Alma Mater Studiorum - Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Triennale in Informatica

SUGLI OPERATORI DI MISURA NELLA COMPUTAZIONE QUANTISTICA

Tesi di Laurea in Sicurezza e Crittografia

Relatore:
Ill.mo Dott. Ugo Dal Lago

Presentata da:
Francesco Barbieri

II Sessione
Anno Accademico 2009/2010

Introduzione

Quantum mechanics: Real Black Magic Calculus

– Albert Einstein

Le leggi che governano il comportamento delle particelle a livello microscopico (ad esempio all'interno di un atomo) non sono le stesse che siamo abituati a vedere nella vita quotidiana. La branca della fisica che studia i fenomeni a livello microscopico è chiamata *meccanica quantistica*.
I fenomeni in campo quantistico sono stati studiati a partire dalla prima metà del secolo scorso e i risultati sono stati sorprendenti, a tal punto che per alcuni di essi non sono ancora state trovate spiegazioni convincenti.

Un modo intuitivo per vedere le differenze tra la meccanica quantistica e quella classica è confrontarle nel campo della dinamica. A livello macroscopico, se volessimo conoscere il luogo in cui siamo in questo momento, potremmo rispondere di essere in aula, o in un qualunque altro luogo ben definito. In termini quantistici, invece, potremmo dire di essere *un po'* in aula, *un po'* a casa e *un po'* in biblioteca. Ma come è possibile? Noi siamo sicuri che un certo oggetto si trovi in una sola posizione in un determinato istante, invece un elettrone ha probabilità non nulla di trovarsi in più posizioni contemporaneamente. Viene naturale chiedersi perchè non si può dire la stessa cosa anche nella meccanica classica, quindi nella vita di tutti i giorni. Perchè noi possiamo essere in un solo posto e invece un elettrone può essere in una posizione non definita? Eppure, tra le altre cose, siamo fatti anche di elettroni: come fa il nostro corpo a contrarre lo stato di tutti i suoi infiniti sistemi

quantistici? Anche se sono state date numerose interpretazioni a questo ed altri fenomeni, ancora oggi non esiste una spiegazione condivisa da tutta la comunità scientifica.

Un altro problema aperto è quello della misura: infatti se si effettua una misurazione su un determinato sistema quantistico questo perturba il suo stato, e la posizione dell'elettrone diventa certa. Uno dei più famosi esempi è quello del gatto di Schrödinger, che può essere allo stesso tempo vivo e morto, fino a che non si controlli *(osservi)* la sua salute. L'esempio può essere riassunto nel seguente modo [5]:

> Si rinchiuda un gatto in una scatola d'acciaio insieme con la seguente macchina infernale: in un contatore di atomi radioattivi si trova una minuscola porzione di sostanza radioattiva, così poca che nel corso di un'ora forse uno dei suoi atomi si disintegra, ma anche in modo parimenti verosimile nessuno; se ciò succede, allora il contatore lo segnala e aziona un martelletto che rompe una fiala con del cianuro. Dopo avere lasciato indisturbato questo intero sistema per un'ora, si direbbe che il gatto è ancora vivo se nel frattempo nessun atomo si fosse disintegrato. La prima disintegrazione atomica lo avrebbe avvelenato. La funzione Ψ dell'intero sistema porta ad affermare che in essa il gatto vivo e il gatto morto non sono stati puri, ma miscelati con uguale peso.

Quindi la misura perturba lo stato, ed è per questo che aprendo la scatola il gatto è vivo o morto, altrimenti sarebbe in entrabi gli stati.

La meccanica quantistica trova varie applicazioni in capo scientifico. Una di queste è il Computer quantistico, cioè un dispositivo che obbedisce alle leggi della meccanica quantistica. Il modello di calcolo basato su questo dispositivo è la Computazione Quantistica. Quali vantaggi può portare questo modello di calcolo?

Nella computazione classica, secondo la tesi seguente

Tesi di Church-Turing "forte" Ogni modello computazionale fisicamente realizzabile può essere simulato da una Macchina di Turing (MdT) con un overhead al più polinomiale. In altre parole, t passi nel modello

scelto possono essere simulati con al più t^c passi di una MdT, dove c è una costante dipendente dal modello.

una MdT può simulare ogni modello computazionale che si può costruire. Quindi se si riuscisse a costruire un Computer Quantistico questo dovrebbe essere simulabile con una MdT. Questa Tesi però si basa sulla Macchina di Turing Classica, la quale rappresenta un dispositivo meccanico di computazione che obbedisce alle leggi della fisica standard. Se si pensasse di costruire un modello di calcolo basato sulle leggi della Meccanica Quantistica (computer quantistico), siamo sicuri che sarebbe possibile simularlo? Sarebbe come chiedersi: "è possibile simulare la meccanica quantistica utilizzando la fisica classica?". Sebbene non sappiamo se ciò sia possibile, ci sono forti evidenze che questo non valga. Infatti esistono funzioni intrattabili per il modello classico e allo stesso tempo calcolabili in tempo polinomiale dal paradigma quantistico. Per esempio la fattorizzazione dei numeri primi può essere risolta in tempo polinomiale con l'algoritmo di Shor (1994). Un altro esempio che il modello classico non può simulare è il parallelismo quantistico, dove più calcoli sono eseguiti nello stesso momento (l'Algoritmo di Deutsch può valutare se una funzione è costante o bilanciata valutandola una sola volta, cioè eseguendo nello stesso momento $f(0) \oplus f(1)$).

Quindi, se esistesse un computer quantistico, la tesi di *Tesi di Church-Turing "forte"* non sarebbe più valida e sarebbe sostituita dalla

Tesi di Church-Turing "forte" Quantistica Ogni modello computazionale fisicamente realizzabile può essere simulato da una MdT Quantistica.

Rimane *solo* una domanda ancora aperta: sarà possibile costruire un computer quantisitico?

In questa tesi di certo non si risponderà ad una domanda di questo calibro, ma ci si limiterà a studiare formalmente una specifica proprietà della Computazione Quantistica. In particolare, il modello di calcolo che si utilizzerà (*circuito quantistico*) può essere rappresentato da una *sequenza* di operazioni. Una sequenza è detta *mista* (circuito misto) se si presentano operazioni classiche e quantistiche in modo alternato (sequenze del tipo Q-C-C-Q-Q-C). Una sequenza in *Forma Normale*, invece, ammette operazioni classiche

solamente all'inizio o alla fine, mentre in mezzo possono esserci solamente operazioni quantistiche (sequenze del tipo C-C-Q-Q-Q-C). Una sequenza di operazioni esclusivamente quantistiche porta numerosi vantaggi, per questo la forma normale è molto importante. Essa infatti separa le operazioni classiche da quelle quantistiche, concentrandole tutte all'interno. Quello che si farà in questa tesi sarà fornire un modo operativo (mediante riscritture) per ottenere la forma normale di una qualsiasi sequenza di operazioni classiche o quantistiche.

Nel primo capitolo si forniranno alcune nozioni di meccanica e di computazione in campo quantistico, necessarie per comprendere la trattazione. Successivamente (secondo capitolo) si definirà in modo formale il modello dei *circuiti quantistici.*

Nell'ultimo capitolo si descriverà la *Forma Normale* di una sequenza e si elencheranno delle semplici regole di riscrittura (che dimostreremo essere corrette) per la normalizzazione. Dimostreremo infine che, semplicemente applicando un numero finito di riscritture ad una qualsiasi sequenza, è possibile ottenere una sequenza equivalente in Forma Normale.

Indice

Capitolo 1

Nozioni Teoriche

In questo capitolo iniziale si vuole fornire al lettore una base teorica per comprendere il seguito della tesi. Per prima cosa si daranno delle nozioni sul modello matematico che sta alla base della computazione quantistica. In un secondo momento si affronteranno, sia in modo intutivo che in modo formale, i quattro postulati fondamentali della meccanica quantistica.

1.1 Computazione Quantistica

In questa sezione si vuole definire il modello matematico che sta alla base della computazione quantistica, fornendo allo stesso tempo un confronto con il paradigma classico.

1.1.1 Quantum Bit

Un Quantum bit *(qubit)* è il bit nella computazione quantistica. Nella logica classica un bit vale *0* oppure *1,* un qubit invece può avere infiniti stati. Si può rappresentare un qubit mediante un vettore unitario in uno spazio vettoriale complesso a due dimensioni ($\mathbb{C}^2$). I vettori $|0\rangle$ e $|1\rangle$ formano una base ortonormale *(base computazionale standard)* e valgono:

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

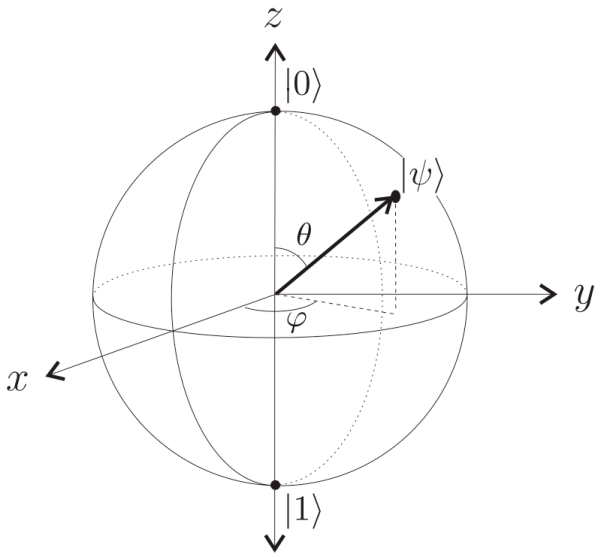

Figure 1.1: Sfera di Bloch

Un qubit $|\psi\rangle$ si rappresenta come:

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

dove $\alpha, \beta \in \mathbb{C}$ e sono dette ampiezze, infatti il qubit è con probabilità $|\alpha|^2$ uguale a 0 e con probabilità $|\beta|^2$ uguale a 1. Visto che si ha una *probabilità,* la somma $|\alpha|^2 + |\beta|^2$ deve essere normalizzata, cioè uguale a 1.

1.1.2 Sfera di Bloch

Un modo intuitivo per rappresentare un qubit è attraverso la sfera di Bloch (vedi Figura 1.1). Questa è una sfera di raggio unitario dove il polo nord indica lo stato $|0\rangle$ e il polo sud $|1\rangle$. I possibili stati di un qubit sono tutti i punti della superficie della sfera, infatti si può dimostrare che c'è corrispondenza biunivoca tra uno stato $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ e un punto sulla sfera rappresentato come:

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

dove $\theta, \varphi \in \mathbb{R}$ sono le coordinate sferiche del punto.

1.1.3 Registri Quantistici

Si è appena visto come rappresentare un solo qubit, ma come è possibile rappresentare un sistema a più qubit? A questo scopo si utilizza un registro quantistico, che di fatto indica in che modo i qubit sono collegati tra loro. Si definisce un registro quantistico, secondo il quarto postulato della meccanica quantistica, come:

$$|i_1\rangle \otimes ... \otimes |i_n\rangle$$

dove $i = \{0, 1\}$ e n è il numero di qubit. Si può anche rappresentare come $|i_1...i_n\rangle$. Il prodotto tensore è un operazione usata per combinare spazi vettoriali per formarne di più grandi, infatti $\otimes : \mathbb{C}^k \times \mathbb{C}^m \to \mathbb{C}^{km}$. Quindi lo spazio totale di un registro quantistico sarà $\mathbb{C}^{2\cdot...\cdot 2} = \mathbb{C}^{2^n}$. Con $n = 200$ si ottiene un numero di stati più grande del numero di atomi nell'universo [3]. Le potenzialità di un registro di questo tipo non sono neanche confrontabili con quelle di un registro classico.

Pensiamo ora ad un semplice sistema a due qubit, dove il primo è $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ e il secondo vale $|\varphi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$. Lo stato totale sarà:

$$|\psi\rangle \otimes |\varphi\rangle = \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle$$

lo stato (dopo una misura) risulterà in $|00\rangle$ con probabilità $|\alpha_0\beta_0|^2$, in $|01\rangle$ con probabilità $|\alpha_0\beta_1|^2$ e così via. Se invece volessimo sapere con che probabilità si ha *solamente* il primo bit a 0, cioè registri del tipo $|0x\rangle$, con $x \in \{0, 1\}$, allora basterebbe sommare le probabilità di $|00\rangle$ e di $|01\rangle$, cioè $|\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2$. L'unica particolarità è che dopo una misurazione lo stato collassa ad uno stato diverso. Si affronterà questo aspetto più avanti, nel terzo Postulato della Meccanica Quantistica.

1.1.4 Trasformazioni Quantistiche

Esistono vari modelli di calcolo nella computazione quanstica, in questa tesi si userà quello dei Circuiti Quantistici (quantum circuits) ampliamente trattati

nel prossimo capitolo. Possiamo immaginare un circuito quantistico come un circuito classico (una rete combinatoria), dotato di linee di input/output e di porte logiche. In ogni punto del circuito si avrà un certo stato che si potrà rappresentare con un registro quantistico.

In generale il passaggio da uno stato quantistico ad un altro si rappresenta tramite matrici unitarie. Una trasformazione quantistica è il corrispettivo delle porte logiche nelle reti combinatorie, infatti si parlerà di porte logiche quantistiche.

Ci si potrebbe chiedere cosa voglia dire *applicare* una porta ad un certo stato quantistico. Dato un vettore $|\psi\rangle$ si applica una certa porta, rappresentata da M, in questo modo

$$M\,|\psi\rangle$$

cioè semplicemente moltiplicando la matrice per il vettore.

Nella rappresentazione mediante sfera di Bloch, una trasformazione è il passaggio da un punto ad un altro della sfera, cioè un insieme di rotazioni rispetto agli assi $\vec{x}$,$\vec{y}$ e $\vec{z}$ (Teorema di Bloch, si vedrà nel Capitolo 3)

Studiamo ora il comportamento delle più comuni porte quantistiche. Si ricorda che una trasformazione quantistica può operare su uno o più qubit. Le porte quantistiche che operano su un solo qubit, a differenza di quelle classiche, non sono banali. Le uniche porte classiche a un bit sono la porta che lascia invariato il bit e il `NOT`, che inverte il bit in input. Nel campo quantistico queste due porte sono chiamate rispettivamente `I` (matrice identità) e `X` e sono rappresentate dalle matrici:

$$\texttt{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \texttt{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Se per esempio si applica la porta `X` allo stato $|0\rangle$ si ha

$$\texttt{X}\,|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

Allo stesso modo $X\,|1\rangle = |0\rangle$.

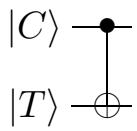

Figure 1.2: Porta `CNOT`: C è il qubit control e T è il qubit target

In campo quantistico esistono tante altre porte ad un solo qubit. Una di queste, molto importante nella computazione quantistica, è chiamata `H` ed è definita come:

$$\texttt{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Questa trasformazione permette di costruire una sovrapposizione dove la probabilità di avere $|0\rangle$ è la stessa di avere $|1\rangle$. Infatti se si applica $\texttt{H}\,|0\rangle$si ottiene

$$\texttt{H}\,|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$$

Quando si misura questo stato si ha $|0\rangle$ e $|1\rangle$ con la stessa probabilità, infatti si ha $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$ per entrambi i qubit. Stessa cosa accade per $|1\rangle$.

Le porte a più quibit funzionano nello stesso modo di quelle ad un qubit. Vediamo in particolare `CNOT`, il cui corrispettivo classico è l'`XOR`. Questa porta opera su due qubit, il primo è detto *control*, il secondo *target*. Il funzionamento è semplice: il qubit target viene invertito (si applica la `X`) se il control è $|1\rangle$, altrimenti lo stato rimane invariato. Dato un qualsiasi registro a due qubit vale:

$$\texttt{CNOT}(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |x \oplus y\rangle$$

La porta `CNOT`, rappresentata in *Figura 1.2*, sarà utile in seguito.

1.2 Meccanica Quantistica

Per prima cosa si vogliono spiegare in modo intuitivo alcuni fenomeni legati alla meccanica quantistica (Sovrapposizione, Misura ed Entanglement), e successivamente si affronteranno in modo formale i quattro postulati fondamentali.

1.2.1 Sovrapposizione, Misura ed Entanglement

L'idea di *Sovrapposizione degli stati* è molto semplice: si pensi ad un elettrone che ruota intorno ad un atomo. L'elettrone può essere con probabilità non nulla sia in un punto A che in un punto B della sua orbita. Questo, anche se può sembrare strano, è un comportamento abbastanza certo, studiato e approvato da tutta la comunità scientifica. Quando invece si misura la posizione nella sua orbita, l'elettrone assume solo la posizione A o la posizione B. Allo stesso modo un qubit può essere sia nello stato uno che nello stato zero, cioè in una sovrapposizione di stati. Se si pensa alla rappresentazione mediante sfera di Bloch è facile immaginare che lo stato del qubit può non essere del tutto zero o del tutto uno. Quando si misura si potrà avere come risultato zero oppure uno, e lo stato del sistema cambierà. Nel terzo Postulato si affronta con maggior rigore questo problema.

L'*entanglement* è un fenomeno poco intuitivo. Due qubit disitinti possono essere collegati tra loro in modo molto stretto, fino al punto, che indipendentemente dalla loro distanza il comportamento di uno può dipendere dal comportamento dell'altro e viceversa. In generale, dato uno sistema a n qubit, se non è possibile decomporre lo stato totale nei qubit che lo compongono, allora questi sono detti entangled. In pratica nessun qubit ha uno stato individuale, ma solo l'insime di tutti ha uno stato ben definito. Una manifestazione molto interessante di questo fenomeno è la quantum pseudo-telepathy: due qubit entangled sono quasi telepatici. Si può immaginare ad una sorta di telepatia, cioè i due qubit riescono ad agire come se si scambiassero informazioni senza comunicare (un esempio semplice può essere trovato in [6]).

1.2.2 Postulati

Cerchiamo di capire da dove derivano i principi descritti in precedenza. Si affrontano ora in modo formale i quattro postulati fondamentali della meccanica quantistica. Naturalmente saranno semplificati in base all'utilizzo che ne faremo nella Computazione Quantistica. I postulati saranno descritti prendendo spunto da [3], tranne il terzo che è descritto nello stesso modo di [2].

Postulato 1 *Ogni sistema fisico isolato ha associato uno spazio di Hilbert complesso, detto spazio degli stati del sistema. Il sistema è completamente descritto dal suo vettore di stato, che è un vettore unitario nello spazio degli stati.*

Dato che si lavorerà con qubit, si considererà lo spazio di Hilbert $\mathbb{C}^2$, che nella computazione quantistica si può considerare semplicemente come uno spazio vettoriale con prodotto interno.

Postulato 2 *L'evoluzione di un sistema quantistico chiuso è descritto da una trasformazione unitaria U: lo stato $|\psi\rangle$ del sistema al tempo t_1 è in relazione con lo stato $|\psi'\rangle$ del sistema al tempo t_2 mediante un operatore unitario U che dipende solo da t_1 e t_2:*

$$|\psi'\rangle = U\,|\psi\rangle$$

Quindi una Trasformazione Quantistica (descritta nella sezione precedente) descrive l'evoluzione di un sistema da un istante ad un altro.

Postulato 3 *Data una base ortonormale $B = \{|\varphi_i\rangle\}$ relativa ad uno spazio di Hilbert $\mathcal{H}_A$ per un sistema A, se si esegue una misura di Von Neumann (rispettivamente alla base B) sullo stato*

$$|\psi\rangle = \sum_i \alpha_i\,|\varphi_i\rangle$$

si avrà in output i con probabilità $|\alpha_i|^2$ e lo stato collasserà in $|\varphi_i\rangle$. Inoltre, dato uno stato $|\psi\rangle = \sum_i \alpha_i\,|\varphi_i\rangle\,|\gamma_i\rangle$ definito nello spazio $\mathcal{H}_A \otimes$

$\mathcal{H}_B$, allora se si esegue una misura di Von Neumann sul sistema A si avrà in output i con probabililità $|\alpha_i|^2$ e lo stato collasserà in $|\varphi_i\rangle |\gamma_i\rangle$.

Quando si parla di misura sono da tenere in considerazione due aspetti: il *risultato* della misura, che dipende dalla probabilità dell'osservabile che si sta misurando e lo *stato del sistema* che si avrà dopo la misura. Cerchiamo di capire meglio tramite un esempio. Si supponga di avere uno stato quantistico

$$|\psi\rangle = \alpha |00\rangle + \beta |01\rangle + \gamma |11\rangle$$

e di voler misurare il primo qubit. Per prima cosa è necessario mettere lo stato nella forma $|0\rangle \otimes (...) + |1\rangle \otimes (...)$ come indicato nella seconda parte del postulato. Si ottiene:

$$\begin{aligned} |\psi\rangle &= |0\rangle \otimes (\alpha |0\rangle + \beta |1\rangle) + |1\rangle (\gamma |1\rangle) = \\ &= (\alpha + \beta) |0\rangle \otimes (\frac{\alpha}{(\alpha+\beta)} |0\rangle + \frac{\beta}{(\alpha+\beta)} |1\rangle) + \gamma |1\rangle \otimes (|1\rangle) \end{aligned}$$

A questo punto possiamo misurare lo stato del primo qubit, che sarà con probabilià $|(\alpha + \beta)|^2$ uguale a 0 e con probabilità $|\gamma|^2$ uguale a 0. Questo è molto intuitivo, infatti sei si considera lo stato iniziale si nota che il primo qubit è 0 nel primo e nel secondo membro della somma, che hanno rispettivamente ampiezza α e β.
Nel caso la misura risultasse 0 allora lo stato del sistema collasserebbe a

$$|\psi\rangle = \frac{\alpha}{(\alpha+\beta)} |0\rangle + \frac{\beta}{(\alpha+\beta)} |1\rangle$$

altrimenti, con risultato 1, si avrebbe $|\psi\rangle = |1\rangle$.

Postulato 4 *Lo spazio degli stati di un sistema fisico composto è il prodotto tensore degli spazi degli stati dei sistemi fisici componenti. Se il sistema è composto da n sottosistemi e il componente i-esimo si trova nello stato $|\psi_i\rangle$, allora lo stato del sistema totale è $|\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$.*

Questo serve per capire come comporre sistemi formati da più qubit, che nella sezione della Computazione Quantistica abbiamo chiamato Registro

Quantistico; questo è stato definito in modo concorde al postulato, infatti per n qubit è definito come $|i_1\rangle \otimes ... \otimes |i_n\rangle$.

Capitolo 2

Circuiti Quantistici

Tra i modelli di calcolo più utilizzati per descrivere la computazione quantistica vi sono i Circuiti Quantistici. Per prima cosa si definirà formalmente un Circuito, e poi si descriveranno circuiti molto semplici detti Operatori. In seguito saranno definite anche delle regole di composizione, che renderanno possibile la creazione di circuiti complessi.

2.1 Circuito Misto

Definiamo in modo formale un circuito quantistico. Lo chiameremo *Misto* perchè ammetterà qualsiasi tipo di operazione, sia che operi su bit classici che su qubit. Lo stato in ogni momento sarà *misto,* nel senso che ci saranno distribuzioni di probabilità insieme a stati quantistici puri. Ma qual è la differenza tra uno stato puro e uno misto? In fondo un qubit è un oggetto che indica con una certa probabilità un certo risultato (si pensi alle ampiezze di probabilità). Non bisogna farsi ingannare: un qubit ha proprietà che non sono "simulabili" tramite una distribuzione di probabilità. Si affronterà la questione e si vedrà un controesempio alla fine del capitolo. Concentriamoci ora sul formalismo dei *Circuiti Misti*.

Definizione 2.1.1. Un *Cicuito Misto* è una quintupla del tipo $(n, m, Inp, Out, \varphi)$ dove

- $n, m \in \mathbb{N}$ rappresentano rispettivamente il numero di linee in ingresso e in uscita al circuito. I vari input sono ordinati ed è possibile riferirsi ad essi tramite un numero naturale che ne rappresenta la posizione

- $Inp : \{1, .., n\} \rightarrow \{ C, Q\}$ dato un indice di un input la funzione denota se è di tipo Classico o Quantistico

- $Out : \{1, .., m\} \rightarrow \{C, Q\}$ dato un indice di un output la funzione denota se è di tipo Classico o Quantistico

- $\varphi : F_{dist}(Conf(n, Inp)) \rightarrow F_{dist}(Conf(n, Inp))$ dove $F_{dist}(S)$ è l'insieme di tutte le distribuzioni di probabiltà con supppoto finito in S. L'argomento $Conf(n, Inp)$ è detto configurazione del circuito. Data una certa funzione *"test Classico/Quantistico"* (come *Inp* e *Out*) e un qualsiasi $t \in \mathbb{N}$, $Conf(t, f)$ è definita per induzione nel seguente modo:

$$Conf(1, f) = \begin{cases} \mathbb{C}^2 & se\, f(1) = Q \\ \{|0\rangle, |1\rangle\} & se\, f(1) = C \end{cases}$$

$$Conf(t+1, f) = Conf(t, f) \otimes \begin{cases} \mathbb{C}^2 & se\, f(t+1) = Q \\ \{|0\rangle, |1\rangle\} & se\, f(t+1) = C \end{cases}$$

Un circuito misto è quindi una trasformazione descritta dalla funzione φ. Il domino e il codomino di φ saranno distribuzioni di probabilità con un numero di elementi finito. Inoltre φ dipende dalle configurazioni $Conf(n, Inp/Out)$, che rappresentano sequenze di bit e qubit in ingresso *(dominio)* e in uscita *(codominio)*. Per esempio, per una configurazione di input di questo tipo: $Conf(3, Inp) = \{|0\rangle, |1\rangle\} \otimes \mathbb{C}^2 \otimes \{|0\rangle, |1\rangle\}$ con $Inp(1) = Inp(3) = C$ e $Inp(2) = Q$ si avrà che il primo e il terzo input saranno bit classici e il secondo sarà un qubit. In questo modo è possibile definire campi di input e output misti, consentendo ad un operatore di agire sia su bit che su qubit. Da notare che quando si lavora su bit si usa il campo $\{|0\rangle, |1\rangle\}$ dove c'è corrispondenza diretta tra $0 \rightarrow |0\rangle$ e tra $1 \rightarrow |1\rangle$. In pratica si vedono i bit classici come qubit che non ammettono sovrapposizioni

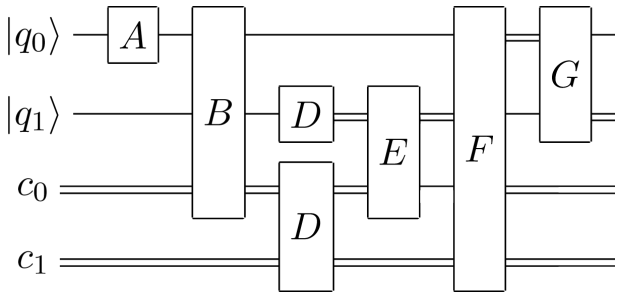

Figure 2.1: Esempio di circuito misto

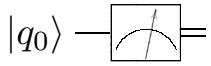

Figure 2.2: Operatore di Misura di un Qubit

(ovviamente non potrebbero essere rappresentate da un bit classico). Un esempio di circuito quantistico misto è rappresentato in *Figura 2.1.* Le linee doppie rappresentano bit classici, quelle singole qubit quantistici.

2.2 Operatori

Si definiscono ora i casi più semplici di circuito: gli *Operatori*.

2.2.1 Operatore di Misura

L'operatore di misura è un interfaccia tra il modello classico e quello quantistico, attraverso la quale dato in input un qubit si può determinare il valore binario corrispondente.

Definizione 2.2.1. L'operatore di misura è rappresentato dalla quintupla $(n, m, Inp, Out, \varphi)$ dove:

- $n = m = 1$ e valgono $Inp(1) = \{Q\}$ e $Out(1) = \{C\}$
- Per definizione di circuito, il dominio e il codominio della funzione di trasformazione saranno:

$$\varphi : F_{dist}(\mathbb{C}^2) \to F_{dist}(\{|\ 0\rangle, |\ 1\rangle\})$$

Il risultato di φ è una distribuzione finita dove gli elementi possibili sono $\{|\ 0\rangle, |\ 1\rangle\}$. Il dominio invece è l'insieme delle distribuzioni finite su supporto $\mathbb{C}^2$. Si prende come testimone di questo insieme $\xi : (\mathbb{C}^2 \to \mathbb{R})$, che rappresenta la distribuzione dove la dimensione degli elementi, presenti in numero finito, è quella di un solo qubit. Si avranno casi del tipo $(\alpha_i \mid 0\rangle + \beta_i \mid 1\rangle) \mapsto p_i$, dove α_i corrisponde all'ampiezza di $\mid 0\rangle$ (β_i si riferisce a $\mid 1\rangle$) in un determinato membro i di ξ, in cui: $i, l \in \mathbb{N}$, $l = |\xi|$, $1 \leq i \leq l$. La probabilità di i è rappresentata da $p_i \in \mathbb{R}$. L'andamento di φ risulterà:

$$\varphi(\xi) = \begin{cases} |0\rangle \mapsto \sum_{i=0}^{l} |\alpha_i|^2 p_i \\ |1\rangle \mapsto \sum_{i=0}^{l} |\beta_i|^2 p_i \end{cases}$$

Se invece si ha una cofigurazione in cui sono presenti più qubit si avrà una distibuzione $\mathcal{D}$ definita come:

$$\mathcal{D} = \begin{cases} \alpha_0^1 |0\rangle \otimes |\psi_0^1\rangle + \alpha_1^1 |1\rangle \otimes |\psi_1^1\rangle \mapsto p_1 \\ \vdots \\ \alpha_l^1 |0\rangle \otimes |\psi_0^1\rangle + \alpha_l^1 |1\rangle \otimes |\psi_l^1\rangle \mapsto p_l \end{cases}$$

e la misura risulterà:

$$\varphi(\mathcal{D}) = |b\rangle \otimes |\psi\rangle \mapsto \sum_{\forall j \in 1,\ldots,l | \psi_b^l = \psi} |\alpha_b^j|^2 p_j$$

dove $b \in \{0, 1\}$ e l è la cardinalità della distribuzione.

In pratica l'opertore di Misura è la rappresentazione del terzo postulato della Meccanica Quantistica nel formalismo dei circuiti quantistici.

2.2.2 Operatore QG

L'operatore QG *(qubit generator)* è l'inverso della misura, infatti dato in input un bit classico genera un bit quantistico.

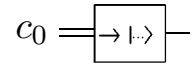

Figure 2.3: Operatore di creazione di qubit a partire da bit classico

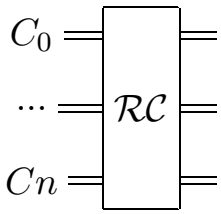

Figure 2.4: Operatore Rete Combinatoria

Definizione 2.2.2. L'operatore QG è rappresentato dalla quintupla $(n, m, Inp, Out, \varphi)$ dove:

- $n = m = 1$ e valgono $Inp(1) = \{C\}$ e $Out(1) = \{Q\}$
- Per definizione di circuito il dominio e il codominio della funzione di trasformazione saranno:

$$\varphi : F_{dist}(\{|0\rangle, |1\rangle\}) \rightarrow F_{dist}(\mathbb{C}^2)$$

  e l'andamento $\forall x \in \{|0\rangle, |1\rangle\}$ e $p \in \mathbb{R}$ sarà:

$$\varphi(\{|x\rangle \mapsto p) = |x\rangle \mapsto p$$

La distribuzione generata da φ rimane la stessa *(stesse probabilità)* ma il bit viene "trasformato" in un qubit. Si noti che φ è la funzione identità. Il punto chiave di questa trasformazione e nel cambio dei possibili valori che può assumere un elemento della distribuzione in ingresso. Dopo l'applicazione di QG non saranno possibili solo i valori $|0\rangle$ e $|1\rangle$, ma ogni valore appartenente a $\mathbb{C}^2$.

2.2.3 Operatore RC

I Circuiti Misti ammettono anche operazioni classiche. Si definisce l'operatore

Rete Combinatoria (RC) che rappresenta una serie di una o più porte logiche, che implementano una certa funzione booleana.

Definizione 2.2.3. Secondo la definizione di circuito $(n, m, Inp, Out, \varphi)$, si ha una rete combinatoria quando:

- $\forall i \in \mathbb{N}$ con $0 \leq i < n$ vale $Inp(i) = \{C\}$
- $\forall j \in \mathbb{N}$ con $0 \leq j < m$ vale $Out(j) = \{C\}$
- Per definizione di circuito, il dominio e il codominio della funzione di trasformazione saranno:

  $$\varphi : F_{dist}(\underbrace{\{|0\rangle, |1\rangle\} \otimes ... \otimes \{|0\rangle, |1\rangle\}}_{n\,volte}) \rightarrow F_{dist}(\underbrace{\{|0\rangle, |1\rangle\} \otimes ... \otimes \{|0\rangle, |1\rangle\}}_{m\,volte})$$

  Per una certa distribuzione ξ l'andamento risulterà:

  $$\varphi(\xi)(y_1, \ldots, y_m) = \sum_{(x_1,\ldots,x_n)\in G} \xi(x_1, \ldots, x_n)$$

  dove G è l'insieme di tutti gli elementi di ξ tali che $f_{bool}(x_1, ..., x_n) = y_1, \ldots, y_m$ e $f_{bool} : \{|0\rangle, |1\rangle\}^n \rightarrow \{|0\rangle, |1\rangle\}^m$ è una funzione booleana.

Si può pensare all'esempio in cui la f_{bool} è una singola porta OR. Se in ingresso si ha una distribuzione ξ dove ogni coppia (x_1, x_2) ha uguale probabilità (cioè $\forall(x_1, x_2)\ \xi(x_1, x_2) = 1/4$) si otterrà un $\varphi_{OR}(\xi)(1) = \sum_{\xi(x_1,x_2)=1} \xi(x_1, x_2) = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4}$ e $\varphi_{OR}(\xi)(0) = ... = \frac{1}{4}$. Questo è proprio il rislutato che ci si aspetta, infatti se si applica un OR a due bit si hanno tre combinazioni su quattro (01, 10, 11) che danno risultato 1 e una (00) che risulta 0.

2.2.4 Operatore U

L'operatore U è una Trasformazione Quantistica. Con l'operatore U si potranno rappresentare tutte le porte quantistiche esistenti.

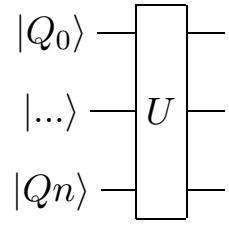

Figure 2.5: Operatore trasformazione lineare U

Definizione 2.2.4. Si definisce U tramite la definizione di operatore $(n, m, Inp, Out, \varphi)$ dove:

- $\forall i \in \mathbb{N}$ con $0 \leq i < n$ vale $Inp(i) = \{Q\}$
- $\forall j \in \mathbb{N}$ con $0 \leq j < m$ vale $Out(j) = \{Q\}$
- Dato che si considerano le transizioni puramente quantistiche si avrà φ definita nel seguente modo:

  $$\varphi : F_{dist}(\mathbb{C}^2) \to F_{dist}(\mathbb{C}^2)$$

  e per una certa distribuzione finita ξ l'andamento risulterà:

  $$\varphi(\xi)(y_1, \ldots, y_m) = \sum_{(x_1,\ldots,x_n)\in G} \xi(x_1, \ldots, x_n)$$

  dove G è l'insieme di tutti gli elementi di ξ tali che $U_q(x_1, ..., x_n) = y_1, \ldots, y_m$ e $U_q : \mathbb{C}^2 \to \mathbb{C}^2$ è una trasformazione unitaria.

Nella definizione della funzione di transizione si è usata la stessa struttura della Rete Combinatoria, ma è importante sapere che una U è una funzione unitaria, quindi reversibile. Dato che si ha una funzione biettiva è possibile rappresentare la φ come:

$$\varphi(\xi) = U(x) \mapsto \xi(x)$$

dove ξ è una distribuzione e $\xi(x)$ è la probabilità di una certa configurazione. Ad esempio, data una distribuzione in ingresso del tipo $(|\psi_0\rangle \mapsto p_0, |\psi_1\rangle \mapsto p_1)$ in out, dopo l'applicazione di U, si avrà $(U|\psi_0\rangle \mapsto p_0, U|\psi_1\rangle \mapsto p_1)$.

2.2.5 Operatore c-U

c-U rappresenta una operatore U la cui esecuzione dipende dal bit di controllo: se è attivo (=1) allora avviene la trasformazione, altrimenti la configurazione in input viene lasciata inalterata.

Definizione 2.2.5. Si definisce U tramite la definizione di circuito $(n, m, Inp, Out, \varphi)$ dove:

- $n = 2$ e valgono $Inp(1) = \{C\}$ e $Inp(2) = \{Q\}$
- $m = 2$ e valgono $Out(1) = \{C\}$ e $Out(2) = \{Q\}$
- φ è definita nel seguente modo:

$$\varphi : F_{dist}(\{|0\rangle, |1\rangle\} \otimes \mathbb{C}^2) \to F_{dist}(\{|0\rangle, |1\rangle\} \otimes \mathbb{C}^2)$$

  per una certa distribuzione ξ in ingresso, l'andamento risulterà:

$$\varphi(\xi) = \begin{cases} |1\rangle \otimes U(x) \mapsto \xi(|1\rangle \otimes x) \\ |0\rangle \otimes x \mapsto \xi(|0\rangle \otimes x) \end{cases}$$

  dove x è qubit su cui si applica la U se il bit di controllo è attivo.

2.3 Regole di composizione

Queste regole servono per comporre circuiti in modo da ottenere computazioni più complesse. Ogni circuito può essere ottenuto dalla *composizione* di uno o più circuiti più semplici (operatori).

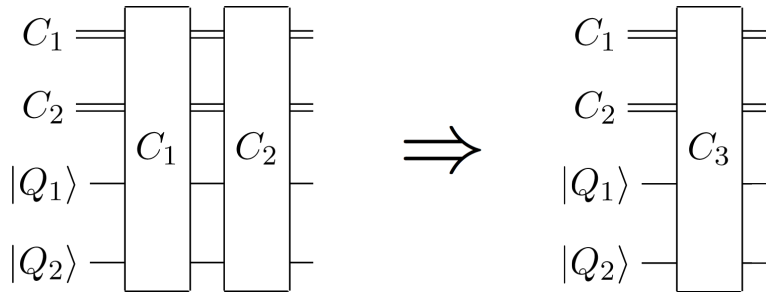

Figure 2.6: Composizione orizzontale

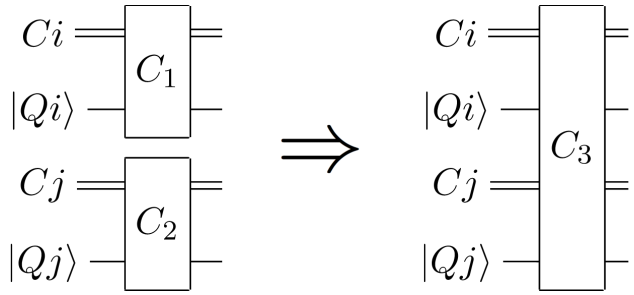

Figure 2.7: Composizione verticale

2.3.1 Composizione Orizzontale

È possibile concatenare circuiti in modo sequenziale (*Figura 2.6*).

Definizione 2.3.1. Dati due circuiti $\mathcal{C}_1 = (n_1, m_1, Inp_1, Out_1, \varphi_1)$ e $\mathcal{C}_2 = (n_2, m_2, Inp_2, Out_2, \varphi_2)$ se si ha $m_1 = n_2$ e $Out_1 = Inp_2$, allora è possibile ottenere un circuito $\mathcal{C}_3 = (n_1, m_2, Inp_1, Out_2, \varphi_2 \circ \varphi_1)$

La funzione di trasformazione risultante è la semplice composizione, infatti $(\varphi_2 \circ \varphi_1)(x) = \varphi_2(\varphi_1(x))$ cioè l'esecuzione "sequenziale".

2.3.2 Composizione Verticale

È possibile concatenare circuiti in modo verticale mediante il prodotto tensore (*Figura 2.7*).

Definizione 2.3.2. Dati due circuiti $\mathcal{C}_1 = (n_1, m_1, Inp_1, Out_1, \varphi_1)$ e $\mathcal{C}_2 = (n_2, m_2, Inp_2, Out_2, \varphi_2)$ è possibile ottenere per *composizione verticale* un circuito $\mathcal{C}_3 = (n_1 + n_2, m_1 + m_2, Inp_1, Out_2, \varphi_1 \otimes \varphi_2)$

Per convincersi che la funzione di trasformazione è proprio $\varphi_1 \otimes \varphi_2$ si pensi alla proprietà del prodotto tensore $(Mv) \otimes (Nw) = (M \otimes N)(v \otimes w)$ dove M e N sono operatori lineari del tipo $M : \mathbb{C}^k \mapsto \mathbb{C}^k$ e $N : \mathbb{C}^l \mapsto \mathbb{C}^l$ mentre $v \in \mathbb{C}^k$ e $w \in \mathbb{C}^l$ sono spazi vettoriali. Inoltre questa regola è corretta rispetto al Postulato 4 della meccanica quantistica dato nel capitolo precedente.

2.4 Distribuzioni e qubit

All'inizio del capitolo ci siamo chiesti perchè non sia possibile simulare un qubit con una distribuzione. Si riporta qui un semplice contro esempio.

Dato un qubit:

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

potremmo pensare di "simularlo" con la distribuzione:

$$\begin{aligned} |0\rangle &\mapsto 1/2 \\ |1\rangle &\mapsto 1/2 \end{aligned}$$

Ma basterebbe applicare un Operatore U, nel particolare la trasformazione `H`, per avere un comportamento diverso. Infatti nel primo caso $\mathtt{H}(|\psi\rangle) = |0\rangle$. Per la distribuzione si ottiene invece:

$$\begin{aligned} \mathtt{H}\,|0\rangle &\mapsto 1/2 \\ \mathtt{H}\,|1\rangle &\mapsto 1/2 \end{aligned}$$

cioè

$$\begin{aligned} \frac{|0\rangle + |1\rangle}{\sqrt{2}} &\mapsto 1/2 \\ \frac{|0\rangle - |1\rangle}{\sqrt{2}} &\mapsto 1/2 \end{aligned}$$

e anche se misurato, non è uguale a $|0\rangle$ come nel caso del singolo qubit, infatti

dopo una misura risulta:

$$\begin{aligned} |0\rangle &\mapsto 1/2 \\ |1\rangle &\mapsto 1/2 \end{aligned}$$

Capitolo 3

Forma Normale dei Circuiti Quantistici

Come già detto, un *circuito Misto* ammette operazioni su bit e qubit in qualsiasi posizione. Un circuito in Forma Normale, invece, è un sottoinsieme del primo e ha una struttura più rigida che separa le computazioni classiche da quelle quantistiche: alle estremità del circuito ci saranno le operazioni che interfacciano il mondo classico con quello quantistico e, nel cuore del circuito, saranno presenti solo operazioni su qbits. Lavorando con circuiti di questo tipo è possibile concentrarsi sulle trasformazioni di stati quantistici puri, senza il rischio di trovarsi in uno stato misto (cioè configurazioni con bit classici e quantistici).
In questo capitolo si darà la defininizione di *Circuito in Forma Normale* e in seguito si descriveranno e dimostreranno regole di riscrittura formali sui circuiti. Infine si dimostrerà che con la sola applicazione delle regole di riscrittura fornite, è possibile ottenere un circuito in *Forma Normale* da uno *Misto.*

3.1 Forma Normale

Definiamo ora un circuito in Forma Normale. La funzione di trasformazione prende in input e fornisce in output bit classici. All'interno del circuito si

potrà "lavorare" esclusivamente con qubit.

Definizione 3.1.1. Un *Cicuito in Forma Normale* è un particolare *Cicuito misto* del tipo $(n, m, Inp_{FN}, Out_{FN}, \varphi_{FN})$ dove

- $\forall i \in \mathbb{N}$ con $0 \leq i < n$ vale $Inp_{FN}(i) = \{C\}$
- $\forall j \in \mathbb{N}$ con $0 \leq j < m$ vale $Out_{FN}(j) = \{C\}$
- La funzione di trasformazione sarà del tipo:

  $$\varphi : F_{dist}(\underbrace{\{|0\rangle, |1\rangle\} \otimes ... \otimes \{|0\rangle, |1\rangle\}}_{n\,volte}) \rightarrow F_{dist}(\underbrace{\{|0\rangle, |1\rangle\} \otimes ... \otimes \{|0\rangle, |1\rangle\}}_{m\,volte})$$

  ed è suddivisa in 5 step:

1. Creazione di "Ancilla" bit, cioè qubit di servizio necessari per alcune trasformazioni
2. Trasformazione di tutti i bit classici in quantistici tramite l'applicazione di QG
3. Trasformazioni unitarie su qubit, sono ammesse solo Operazioni U
4. Misura dei qubit destinati all'output del circuito tramite l'Operatore di Misura
5. Eliminazione degli "Ancilla" bit

Si noti (*Figura 3.1*) che le operazioni classiche (parti 1,2,4,5 di φ) sono separate dalle operazioni puramente quantistiche (parte 3 di φ). Queste ultime operazioni sono ciò che veramente conta in un circuito in FN, il resto è solo un interfaccia per il mondo classico.

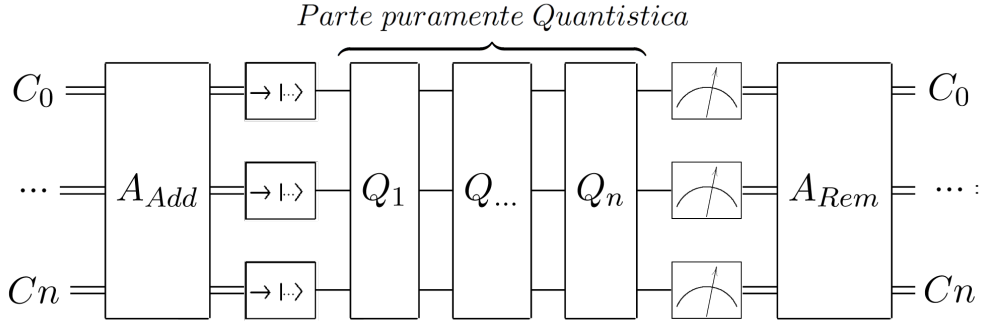

Figure 3.1: *Ciucuito in Forma Normale. A_{Add} e A_{Rem} sono le operazioni di aggiunta e rimozione degli Ancilla bit. Si noti che nella parte quantistica si lavora solo su qubit, e nell'ingresso e nell'uscita del circuito ci sono solo bit classici.*

3.2 Valutazione della Forma Normale

Si definisce ora una proprietà dei Circuiti Quantistici, il *peso,* che indica *quanto* un circuito è vicino alla Forma Normale. Un circuito Misto avrà un peso direttamente proporzionale alla quantità di operazioni "classiche" presenti nella parte quantistica del circuito. Questa caratteristica dei circuiti sarà molto utile per dimostrare che una regola di riscrittura fa *avvicinare* il circuito alla sua Forma Normale. Se il peso di un circuito è zero allora è in Forma Normale.

Definizione 3.2.1. Il Peso *(Weight)* di un circuito è la somma di tutti i pesi degli elementi che lo compongono. Ogni operatore ha un certo peso:

- $Weight(QG) =$ il numero degli operatori a sinistra della porta
- $Weight(Mis) =$ il numero degli operatori a destra della porta
- $Weight(RC) =$
  $= Weight($U con New su ogni input e Misure su ogni output$) + 1$
- $Weight(U) = 0$
- $Weight(cU) = 1$

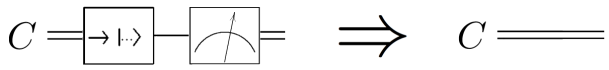

Figure 3.2: Regola eliminazione della coppia QG-Misura

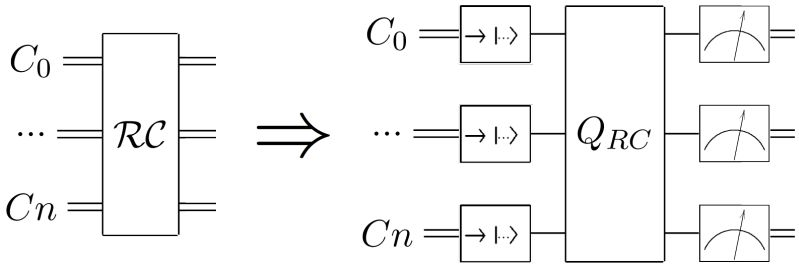

Figure 3.3: Riscrittura di una Rete Combinatoria

3.3 Definizioni delle Regole di Riscrittura

Si descrivono ora le regole di riscrittura, con cui sarà possibile ottenere un Circuito in Forma Normale da un Circuito Misto. In ogni riscrittura le configurazioni di input e output rimarranno le stesse, quello che cambierà sarà la funzione di transizione. Naturalmente cambierà il modo di calcolare una funzione, non quello che calcola. Nella prossima sezione si dimostrerà la correttezza di ogni le riscritture.

3.3.1 Coppia QG - Misura

Se si ha un circuito del tipo $\mathcal{C} = (n, m, Inp, Out, \varphi)$ dove $n = m = 1$, con $Inp(1) = Out(1) = \{C\}$ e $\varphi_C = \varphi_{mis} \circ \varphi_{new}$, è possibile sostituirlo con $\mathcal{C}_\mathcal{S} = (n, m, Inp, Out, I)$ dove I è la funzione identità e φ_{new} e φ_{mis} sono le trasformazioni degli Operatori QG e Misura.
In pratica se su una linea del circuito si presentano un Operatore QG che precede un Operatore di Misura allora è consentito eliminare entrambi gli Opeatori (vedi *Figura 3.2*).

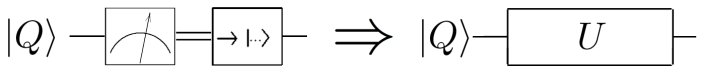

Figure 3.4: Riscrittura di una coppia Misura-QG

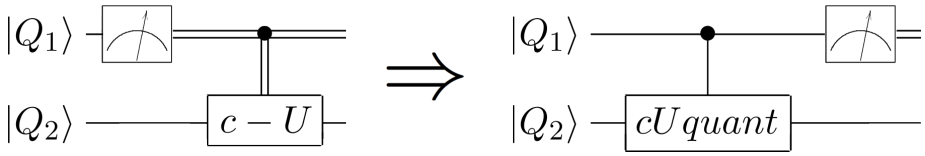

Figure 3.5: Riscrittura di una Controlled U

3.3.2 Rete Combinatoria

Se si ha Rete Combinatoria si può riscrivere con un circuito del tipo $\mathcal{C}_{\mathcal{S}} = (n, m, Inp, Out, \varphi)$ dove n, m, Inp, Out sono le stesse della Rete Combinatoria, ma la funzione di trasformazione diventa

$$\varphi_S = (\underbrace{\varphi_{mis} \otimes ... \otimes \varphi_{mis}}_{m\,volte}) \circ \varphi_{U_{RC}} \circ (\underbrace{\varphi_{new} \otimes ... \otimes \varphi_{new}}_{n\,volte})$$

dove $\varphi_{U_{RC}}$ è la funzione con lo stesso andamento di φ_{RC} ma lavora solo su qubit.
Se si incontra una Rete Combinatoria si può sostituire con: una serie di QG su tutte le linee in ingresso, un Operatore U ed infine un Operatore di Misura per ogni qubit in output (*vedi Figura 3.3*).

3.3.3 Coppia Misura - QG

Una coppia *Misura - QG* si può sostituire con una certa operazione unitaria (*vedi Figura 3.4*).

3.3.4 Operazione Unitaria Controllata

Dato un circuito $\mathcal{C} = (n, m, Inp, Out, \varphi)$ dove $n = m = 1$, con $Inp(1) = Out(1) = \{C\}$ cioè

$$\varphi = \varphi_{c-U} \circ (I \otimes \varphi_{mis})$$

allora è possibile sostituirlo con un circuito con stesse configurazioni di ingresso e uscita ma con la funzione di trasformazione seguente:

$$\varphi_S = (I \otimes \varphi_{mis}) \circ \varphi_U$$

dove φ_U è una specifica trasformazione unitaria che si comporta come una controlled-U, ma il bit di controllo è quantistico.
In altri termini, se l'output di un Operatore di Misura è usato come bit di controllo per un Operazione Controlled-U allora si può sostituire il circuito con uno equivalente, formato da un Operazione U con 2 qubit in ingresso (che si comporta come una controlled-U, ma il bit di controllo è quantistico) e a seguire l'Operatore di Misura sul primo qubit. Questa riscrittura è rappresentata in *Figura 3.5.*

3.4 Dimostrazioni di Correttezza delle Regole di Riscrittura

A questo punto si vuole dimostrare la correttezza di ogni riscrittura: ogni volta che si effettua una riscrittura l'andamento della funzione di trasformazione del circuito non deve cambiare. Ciò che calcola il circuito non deve cambiare, cambierà solo la sua forma.

3.4.1 Coppia New - Misura

E' abbastanza semplice convincersi che se si parte da un bit classico, si trasforma in quantistico con QG e senza fare nessun'altra operazione si misura lo stato, allora il bit iniziale rimane invariato, cioè è possibile evitare di applicare le due porte.

3.4.2 Rete Combinatoria

In questa riscrittura si usano qubit al posto di bit classici, ma questo non è un problema, perchè non si avranno mai sovrapposizione degli stati. In

In			Out		
a	b	c	a	b	c
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	*0*	*1*	*1*	*0*	*1*
1	*1*	*0*	*1*	*1*	*1*
1	1	1	1	1	0

Tabella 3.1: Tabella di verità per la Porta di Toffoli

pratica si usano i qubit che appartengono al campo $\mathbb{C}^2$ come vettori appartenenti a $\{|0\rangle, |1\rangle\}$. Infatti, dopo aver creato con QG i qubit, si applica una trasformazione lineare, che avendo lo stesso comportamento di un circuito classico (dimostrato in seguito) non potrà generare nessuna sovrapposizione. A questo punto si misureranno valori certi, quindi l'unica utilità della misura è trasformare oggetti di $\mathbb{C}^2$ in $\{|0\rangle, |1\rangle\}$

Consideriamo ora il problema della simulazione della funzione RC.
E' sempre possibile simulare il comportamento di una computazione classica utilizzando circuiti quantistici. In particolare, la porta di Toffoli (quantistica) è universale per ogni computazione classica. Infatti utilizzando la sola porta di Toffoli è possibile riscrivere le porte *Nand* e *Fanout*, che a loro volta possono simulare ogni computazione classica (univeralità di *Nand* e *Fanout*) La porta di Toffoli opera su tre qubit e il funzionamento è descritto dalla *Tabella*3.1 . La trasformazione è la stessa della funzione identità, tranne per le combinazioni *101* e *110* in cui viene invertito il bit su *c*. Si può immaginare la porta di Toffoli come un cnot (controlled not) con due control (a e b) che invertono il bit target (l'ultimo bit, cioè c) se sono entrambi uguali a uno. Dati tre qubit in ingresso(a, b, c), la funzione calcolata dalla porta di Toffoli è:

$$(a, b, c) \rightarrow (a, b, c \oplus ab)$$

L'operazione di *Fanout* si può ottenere con Toffoli, passando in ingresso i bit $(a = 1, b, c = 0)$. In questo modo si otterrà la copia del bit b in output (cioè

sul terzo quibit), infatti se si esegue toffoli si avrà $0 \oplus 1b$ che corrisponde proprio a b. La porta *Nand* si ottiene con $(a, b, c = 1) \rightarrow (a, b, 1 \oplus ab) = \neg ab$. L'unico inconveniente, ma facilmente risolvibile, di questa riscrittura è la necessità di ancilla bit (bit di troppo in input) e garbage bit (bit di troppo in output). Si pensi ad esempio che per *Nand* ci nel caso quantistico ci sono tre qubit in ingresso e tre in uscita, ma in un circuito classico ne basterero due in ingresso e uno in uscita.

3.4.3 Coppia Misura - QG

La correttezza di questa regola deriva da un risultato dell'articolo [4], da cui può essere estratto il seguente lemma:

Lemma 3.4.1. *Ogni porta quantistica può essere sostituita da una trasformazione lineare (cioè una certa U) e un numero finito di Ancilla bit.*

Quindi è possibile sostituire la coppia *Misura-QG* con una certa U_{M-QG}.

3.4.4 Operazione Unitaria Controllata

Per dimostrare la correttezza di questa riscrittura è necessario conoscere un teorema fondamentale per la computazione quantistica: il Teorema di Bloch per le matrici 2×2. Questo teorema dice che ogni operazione su un singolo qubit può essere vista come un insieme di rotazioni intorno agli assi $\vec{x}$,$\vec{y}$ e $\vec{z}$ della spera di Bloch. Le rotazioni sono definite come:

$$R_x(\theta) = \begin{bmatrix} cos(\theta/2) & -isin(\theta/2) \\ -isin(\theta/2) & cos(\theta/2) \end{bmatrix}$$

$$R_y(\theta) \begin{bmatrix} cos(\theta/2) & -sin(\theta/2) \\ sin(\theta/2) & cos(\theta/2) \end{bmatrix}$$

$$R_z(\theta) = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{bmatrix}$$

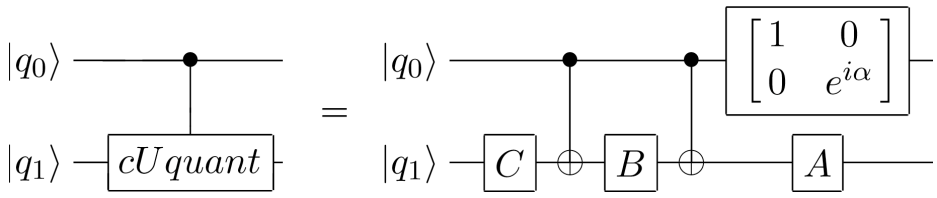

Figure 3.6: Porta controllata da Qubit

Teorema 3.4.2. *Per ogni matrice unitaria 2×2, U esistono numeri reali α, γ e δ tali che*

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_x(\delta)$$

Da cui segue:

Corollario 3.4.3. *Se si suppone che U sia una trasformazione unitaria su un singolo qubit (matrice 2×2), allora esistono operatori unitari (che operano anch'essi su singoli qubit) A, B e C tali che $ABC = I$ e $U = e^{i\alpha} AXBXC$ per qualche $\alpha \in \mathbb{R}$.*

Tramite questo corollario è possibile dimostrare che la riscrittura di *Figura 3.5* è corretta. Si farà vedere che i due circuiti hanno la stessa funzione di transizione φ. Nel circuito riscritto (quello sulla destra di *Figura 3.5*) si utilizzerà la porta controllata da qubit descritta in *Figura 3.6.* Come prima idea facciamo vedere che l'equivalenza vale per un solo qubit in input (cioè una distribuzione in cui l'unico elemento ha probabilità 1). Si avrà quindi lo stato iniziale del circuito in

$$\alpha |0\rangle \otimes |\psi_0\rangle + \beta |1\rangle \otimes |\psi_1\rangle \mapsto 1$$

Vediamo ora come viene traformato con entrambi i circuiti. Se si considera il circuito da riscrivere (quello sulla sinistra di *Figura 3.5*), dopo aver eseguito la misura sul primo qubit si avrà:

$$\begin{aligned} |0\rangle \otimes |\psi_0\rangle &\mapsto |\alpha|^2 \\ |1\rangle \otimes |\psi_1\rangle &\mapsto |\beta|^2 \end{aligned}$$

Se si applica la controlled U si otterrà

$$\begin{aligned} |0\rangle \otimes |\psi_0\rangle &\mapsto |\alpha|^2 \\ |1\rangle \otimes U|\psi_1\rangle &\mapsto |\beta|^2 \end{aligned}$$

Nel caso invece si sottoponga lo stato iniziale al secondo circuito (sulla destra), si avrà la seguente computazione:
lo stato appena prima della misura finale (cioè applicando "cU quant" descritta in *Figura 3.6*) sarà

$$\begin{aligned} \alpha|0\rangle \otimes ABC|\psi_0\rangle + \beta e^{i\alpha}|1\rangle \otimes AXBXC|\psi_1\rangle &= \\ = \alpha|0\rangle \otimes ABC|\psi_0\rangle + \beta|1\rangle \otimes e^{i\alpha}AXBXC|\psi_1\rangle & \end{aligned}$$

e per il corollario visto prima si avrà

$$\alpha|0\rangle \otimes I|\psi_0\rangle + \beta|1\rangle \otimes U|\psi_1\rangle$$

e applicando la misura si otterrà

$$\begin{aligned} |0\rangle \otimes I|\psi_0\rangle &\mapsto |\alpha|^2 \\ |1\rangle \otimes U|\psi_1\rangle &\mapsto |\beta|^2 \end{aligned}$$

che è equivalente allo stato ottenuto dal primo circuito. Quindi la trasformazione è corretta per distribuzioni con un solo elemento.

Valutiamo ora il caso un cui in input si presenti una distribuzione qualsiasi. Si avrà in output una distibuzione $\mathcal{D}$ del tipo:

$$\mathcal{D} = \begin{cases} \alpha_0^1|0\rangle \otimes |\psi_0^1\rangle + \alpha_1^1|1\rangle \otimes |\psi_1^1\rangle \mapsto p_1 \\ \vdots \\ \alpha_l^1|0\rangle \otimes |\psi_0^1\rangle + \alpha_l^1|1\rangle \otimes |\psi_l^1\rangle \mapsto p_l \end{cases}$$

dove l è il numero degli elementi di $\mathcal{D}$.

Nel circuito con controlled-U classica dopo la misura sul primo qubit si avrà:

$$\mathcal{D}' = \begin{cases} |0\rangle \otimes |\gamma_0^1\rangle \mapsto \sum_{\forall j \in 1,\dots,l | \psi_0^j = \gamma_0^1} |\alpha_0^j|^2 p_j \\ |1\rangle \otimes |\gamma_1^2\rangle \mapsto \sum_{\forall j \in 1,\dots,l | \psi_1^j = \gamma_1^1} |\alpha_1^j|^2 p_j \\ \vdots \\ |0\rangle \otimes \left|\gamma_0^{n-1}\right\rangle \mapsto \sum_{\forall j \in 1,\dots,l | \psi_0^j = \gamma_0^{n-1}} |\alpha_0^j|^2 p_j \\ |1\rangle \otimes |\gamma_1^n\rangle \mapsto \sum_{\forall j \in 1,\dots,l | \psi_1^j = \gamma_1^n} |\alpha_1^j|^2 p_j \end{cases}$$

durante la misura si associano le coppie $|x\rangle \otimes |\psi_x^i\rangle$ di diversi elementi ma che hanno stesso valore. Applicando la cU si ha:

$$\mathcal{D}'' = \begin{cases} |0\rangle \otimes |\gamma_0^1\rangle \mapsto \sum_{\forall j \in 1,\dots,l | \psi_0^j = \gamma_0^1} |\alpha_0^j|^2 p_j \\ |1\rangle \otimes U|\gamma_1^2\rangle \mapsto \sum_{\forall j \in 1,\dots,l | \psi_1^j = \gamma_1^1} |\alpha_1^j|^2 p_j \\ \vdots \\ |0\rangle \otimes \left|\gamma_0^{n-1}\right\rangle \mapsto \sum_{\forall j \in 1,\dots,l | \psi_0^j = \gamma_0^{n-1}} |\alpha_0^j|^2 p_j \\ |1\rangle \otimes U|\gamma_1^n\rangle \mapsto \sum_{\forall j \in 1,\dots,l | \psi_1^j = \gamma_1^n} |\alpha_1^j|^2 p_j \end{cases}$$

Ora consideriamo il circuito con controllo quantistico e misura in seguito. Nel caso si sottoponga la distribuzione $\mathcal{D}$, che però chiameremo $\mathcal{G}$, in ingresso si avrà (come visto nel caso con un solo bit):

$$\mathcal{G}' = \begin{cases} \alpha_0^1 |0\rangle \otimes I |\psi_0^1\rangle + \alpha_1^1 |1\rangle \otimes U |\psi_1^1\rangle \mapsto p_1 \\ \vdots \\ \alpha_l^1 |0\rangle \otimes I |\psi_0^1\rangle + \alpha_l^1 |1\rangle \otimes U |\psi_l^1\rangle \mapsto p_l \end{cases}$$

e dopo la misura

$$\mathcal{G}'' = \begin{cases} |0\rangle \otimes |\gamma_0^1\rangle \mapsto \sum_{\forall j \in 1,\ldots,l | \psi_0^j = \gamma_0^1} |\alpha_0^j|^2 p_j \\ |1\rangle \otimes U|\gamma_1^2\rangle \mapsto \sum_{\forall j \in 1,\ldots,l | U\psi_1^j = U\gamma_1^1} |\alpha_1^j|^2 p_j \\ \vdots \\ |0\rangle \otimes \left|\gamma_0^{n-1}\right\rangle \mapsto \sum_{\forall j \in 1,\ldots,l | \psi_0^j = \gamma_0^{n-1}} |\alpha_0^j|^2 p_j \\ |1\rangle \otimes U|\gamma_1^n\rangle \mapsto \sum_{\forall j \in 1,\ldots,l | U\psi_1^j = U\gamma_1^n} |\alpha_1^j|^2 p_j \end{cases}$$

$\mathcal{G}''$ e $\mathcal{D}''$ sono equivalenti? La risposta è sì. Infatti gli elementi "$|0\rangle \otimes |\gamma_0^i\rangle$" con i qualunque sono equivalenti e hanno stessa probabilità in entrambe le distribuzioni. Gli elementi che potrebbero sembrare diversi sono quelli del tipo "$|1\rangle \otimes ...$" infatti si ha per $\mathcal{D}''$:

$$|1\rangle \otimes U\left|\gamma_1^i\right\rangle \mapsto \sum_{\forall j \in 1,\ldots,l | \psi_1^j = \gamma_1^i} |\alpha_1^j|^2 p_j$$

e per $\mathcal{G}''$:

$$|1\rangle \otimes U\left|\gamma_1^i\right\rangle \mapsto \sum_{\forall j \in 1,\ldots,l | U\psi_1^j = U\gamma_1^n} |\alpha_1^j|^2 p_j$$

Si nota che la differenza sta nella condizione della sommatoria, ma è ovvio che $\psi_1 = \gamma_1$ se e solo se $U\psi_1 = U\gamma_1$.

3.5 Circuiti Misti in Forma Normale

A questo punto si dimostra che con la sola applicazione di regole di riscrittura è possibile ottere un circuito in forma normale.

Teorema 3.5.1. *Ogni Circuito Misto è sempre riducibile alla Forma Normale: dato un qualsiasi Circuito Misto C, applicando un numero finito di riscritture, è possibile ottenere un circuito in Forma Normale C_{FN} equivalente.*

Dimostrazione: Si vuole ricondurre un Circuito Misto con $w > 0$ ad uno equivalente in Forma Normale, cioè con $w = 0$. Si procederà per indu-

zione su w.

Caso base $w = 0$

Per definizione di Weight se ho un circuito con $w = 0$ allora sono già in Forma Normale, infatti non avrò nessuna operazione che gestisce bit classici all'interno della parte quantistica.

Caso induttivo $w > 0$

In questo caso si avranno Operatori che lavorano su bit classici all'interno della parte quantistica. Gli Operatori di questo tipo sono le RC, cU, QG e Misura. Se il circuito avesse $w > 0$ a causa di una Rete Combinatoria, allora, applicando la regola ad essa associata, si potrebbe eliminare la RC sostituendola con una U e delle porte QG e di Misura. Quindi, avendo circuiti senza Reti Combinatorie all'interno della parte quantistica, si possono valutare i casi restanti. Si potrà avere una controlled U, dove il bit di controllo classico deve essere per forza generato da una misura, perché è l'unico operatore restante con bit classico in output. Grazie alla regola misura-controlled U, è possibile riscrivere un circuito di quel tipo in uno in cui il controllo della U è quantistico, e la misura è slittata a destra della U. A questo punto rimangono solo Misure e QG. Sia che siano presenti in forma Misura-QG che QG-Misura è possibile applicare una regola, e riscrivere il circuito in uno in cui nella parte quantistica non è presente nessun bit classico.

Quindi per ogni circuito con $w > 0$ è sempre possibile applicare una regola corretta, cioè che non cambia la funzione di trasformazione del circuito, ma il peso totale decresce? Se ogni regola facesse calare w, allora sarebbe vero che $w_{trasformato} < w_{non\,trasformato}$ e quindi potremmo ricondurci al caso base in un numero finito di passi perchè $w \in \mathbb{N}$. Manca solo da dimostrare che ogni regola fa calare il peso del circuito. Indicheremo con C il circuito di partenza e con C_T il circuito trasformato con una regola di riscrittura. Si dimostra ora che per ogni riscrittura vale:

$$Weight(C) > Weight(C_T)$$

Procediamo per casi. Per la Coppia Misura - QG si ha:

$$Weight(Misura) + Weight(QG) > 0$$

che è vera dato che il peso della Misura e di QG non sono nulli. Per la regola della Rete Combinatoria $(n, m, ...)$ si ha:

$$Weight(RC) > n * Weight(QG) + Weight(U) + m * Weight(Misura)$$

che è vero per definizione di $Weight(RC)$
Per la Coppia QG-Misura:

$$Weight(Misura) + Weight(Misura) > Weight(U)$$

infatti è sicuramente vero

$$Weight(Misura) + Weight(QG) > 0$$

Rimane solo da dimostrare che il peso cala anche per la regola della Misura-cU. Indicando con $Misura1$ la misura nella posizione di partenza (a sinistra della cU) e con $Misura2$ la misura dopo essere stata trasformata (a destra della Q), si avrà:

$$Weight(Misura1) + Weight(cU) > Weight(U) + Weight(Misura2)$$

Questa relazione è vera infatti

$$Weight(Misura1) + Weight(cU) > 0 + Weight(Misura2)$$

ma sappiamo che vale

$$Weight(Misura1) > Weight(Misura2)$$

perchè la misura si è spostata a destra di una porta e il suo peso (per definizione) decresce.

Conclusioni

The beautiful aspect to this is the scientists who developed this were not trying to make a cell phone; they were not trying to invent a CD player. If you went to Schrödinger in 1926 and said, "Nice equation, Erwin. What's it good for?" He's not going to say, "Well, if you want to store music in a compact digital format..."

But without the curiosity-driven understanding of how atoms behave, how they interact with each other, and how they interact with light, the world we live in would be profoundly different

– John Matson

Riepilogo

Dopo aver affrontato alcune nozioni teoriche sulla meccanica e la computazione quantistica, ci siamo concentrati sul modello dei Circuiti Quantistici: nel particolare abbiamo definito un Circuito Misto che ammette operazioni su bit e qubit in qualsiasi posizione. In questi circuiti lo stato in ogni momento è misto, nel senso che ci sono distribuzioni di probabilità insieme a stati quantistici puri. Successivamente abbiamo definito la nozione di circuito in Forma Normale. I circuiti in Forma Normale, che sono un sottoinsieme dei Circuiti Misti, hanno una struttura più rigida, in quando separano le computazioni classiche da quelle quantistiche: alle estremità del circuito ci sono le operazioni che interfacciano il mondo classico con quello quantistico e, nel cuore

del circuito, sono presenti solo operazioni su qbit. Lavorando con circuiti di questo tipo è possibile concentrarsi sulle trasformazioni di stati quantistici puri, senza il rischio di trovarsi in uno stato misto (cioè configurazioni con bit classici e quantistici). Infine abbiamo introdotto alcune regole di riscrittura e, dopo aver dimostrato la loro correttezza, abbiamo mostrato come, con la sola applicazione di queste regole, è possibile ottenere un circuito in Forma Normale da uno Misto.

Sviluppi Futuri

Se si volesse continuare a sviluppare questa tesi, si potrebbe confrontare questo modello matematico (quantum circuits) con altri modelli di calcolo (MdT con controllo classico, Measurement Calculus, ...). Nel campo della ricerca, questo studio sarà utile per ottenere, in modo semplice e automatico, un circuito in FN. L'equivalenza tra un circuito misto e uno in FN era già stata dimostrata da [4], ma in quello studio si era utilizzato il modello delle "density matrix" per descrivere gli stati misti, mentre in questa tesi si è scelto di lavorare direttamente con le distribuzioni di probabilità.

La tecnica delle riscritture, e quindi la possibilità di ridurre un circuito in FN, si rivela molto utile per sfruttare a pieno le potenzialità della Meccanica Quantistica. Infatti, sapendo che si può sempre arrivare alla forma normale di un circuito, è possibile scrivere algoritmi misti, sapendo di poter effettuare in seguito una riduzione.

Bibliografia

[1] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[2] P. R. Kaye, R. Laflamme and M. Mosca, *An Introduction to Quantum Computing*, Oxford University Press, New York, US, 2007.

[3] A. Di Pierro, *Quantum Computing,* Dispense per il corso di Informatica Quantistica, Università di Verona, 2010. URL: `http://profs.sci.univr.it/~dipierro/InfQuant/articles/Lezioni-IQ.pdf`

[4] D. Aharonov, A. Kitaev and N. Nisan, *Quantum Circuits with Mixed States*, 2008, URL: `http://arxiv.org/abs/quant-ph/9806029v1`

[5] J.A. Wheeler and W.H. Zurek, *Quantum Theory and Measurement*, Princeton university Press, New Jersey, US 1983)

[6] M. Main, Quantum Pseudo-Telepathy Save the World, Bulletin of the European Association for Theoretical Computer Science, Ottobre 2009.