7 INTRODUZIONE AI CODICI DI CORREZIONE DEGLI ERRORI PER COMPUTER QUANTISTICI

1 — CORREZIONE DEGLI ERRORI NEI COMPUTER CLASSICI

Sebbene molto stabili i computer e le reti classiche possono andare in contro ad errori. Ad esempio, se noi immagazziniamo in un hardisk o mandiamo attraverso una rete una stringa di bit, è possibile che l'inevitabile rumore generi dei *bit flip*; ovvero trasformi alcuni bit che inizialmente avevano valore 0 in bit con valore 1 e viceversa.

Uno dei metodi più semplici e allo stesso tempo più efficaci per ovviare a questi errori è immagazzinare l'informazione logica in un numero maggiore di bit fisici. Ad esempio, il bit logico 0 può essere codificato con una stringa di tre 0, ovvero 000. Analogamente il bit logico 1 verrà codificato con la stringa 111.

Supponiamo adesso che a causa del rumore uno dei bit fisici che identificano il bit logico 0 subisca uno *bit flip*: $000 \to 100$. Grazie alla ridondanza di informazione usata, è possibile riconoscere e correggere l'errore. Basta ad esempio misurare tutti e tre i bit e usare il protocollo di *voto di maggioranza* (*majority voting*): se la maggioranza dei bit ha valore 0 assumiamo che il bit logico sia 0 e correggiamo l'errore trovato; analogamente, se la maggioranza dei bit ha valore 1 assumiamo che il bit logico sia 1.

Da questo esempio, è chiaro che il numero di bit usati deve essere dispari. Inoltre, il loro numero dipende da quanto è importante il rumore. Questa secondo punto necessita di un piccolo approfondimento. Riprendiamo l'esempio di sopra. Possiamo usare tre bit fisici solo se la probabilità che due bit cambino contemporaneamente è piccola. Infatti, se due bit contemporaneamente andassero incontro ad un *flip* ci ritroveremo con la stringa, ad esempio, 101. A questo punto, il protocollo di voto di maggioranza, ci indurrebbe a considerare il bit logico come 1 mentre inizialmente era 0.

In maniera più quantitativa, se la probabilità di un singolo *bit flip* è p, la probailità che due bit vengano trasformati è $3p^2(1-p)$ mentre quella che tutti e tre vengano trasformati è p^3 [1]. La probailità che due bit saltino è la somma delle due probabilità : $3p^2(1-p) + p^3 = 3p^2 - 2p^3$. Questa deve essere piu' piccola della probaiblità p di un singolo salto. Arriviamo quindi alla condizione

$$3p^2 - 2p^3 < p \tag{7.1.1}$$

che è verificata se $p < 1/2$.

1 Nel calcolo della probabilità dobbiamo tener conto anche dei modi in cui i bit possono saltare. La probabilità che saltino due bit ma che il terzo rimanga uguale è $p^2(1-p)$. In questo processo potrebbero saltare il primo e il secondo (mentre il terzo rimane stabile), il primo e il terzo (mentre il secondo rimane stabile) oppure il secondo e il terzo (mentre il primo rimane stabile). Dato che abbiamo tre modi in cui il processo può avvenire, la probabilità totale sarà $3p^2(1-p)$.

Siamo arrivati alla conclusione che per un qualsiasi processo in cui la probabilità di *bit flip* è minore di $1/2$, bastano tre bit affinchè il protocollo di voto di maggioranza dia buoni risultati. Vorremo però poter diminuire la probailità di errore in modo tale da poter rendere stabili e sicuri la trasmissione, l'immagazzinamento de l'elaborazione dei dati. Ci sono due modi per farlo. Il primo è usare un hardware che sia più stabile e quindi che abbia una probabilità più bassa di subire *bit flip* contemporanei.

L'alternativa più interessante è usare un numero di di bit maggiore. Se la probabilità che un singolo bit salti è $P = 1/2 + \epsilon$ (quindi arbitrariamente vicina alla soglia $1/2$), si può dimostrare che per un numero N grande di bit fisici, la probabilità di errore decresce come $P_{errore} \propto e^{-N\epsilon^2}$.

Siamo arrivati alla conclusione che, con un numero grande di bit, è possibile rendere i nostri dati stabili anche se sottoposti ad una sorgente di rumore. Il numero di bit da usare sarà determinato dalla probabilità di errore del nostro hardware.

II — CASO QUANTISTICO: I PROBLEMI

Rispetto ai computer classici, quelli quantistici sembrano avere degli svantaggi intrinseci. Innanzitutto, i sistemi quantistici sono più delicati e instabili dei corrispondenti classici. Si aggiungono però altre limitazioni legate alla struttura stessa della meccanica quantistica. In particolare,

1. Lo stato del sistema non può essere copiato come dimostrato dal teorema no-cloning (se c. 4.2.1). Questo impedisce di duplicare l'informazione e sfruttare le copie per estrarre l'informazione corretta.

2. In generale, il sistema non può essere misurato senza disturbare lo stato del sistema. Dobbiamo fare particolare attenzione nell'estrarre informazione perchè la misura potrebbe portare al collasso e distruggere la sovrapposizione di stati quantistici. In sostanza, dobbiamo trovare un modo di estrarre l'informazione senza disturbare lo stato.

3. Ci sono altri tipo di errore di cui dobbiamo tenere conto:
   a) Come nel caso classico, il *bit flip* corrisponde alla transizione $|0\rangle \to |1\rangle$ e $|1\rangle \to |0\rangle$.
   b) errori piccoli in cui il sistema non ha una transizione completa ma transisce verso una sovrapposizione di stati; per esempio, $|0\rangle \to \gamma|0\rangle + \delta|1\rangle$.
   c) La fase relativa fra gli stati può essere modificata per effetto del rumore; per esempio, $\alpha|0\rangle + \beta|1\rangle \to \alpha|0\rangle + e^{i\phi}\beta|1\rangle$

III — CODICI DI CORREZIONE DEGLI ERRORI QUANTITICI

Il più semplice codice di correzione degli errori quantistico sfrutta, come l'analogo classico, il voto di maggioranza. Per prima cosa dobbiamo moltiplicare l'informazione.

A questo proposito definiamo i qubit logici come stati composti da un numero dispari di qubit fisici. Ad esempio, se si usano tre qubit avremo

$$\begin{aligned} |0_L\rangle &\equiv |000\rangle \\ |1_L\rangle &\equiv |111\rangle \end{aligned} \tag{7.3.1}$$

Lo stato quantistico generico sarà dunque scritto come $\alpha|0_L\rangle + \beta|1_L\rangle$ e si può ottenere a partire dallo stato a singolo qubit con delle semplici porte CNOT

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |00\rangle \xrightarrow{C_1NOT_2} (\alpha|00\rangle + \beta|11\rangle) \otimes |0\rangle \xrightarrow{C_1NOT_3} \alpha|0_L\rangle + \beta|1_L\rangle \tag{7.3.2}$$

Si noti che una misura diretta dello stato, ad esempio nella base canonica, distruggerebbe la sovrapposizione e quindi parte dell'informazione. É necessario quindi trovare degli osservabili che permettano di estrarre l'informazione desiderata senza perturbare lo stato del sistema.

Concentriamoci prima sui primi due qubit. Un operatore di questo tipo è $Z_1 \otimes Z_2$; ovvero l'operatore che misura *contemporaneamente* il valore dell'operatore Z di Pauli del primo e del secondo qubit. Si noti che gli stati della base a due qubit $\{|00\rangle, |10\rangle, |01\rangle, |11\rangle\}$ sono tutti autostati dell'operatore $Z_1 \otimes Z_2$. Inoltre ricordando che $Z_i|0\rangle_i = -|0\rangle_i$ e $Z_i|1\rangle_i = |1\rangle_i$ abbiamo che, ad esempio, misurando $Z_1 \otimes Z_2$ per lo stato $|00\rangle$ avremo $(-1)^2 = 1$. Riassumendo

$$\begin{aligned} Z_1 \otimes Z_2|00\rangle &= |00\rangle \\ Z_1 \otimes Z_2|01\rangle &= -|01\rangle \\ Z_1 \otimes Z_2|10\rangle &= -|10\rangle \\ Z_1 \otimes Z_2|11\rangle &= |11\rangle . \end{aligned} \tag{7.3.3}$$

Dalla teoria della misura deduciamo che se dovessimo avessimo solo stati della base a due qubit, una misura di $Z_1 \otimes Z_2$ non disturberebbe lo stato. In generale però dovremmo tener conto che il sistema sarà in una sovrapposizione di stati della base.

7.3.1 Errore *blit flip*

Vediamo cosa succede se il sistema va incontro ad un *blit flip* per il primo qubit. Lo stato del sistema sarà

$$|\Psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle = \alpha|000\rangle + \beta|111\rangle \xrightarrow{errore} \alpha|100\rangle + \beta|011\rangle = |\Phi\rangle \tag{7.3.4}$$

Applicando l'operatore $Z_1 \otimes Z_2$ allo stato $|\Phi\rangle$ (usando le regole ottenute sopra) abbiamo

$$Z_1 \otimes Z_2(\alpha|100\rangle + \beta|011\rangle) = (-\alpha|100\rangle - \beta|011\rangle) = -|\Phi\rangle . \tag{7.3.5}$$

Facendo lo stesso sullo stato senza errori $|\Psi\rangle$ abbiamo

$$Z_1 \otimes Z_2(\alpha|000\rangle + \beta|111\rangle) = (\alpha|000\rangle + \beta|111\rangle) = |\Psi\rangle\,. \tag{7.3.6}$$

Concludiamo che entrambi gli stati sono autostati dell'operatore $Z_1 \otimes Z_2$ ma con autovalore diverso. Quindi, una misura dell'operatore $Z_1 \otimes Z_2$ distruggerà la sovrapposizione di stati $|\Psi\rangle$ e $|\Phi\rangle$. Però nel caso il sistema sia in $|\Psi\rangle$ *oppure* in $|\Phi\rangle$ la misura di $Z_1 \otimes Z_2$ permetterà di estrarre l'informazione desiderata. Se dalla misura otteniamo l'autovalore $+1$ deduciamo che non ci sono stati errori; se otteniamo -1 deduciamo che c'è stato un errore.

Lo schema però non è ancora completo. Infatti se ci fosse un errore nel secondo qubit avremmo

$$|\Psi\rangle = \alpha|000\rangle + \beta|111\rangle \xrightarrow{errore} \alpha|010\rangle + \beta|101\rangle = |\Phi\rangle \tag{7.3.7}$$

In questo caso, la misura dell'operatore $Z_1 \otimes Z_2$ darà esattamente gli stessi risultati di sopra. In sostanza la singola misura di $Z_1 \otimes Z_2$ evidenzia che c'è stato un errore ma non ci permette di sapere se è avvenuto sul primo o sul secondo qubit. Questa incertezza ci impedisce di correggere l'errore.

Per identificare anche la posizione in cui è avvenuto l'errore è necessario misurare un altro operatore complementare come $Z_1 \otimes Z_3$. Supponiamo che l'errore sia avvenuto sul primo qubit; avremo

$$Z_1 \otimes Z_3(\alpha|100\rangle + \beta|011\rangle) = (-\alpha|100\rangle - \beta|011\rangle) = -|\Phi\rangle\,(\alpha|100\rangle + \beta|011\rangle). \tag{7.3.8}$$

Quindi otterremo l'autovalore -1. Se invece l'errore fosse avvenuto sul secondo qubit, avremo

$$Z_1 \otimes Z_3(\alpha|010\rangle + \beta|101\rangle) = \alpha|010\rangle + \beta|101\rangle \tag{7.3.9}$$

che è associato all'autovalore e alla misura $+1$. Una misura combinata di $Z_1 \otimes Z_2$ e di $Z_1 \otimes Z_3$ darà quindi la coppia di risultati $\{-1,-1\}$ se l'errore è avvenuto sul primo qubit e $\{-1,1\}$ se è avvenuto sul secondo. Una volta identificato il qubit perturbato, potremmo intervenire applicando una porta di correzione; X_1 nel primo caso e X_2 nel secondo caso.

7.3.2 Errori "piccoli"

Un sistema quantistico può andare incontro a perturbazioni (errori) che non modificano completamente il valore del qubit ma generano sovrapposizioni indesiderate. Ad esempio, $|0\rangle \to \gamma|0\rangle + \delta|1\rangle$ dove, per semplicità consideriamo γ e δ reali e, visto che la perturbazione è considerata piccola abbiamo che $|\gamma| \gg |\delta|$. Se il $|0\rangle$ va incon-

tro alla trasformazione di sopra, dovremmo per forza avere che $|1\rangle \rightarrow \gamma|1\rangle - \delta|0\rangle$ [2].

Se questo tipo di errore avviene sul primo qubit si avrà una sovrapposizione di più stati

$$|\Psi\rangle = \alpha|000\rangle + \beta|111\rangle \xrightarrow{errore} \alpha\gamma|000\rangle + \alpha\delta|100\rangle + \beta\gamma|111\rangle - \beta\delta|011\rangle = |\Phi\rangle . \tag{7.3.10}$$

Usando le regole di sopra abbiamo che

$$Z_1 \otimes Z_2|\Phi\rangle = \alpha\gamma|000\rangle - \alpha\delta|100\rangle + \beta\gamma^*|111\rangle + \beta\delta^*|011\rangle) \neq |\Phi\rangle . \tag{7.3.11}$$

Ne consegue che $|\Phi\rangle$ non è un autostato di $Z_1 \otimes Z_2$ e che quindi verrà perturbato dalla misura. Per vedere come, lo scriviamo evidenziando gli autostati di $Z_1 \otimes Z_2$ aventi lo stesso valore

$$\begin{aligned} |\Phi\rangle &= \gamma\Big[\alpha|000\rangle + \beta|111\rangle\Big] + \delta\Big[\beta|011\rangle - \alpha|100\rangle\Big] \\ &= \gamma|\phi_+\rangle + \delta|\phi_-\rangle . \end{aligned} \tag{7.3.12}$$

Lo stato $|\phi_+\rangle$ (sovrapposizione di $|00\rangle$ e $|11\rangle$) è un autostato di $Z_1 \otimes Z_2$ con autovalore $+1$ e lo stato $|\phi_-\rangle$ (sovrapposizione di $|01\rangle$ e $|10\rangle$) è un autostato di $Z_1 \otimes Z_2$ con autovalore -1. Dalla teoria edlla misura (sezione 3.3) sappiamo che la misura di $Z_1 \otimes Z_2$ darà $+1$ con probabilità γ^2 e il sistema collasserà sullo stato $|\phi_+\rangle$ oppure otterremo -1 con probabilità δ^2 se il sistema collassa sullo stato $|\phi_-\rangle$.

Data la condizione di errore "piccolo" $\gamma^2 \gg \delta^2$, la maggior parte delle volte otterremo $+1$ e il sistema dopo la misura si troverà nello stato $|\phi_+\rangle = \alpha|000\rangle + \beta|111\rangle$. Questo è lo stato logico iniziale senza errore. Quindi la misura proiettiva ha automaticamente corretto l'errore senza ulteriori modifiche.

Cosa succede se otteniamo -1? In questo caso, il sistema si troverà nello stato con errore $|\phi_-\rangle = \beta|011\rangle - \alpha|100\rangle$. Però l'output -1 ci segnala la presenza dell'errore che può essere eliminato con l'applicazione di porte logiche correttive. Ad esempio, in questo caso, l'applicazione di una porta X_1 (NOT sul primo qubit) da $|\phi_-\rangle \rightarrow |\phi_+\rangle$ che è lo stato originale.

É importante evidenziare che, come sopra, la singola misura di $Z_1 \otimes Z_2$ non è sufficiente per sapere che c'è stato un errore ma non per individuarne la posizione (l'errore potrebbe essere anche sul secondo qubit). Quindi per poter applicare le porte correttive è necessario misurare anche l'osservabile $Z_1 \otimes Z_3$.

Riassumendo, le misure degli osservabili $Z_1 \otimes Z_2$ e $Z_1 \otimes Z_3$ permettono di controllare se è e dove è avvenuto un errore e correggerlo.

2 Si noti che questa è una trasformazione unitaria che preserva il prodotto scalare. Dato che gli stati iniziali $|0\rangle$ e $|1\rangle$ sono ortogonali, gli stati finali devono essere ortogonali. Ne consegue la regola di trasformazione per lo stato $|1\rangle$.

7.3.3 Errore sulla fase

Nella meccanica quantistica la differenza di fase fra gli stati è osservabile. Ne consegue che anche la fase relativa può essere perturbata e portare ad un disturbo o distruzione dell'informazione originale. Oltre agli errori trattati fin ora, i qubit possono incorrere in un *errore di fase*. Questo è un errore puramente quantistico visto che non c'è alcuna corrispondenza classica.

Consideriamo gli errori in cui la fase relativa fra due stati sovrapposizione cambia di segno detto di *phase flip*; questo può essere schematizzato come

$$\begin{aligned} |0\rangle &\xrightarrow[\text{phase error}]{} |0\rangle \\ |1\rangle &\xrightarrow[\text{phase error}]{} -|1\rangle \end{aligned} \tag{7.3.13}$$

ovvero, come una trasformazione unitaria in cui solo lo stato $|1\rangle$ cambia segno.

Se anche uno solo dei qubit che compongono lo stato logico $|\Phi\rangle$ andasse incontro a un *phase flip* si avrebbe

$$\alpha|000\rangle + \beta|111\rangle \xrightarrow[\text{phase flip}]{} \alpha|000\rangle - \beta|111\rangle . \tag{7.3.14}$$

Si noti che la misura degli osservabili $Z_1 \otimes Z_2$ e $Z_1 \otimes Z_3$ non permette di identificare l'errore. Notiamo però che se invece di avere gli stati della base canonica $\{|0\rangle, |1\rangle\}$ avessimo gli stati della base $\{|+\rangle, |-\rangle\}$ si avrebbe

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \xleftrightarrow[\text{phase flip}]{} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle . \tag{7.3.15}$$

Quindi, nella base $\{|+\rangle, |-\rangle\}$, il *phase flip* è equivalente ad un *bit flip* che scambia gli stati della base. Ne consegue che per identificare e correggere i *phase flip* è sufficiente implementare lo stesso schema dei *bit flip* nella base $\{|+\rangle, |-\rangle\}$.

Nello specifico, se partiamo dallo stato $|\Phi\rangle = \alpha|000\rangle + \beta|111\rangle$, applichiamo tre porte di Hadamard ai tre qubit

$$|\Phi\rangle \xrightarrow[H^{\otimes 3}]{} \alpha|+++\rangle + \beta|---\rangle . \tag{7.3.16}$$

Dato $\{|+\rangle, |-\rangle\}$ sono autostati dell'operatore X, i.e., $X|+\rangle = |+\rangle$ e $X|-\rangle = -|-\rangle$, dovremmo misurare gli operatori $X_1 \otimes X_2$ e $X_1 \otimes X_3$. Esattamente come discusso prima, in assenza di errori (ovvero sullo stato $|\Phi\rangle$) otterremo semplicemente gli autovalori $+1$ e $+1$.

Supponiamo che il primo qubit vada incontro ad un *phase flip*

$$\alpha|+++\rangle + \beta|---\rangle \xrightarrow[\text{phase flip}]{} \alpha|-++\rangle + \beta|+--\rangle . \tag{7.3.17}$$

In questo caso, le misure di $X_1 \otimes X_2$ e $X_1 \otimes X_3$ daranno come risultati -1 e -1, rispettivamente, e permetteranno di individuare l'errore e di correggerlo appli-

cando l'operatore Z_1 [3]. Dopo aver fatto le misure e, nel caso, applicati gli operatori di correzione, è necessario tornare alla base canonica applicando altre tre porte di Hadamard.

I protocolli presentati permettono di individuare e correggere gli errori indotti dal rumore. Dato che però non si sa quando questi possono avvenire, è necessario applicarli con una certa frequenza in modo tale da mantenere il sistema nello spazio logico.

IV — PROTOCOLLO COMPLETO

Fino ad questo punto abbiamo discusso le idee fondamentali dei codici di correzione degli errori. Abbiamo mostrato che si possono trovare degli operatori che permettono di stabilire (tramite la misura) se e dove c'è stato un errore. Il punto cruciale è di codificare gli stati logici in modo tale che siano autostati degli operatori che poi andiamo a misurare. In questo modo, la misura permette di estrarre l'informazione riguardante l'errore senza distruggere la sovrapposizione di stati.

Queste idee possano essere usate per i *bit flip* e *phase flip* (con differenti operatori da misurare). Sebbene contengano le idee fondamentali, i protocolli discussi non sono completi. Per poter implementare contemporaneamente i protocolli di correzione per i *bit flip* e *phase flip*, tre qubit non sono sufficienti ed è necessario usare 9 qubit. Il protocollo completo per la correzione degli errori fu proposto da Peter Shor nel 1995 **[Shor1995]** ed è quello che discutiamo nel seguito del capitolo.

In questo protocollo i 9 qubit sono divisi in 3 blocchi e i qubit logici $|0_L\rangle$ e $|1_L\rangle$ sono definiti con

$$\begin{aligned} |0_L\rangle &\equiv \frac{|000\rangle + |111\rangle}{\sqrt{2}} \frac{|000\rangle + |111\rangle}{\sqrt{2}} \frac{|000\rangle + |111\rangle}{\sqrt{2}} \\ |1_L\rangle &\equiv \frac{|000\rangle - |111\rangle}{\sqrt{2}} \frac{|000\rangle - |111\rangle}{\sqrt{2}} \frac{|000\rangle - |111\rangle}{\sqrt{2}} \end{aligned} \tag{7.4.1}$$

É conveniente introdurre una notazione speciale per indicare i blocchi di tre qubit

$$\begin{aligned} |\bar{0}\rangle &\equiv \frac{|000\rangle + |111\rangle}{\sqrt{2}} \\ |\bar{1}\rangle &\equiv \frac{|000\rangle - |111\rangle}{\sqrt{2}} \end{aligned} \tag{7.4.2}$$

IIn questo modo, i qubit logici si possano riscrivere come $|0_L\rangle = |\bar{0}\rangle\,|\bar{0}\rangle\,|\bar{0}\rangle$ e $|1_L\rangle = |\bar{1}\rangle\,|\bar{1}\rangle\,|\bar{1}\rangle$ e il generico stato (logico) del qubit come

$$|\psi\rangle = \alpha\,|0_L\rangle + \beta\,|1_L\rangle = \alpha\,|\bar{0}\rangle\,|\bar{0}\rangle\,|\bar{0}\rangle + \beta\,|\bar{1}\rangle\,|\bar{1}\rangle\,|\bar{1}\rangle\,. \tag{7.4.3}$$

A questo punto possiamo fare alcune osservazioni. La prima è che i blocchi sono sovrapposizioni equipesate (e normalizzate) degli stati $|000\rangle$ e $|111\rangle$ e differiscono solo per la fase relativa. La seconda è che lo stato logico in eq. 7.4.3 rassomiglia a

3 L'operatore Z_1 scambia gli stati $|+\rangle \leftrightarrow |-\rangle$.

quello discusso nella sezione 7.3; possiamo quindi aspettarci, con i dovuti cambiamenti, di poter implementare un codice di correzione simile a quello già discusso.

7.4.1 *Bit flip*

Supponiamo che avvenga un *bit flip* su primo qubit (naturalmente lo stesso schema si può usare per determinare l'errore su ogni qubit). In questo caso ci basta considerare l'effetto sul primo blocco

$$\begin{aligned} |\bar{0}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}} &\rightarrow \frac{|100\rangle + |011\rangle}{\sqrt{2}} \\ |\bar{1}\rangle = \frac{|000\rangle - |111\rangle}{\sqrt{2}} &\rightarrow \frac{|100\rangle - |011\rangle}{\sqrt{2}}. \end{aligned} \tag{7.4.4}$$

Anche in questo caso, misuriamo gli operatori $Z_1 \otimes Z_2$ e $Z_1 \otimes Z_3$.

Analogamente alla discussion in sez. 7.3, si può dimostrare che gli stati $|\bar{0}\rangle$ e $|\bar{1}\rangle$ sono autostati di $Z_1 \otimes Z_2$ entrambi con autovalore $+1$ mentre gli stati con l'errore (a destra nell'equazione) sono autostati di $Z_1 \otimes Z_2$ con autovalore -1.

Quindi, la misura di questi osservabili non distruggerà lo stato $|\psi\rangle$ nè la sovrapposizione nel blocco ma il differente valore ottenuto, ovvero ± 1, permetterà di capire se c'è stato un errore.

Allo stesso modo, la misura successiva e combinata dell'operatore $Z_1 \otimes Z_3$ permetterà di individuare la posizione l'errore che quindi potrà essere successivamente corretto.

7.4.2 *Phase flip*

Per individuare e correggere l'errore sulla fase *si confrontano i blocchi* invece che i qubit. Un *phase flip* sul primo blocco (è irrilevante quale dei primi tre qubit subisca l'errore) genera la trasformazione

$$\begin{aligned} |\bar{0}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}} &\rightarrow \frac{|000\rangle - |111\rangle}{\sqrt{2}} = |\bar{1}\rangle \\ |\bar{1}\rangle = \frac{|000\rangle - |111\rangle}{\sqrt{2}} &\rightarrow \frac{|000\rangle + |111\rangle}{\sqrt{2}} = |\bar{0}\rangle \end{aligned} \tag{7.4.5}$$

che è equivalente al *flip* del *blocco* $|\bar{0}\rangle \leftrightarrow |\bar{1}\rangle$.

L' operatore che ci interessa in questo caso è $X_1 \otimes X_2 \otimes X_3$. Ricordando che $X_i |0\rangle = |1\rangle$ e $X_i |1\rangle = |0\rangle$, possiamo verificare che

$$\begin{aligned} X_1 \otimes X_2 \otimes X_3 |\bar{0}\rangle = X_1 \otimes X_2 \otimes X_3 \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}} \right) &= \frac{|000\rangle + |111\rangle}{\sqrt{2}} = |\bar{0}\rangle \\ X_1 \otimes X_2 \otimes X_3 |\bar{1}\rangle = X_1 \otimes X_2 \otimes X_3 \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}} \right) &= -\frac{|000\rangle - |111\rangle}{\sqrt{2}} = -|\bar{1}\rangle . \end{aligned} \tag{7.4.6}$$

Quindi i blocchi $|\bar{0}\rangle$ e $|\bar{1}\rangle$ sono autostati di $X_1 \otimes X_2 \otimes X_3$ rispettivamente con autovalore $+1$ e -1. In altri termini, se misuriamo l'operatore $X_1 \otimes X_2 \otimes X_3$, possiamo ottenere l'informazione sulla fase relativa del blocco senza tuttavia distruggere la sovrapposizione di stati.

In maniera analoga, l'operatore $(X_1 \otimes X_2 \otimes X_3)(X_4 \otimes X_5 \otimes X_6)$ ci darà informazione *contemporanea* sulla fase del primo e del secondo blocco. In altri termini, ci permette di sapere se le fasi relative del primo e del secondo blocco sono uguali o diverse fra loro.

Si può verificare direttamente che gli stati senza errore $|0_L\rangle = |\bar{0}\rangle|\bar{0}\rangle|\bar{0}\rangle$ e $|1_L\rangle = |\bar{1}\rangle|\bar{1}\rangle|\bar{1}\rangle$ sono autostati dell'operatore $(X_1 \otimes X_2 \otimes X_3)(X_4 \otimes X_5 \otimes X_6)$ con autovalore $+1$. Allo stesso modo, gli stati in cui la fase è cambiata nel primo blocco $|\bar{1}\rangle|\bar{0}\rangle|\bar{0}\rangle$ e $|\bar{0}\rangle|\bar{1}\rangle|\bar{1}\rangle$ hanno fase diversa e sono autostati dell'operatore $(X_1 \otimes X_2 \otimes X_3)(X_4 \otimes X_5 \otimes X_6)$ con autovalore -1.

Quindi la misura dell'operatore $(X_1 \otimes X_2 \otimes X_3)(X_4 \otimes X_5 \otimes X_6)$ ci permette di stabilire se la fase del primo o secondo blocco è cambiata. Esattamente come nel caso di *bit flip*, la misura di dell'operatore $(X_1 \otimes X_2 \otimes X_3)(X_7 \otimes X_8 \otimes X_9)$ ci permetterà di individuare la posizione dell'errore. Una volta individuato il blocco in cui la fase è cambiata basterà applicare un operatore Z_i (dove, per il primo blocco, i può essere uguale a $1, 2$ o 3) per correggere l'errore.

7.4.3 Errori piccoli

Le osservazioni appena fatte, ci permettono di chiarire anche cosa succede nel caso di errori piccoli. Come visto in sez. 7.3.2, la misura dell'operatore $Z_1 \otimes Z_2$ permette con probabilità $|\gamma|^2 \gg |\delta|^2$ corregge automaticamente l'errore avvenuto.

Abbiamo pur sempre una (piccola) probabilità $|\delta|^2$ di far collassare il sistema nello stato $\beta|011\rangle - \alpha|100\rangle$. In questo caso, la misura di $Z_1 \otimes Z_2$ e $Z_1 \otimes Z_3$ permetterà di stabilire che c'è stato un *bit flip* nel primo qubit e di correggerlo applicando un operatore X_1 per ottenere $-(\alpha|000\rangle - \beta|111\rangle)$.

Sebbene gli stati logici siano adesso corretti (ovvero $|000\rangle$ e $|111\rangle$ con i rispettivi coefficienti α e β), la fase relativa è diversa dallo stato logico ideale ed 'he necessario un ulteriore passaggio.

Con l'estensione del protocollo di correzione a 9 qubit questo è relativamente semplice. Infatti il nuovo stato corretto è $|\bar{1}\rangle$ (invece di $|\bar{0}\rangle$ come vorremmo). Quindi basterà usare il protocollo appena discusso per individuare e correggere il *phase flip* e riottenere lo stato logico corretto.

7.4.4 Protocollo di Shor

Vediamo ora un protocollo di correzione degli errori alternativo al precedente. Anche'esso è stato proposto da Peter Shor e prende quindi il suo nome.

L'idea di base è simile: l'informazione di un singolo qubit viene codificata in 9 qubit divisi in blocchi da 3. La differenza sostanziale sta nel fatto che il codice restituisce il qubit iniziale corretto senza necessità di misura e correzione. Gli otto

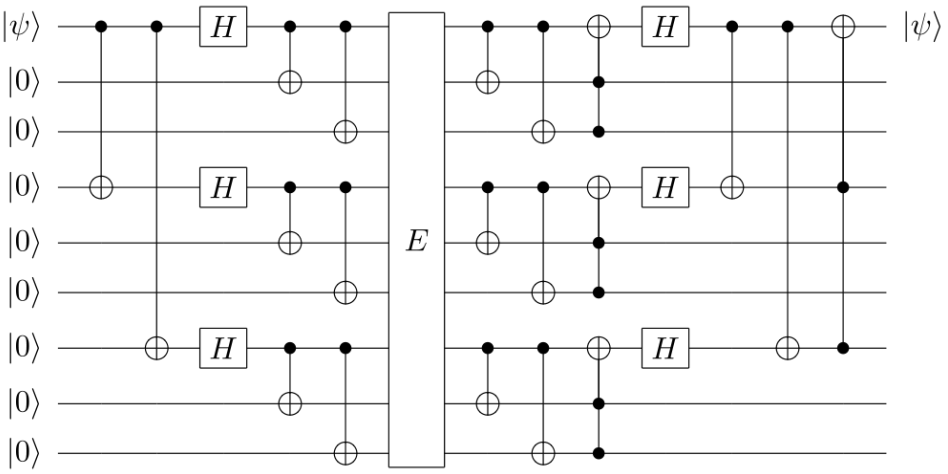

Figure 21: Il protocollo di Shor con 9 qubit. Il blocco centrale rappresenta l'errore. Le altre porte sono mostrate in Fig. 22

qubit aggiuntivi devono essere scartati o riinizializzati allo stato $|0\rangle$. Quindi il risparmio in termini di misure e correzioni viene pagato in termini di dimensione del hardware o di complessità nella procedura di riinizializzazione [4]

Il protocollo come sequenza di porte logiche è mostrato in Fig. 21. Le porte controllate utilizzate sono mostrate in Fig. 22 a) e sono la porta CNOT e quella di Toffoli. Visto che lavoriamo in uno spazio a molti qubit, per queste porte sarà necessario indicare il o i qubit di controllo e quelli *target*. Denoteremo quindi con C_iNOT_j una porta CNOT con il controllo sul qubit i e target j e con T_{ijk} la porta di Toffoli con controllo sui qubit i e j e target sul qubit k [Fig. 22 a)]

Per capire il funzionamento del protocollo di Shor è conveniente dividerlo in piccole sequenze di porte logiche. Ad esempio, la sequenza in Fig. 22 b) permette di costruire il blocchi in Eq. (7.4.2). Se, ad esempio, partiamo dallo stato $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ e gli associamo due qubit $|00\rangle$, con la sequenze Fig. 22 b) otterremo

$$|\psi\rangle \to \frac{1}{\sqrt{2}}\Big[\alpha(|000\rangle + |111\rangle) + \beta(|000\rangle - |111\rangle)\Big] = \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle = |\psi_1\rangle\,. \qquad (7.4.7)$$

4 La procedura di riinizializzazione allo stato $|0\rangle$ non può essere fatto con un operatore unitario e quindi con una normale porta logica. É neessario usare l'ambiente esterno e far "decadere" i qubit eccitati, i.e., nello stato $|1\rangle$, nello stato $|0\rangle$.

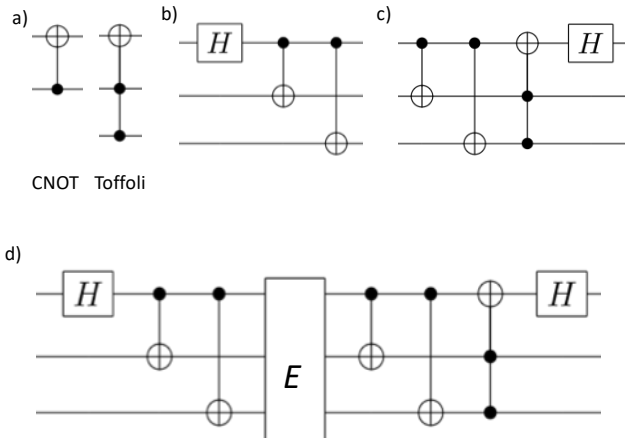

Figure 22: a) La rappresentazione grafica delle porte CNOT e di Toffoli. b) La sequenza di porte logiche per duplicare l'informazione logica su 3 qubit. c) La sequenza di porte logiche per correggere l'errore di *bit flip* su tre qubit.

7.4.5 *Bit flip*

Supponiamo adesso che ci sia un *bit flip* sul primo qubit. Come al solito questo viene descritto con l'applicazione di una porta X_1 (dove l'indice indica il qubit su cui è applicata). La sequenza di porte in Fig. 22 c) darà

$$\begin{aligned} |\psi_1\rangle \quad &\xrightarrow{X_1} \quad \frac{1}{\sqrt{2}}\Big[\alpha(|100\rangle + |011\rangle) + \beta(|100\rangle - |011\rangle)\Big] \\ &\xrightarrow[C_1NOT_3]{C_1NOT_2} \quad \frac{1}{\sqrt{2}}\Big[\alpha(|1\rangle + |0\rangle)\,|11\rangle + \beta(|1\rangle - |0\rangle)\,|11\rangle\Big] = |\psi_2\rangle\,. \end{aligned} \tag{7.4.8}$$

Gli ultimi due qubit sono entrambi "accesi" quindi la porta di Toffoli T_{231} agirà come una porta NOT sul primo qubit. Con la successiva porta di Hadamard H_1 otteniamo

$$\begin{aligned} |\psi_2\rangle \quad &\xrightarrow{T_{231}} \quad \frac{1}{\sqrt{2}}\Big[\alpha(|0\rangle + |1\rangle) + \beta(|0\rangle - |1\rangle)\Big]\,|11\rangle \\ &\xrightarrow{H_1} \quad \Big(\alpha\,|0\rangle + \beta\,|1\rangle\Big)\,|11\rangle = |\psi\rangle\,|11\rangle\,. \end{aligned} \tag{7.4.9}$$

Come possiamo vedere, il risultato finale è che il primo qubit è tornato quello originale ma i due qubit ancilla hanno cambiato il loro valore.

Per completezza riportiamo anche il calcolo nel caso di un errore sul secondo qubit

$$\begin{aligned}
|\psi_1\rangle \quad &\xrightarrow{X_2} \quad \frac{1}{\sqrt{2}}\Big[\alpha(|010\rangle + |101\rangle) + \beta(|010\rangle - |101\rangle)\Big] \\
&\xrightarrow[C_1NOT_3]{C_1NOT_2} \quad \frac{1}{\sqrt{2}}\Big[\alpha(|0\rangle + |1\rangle)\,|10\rangle + \beta(|0\rangle - |1\rangle)\,|10\rangle\Big] \\
&\xrightarrow{T_{231}} \quad \frac{1}{\sqrt{2}}\Big[\alpha(|0\rangle + |1\rangle) + \beta(|0\rangle - |1\rangle)\Big]\,|10\rangle \\
&\xrightarrow{H_1} \quad \Big(\alpha\,|0\rangle + \beta\,|1\rangle\Big)\,|10\rangle = |\psi\rangle\,|10\rangle\,. \qquad (7.4.10)
\end{aligned}$$

Si noti che in questo caso la porta di Toffoli agisce come l'identità . Nuovamente, il risultato finale è che il primo qubit e' quello originale mentre i secondi due vengono cambiati in $|10\rangle$. Analogamente, si può dimostrare che nel caso di errore sul terzo qubit del blocco lo stato finale sarà $|\psi\rangle\,|01\rangle$ mentre in assenza di errori si avrà (banalmente) $|\psi\rangle\,|00\rangle$.

Possiamo fare un'osservazione. La prima è che mentre il primo qubit ritorna quello originale, gli altri due sono usati per ampliare lo spazio e per immagazzinare l'informazione indesiderata. Dovranno quindi essere eliminati e non potranno essere riutilizzati. Un'ulteriore applicazione del codice di correzione dovrebbe quindi prevedere nuovi qubit con un considerevole aumento del hardware quantistico. Un'alternativa è riinizializzare gli stessi qubit nello stato $|00\rangle$ lascindo che decadano per effetto del rumore esterno.

7.4.6 *Phase flip*

Come nel protocollo in sec. 7.4, l'errore di *phase flip* viene corretto con il confronto fra i blocchi (non fra i qubit). Ricordiamo che, se il *phase flip* avviene su uno dei tre qubit che compongono il blocco, questo induce la trasformazione in Eq. (7.4.5): $|\bar{0}\rangle \leftrightarrow |\bar{1}\rangle$. Notiamo inoltre che la trasformazione in Fig. 22 b) e in Eq. (7.4.7) darà

$$\begin{aligned}
|000\rangle \quad &\xrightarrow{\text{Fig 22 b)}} \quad \frac{|000\rangle + |111\rangle}{\sqrt{2}} = |\bar{0}\rangle \\
|100\rangle \quad &\xrightarrow{\text{Fig 22 b)}} \quad \frac{|000\rangle - |111\rangle}{\sqrt{2}} = |\bar{1}\rangle \qquad (7.4.11)
\end{aligned}$$

Per la trasformazione inversa Fig. 22 c) dobbiamo tenere in conto la presenza della porta di Toffoli T_{231}. Sul blocco $|\bar{0}\rangle$ otteniamo

$$|\bar{0}\rangle \quad \xrightarrow[C_1NOT_3]{C_1NOT_2} \quad \frac{|000\rangle + |100\rangle}{\sqrt{2}} \xrightarrow{T_{231}} \frac{|000\rangle + |100\rangle}{\sqrt{2}} \xrightarrow{H_1} |000\rangle\,. \qquad (7.4.12)$$

Quindi la porta di Toffoli agisce come l'identità . In modo analogo si ottiene

$$|\bar{1}\rangle \quad \xrightarrow[C_1NOT_3]{C_1NOT_2} \quad \frac{|000\rangle - |100\rangle}{\sqrt{2}} \xrightarrow{T_{231}} \frac{|000\rangle - |100\rangle}{\sqrt{2}} \xrightarrow{H_1} |100\rangle\,. \qquad (7.4.13)$$

Quindi abbiamo verificato che la sequenza in Fig. 22 c) è l'opposta di quella in in Fig. 22 b) per i suddetti stati.

Siamo in grado ora di verificare che la trasformazione in Fig. 22 d) corregge anche gli errori di *phase flip*. Scriviamo lo stato a 9 qubit come $|\psi\rangle = \alpha|\bar{0}\bar{0}\bar{0}\rangle + \beta|\bar{1}\bar{1}\bar{1}\rangle$ e supponiamo che avvenga un *phase flip* sul primo blocco

$$|\psi\rangle \xrightarrow{\text{phase flip}} \alpha|\bar{1}\bar{0}\bar{0}\rangle + \beta|\bar{0}\bar{1}\bar{1}\rangle = |\psi_1\rangle\,. \tag{7.4.14}$$

Come visto sopra, le porte di Toffoli T_{231}, T_{564} e T_{897} in Fig. 21 agiscono come l'identità . Usando la trasformazione in inversa in Fig. 22 c), abbiamo

$$|\psi_1\rangle \to \alpha|100\rangle|000\rangle|000\rangle + \beta|000\rangle|100\rangle|100\rangle = |\psi_2\rangle\,. \tag{7.4.15}$$

Le successive porte C_1NOT_4, C_1NOT_7 e T_{471} agiranno come

$$\begin{aligned} |\psi_2\rangle \quad &\xrightarrow[C_1NOT_4]{C_1NOT_7} \quad \alpha|100\rangle|100\rangle|100\rangle + \beta|000\rangle|100\rangle|100\rangle \\ &\xrightarrow{T_{471}} \quad \alpha|000\rangle|100\rangle|100\rangle + \beta|100\rangle|100\rangle|100\rangle \\ &= \quad \Big(\alpha|0\rangle + \beta|1\rangle\Big)|00\rangle|100\rangle|100\rangle = |\psi\rangle|00\rangle|100\rangle|100\rangle\,. \end{aligned} \tag{7.4.16}$$

Abbiamo verificato che il circuito ripristina lo stato iniziale $|\psi\rangle$ a discapito degli altri qubit.