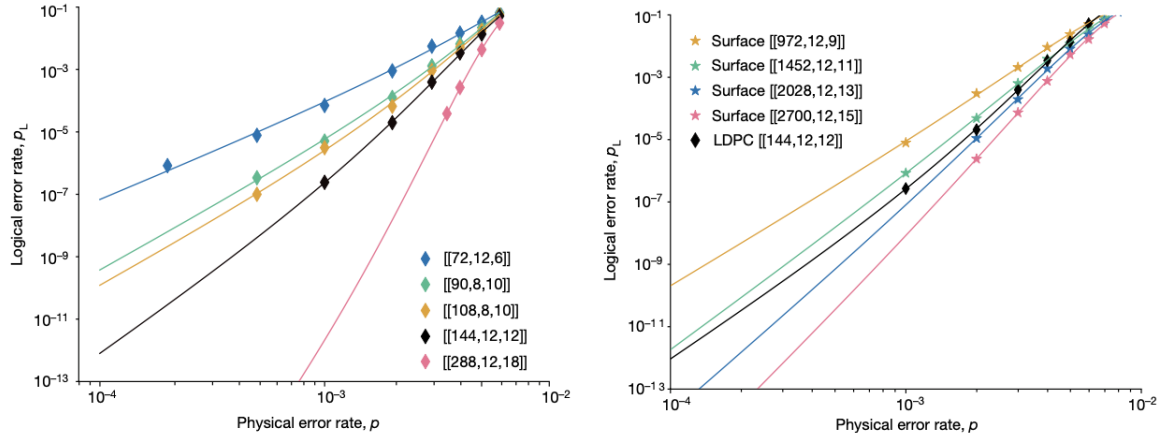



**Figura 3.7:** *Schema del circuito di misura della sindrome che si basa su sette strati di CNOT. In questa rappresentazione è incluso un data qubit per ogni registro; ogni data qubit è accoppiato con 3 X-check e 3 Z-check* [1].

Il protocollo totale di correzione degli errori effettua $N_c \gg 1$ cicli di misura della sindrome e poi chiama il decodificatore. La correzione ha successo se l'errore riscontrato e quello avvenuto coincidono, per cui è possibile applicare l'inverso e correggere l'errore; al contrario se i due differiscono per un operatore logico non triviale si genera un errore logico.

Presa $p$ la probabilità di fallimento di ogni operazione di un circuito considerato, allora $p_L$ corrisponde alla probabilità di un errore logico (questo cambio di notazione risulta essere utile nella comprensione dei grafici). Sia $P_L(N_c)$ la probabilità dopo $N_c$ cicli di misura della sindrome; allora la probabilità di errore logico è data da $p_L = 1 - (1 - P_L(N_c))^{1/N_c} \approx P_L(N_c)/N_c$, ovvero la probabilità di errore logico per singolo ciclo; normalmente si sceglie $N_c = d$. In Figura 3.8a è riportato il tasso di errore logico per tasso di errore fisico considerando diversi BB codes.




**(a)** **(b)**

**Figura 3.8:** (a) *Il grafico riporta l'andamento del tasso di errore logico in funzione di quello fisico. I rombi rappresentano i dati simulati per diversi tipi di BB codes.* (b) *Confronto tra un BB code* [[144,12,12]] *e alcuni surface codes. Si noti la differenza sostanziale nel numero di qubit fisici per ottenere caratteristiche simili* [1].

La pseudo-threshold $p_0$ dei BB codes è definita come la soluzione dell'equazione di rottura di parità $p_L(p) = k_p$ dove $k_p$ è la probabilità che almeno uno dei $k$ qubit codificati sia sottoposto ad un errore; in questo caso si ha $p_0 \approx 0.7\%$ come per i surface codes.

Consideriamo un $p = 10^{-3}$, codificare 12 qubit logici utilizzando un codice a distanza d=12 porterebbe il valore del tasso di errore logico a $p_L = 2 \times 10^{-7}$ che equivale a preservare 12 qubit per un milione di cicli. Il numero totale di qubit in questo caso è 288. Per fare un confronto, come mostrato anche in Figura 3.8b, utilizzando un surface code sarebbero necessari più di 3000 qubit fisici per portare il tasso di errore da $p = 10^{-3}$ a $p_L \approx \times 10^{-7}$. I BB LDPC codes richiedono quindi 1/10 dei qubit fisici richiesti da un surface code. Considerazioni più tecniche sui BB codes sono riportate su [1].

# Conclusioni

All'interno di questo elaborato sono stati presentati gli aspetti principali che riguardano la computazione quantistica e, in particolare, il problema della correzione degli errori. L'introduzione fatta nel primo capitolo è stata utile per poter comprendere a pieno la struttura di un codice di correzione degli errori quantistici da un punto di vista teorico e per poterne studiare al meglio i vari vantaggi e svantaggi computazionali. In particolare è stato possibile analizzare come i codici di correzioni più recenti sono contraddistinti da un miglioramento sostanziale delle prestazioni. Sebbene in questo caso sia stata data la precedenza a concetti e innovazioni teoriche, i progressi pratici e computazionali di questa disciplina sono in rapida ascesa, tuttavia un utilizzo ottimale dell'enorme potenza della computazione quantistica è ancora lontano. In questo elaborato sono stati individuati alcuni dei temi principali che contraddistinguono la ricerca attuale come, ad esempio, un miglioramento della scalabilità, una diminuzione dell'overhead e la creazione di porte logiche resistenti agli errori.

# Bibliografia


[1] Sergey Bravyi et al., *"High-threshold and low-overhead fault-tolerant quantum memory"*, Nature, No. 627, p. 778 (2024).

[2] Nikolas P. Breuckmann e Jens Niklas Eberhardt, *"Quantum LDPC Codes"*, PRX Quantum, Vol. 2 No. 4, p. 040101 (2021).

[3] Eric Dennis et al., *"Topological quantum memory"*, Journal of Mathematical Physics, Vol. 43 No. 9, p. 4452 (2002).

[4] David Deutsch, *"Quantum theory, the Church-Turing principle and the universal quantum computer"*, Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, Vol. 400 No. 1818, p. 97 (1985).

[5] Jack Edmonds, *"Paths, Trees, and Flowers"*, Canadian Journal of Mathematics, No. 17, p. 449 (1965).

[6] Richard P. Feynman, *"Simulating Physics with Computers"*, International Journal of Theoretical Physics, Vol. 21 No. 6/7, p. 467 (1982).

[7] Austin G. Fowler et al., *"Surface codes: Towards practical large-scale quantum computation"*, Phys. Rev. A 86, Vol. 86 No. 3, p. 032324 (2012).

[8] Daniel Gottesman, *"Fault-Tolerant Quantum Computation with Constant Overhead"* (2013), `https://arxiv.org/abs/1310.2984`.

[9] Mikio Nakahara, *"Geometry, Topology and Physics"*, Institute of Physics publishing (2003).

[10] Michael A. Nielsen e Isaac L. Chuang, *"Quantum Computation and Quantum Information"*, Cambridge University Press (2010).

[11] John Preskill, *"Lecture Notes for California Institute of Technology"* (2015), `http://theory.caltech.edu/~preskill/ph229/`.

[12] Joschka Roffe, *"Quantum Error Correction: An Introductory Guide"*, Contemporary Physics, Vol. 60 No. 3, p. 226 (2019).

[13] Peter W. Shor, *"Algorithms for quantum computation: discrete logarithms and factoring"*, Proceedings 35th Annual Symposium on Foundations of Computer Science, p. 124 (1994).