Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Informatica

Sulla Pseudo-Telepatia Quantistica

Relatore:
Chiar.mo Prof.
Dal Lago Ugo

Presentata da:
Tomasetti Luca

II Sessione
2014 / 2015

Desidero ricordare tutti coloro che mi hanno aiutato nella stesura della tesi con suggerimenti, critiche ed osservazioni: a loro va tutta la mia gratitudine.

Un ringraziamento particolare va alla mia famiglia e a tutti i miei amici che mi hanno aiutato e supportato in questo periodo; questo lavoro è dedicato a voi.

Indice

1 Introduzione **6**

1.1 Come Nasce l'Informatica Quantistica? 6

1.2 Breve Storia della Pseudo-Telepatia 8

1.3 Di Che Cosa Tratta Questa Tesi? 9

2 Qubits e Meccanica Quantistica **10**

2.1 Stato di un Sistema Fisico Classico 10

2.2 Postulati della Meccanica Quantistica 11

2.2.1 Primo Postulato 11

2.2.2 Secondo Postulato 12

2.2.3 Terzo Postulato 13

2.3 Descrizione e Proprietà di un Sistema Quantistico 13

2.3.1 Proprietà dello Stato di un Sistema Quantistico 14

2.4 Entanglement 16

2.5 Qubit 18

2.6 Circuiti Quantistici 20

2.6.1 Porte Logiche Quantistiche a un Qubit 20

2.6.2 Porte Logiche a più Qubits 21

2.7 Principi dell'Informatica Quantistica 22

3 Pseudo-Telepatia **24**

3.1 Sulle Strategie Classiche 26

3.2 Una Strategia Quantistica 27

3.2.1 Caso delle Tre Pietre Levigate 29

3.2.2 Caso delle Due Pietre Grezze e Una Levigata 30

4 Confronto fra Strategie **34**

4.1 Generalizzazione del Gioco con un Numero n di Giocatori 34

4.2 Protocollo Quantistico Perfetto 35

4.3 Confronto tra Protocolli Classici e Probabilistici 37

4.3.1 Strategia Classica 37

4.3.2 Strategia Probabilistica 42
4.4 Dispositivi Quantistici Imperfetti 43

5 Conclusioni **46**

Capitolo 1

Introduzione

Agli inizi del ventesimo secolo alcuni esperimenti hanno messo in evidenza i limiti della fisica deterministica nella descrizione dei fenomeni microscopici, cioè a scale di grandezza pari o inferiori ad un atomo. La meccanica quantistica è la teoria che spiega questi fenomeni.

La nascita della meccanica quantistica insieme alla divulgazione dei suoi principi fondamentali ha stimolato negli studiosi di tutto il mondo l'elaborazione di nuove teorie e tecnologie, come ad esempio il laser, il microscopio elettronico e i pannelli fotovoltaici.

L'informatica quantistica nasce come paradigma di calcolo alternativo basato sui principi della meccanica quantistica; essa è un meccanismo teorico che racchiude un insieme di tecniche di calcolo che utilizzano i quanti per l'elaborazione delle informazioni.

1.1 Come Nasce l'Informatica Quantistica?

La teoria classica della computazione si basa sulla Macchina di Turing. La macchina è definita da un insieme di regole che definiscono il suo comportamento su un nastro di input-output, che equivale ad un nastro di lettura e scrittura. Il nastro può essere immaginato avente una lunghezza infinita, diviso in celle che hanno una lunghezza fissata. Ogni cella contiene un carattere di un alfabeto dato, compreso un carattere vuoto di inizializzazione. La macchina di Turing possiede una testina che si sposta lungo il nastro leggendo, scrivendo o cancellando i simboli nelle celle del nastro; la macchina analizza il nastro, una cella alla volta.

Ad ogni passo, la macchina legge un carattere sul nastro ed in base al simbolo letto cambia il suo stato interno scrivendo un simbolo sul nastro oppure spostando la testina a sinistra o a destra di una posizione.

La sua importanza è tale che tuttora, per definire in modo formalmente preciso la nozione di algoritmo, si tende a ricondurlo alle elaborazioni effettuabili con macchine di Turing.

La macchina segue un insieme di regole e di principi enunciati dal suo creatore, il matematico britannico Alan Turing, nel 1936 [10], ed elaborati successivamente dal fisico ed informatico ungherese John von Neumann in una sua pubblicazione del 1945 [13].

Nonostante i progressi nel campo tecnologico che permisero la creazione e produzione di dispositivi sempre più veloci rispetto a quelli che potevano essere realizzati nella prima metà del ventesimo secolo, le regole ed i principi elencati dalla Macchina di Turing sono sempre rimasti immutati.

L'assunzione alla base di questi principi è che la Macchina di Turing idealizza un dispositivo meccanico di computazione che segue le leggi del moto della fisica deterministica, ossia lo stato del nastro e della testina sono sempre univocamente identificabili. Per questa ragione la Macchina di Turing è totalmente deterministica.

Agli inizi degli anni ottanta le scienze fisiche affrontarono una vera e propria rivoluzione: iniziò ad affacciarsi l'idea di realizzare un calcolatore quantistico, il quale per eseguire le classiche operazioni di scrittura e lettura dei dati avrebbe utilizzato i fenomeni tipici della meccanica quantistica. La risposta della comunità scientifica fu l'introduzione di una nuova teoria, detta computazione quantistica.

Questa nuova teoria partì dalle considerazioni elaborate dal fisico americano Charles Bennett che dimostrò la possibilità di costruire una speciale Macchina di Turing chiamata reversibile [2], ossia in grado di realizzare una computazione che poteva sempre essere eseguita in modo da far ritornare la testina allo stato iniziale ripercorrendo all'indietro tutti i passi di computazione compiuti sul nastro; Paul Benioff dimostrò che una delle condizioni necessarie per realizzare una Macchina di Turing Quantistica è la reversibilità [1].

Negli anni successivi venne dimostrato dal fisico teorico Richard Feynman, nel suo famoso lavoro dal titolo "Simulating physics with computers", che nessuna Macchina di Turing classica avrebbe potuto simulare certi fenomeni fisici senza subire un drastico rallentamento delle sue prestazioni e che un simulatore quantistico universale non è soggetto a questa limitazione, quindi avrebbe potuto effettuare le simulazioni in maniera più efficiente [3].

Dopo varie osservazioni, Feynman suggerì un nuovo modello computazionale, basato su leggi puramente quantistiche, che avrebbe utilizzato solamente una quantità polinomiale di risorse nel numero di particelle per simulare il comportamento di una macchina di Turing.

Il risultato degli studi di Feynman diede vita ad una lunga serie di lavori. Le peculiari proprietà del formalismo della meccanica quantistica permisero l'ideazione di una nuova classe di algoritmi quantistici capaci di risolvere in maniera efficiente problemi di computazione classici ritenuti intrattabili, gettando così nuova luce sulla teoria della complessità.

L'ipotesi di Feynman venne dimostrata e formalizzata nel 1985 dal fisico britannico David Deutsch nel suo famoso articolo [5] nel quale descrisse le caratteristiche della

Macchina di Turing Quantistica Universale.

Questa macchina teorica rappresenta nella teoria della calcolabilità quantistica esattamente quello che la Macchina di Turing Universale rappresenta per la calcolabilità classica. Dato che una Macchina di Turing Universale può simulare in maniera efficiente qualsiasi Macchina di Turing, allo stesso modo, la Macchina di Turing Quantistica Universale, a livello teorico, è in grado di simulare qualsiasi computer quantistico in un tempo al massimo polinomiale.

L'idea di Deutsch ha portato alla concezione moderna dell'informatica quantistica. Dimostrando la validità della teoria di Feynman, Deutsch ha posto le basi per un nuovo tipo di informatica.

L'informatica quantistica è un insieme di tecniche utilizzabili attraverso l'impiego di un computer quantistico, in grado di risolvere in maniera più veloce certi tipi di problemi rispetto ad un computer classico. L'esempio più famoso che mette in luce questa particolare caratteristica dell'informatica quantistica è l'algoritmo di Shor, ad oggi uno dei più importanti e più studiati algoritmi della computazione quantistica.

Peter Shor, uno scienziato di Bell Labs, concepì nel 1994 [19] un algoritmo per risolvere il problema della fattorizzazione dei numeri interi in numeri primi in un tempo polinomiale se e solo se l'algoritmo fosse stato eseguito su un computer quantistico.

L'algoritmo di Shor suscitò grande interesse per via della sua utilità nel combattere la crittografia classica: infatti la sicurezza di molti sistemi crittografici è basata sulla difficoltà di fattorizzare numeri grandi. Nel caso venisse trovato un metodo sicuro e veloce per questa fattorizzazione, molti sistemi crittografici diventerebbero insicuri. Sebbene non sia stato ancora dimostrato che con un computer classico non è possibile fattorizzare numeri primi in un tempo polinomiale, l'algoritmo classico attualmente più veloce impiega comunque tempi esponenziali.

Una importante tecnica dell'informatica quantistica e protagonista principale di questa tesi è la cosiddetta pseudo-telepatia quantistica.

1.2 Breve Storia della Pseudo-Telepatia

L'idea di questa straordinaria tecnica è maturata nel 1999, quando tre ricercatori dell'università di Montreal, Gilles Brassard, Richard Cleve e Alain Tapp, scrissero un articolo dal titolo "The cost of exactly simulating quantum entanglement with classical communication" [12].

Nell'articolo, i tre ricercatori, dimostrarono l'esistenza di una strategia quantistica vincente per alcune tipologie di giochi nei quali, in assenza di un fenomeno chiamato entanglement (un principio peculiare della meccanica quantistica descritto in dettaglio più avanti) è possibile trovare una strategia vincente solo se ai partecipanti è permessa

la comunicazione tra loro, fatto del tutto irrilevante in presenza del fenomeno citato in precedenza.

La strategia descritta venne successivamente introdotta con il nome di "pseudo-telepatia quantistica" in un altro articolo sempre degli stessi ricercatori di Montreal [6]. Con l'aggiunta del prefisso "pseudo", gli autori dell'articolo hanno cercato di far intendere che la loro teoria non riguardasse una vera e propria comunicazione telepatica, bensì un processo che eliminasse il bisogno dello scambio di informazioni tra i giocatori al fine di arrivare alla vittoria.

La pseudo-telepatia quantistica è una tecnica particolare dell'informatica quantistica nella quale un numero arbitrario di giocatori riesce a concludere e vincere con una percentuale significativamente maggiore rispetto ad una strategia deterministica certe determinate tipologie di giochi senza la necessità di comunicazione e di scambio di informazioni.

1.3 Di Che Cosa Tratta Questa Tesi?

La tesi cercherà di affrontare nel dettaglio la teoria della pseudo-telepatia quantistica analizzando le basi dei concetti fondamentali nei primi capitoli, mentre successivamente si dimostrerà che l'argomento in esame è la soluzione ideale per alcune tipologie di giochi rispetto ad altre strategie, come quelle classiche e probabilistiche:

- Nel Capitolo 2 esplicherò i fondamenti della meccanica quantistica, enunciando i suoi principi fondamentali e descrivendo a linee generali cosa sia un qubit e a cosa serva.
- Il Capitolo 3 entrerà nel cuore della tesi spiegando nel dettaglio il fenomeno della pseudo-telepatia quantistica attraverso la descrizione di un gioco con tre partecipanti.
- Nel Capitolo 4 verrà generalizzato l'esempio del gioco preso in questione fino ad un numero imprecisato n di giocatori al fine di dimostrare che la pseudo-telepatia, confrontata con le altre tecniche, è la soluzione con la percentuale di successo più alta.
- Nell'ultimo capitolo si traggono le conclusioni della tesi.

Capitolo 2

Qubits e Meccanica Quantistica

In questo capitolo vengono poste le basi per la comprensione della tesi spiegando in maniera più dettagliata alcuni elementi e definendo diversi termini che da qui in avanti verranno utilizzati.

2.1 Stato di un Sistema Fisico Classico

In generale, in fisica, un sistema deterministico viene definito come un insieme di oggetti, al quale vengono analizzate le proprietà ed eventualmente la sua evoluzione con il passare del tempo. Un sistema viene classificato in tre modi differenti, in base a come esso interagisce con altri sistemi esterni:

- Isolato: se le uniche interazioni che possiede sono quelle tra oggetti del sistema, quindi non c'è scambio di energia.
- Chiuso: se la sua componente materiale non subisce variazioni nel tempo ma è comunque possibile uno scambio di energia con altri sistemi.
- Aperto: se sia la sua composizione materiale che energetica possono variare come conseguenza di interazioni con altri sistemi.

Lo stato di un sistema fisico deterministico rappresenta la descrizione istantanea del valore assunto da alcune variabili che fanno parte del sistema; esso può cambiare nel tempo ed in ogni istante può essere determinato in maniera univoca.

D'altra parte, lo stato di un sistema probabilistico può essere decritto da una funzione $P : S \to \mathbb{R}_{[0,1]}$ tale che $\sum_{x \in S} P(x) = 1$, la quale rappresenta un'approssimazione probabilistica del sistema.

$S = \{x_1, \ldots, x_n\} \subseteq \mathbb{R}^n$ è l'insieme finito degli stati, dove ogni stato è rappresentato come una probabilità, quindi la funzione appena descritta sottolinea la natura probabilistica del sistema: la somma di tutti i componenti dell'insieme deve dare come risultato 1, il che significa che il sistema si troverà necessariamente in uno dei suoi stati.

Un ulteriore metodo per descrivere lo stato di un sistema è la sua rappresentazione attraverso un vettore che fa parte dell'insieme $\mathbb{R}^{|S|}$:

$$\begin{pmatrix} P(x_1) \\ \vdots \\ P(x_n) \end{pmatrix} = \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}$$

Ogni stato x_i ha una certa probabilità p_{ij} che il sistema evolva in ciascuno degli altri stati x_j. Il diagramma mostrato nella Figura 2.1, nel quale vengono descritti gli stati di un sistema dopo due lanci consecutivi di una moneta (probabilità che esca testa o croce $= \left(\frac{1}{2}\right)$) è un semplice esempio di evoluzione probabilistica di un sistema.

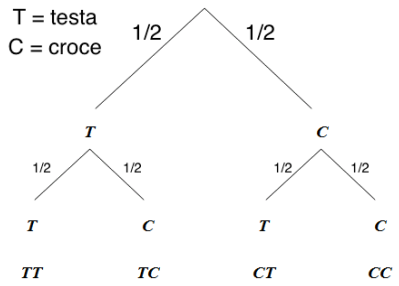

Figura 2.1: Evoluzione probabilistica

L'evoluzione probabilistica di un sistema $S = \{x_1, \ldots, x_n\} \subseteq \mathbb{R}^n$ a n stati viene descritta in modo compatto da una matrice M in $\mathbb{R}^{n \times n}$:

$$M = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{pmatrix}$$

Dato che ogni componente p_{ij} della matrice è la probabilità di passare dallo stato i allo stato j, la somma di ogni componente di una colonna della matrice deve essere pari ad 1.

2.2 Postulati della Meccanica Quantistica

Al fine di introdurre nel migliore dei modi i concetti relativi alla computazione quantistica è necessario esporre i tre postulati fondamentali della meccanica quantistica importanti alla comprensione della tesi.

2.2.1 Primo Postulato

Postulato 1 *Lo stato di un sistema fisico chiuso è interamente descritto da un vettore di numeri complessi.*

Lo stato è descritto dal seguente vettore:

$$V = \begin{pmatrix} V_{11} \\ \vdots \\ V_{n1} \end{pmatrix} \tag{2.1}$$

Il numero di componenti n del vettore dipende da quanto il sistema risulta complicato, per questo motivo n è chiamato il grado di libertà o dimensione del sistema.

Il primo postulato definisce l'ambiente in cui si colloca la meccanica quantistica: un sistema fisico chiuso è un'entità che non interagisce con il resto dell'universo.

Questo postulato può essere spiegato in maniera più comprensibile attraverso un semplice esempio: si consideri una moneta, la quale ha due stati, testa e croce. Il grado di libertà del sistema è $n = 2$. Si assuma che i due stati corrispondano a stati quantistici:

- *testa* corrisponde allo stato quantistico descritto dal vettore $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
- *croce* corrisponde allo stato quantistico descritto dal vettore $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Se la moneta viene posta in una scatola totalmente chiusa, essa inizierà a comportarsi come una "moneta quantistica". Per questo ragione, seguendo la 2.1, il seguente stato diventa perfettamente ammissibile:

$$V = testa + croce = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \tag{2.2}$$

La moneta è in una *sovrapposizione* di testa e croce, in parole povere la "moneta quantistica" può trovarsi allo stesso tempo sia nello stato *testa* sia in quello *croce*.

L'esempio appena mostrato non rende giustizia alla complessità della teoria quantistica. In un sistema convivono molti più stati: è come se gli stati *testa* e *croce* fossero due assi del piano cartesiano, tutti i possibili stati in cui il vettore V può collassare sono descritti dentro la superficie di una sfera di raggio unitario che poggia sul piano cartesiano; il concetto è spiegato nel dettaglio nella sezione 2.5.

2.2.2 Secondo Postulato

Postulato 2 *Un sistema fisico chiuso in uno stato V, dopo un certo periodo di tempo, si evolverà in un nuovo stato W in accordo con la formula*

$$W = UV$$

dove U è una matrice unitaria $(n \times m)$ *di numeri complessi.*

Il secondo postulato definisce come lo stato di un sistema quantistico cambia con lo scorrere del tempo. Per osservare l'evoluzione del sistema bisogna moltiplicarlo per una matrice che descrive la sua evoluzione (questa matrice viene chiamata U); U può essere qualsiasi matrice di numeri complessi a patto che soddisfi due proprietà: deve essere una matrice $(n \times n)$ e soprattutto deve essere unitaria, cioè deve essere una matrice invertibile e la sua inversa (U^{-1}) deve essere uguale alla sua coniugata trasposta: $U^{-1} = U^t$.

2.2.3 Terzo Postulato

Postulato 3 *Se un sistema fisico quantistico si trova in uno stato V, la probabilità che l'osservazione di una grandezza dia come risultato un valore i è direttamente proporzionale a $|V_{i1}|^2$*

Il terzo postulato esplicita come effettuare delle misure sul sistema e in quale stato il sistema si troverà dopo tali misure.

La misura nella meccanica quantistica equivale ad un processo probabilistico, dato che la somma di tutte le probabilità p_n è 1, si avrà la certezza che un determinato stato i collasserà con una probabilità p_i:

$$p_1 + \ldots + p_n = |V_{11}|^2 + \ldots + |V_{n1}|^2 = 1$$

La prima uguaglianza è data dall'applicazione del terzo postulato mentre la seconda uguaglianza è una conseguenza del primo postulato poiché si sta trattando di matrici unitarie.

Si consideri lo stato derivato dalla funzione 2.2 dell'esempio precedente e si decida di misurarlo. Con una probabilità $p_1 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$ il sistema darà come risultato lo stato:

$$testa = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Con la stessa probabilità $p_2 = \frac{1}{2}$, lo stato del sistema risulterà *croce*.

2.3 Descrizione e Proprietà di un Sistema Quantistico

Lo stato di un sistema quantistico viene descritto matematicamente da un vettore dello spazio di Hilbert, le cui componenti sono numeri complessi.

Lo spazio di Hilbert è uno spazio vettoriale che generalizza la nozione di spazio euclideo; introdotto dal celebre matematico tedesco David Hilbert, lo spazio viene definito attraverso la notazione: $\mathbf{H} = (H, \langle \cdot, \cdot \rangle)$; dove H è uno spazio vettoriale reale o complesso sul quale è definito un prodotto scalare interno $\langle \cdot, \cdot \rangle$.

Un generico stato quantistico viene rappresentato attraverso il vettore:

$$X = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \tag{2.3}$$

Le componenti $c_i \in \mathbb{C}^n$ del vettore sono numeri complessi, per questo motivo deve valere la seguente condizione:

$$\sum_{i=1}^{n} |c_i|^2 = 1$$

In altre parole, la somma di tutte le norme al quadrato dei componenti del vettore dello stato quantistico deve dare come risultato 1. La norma di un numero complesso $c_i = a+bi$ è data dall'espressione $a^2 + b^2$.

Lo stato di un sistema quantistico, descritto attraverso la funzione 2.3, può essere anche riscritto attraverso un'ulteriore notazione:

$$X = c_1\vec{x_1} + \ldots + c_n\vec{x_n} \tag{2.4}$$

dove $\vec{x_1}, \ldots, \vec{x_n}$ è la base computazionale del sistema.

Le componenti $\vec{x_i}$ della base computazionale hanno tutte un valore 0, tranne la componente i-esima che possiede valore 1.

2.3.1 Proprietà dello Stato di un Sistema Quantistico

Evoluzione

Un sistema evolve in maniera lineare, soddisfacendo il principio di sovrapposizione degli effetti, il quale stabilisce che l'effetto di una somma di perturbazioni in ingresso è uguale alla somma degli effetti prodotti da ogni singola perturbazione.

Per questa ragione, l'evoluzione del sistema può essere interamente descritta attraverso una matrice come la seguente:

$$\begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \tag{2.5}$$

La matrice che descrive il sistema deve rispettare la stessa condizione del vettore rappresentante lo stato quantistico: la sommatoria della norma degli stati del vettore deve dare come risultato il valore 1.

$$\sum_{i=1}^{n} |d_i|^2 = 1$$

Per poter soddisfare questa condizione, la matrice $Q = (a_{ij})$ deve essere una matrice unitaria.

Misura

Il concetto di misura è una delle caratteristiche fondamentali che differenziano la meccanica quantistica dalla fisica classica. Non è possibile conoscere e misurare lo stato di un sistema quantistico perché non è che la rappresentazione lineare di stati secondo le rispettive densità di probabilità; misurando un sistema quantistico, esso viene inevitabilmente ed inesorabilmente distrutto. Secondo quanto scrive il premio Nobel Erwin Schrödinger nel suo famoso articolo del paradosso del gatto, elaborato nel 1935 [14], al contrario della fisica classica dove è sempre possibile avere uno spettatore in grado di conoscere ogni dettaglio di un determinato sistema, nella meccanica quantistica non ha senso assegnare un valore ad una proprietà di un dato sistema senza che questa sia stata attivamente misurata da un osservatore.

Le leggi quantistiche stabiliscono che il processo di misura non è descrivibile come la semplice evoluzione temporale del sistema, dell'osservatore e degli apparati sperimentali considerati assieme.

Espresso in altri termini questo significa che dato il vettore corrispondente allo stato quantistico composto da un unico valore proprio perché solo il componente i-esimo $\vec{x_i}$ possiede un valore diverso da 0, espresso attraverso la notazione della formula 2.4: $X = (c_i\vec{x_i})$, non bisogna pensare alla quantità $|c_i|^2$ come alla probabilità dello stato $\vec{x_i}$. Il sistema passa dallo stato $X = (c_i\vec{x_i})$ a ciascuno degli stati $\vec{x_j}$ con una probabilità pari a $|c_j|^2$.

Dopo questo cambio di stato, il sistema si trova in uno stato classico nel quale è possibile osservarlo, ricordando però che l'osservazione di uno stato di un sistema quantistico altera inesorabilmente lo stato del sistema stesso dato che una volta misurata e determinata con precisione una quantità del sistema non si può in nessun modo determinare quale fosse il suo valore prima della misura.

Composizione

Dati due sistemi quantistici H_n e H_m descritti attraverso la formula 2.4:

$$H_n = c_1\vec{x_1} + \ldots + c_n\vec{x_n}$$

$$H_m = d_1\vec{y_1} + \ldots + d_m\vec{y_m}$$

La loro composizione avrà come risultato un nuovo sistema quantistico:

$$H_{nm} = H_n \otimes H_m$$

Il sistema risultante è dato dalla seguente matrice:

$$H_{nm} = (c_1 d_1)\vec{x_1} \otimes \vec{y_1} + (c_1 d_2)\vec{x_1} \otimes \vec{y_2} + \ldots + (c_1 d_m)\vec{x_1} \otimes \vec{y_m} + \ldots$$
$$+(c_2 d_1)\vec{x_2} \otimes \vec{y_1} + \ldots + (c_2 d_m)\vec{x_2} \otimes \vec{y_m} + \ldots + (c_n d_m)\vec{x_n} \otimes \vec{y_m}$$

La base computazionale derivata di H_{nm} è:

$$H_{nm} = \vec{x_1}\vec{y_1}, \vec{x_1}\vec{y_2}, \ldots, \vec{x_2}\vec{y_1}, \vec{x_2}\vec{y_2}, \ldots, \vec{x_n}\vec{y_m}$$

E' possibile estendere questa operazione a tutti gli stati H_n e H_m:

$$\left(\sum_{i=1}^{n} c_i \vec{x_i}\right) \otimes \left(\sum_{j=1}^{m} d_j \vec{y_j}\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} c_i d_j \vec{x_i} \otimes \vec{y_j}$$

Se uno stato X di $H_n \otimes H_m$ è tale che: $X = Y \otimes Z$, allora X è detto decomponibile, altrimenti viene chiamato entangled. Uno stato entangled, nella sua definizione più semplice, è uno stato di almeno due particelle non descrivibile come prodotto di stati di particella singola.

2.4 Entanglement

E' possibile realizzare un insieme costituito da due o più particelle. Ciò comporta che il valore misurato per una particella di una proprietà definita dell'insieme influenzi istantaneamente il corrispondente valore dell'altra, che risulterà tale da mantenere il valore globale iniziale. Questo fenomeno rimane comunque vero anche nel caso in cui le due particelle si trovino distanziate, senza alcun limite spaziale.

La descrizione appena data va sotto il nome di entanglement. Il termine, tradotto letteralmente come "groviglio", fu introdotto da Erwin Schrödinger in una recensione del famoso articolo sul paradosso EPR [15], che nel 1935 rivelò a livello teorico il fenomeno.

Infatti nel 1935, i fisici Albert Einstein, Boris Podolsky e Nathan Rosen, scrissero un articolo nel quale ritenevano che il fenomeno dell'entanglement fosse paradossale. Questa tesi nacque dall'assunzione delle tre ipotesi della meccanica quantistica:

- Principio di realtà: esiste una realtà indipendente dai nostri schemi concettuali, dalle nostre pratiche linguistiche e dalle nostre credenze.
- Principio di località: oggetti distanti non possono avere influenza istantanea l'uno sull'altro. Einstein infatti afferma:

  > "La seguente idea caratterizza l'indipendenza relativa di oggetti molto lontani nello spazio (A e B): un'influenza esterna su A non ha un'influenza

diretta su B; ciò è noto come il Principio di Azione Locale, che è usato regolarmente solo nella teoria di campo. Se questo assioma venisse ad essere completamente abolito, l'idea dell'esistenza di sistemi quasi-chiusi, e perciò la postulazione delle leggi che possono essere verificate empiricamente nel senso accettato, diverrebbe impossibile" [16].

- Principio di completezza: un insieme di assiomi è sufficiente a dimostrare tutte le verità di una teoria quindi a decidere delle verità o falsità qualunque enunciato formulabile nel linguaggio della teoria.

Per risolvere il paradosso era necessario che una delle tre ipotesi cadesse, ma tenendo conto che le prime due dovevano per forza essere vere, in quanto evidenti, i tre autori giunsero alla conclusione che la meccanica quantistica dovesse contenere delle variabili nascoste e quindi risultasse incompleta.

Prove ed esperimenti hanno dimostrato che il famoso paradosso EPR aveva un problema di fondo. Per questa ragione, l'interpretazione maggiormente condivisa della meccanica quantistica contempla ad un tempo aspetti locali, come la teoria quantistica dei campi, e sopratutto aspetti non locali, ovvero l'entanglement, rifiutando il principio di realtà.

Questa interpretazione ha portato a dei risultati sperimentali sorprendenti. Nel dicembre del 2011 un gruppo di ricercatori dell'università di Oxford ha dimostrato che l'entanglement quantistico può manifestarsi in maniera relativamente vistosa anche nel mondo macroscopico.

Come viene descritto nel loro articolo [17], i ricercatori sono riusciti a porre in uno stato di "non separabilità" quantistica due diamanti di circa un millimetro di diametro, collocati ad una distanza di 15 centimetri l'uno dall'altro e, cosa non meno significativa, a temperatura ambiente.

Un risultato simile è stato realizzato nel settembre del 2014, quando un gruppo di fisici annunciò [18] di aver creato un nuovo stato della materia collegando un elevato numero di atomi di rubidio in modo che il loro destino fosse strettamente interconnesso; l'enorme nuvola di atomi così creata va sotto il nome di "singoletto di spin macroscopico".

In generale, dato un sistema a n qubit, se non è possibile decomporre lo stato totale dei qubit che lo compongono, allora questi sono detti entangled; in pratica nessun qubit possiede uno stato individuale, ma solo l'insieme di tutti ha uno stato ben definito.

La pseudo-telepatia quantistica, che sta alla base di questa tesi, è una manifestazione molto importante ed interessante di questo fenomeno: due qubit in uno stato entangled sono quasi telepatici, si può immaginare una sorta di telepatia, cioè i due qubit riescono ad agire come se si scambiassero determinate informazioni senza comunicare tra loro [4].

2.5 Qubit

Il qubit, abbreviazione di quantum bit, è l'unità fondamentale dell'informatica quantistica; esso rappresenta il concetto di quanto di informazione, la più piccola porzione in cui una qualsiasi informazione codificata può essere scomposta; è l'unità di misura dell'informazione codificata.

Il qubit rappresenta per la computazione quantistica quello che il bit rappresenta per la computazione classica. Mentre il bit è una variabile che può assumere solamente due stati chiamati semplicemente 0 e 1; un qubit invece può avere un numero infinito di combinazioni lineari della base ortonormale così da permettere, almeno in linea teorica, la rappresentazione in un unico qubit di infiniti stati.

Queste affermazioni risultano errate proprio perché un qubit, potenzialmente rappresentabile da un numero infinito di stati, dopo essere stato misurato, può essere individuato soltanto da due stati: $|0\rangle$ e $|1\rangle$; questo tipo di annotazione, chiamata notazione bra-ket, è stata introdotta dal matematico e fisico Paul Dirac nel 1939 [7] per descrivere uno stato quantistico; il nome bra-ket deriva dal fatto che il prodotto scalare di due stati W e X è denotato attraverso una bracket $\langle W|X\rangle$ consistente di due parti: la sinistra $\langle W|$ chiamata bra e la parte destra $|X\rangle$ chiamata ket. Un ket di stato descrive in modo completo uno stato quantistico.

La misura del qubit ne cambia inevitabilmente lo stato riducendo la sovrapposizione in uno dei due specifici stati rappresentati dai vettori della base computazionale, come evidenziato nel terzo postulato della meccanica quantistica.

Quindi, dopo aver misurato un qubit, il numero delle informazioni ottenibili è lo stesso di un bit classico; questo fondamentale risultato è stato dimostrato dal matematico russo Alexander Holevo nel 1973 [11].

In accordo con il primo postulato, un generico qubit $|\Psi\rangle$ viene rappresentato da un vettore unitario di uno spazio di Hilbert:

$$|\Psi\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv \alpha|0\rangle + \beta|1\rangle \tag{2.6}$$

dove α, β sono due numeri complessi, chiamati ampiezze, tali per cui $|\alpha|^2 + |\beta|^2 = 1$.

Nel caso classico, è sempre possibile esaminare un bit e controllare quale sia il suo stato se 0 oppure 1; al contrario, nel caso quantistico, non è possibile esaminare un qubit per determinare il suo stato, cioè non è possibile determinare i due coefficienti α e β.

I due vettori $|0\rangle$ e $|1\rangle$ del qubit hanno come valori:

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

Il terzo postulato della meccanica quantistica esprime la possibilità di acquisire una quantità limitata di informazioni relative allo stato quantistico. Quando viene misurato lo stato di un qubit possiamo ottenere il risultato $|0\rangle$ con una probabilità $|\alpha|^2$ oppure possiamo ottenere $|1\rangle$ con una probabilità di $|\beta|^2$.

Mentre il bit classico può essere immaginato come una moneta che, una volta lanciata, cadrà a terra mostrando una delle due facce; il qubit può essere immaginato come una moneta che, una volta lanciata e caduta a terra, continuerà a ruotare su se stessa senza arrestarsi fino a quando qualcuno non ne fermi la rotazione per obbligarla a mostrare finalmente una delle sue due facce.

L'impossibilità di determinare lo stato di un qubit insieme alla sua posizione rende di difficile concezione la sua rappresentazione geometrica poiché formalmente, essendo un punto di uno spazio vettoriale bidimensionale a coefficienti complessi, possiede quattro gradi di libertà ma la condizione di completezza da un lato e l'impossibilità di osservare il fattore di fase dall'altro riducono a due i suoi gradi di libertà.

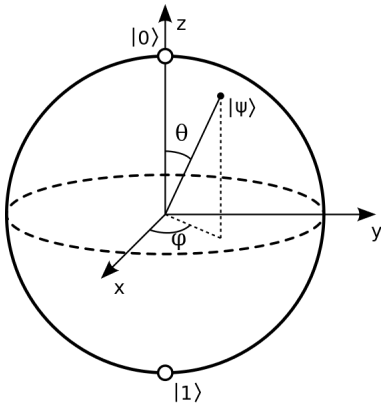

Figura 2.2: Sfera di Bloch

L'unico modo per rappresentare un qubit è attraverso una particolare figura geometrica, la sfera di Bloch [Figura 2.2]. La sfera di Bloch 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 è possibile dimostrare che esiste una corrispondenza biunivoca tra uno stato $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ ed un punto qualsiasi sulla sfera rappresentato come:

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

dove θ, $\phi \in R$ sono le coordinate sferiche del punto.

2.6 Circuiti Quantistici

Analogamente ad un computer classico, un computer quantistico è formato da circuiti quantistici costituiti da porte logiche quantistiche elementari.

2.6.1 Porte Logiche Quantistiche a un Qubit

Nel caso classico esiste un'unica porta logica a un bit, la porta NOT, che implementa l'operazione logica di negazione finita mediante una tabella di verità in cui $1 \rightarrow 0$ e $0 \rightarrow 1$.

Per definire un'operazione analoga su un qubit, non si può limitare le sue azioni sugli stati di base $|0\rangle$ e $|1\rangle$, ma bisogna specificare anche come deve essere trasformato un qubit che si trova in una sovrapposizione degli stati $|0\rangle$ e $|1\rangle$. Intuitivamente, il NOT dovrebbe scambiare i ruoli dei due stati fondamentali e trasformare $\alpha|0\rangle + \beta|1\rangle$ in $\alpha|1\rangle + \beta|0\rangle$. Chiaramente $|0\rangle$ si trasformerebbe in $|1\rangle$ e $|1\rangle$ in $|0\rangle$.

La matrice corrispondente al NOT quantistico è chiamata per motivi storici X ed è definita da:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.7}$$

Si verifica che l'applicazione di X ad un qubit $\alpha|0\rangle + \beta|1\rangle$ (scritto in notazione vettoriale) è:

$$X \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

Contrariamente al caso classico in cui è possibile definire una sola operazione su un singolo bit, nel caso quantistico esistono molte operazioni non banali su di un singolo qubit. Oltre al NOT, esistono altre due operazioni famose che sono la porta Z:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.8}$$

la quale agisce solo sulla componente $|1\rangle$ scambiandone il segno e la porta di *Hadamard* (H):

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.9}$$

Quest'ultima operazione è una delle più utili e viene usata spesso nella definizione di circuiti quantistici. Il suo effetto è quello di trasformare uno stato di base in una sovrapposizione che risulti, dopo una misurazione nella base computazionale, essere 0 oppure 1 con uguale probabilità. Ad esempio, applicando H a $|0\rangle$ si ottiene:

$$H \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

cioè lo stato $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$.

L'effetto di H si può quindi vedere come un NOT eseguito a metà in modo che lo stato risultante non sia né 0 né 1, bensì una sovrapposizione coerente dei due stati di base.

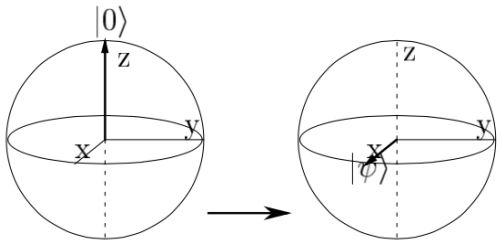

Figura 2.3: Applicazione della porta di Hadamard vista attraverso la sfera di Bloch

Nella sfera di Bloch l'operazione H corrisponde ad una rotazione di 90° della sfera intorno all'asse y seguita da una riflessione attraverso il piano (x, y). In Figura 2.3 è mostrato l'effetto dell'applicazione di H al qubit $|0\rangle$.

Le porte logiche a un qubit X, Z e H sono rappresentate graficamente in Figura 2.4.

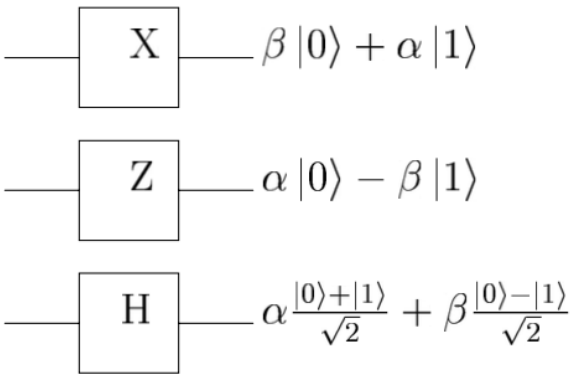

Figura 2.4: Le porte X, Z e H

2.6.2 Porte Logiche a più Qubits

Le operazioni sui registri quantistici di due o più qubit sono necessarie per descrivere le trasformazioni di stati composti e in particolare degli stati *entangled*.

Le più importanti porte logiche che implementano operazioni su due bit classici sono le porte AND, OR, XOR, NAND e NOR.

L'analogo quantistico di XOR è la porta CNOT (controlled-not) che opera su due qubit: il primo è chiamato qubit di controllo e il secondo è il qubit target. Se il controllo è

zero allora il target viene lasciato inalterato; se il qubit di controllo è uno, allora il target viene negato, cioè:

$$|00\rangle \to |00\rangle, |01\rangle \to |01\rangle, |10\rangle \to |11\rangle, |11\rangle \to |10\rangle.$$

Equivalentemente, CNOT si può vedere come:

$$|A, B\rangle \to |A, B \oplus A\rangle$$

dove A è il qubit di controllo, B è il target e $\oplus$ è la somma modulo 2, cioè l'operazione classica XOR. La porta CNOT è rappresentata graficamente dal circuito in Figura 2.5.

Figura 2.5: Porta CNOT

La rappresentazione di CNOT come matrice unitaria è la seguente:

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

dove la prima colonna descrive la trasformazione del vettore della base computazionale $|00\rangle$, la seconda quella del vettore $|01\rangle$, la terza di $|10\rangle$ e la quarta di $|11\rangle$.

2.7 Principi dell'Informatica Quantistica

Esistono diverse regole che stanno alla base della computazione quantistica che differiscono notevolmente dalla regole classiche. In realtà, è possibile dimostrare che le Macchine di Turing Quantistiche non solo permettono di raggiungere la stessa affidabilità nei calcoli, ma riescono a eseguire compiti che le Macchine di Turing classiche non potrebbero svolgere.

Di seguito vengono elencati i principi fondamentali di una Macchina di Turing Quantistica:

- No-cloning: un'informazione quantistica non può essere copiata con fedeltà assoluta e quindi neanche letta con fedeltà assoluta.

- L'informazione quantistica può essere trasferita con fedeltà assoluta, a patto che l'originale venga distrutta nel processo (teletrasporto quantistico ottenuto per la prima volta da Nielsen, Klinn e LaFlamme nel 1998).

- Ogni misura compiuta su di un sistema quantistico distrugge la maggior parte dell'informazione, lasciandolo in uno stato base. L'informazione distrutta non può essere recuperata, questo principio è una derivazione del terzo postulato della meccanica quantistica.

- Anche se in qualche caso si rivela possibile conoscere esattamente in che stato base si troverà il sistema dopo una misura, il più delle volte si avrà una previsione probabilistica.

- Alcune misure osservabili non possono avere simultaneamente valori definiti con precisione, per il principio di indeterminazione di Heisenberg. Ciò impedisce sia di stabilire con esattezza le condizioni iniziali prima del calcolo, sia di leggere i risultati con precisione.

- L'informazione quantistica può essere codificata tramite correlazioni non-locali tra parti differenti di un sistema fisico (entanglement).

Capitolo 3

Pseudo-Telepatia

La pseudo-telepatia quantistica è il risultato dell'applicazione dell'informatica quantistica alla complessità della comunicazione; grazie al fenomeno dell'entanglement, descritto in dettaglio nel capitolo precedente, due o più entità in un ambiente quantistico riescono a portare a termine un determinato compito (nel nostro caso un gioco) senza nessun bisogno di comunicazione tra le parti, quindi senza nessuno scambio di informazioni.

Questo fenomeno può essere spiegato attraverso una serie di giochi molto semplici ma che seguono una regola fondamentale: i partecipanti prima dell'inizio si consultano sulla strategia da seguire; una volta decisa la strategia ed iniziato il gioco, vengono separati e portati ad una enorme distanza gli uni dagli altri, cosicché non vi sia possibilità di comunicazione tra loro in tempi brevi; solamente dopo essere stati separati i giocatori possono iniziare a svolgere il compito di misura sui rispettivi qubit.

Nelle pagine successive verrà spiegato il meccanismo attraverso il quale si può utilizzare la pseudo-telepatia per portare a termine un compito senza il bisogno di comunicazione tra le parti. Il gioco può essere realizzato da un numero arbitrario n di giocatori; nel nostro specifico caso, il gioco viene realizzato da tre persone chiamate semplicemente A, B e C che dovranno trovarsi ad una grande distanza l'una dall'altra. Nell'esempio i giocatori, dopo aver deciso la strategia da utilizzare, vengono trasportati in tre pianeti differenti, come mostrato in Figura 3.1, in modo da soddisfare il requisito fondamentale della pseudo-telepatia quantistica.

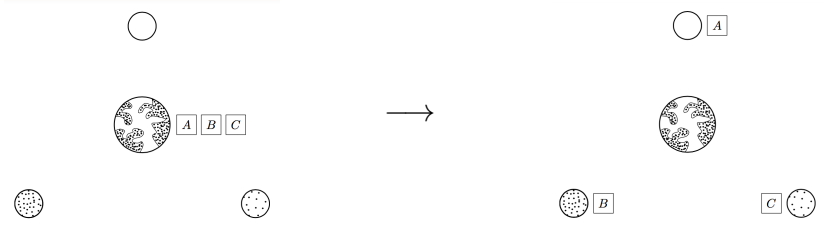

Figura 3.1: A, B, C vanno in tre mondi diversi

I tre giocatori, dopo aver raggiunto i rispettivi pianeti in cui dovranno svolgere la loro prova, ricevono simultaneamente una pietra; essa potrà avere solo due diverse forme,

levigata o grezza. Il gioco permette solamente due tipi di combinazione nella distribuzione delle pietre alle tre persone: le pietre vengono distribuite tutte e tre di forma levigata oppure una di forma levigata e le altre due di forma grezza.

Come è facile intuire, si creano quattro possibili casi, tutti equiprobabili:

- A, B, C possiedono una pietra levigata
- A possiede una pietra levigata, B e C possiedono una pietra grezza.
- B possiede una pietra levigata, A e C possiedono una pietra grezza.
- C possiede una pietra levigata, A e B possiedono una pietra grezza.

In Figura 3.2 viene mostrato un diagramma con i quattro possibili casi; il quadrato nero a fianco della lettera indica che quel giocatore possiede una pietra levigata, se il quadrato è bianco vuol dire che il giocatore possiede una pietra grezza.

Una volta ricevute le pietre, ogni persona ha la possibilità di fare due scelte: tenere la pietra o restituirla. Ogni partecipante dovrà compiere la sua scelta in modo autonomo, senza conoscere quale decisione sia stata presa dalle altre due persone.

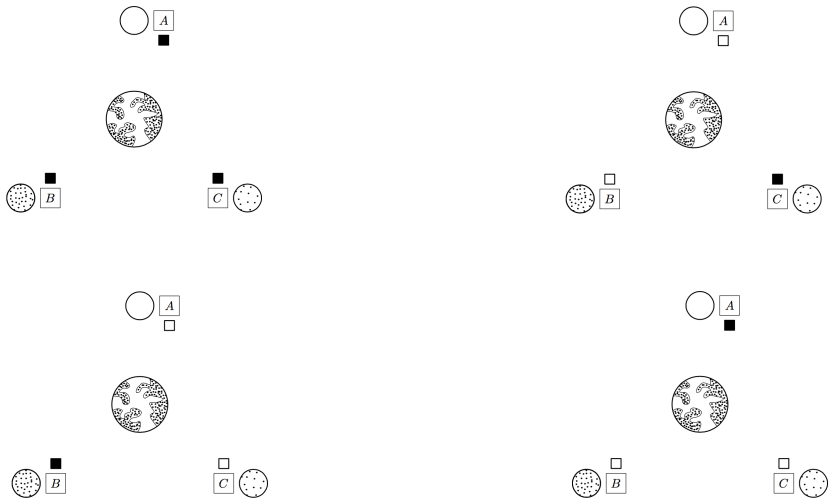

Figura 3.2: I 4 casi possibili

La scelta di tenere o restituire la pietra deve essere fatta simultaneamente dai tre partecipanti; dopo che le scelte sono state effettuate, bisogna valutare se il compito è stato portato a termine o meno.

Per verificare se i tre giocatori hanno vinto o perso il gioco bisogna tenere conto del numero di pietre che A, B e C hanno ancora nelle mani in base a quale caso sia capitato.

Nel caso in cui i tre partecipanti abbiano ricevuto tre pietre levigate, per vincere devono fare in modo che il numero totale delle pietre rimaste ai giocatori sia dispari, quindi devono possedere o 1 pietra oppure 3. Se i tre giocatori ricevono una pietra levigata e due pietre grezze, per riuscire a vincere la somma delle pietre rimaste nelle loro mani dovrà risultare un numero pari.

3.1 Sulle Strategie Classiche

Il problema presentato non può essere risolto in maniera classica, seguendo una strategia deterministica proprio perché non esiste una strategia deterministica vincente per questo tipo di problema. Dimostro quanto detto attraverso un ragionamento per assurdo: supponiamo che esista una strategia classica sempre vincente.

Si definiscono sei variabili che servono per conoscere se una persona ha restituito la pietra oppure l'ha tenuta:

- $A_L = 0$ se A decide di ridare indietro la pietra levigata; $A_L = 1$ altrimenti.
- $A_S = 0$ se A decide di restituire la pietra grezza, $A_S = 1$ altrimenti.
- $B_L = 0$ se B decide di ridare indietro la pietra levigata; $B_L = 1$ altrimenti.
- $B_S = 0$ se B decide di restituire la pietra grezza, $B_S = 1$ altrimenti.
- $C_L = 0$ se C decide di ridare indietro la pietra levigata; $C_L = 1$ altrimenti.
- $C_S = 0$ se C decide di restituire la pietra grezza, $C_S = 1$ altrimenti.

Attraverso queste variabili si possono trasformare i quattro casi possibili del problema in altrettante equazioni che descrivono meglio la situazione. Nel caso delle tre pietre levigate la situazione vincente si realizza se si verifica la condizione:

$$A_L + B_L + C_L \equiv 1 \pmod 2 \tag{3.1}$$

Allo stesso modo, per i restanti casi delle due pietre grezze e una levigata la situazione di vincita corrisponde al sistema composto dalle tre equazioni:

$$A_L + B_S + C_S \equiv 0 \pmod 2 \tag{3.2}$$

$$A_S + B_L + C_S \equiv 0 \pmod 2 \tag{3.3}$$

$$A_S + B_S + C_L \equiv 0 \pmod 2 \tag{3.4}$$

Sommando tutte le equazioni derivate dai quattro possibili casi, viene fuori l'assurdo del ragionamento poiché:

$$2A_L + 2B_L + 2C_L + 2A_S + 2B_S + 2C_S \equiv 1 \pmod 2 \tag{3.5}$$

L'equazione 3.5, corretta dal punto di vista sintattico, conduce ad un assurdo perché il membro di sinistra è inevitabilmente un numero pari che sarà diverso dal membro a destra dell'uguale, il quale è sempre un numero dispari perché il suo resto modulo 2 ha come risultato 1. L'equazione finale così trovata dimostra che qualsiasi combinazione di pietre

venga affidata ai tre giocatori in un ambiente classico, almeno una delle equazioni non viene soddisfatta. L'eguaglianza 3.5 dimostra che non esiste nessuna strategia classica deterministica vincente su ogni combinazione assegnata di pietre.

3.2 Una Strategia Quantistica

Nonostante il fatto che sia stato dimostrato impossibile risolvere questo tipo di problema con una strategia classica, alcuni studiosi dell'università di Montreal, il professore Gilles Brassard, Anne Broadbent e Alain Tapp, sono riusciti ad elaborare una strategia vincente facendo uso della computazione quantistica [6].

La ricerca effettuata dall'università di Montreal descrive un concetto fondamentale alla base dell'informatica quantistica: un computer quantistico si dimostra in grado di risolvere in una quantità di tempo ragionevole alcune tipologie di problemi rispetto ad un computer classico che impiegherebbe una quantità di tempo esponenziale o addirittura non riuscirebbe ad arrivare ad una soluzione; grazie ad un computer quantistico è possibile ricercare una strategia non classica sempre vincente in grado di risolvere il problema di questo gioco.

Dallo stesso articolo si dimostra che i partecipanti vincono in maniera sistematica senza il bisogno di comunicazione tra loro; analizzata da un punto di vista classico, la ricerca sembra affidarsi ad una specie di magica comunicazione, una sorta di telepatia che può essere intesa come una comunicazione istantanea tra le parti, per soddisfare i requisiti del gioco.

La soluzione teorica proposta non si basa sul fenomeno della telepatia, ma viene sfruttato un principio fondamentale della meccanica quantistica: l'entanglement, fenomeno che può essere usato con successo per ridurre, ed addirittura eliminare, la quantità di informazioni e di dati necessari per svolgere determinati compiti. Questo fenomeno è conosciuto sotto il nome di pseudo-telepatia quantistica, la quale può richiamare alla mente in modo fuorviante una qualche comunicazione di tipo telepatico.

L'effetto dell'entanglement favorisce nuove opzioni per la creazione di strategie vincenti per quei giochi che non ammettono protocolli classici efficaci per la loro risoluzione.

In accordo con l'articolo, per poter vincere in maniera sistematica il gioco, i tre giocatori devono iniziare la partita scegliendo di condividere, con un computer quantistico, un qubit ciascuno in uno stato di entanglement; questi tre qubit, seguendo la formula 2.6, saranno descritti dal seguente vettore unitario in uno spazio di Hilbert:

$$\left(\frac{1}{\sqrt{2}}\right)(|KKK\rangle + |YYY\rangle) \tag{3.6}$$

Il valore K alla i-esima posizione sta a significare che l'i-esimo giocatore sceglie di tenere la pietra, mentre il valore Y indica che la pietra verrà gettata.

Naturalmente, le tre persone non possono misurare i loro qubit poiché il principio di indeterminazione di Heisenberg, una delle colonne portanti della meccanica quantistica, asserisce che non è possibile conoscere lo stato di una particella (in questo caso il qubit) senza perturbarlo in maniera irreparabile.

Se si eseguisse una misura dello stato del sistema al momento iniziale, si avrebbe il 50% di probabilità di ottenere come stati dei qubit tre K, il 50% di probabilità tre stati Y e nessuna altra possibile combinazione.

Quello che A, B e C possono fare, dopo essere andati ad una distanza enorme uno dall'altro, è utilizzare due diverse trasformazioni unitarie sul proprio qubit, in base a quale tipo di pietra sia capitato a loro.

La prima trasformazione unitaria, chiamata S, ridefinisce i termini del qubit preso in esame:

$$S|0\rangle \longrightarrow |0\rangle \tag{3.7}$$

$$S|1\rangle \longrightarrow i|1\rangle \tag{3.8}$$

La seconda trasformazioni unitaria è chiamata di Walsh-Hadamard (H) e si basa sulla formula 2.9, analizzata nel paragrafo 2.6.1:

$$H|0\rangle \longrightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{3.9}$$

$$H|1\rangle \longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \tag{3.10}$$

La strategia riguardante il caso delle tre pietre levigate consiste nell'applicazione da parte di ogni partecipante della trasformazione di Walsh-Hadamard sul proprio qubit; d'altra parte, nei tre casi delle due pietre grezze e una levigata, coloro i quali hanno ricevuto una pietra grezza dovranno preventivamente applicare al proprio qubit una tra le formule 3.7 e 3.8 successivamente tutti dovranno trasformare il qubit attraverso l'applicazione di Walsh-Hadamard.

Ognuna delle trasformazioni lineari cambia lo stato iniziale del sistema secondo le formule 3.9 e 3.10, dove il termine K corrisponde al qubit $|0\rangle$ mentre Y equivale al qubit $|1\rangle$, convertendo uno stato della forma $\alpha|xyz\rangle$ in due nuovi termini:

Il giocatore A se possiede una pietra *levigata* applica al suo qubit l'operatore H:

- se $x = K$ allora $\alpha|xyz\rangle \longrightarrow \frac{\alpha}{\sqrt{2}}(|Kyz\rangle + |Yyz\rangle)$
- se $x = Y$ allora $\alpha|xyz\rangle \longrightarrow \frac{\alpha}{\sqrt{2}}(|Kyz\rangle - |Yyz\rangle)$

Il giocatore A se possiede una pietra *grezza* applica al suo qubit prima l'operatore S e successivamente H:

- se $x = K$ allora $\alpha|xyz\rangle \longrightarrow \frac{\alpha}{\sqrt{2}}(|Kyz\rangle + |Yyz\rangle)$
- se $x = Y$ allora $\alpha|xyz\rangle \longrightarrow i\frac{\alpha}{\sqrt{2}}(|Kyz\rangle - |Yyz\rangle)$

Il giocatore B se possiede una pietra *levigata* applica al suo qubit l'operatore H:

- se $y = K$ allora $\alpha|xyz\rangle \longrightarrow \frac{\alpha}{\sqrt{2}}(|xKz\rangle + |xYz\rangle)$
- se $y = Y$ allora $\alpha|xyz\rangle \longrightarrow \frac{\alpha}{\sqrt{2}}(|xKz\rangle - |xYz\rangle)$

Il giocatore B se possiede una pietra *grezza* applica al suo qubit prima l'operatore S e successivamente H:

- se $y = K$ allora $\alpha|xyz\rangle \longrightarrow \frac{\alpha}{\sqrt{2}}(|xKz\rangle + |xYz\rangle)$
- se $y = Y$ allora $\alpha|xyz\rangle \longrightarrow i\frac{\alpha}{\sqrt{2}}(|xKz\rangle - |xYz\rangle)$

Il giocatore C se possiede una pietra *levigata* applica al suo qubit l'operatore H:

- se $z = K$ allora $\alpha|xyz\rangle \longrightarrow \frac{\alpha}{\sqrt{2}}(|xyK\rangle + |xyY\rangle)$
- se $z = Y$ allora $\alpha|xyz\rangle \longrightarrow \frac{\alpha}{\sqrt{2}}(|xyK\rangle - |xyY\rangle)$

Il giocatore C se possiede una pietra *grezza* applica al suo qubit lprima l'operatore S e successivamente H:

- se $z = K$ allora $\alpha|xyz\rangle \longrightarrow \frac{\alpha}{\sqrt{2}}(|xyK\rangle + |xyY\rangle)$
- se $z = Y$ allora $\alpha|xyz\rangle \longrightarrow i\frac{\alpha}{\sqrt{2}}(|xyK\rangle - |xyY\rangle)$

3.2.1 Caso delle Tre Pietre Levigate

Mostriamo cosa succede nel caso in cui siano date ai partecipanti al gioco, tre pietre levigate. L'ordine in cui i giocatori cambiano lo stato del sistema è del tutto irrilevante.

Il giocatore A si sposta ad una distanza lontanissima dagli altri due, riceve la pietra, osserva che è di forma levigata e quindi applica la trasformazione unitaria di Walsh-Hadamard; dopo l'esecuzione della trasformazione unitaria sul primo qubit appartenente ad A dei tre sistemi descritti da 3.6; verrà convertito nello stato seguente:

$$\left(\frac{1}{\sqrt{2}} \times \frac{1}{\sqrt{2}}\right)(|KKK\rangle + |YKK\rangle + |KYY\rangle - |YYY\rangle) = \\ = \frac{1}{2}(|KKK\rangle + |YKK\rangle + |KYY\rangle - |YYY\rangle)$$

Allo stato appena trovato il secondo giocatore B, dopo aver osservato la forma della sua pietra, applica anche lui la trasformazione unitaria di Walsh-Hadamard; quello che trova come risultato è il seguente sistema:

$$\left(\frac{1}{\sqrt{2}} \times \frac{1}{2}\right)(|KKK\rangle + |KYK\rangle + |YKK\rangle + |YYK\rangle + \\ + |KKY\rangle - |KYY\rangle - |YKY\rangle + |YYY\rangle)$$

Applico lo stesso ragionamento al giocatore C; il sistema risultante è il seguente:

$$\left(\frac{1}{4}\right)(|KKK\rangle + |KKY\rangle + |KYK\rangle + |KYY\rangle + |YKK\rangle + |YKY\rangle + \\ + |YKK\rangle + |YYY\rangle + |KKK\rangle - |KKY\rangle - |KYK\rangle + |KYY\rangle - \\ - |YKK\rangle + |YKY\rangle + |YKK\rangle - |YYY\rangle)$$

Dopo aver unito i termini simili e aver semplificato tutte le possibili triple, il sistema risultante contiene quattro termini, che sono le possibili combinazioni per le tre persone di vincere il gioco:

$$\frac{1}{2}(|KKK\rangle + |KYY\rangle + |YKY\rangle + |YYK\rangle)$$

Se ora A, B e C osservano i propri qubit, essi collasseranno con uguale probabilità in uno qualunque degli stati di cui è sovrapposizione lo stato complessivo. Se un giocatore osservando il suo qubit trova come risultato K, tiene la sua pietra, altrimenti se osserva Y la butta. Si nota che in questo modo il numero di pietre tenute dai tre giocatori è sempre dispari e il gioco porta sempre ad una vittoria.

3.2.2 Caso delle Due Pietre Grezze e Una Levigata

Si osservi cosa succede negli altri tre casi, in cui vengono assegnate ai tre giocatori due pietre di forma grezza e una pietra di forma levigata. Si ricordi che per vincere il gioco in questo caso è necessario che la somma delle pietre rimaste in mano ai tre giocatori sia un numero pari.

Seguendo lo stesso ragionamento della sezione precedente, A, B e C si spostano ad una distanza enorme gli uni dagli altri, ricevono la pietra, e ne osservano la forma.

I due partecipanti che ricevono la pietra grezza dovranno applicare al proprio qubit una tra le formule 3.7 e 3.8; successivamente applicargli la trasformazione unitaria di Walsh-Hadamard, descritta dalle formule 3.9 e 3.10; mentre il giocatore che riceve la pietra levigata applica sul suo qubit solamente la trasformazione di Walsh-Hadamard, come nel caso delle tre pietre levigate. Anche in questi casi l'ordine dei giocatori con cui vengono eseguiti i calcoli è indifferente.

Partendo sempre dai tre sistemi descritti dal vettore di 3.6 verrà applicata la trasformazione sui qubit corrispondenti. Analizziamo i tre casi possibili:

Caso 1: il giocatore A riceve la pietra levigata, B e C ricevono le due pietre grezze

In questo caso particolare, dato che l'ordine dei giocatori è irrilevante ai fini dei calcoli, il partecipante B effettua per primo le trasformazioni sullo stato iniziale:

$$\left(\frac{1}{\sqrt{2}} \times \frac{1}{\sqrt{2}}\right)(|KKK\rangle + |KYK\rangle + i|YKY\rangle - i|YYY\rangle) =$$
$$= \left(\frac{1}{2}\right)(|KKK\rangle + |KYK\rangle + i|YKY\rangle - i|YYY\rangle)$$

Nello stesso momento, A controlla il suo stato ed effettua la trasformazione di Walsh-Hadamard:

$$\left(\frac{1}{2\sqrt{2}}\right)(|KKK\rangle + |YKK\rangle + |KYK\rangle + |YYK\rangle +$$
$$+i|KKY\rangle - i|YKY\rangle - i|KYY\rangle + i|YYY\rangle)$$

Il risultato finale sotto indicato viene già semplificato nella sua componente a sinistra del braket; dallo stato risultante vengono eseguite le trasformazioni di C:

$$\left(\frac{1}{4}\right)(|KKK\rangle + |KKY\rangle + |YKK\rangle + |YKY\rangle +$$
$$+|KYK\rangle + |KYY\rangle + |YYK\rangle + |YYY\rangle -$$
$$-|KKK\rangle + |KKY\rangle + |YKK\rangle + |YKY\rangle +$$
$$+|KYK\rangle + |KYY\rangle - |YYK\rangle + |YYY\rangle)$$

Dopo le opportune semplificazioni il sistema finale risultante contiene quattro termini, che sono le possibili combinazioni per le tre persone di vincere il gioco:

$$\frac{1}{2}(|KKY\rangle + |YKK\rangle + |KYK\rangle + |YYY\rangle)$$

Esattamente come nel caso delle tre pietre levigate, la condizione per vincere è rispettata poiché il numero delle componenti K è sempre pari in ogni possibile stato.

Caso 2: il giocatore B riceve la pietra levigata, A e C ricevono le due pietre grezze

Il partecipante B effettua per primo la sua trasformazione di Walsh-Hadamard sullo stato iniziale:

$$\left(\frac{1}{2}\right)(|KKK\rangle + |KYK\rangle + |YKY\rangle + |YYY\rangle)$$

Allo stesso modo, C controlla il proprio stato ed effettua le trasformazioni:

$$\begin{aligned}\left(\frac{1}{2\sqrt{2}}\right)(|KKK\rangle + |KKY\rangle + |KYK\rangle + |KYY\rangle + \\ +i|YKK\rangle - i|YKY\rangle - i|YKK\rangle + i|YYY\rangle)\end{aligned}$$

Come nel caso precedente, il risultato finale sotto indicato viene già semplificato nella sua componente a sinistra del braket con le stesse espressioni. Dallo stato risultante vengono eseguite le trasformazioni di A;

$$\begin{aligned}\left(\frac{1}{4}\right)(|KKK\rangle + |YKY\rangle + |KKY\rangle + |YKY\rangle + \\ +|KYK\rangle + |YYK\rangle + |KYY\rangle + |YYY\rangle - \\ -|KKK\rangle + |YKK\rangle + |KKY\rangle - |YKY\rangle + \\ +|KYK\rangle - |YYK\rangle - |KYY\rangle + |YYY\rangle)\end{aligned}$$

Dopo le opportune semplificazioni il sistema finale risultante contiene quattro termini, che sono le possibili combinazioni per le tre persone di vincere il gioco:

$$\frac{1}{2}(|YKK\rangle + |KKY\rangle + |KYK\rangle + |YYY\rangle)$$

Esattamente come nel precedente caso delle due pietre grezze e una levigata, la condizione per vincere è rispettata poiché il numero delle componenti K è sempre pari in ogni possibile stato.

Caso 3: il giocatore C riceve la pietra levigata, A e B ricevono le due pietre grezze

Il partecipante A effettua per primo le sue trasformazioni sullo stato iniziale:

$$\left(\frac{1}{2}\right)(|KKK\rangle + |YKK\rangle + i|KYY\rangle - i|YYY\rangle)$$

B controlla il suo stato ed effettua le trasformazioni:

$$\left(\frac{1}{2\sqrt{2}}\right)(|KKK\rangle + |KYK\rangle + |YKK\rangle + |YYK\rangle + \\ +i|KKY\rangle - i|KYY\rangle - i|YKY\rangle + i|YYY\rangle)$$

Come nei casi precedenti, il risultato finale sotto indicato viene già semplificato nella sua componente a sinistra del braket con le stesse espressioni. Dallo stato risultante vengono eseguite la trasformazione unitaria di Walsh-Hadamard del partecipante C;

$$\left(\frac{1}{4}\right)(|KKK\rangle + |KKY\rangle + |KYK\rangle + |KYY\rangle + \\ +|YKK\rangle + |YKY\rangle + |YYK\rangle + |YYY\rangle - \\ -|KKK\rangle + |KKY\rangle - |KYK\rangle + |KYY\rangle + \\ +|YKK\rangle - |YKY\rangle - |YYK\rangle + |YYY\rangle$$

Dopo le opportune semplificazioni il sistema finale risultante contiene quattro termini, che sono le possibili combinazioni per le tre persone di vincere il gioco:

$$\frac{1}{2}(|YKK\rangle + |KKY\rangle + |KYK\rangle + |YYY\rangle)$$

Proprio come nei due precedenti casi delle due pietre grezze e una levigata, la condizione per vincere è rispettata poiché il numero delle componenti K è sempre pari in ogni possibile stato.

Nei tre casi presentati, i giocatori controllano lo stato del sistema in ordine diverso proprio per dimostrare che l'ordine in cui viene osservato lo stato del sistema è del tutto indifferente al fine del risultato finale.

Le trasformazioni unitarie utilizzate creano correlazione tra i componenti individuali delle triple; l'aspetto più importante di tutto ciò è che queste correlazioni non possono uscire come risultato di un'espressione in un mondo basato sulla fisica classica.

Un altro risultato interessante della computazione si nota alla fine del processo: i partecipanti sanno che attraverso questo metodo hanno vinto il gioco, ma non esiste un modo per loro di conoscere quale tipo di pietra, se levigata o grezza, avevano le altre due persone; la computazione quantistica garantisce il successo e la vittoria del gioco ma non esiste nessuno scambio di informazioni tra le persone, infatti nessun messaggio è stato scambiato tra le parti durante questo esperimento quantistico.

Capitolo 4

Confronto fra Strategie

4.1 Generalizzazione del Gioco con un Numero n di Giocatori

In questo capitolo, l'esempio di gioco mostrato nel capitolo precedente, verrà generalizzato aggiungendo un numero arbitrario n di giocatori; questa possibilità oltre a semplificare il tutto e a rendere l'applicazione della pseudo-telepatia quantistica il più generale possibile, permette un confronto molto efficace con altre strategie classiche ma probabilistiche.

Un'ulteriore semplificazione realizzata è stato il cambio delle variabili proprio per rendere il più generale possibile il gioco analizzato: al posto di dare in input una pietra levigata o grezza e decidere se tenere o gettare via la pietra ricevuta, ogni giocatore riceve un bit x_i e produce un bit di output y_i.

Per qualsiasi valore $n \geq 3$, siano dati gli n partecipanti $A_1, \ldots, A_n$. La fase di inizializzazione del gioco consiste nello scambio reciproco da parte dei giocatori di variabili casuali (strategia classica) oppure di entanglement quantistico (strategia quantistica).

Viene consegnato a ciascun giocatore A_i un bit di input x_i, al quale egli deve rispondere, senza che sia ammessa comunicazione classica, con gli altri giocatori A_j, con $j \neq i$, con l'emissione di un bit di output y_i.

Il gioco ha un unico vincolo: il numero di componenti $x_i = 1$ deve essere pari. Il gioco viene considerato vinto se la seguente espressione è soddisfatta:

$$\sum_i^n y_i \equiv \frac{1}{2} \sum_i^n x_i \pmod 2 \tag{4.1}$$

sapendo che $\sum_i^n x_i \equiv 0 \pmod 2$ poiché rappresenta il vincolo del gioco. In altre parole, se la somma dei bit in output è dispari allora il numero di bit in input uguali a 1 è pari ma non è divisibile per 4. Al contrario, se la somma dei bit in output è pari allora la somma dei bit in input è divisibile per 4.

4.2 Protocollo Quantistico Perfetto

Un protocollo viene definito perfetto se consente ai partecipanti di vincere su ogni input che soddisfi il predicato *n-ario*. Diciamo inoltre che un protocollo quantistico esibisce pseudo-telepatia se è perfetto a patto che i partecipanti condividano all'inizio entanglement quantistico, mentre non esiste alcun protocollo classico perfetto. Ciascun partecipante del gioco G_n riceve un singolo bit x_i di input al quale deve rispondere con un bit di output y_i senza consultare gli altri giocatori.

La premessa è sempre la stessa: nell'input il numero complessivo di bit $x_i = 1$ deve essere pari:

$$\sum_{i=1}^{n} x_i \equiv 0 \pmod 2$$

Al fine di vincere il gioco, occorre che sia soddisfatta la relazione 4.1; vengono classificate le due variabili $x = (x_1, x_2, \ldots, x_n)$ come la *domanda* e $y = (y_1, y_2, \ldots, y_n)$ come la *risposta*.

Si considerino i seguenti stati quantistici in entanglement generalizzati a n-qubit:

$$|\Theta_n^+\rangle = \frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle \tag{4.2}$$

$$|\Theta_n^-\rangle = \frac{1}{\sqrt{2}}|0^n\rangle - \frac{1}{\sqrt{2}}|1^n\rangle \tag{4.3}$$

Osservando quale effetto provoca su questi stati quantistici l'applicazione delle trasformazioni unitarie 3.7, 3.8, 3.9 e 3.10, si nota che applicare la trasformazione unitaria S consiste nello scambiare lo stato $|\Theta_n^+\rangle$ con lo stato $|\Theta_n^-\rangle$ e viceversa; questo implica che se n qubit di $|\Theta_n^+\rangle$ vengono distribuiti fra un numero n di giocatori e viene applicata S ad esattamente un numero m di essi, con $m < n$, allora lo stato finale potrà essere:

$$|\Theta_n^+\rangle \text{ se } m \equiv 0 \pmod 2$$

$$|\Theta_n^-\rangle \text{ se } m \equiv 1 \pmod 2$$

L'applicazione della trasformazione di Walsh-Hadamard trasforma lo stato $|\Theta_n^+\rangle$ in una sovrapposizione omogenea di stati con un numero pari di 1, mentre trasforma $|\Theta_n^-\rangle$ in una combinazione simile di termini con un numero dispari di 1:

$$(H^{\otimes n})|\Theta_n^+\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{\substack{\triangle(y) \equiv 0 \\ (\text{mod } 2)}} |y\rangle \tag{4.4}$$

$$(H^{\otimes n})|\Theta_n^-\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{\substack{\triangle(y) \equiv 1 \\ (\text{mod } 2)}} |y\rangle \tag{4.5}$$

dove il termine $\triangle(y) = \sum y_i$ è chiamato peso di Hamming di y.

Il peso di Hamming di una stringa di lunghezza k è la sua distanza di Hamming dalla stringa costituita da k zeri; in altre parole sarebbe il numero di elementi diversi da zero di una stringa, per una stringa binaria sarebbe semplicemente la somma di tutti i caratteri 1.

Da queste affermazioni è possibile enunciare il seguente teorema:

Teorema 1 *Il gioco G_n ammette un protocollo quantistico perfetto, se tutti i giocatori coinvolti hanno la possibilità di condividere entanglement quantistico.*

Dimostrazione.

Dopo la fase di inizializzazione, dove ogni partecipante A_i ha acquisito un bit dello stato $|\Theta_n^+\rangle$ e si è separato dagli altri, riceverà il bit x_i dell'input ed eseguirà le seguenti operazioni:

1. Se $x_i = 1$, il giocatore esegue la trasformazione S sul suo qubit, altrimenti non fa nulla;
2. Applica la trasformazione di Walsh-Hadamard H al suo qubit;
3. Misura il suo qubit ed ottiene l'output y_i;
4. Produce y_i come bit di output.

Per la premessa, il numero di 1 nella domanda deve essere pari, quindi un numero pari di partecipanti dovrà applicare S al suo bit. Se la somma di tutti i bit in input è un multiplo di 4, ovvero:

$$\frac{1}{2}\sum_{i=1}^{n} x_i \equiv 0 \ (\text{mod } 2)$$

il sistema complessivo tornerà allo stato $|\Theta_n^+\rangle$ dopo l'applicazione del punto 1. Perciò l'applicazione di H al passo 2 porterà ad una sovrapposizione omogenea di ket con un numero pari di 1, una combinazione di $|y\rangle$ tali che $\triangle(y) = 0 \ (\text{mod } 2)$.

Siccome i giocatori emettono come output il numero osservato al momento della misura, si avrà:

$$\sum_{i=1}^{n} y_i \equiv 0 \pmod 2$$

Grazie a queste due ultime espressioni, si dimostra che la condizione 4.1 per vincere il gioco è soddisfatta.

Controllando la situazione opposta, dove il numero di partecipanti che riceve 1 in input e che quindi effettua la trasformazione unitaria S è dispari, ovvero:

$$\frac{1}{2}\sum_{i=1}^{n} x_i \equiv 1 \pmod 2$$

si avrà che lo stato dopo la prima operazione di trasformazione S diventerà $|\Theta_n^-\rangle$. L'applicazione della trasformazione H produrrà degli stati per cui $\triangle(y) = 1 \pmod 2$:

$$\sum_{i=1}^{n} y_i \equiv 1 \pmod 2$$

Allo stesso modo del caso del numero pari di partecipanti che effettua la trasformazione unitaria S, la relazione finale trovata soddisfa la condizione iniziale 4.1.

4.3 Confronto tra Protocolli Classici e Probabilistici

Si definisce un protocollo vincente con una *probabilità* p se è in grado di vincere ogni istanza del gioco, che soddisfa la premessa, con una probabilità almeno p.

Si classifica invece un protocollo che è in grado di vincere in *proporzione* p, se la strategia in questione vince con probabilità p su istanze scelte in maniera casuale secondo una distribuzione uniforme fra tutte le istanze che soddisfano la premessa.

Attraverso le definizioni dei due protocolli si intuisce che ogni strategia che vince con *probabilità* p, vince anche in *proporzione* p; il contrario generalmente non è vero: è possibile che protocolli soddisfacenti su molte istanze falliscano in maniera sistematica su altre istanze.

4.3.1 Strategia Classica

Avvalendoci del seguente teorema, si afferma che non esiste alcun protocollo classico, per il gioco G_n, che porti al successo in base all'input per una probabilità strettamente superiore a $\frac{1}{2}$.

La proporzione risultante dal teorema mette in luce un fatto fondamentale: ogni strategia deterministica perde di efficacia all'aumentare del numero di partecipanti n.

Teorema 2 *La miglior strategia deterministica possibile per il gioco G_n ha successo in proporzione $\frac{1}{2} + 2^{-[n/2]}$.*

Dimostrazione.

Dato che una delle richieste per soddisfare il gioco è l'assenza di comunicazione tra i partecipanti, la soluzione migliore per quei giocatori che seguono un protocollo deterministico è quella di preparare una strategia prima che il gioco cominci.

La strategia scelta è semplice: bisogna far dipendere ogni risposta del giocatore A_i dal suo bit x_i di input.

Ogni giocatore possederà una strategia individuale $s_i \in \{00, 01, 10, 11\}$, dove il primo bit della coppia rappresenta l'output y_i della strategia, se il bit x_i di input equivale a zero, mentre il secondo bit denota l'output y_i, se il bit x_i di input equivale a uno.

In altre parole:

- 00 rappresenta la strategia costante $y_i = 0$,
- 11 esprime la strategia costante $x_i = 0$,
- 01 denota la strategia basata su $y_i = x_i$,
- 10 riproduce la strategia complementare $y_i = \overline{x_i}$.

Senza perdere di generalità, la strategia collettiva $s = s_1, s_2, s_3, \ldots, s_n$ rappresenta la strategia deterministica globale scelta dai partecipanti al gioco:

$$s = \overbrace{01, 01, \ldots, 01}^{k-l}, \overbrace{10, 10, \ldots, 10}^{l}, \overbrace{00, 00, \ldots, 00}^{n-k-m}, \overbrace{11, 11, \ldots, 11}^{m}$$

La lunghezza totale della strategia collettiva s, così realizzata, è n. La variabile k rappresenta il numero di giocatori che utilizzeranno una delle strategie $[01, 10]$; rispettivamente rappresentate da $k - l$ e l. I giocatori che utilizzeranno le strategie costanti $[00, 11]$ sono rappresentati dalle variabili $n - k - m$ e m.

Utilizzando s si scopre che il peso di Hamming $\triangle(y)$ della risposta è dato dalla seguente espressione:

$$\triangle(y) = \triangle(x_1, \ldots, x_{k-l}) + \triangle(\overline{x_{k-l+1}}, \ldots, \overline{x_k}) + \triangle(\overbrace{00\ldots0}^{n-k-m}) + \triangle(\overbrace{11\ldots1}^{m}) \pmod 2$$

dato che stiamo ragionando con numeri binari, il peso di Hamming di una stringa binaria è la somma dei caratteri uguali ad 1 e può essere visto come la sommatoria dei componenti di quella stringa:

$$\triangle(y) \equiv \sum_{i=1}^{n} y_i \pmod 2$$

Quindi le componenti $\triangle(\overbrace{11\ldots1}^{m})$ e $\triangle(\overbrace{00\ldots0}^{n-k-m})$ avranno rispettivamente come risultato m e 0 mentre la componente $\triangle(\overline{x_{k-l+1}}, \ldots, \overline{x_k})$ coincide con $l + \triangle(x_{k-l+1}, \ldots, x_k) \pmod 2$.

L'espressione semplificata è la seguente:

$$\triangle(y) \equiv \triangle(x_1, \cdots, x_k) + l + m \pmod 2$$

Per $a, b \in 0, 1$, verrano indicati diversi insieme $S^k_{a,b}$ composti dalle domande x con alcune condizioni: le prime k componenti devono avere come peso di Hamming il risultato $a \pmod 2$, mentre tutte le dovranno avere come peso di Hamming $2b \pmod 4$.

$$S^k_{a,b} = \{x | \triangle(x_1, \cdots, x_k) \equiv a \pmod 2 \ \wedge \triangle(x_1, \cdots, x_n) \equiv 2b \pmod 4 \ \}. \tag{4.6}$$

Se $l+m$ è un numero pari, allora le stringhe che portano a soddisfare l'equazione 4.1 sono quelle presenti negli insiemi $S^k_{0,0}$ e $S^k_{1,1}$ e quindi si avrà esattamente $|S^k_{0,0}| + |S^k_{1,1}|$ domande che ricevono una risposta vincente.

Invece, se $l+m$ risulterà un numero dispari, le stringhe che soddisfano la 4.1 sono date dagli insiemi $S^k_{0,1}$ e $S^k_{1,0}$; per questo ragione saranno presenti esattamente $|S^k_{1,0}| + |S^k_{0,1}|$ domande che danno una risposta vincente.

Le due sentenze appena enunciate hanno bisogno di qualche spiegazione in più, infatti poiché stiamo lavorando con numeri binari, la 4.1 può essere vista come:

$$\triangle(x_1, \cdots, x_k) + l + m \equiv \frac{1}{2} \left(\triangle(x_1, \cdots, x_n)\right) \pmod 2$$

allora gli insiemi che soddisfano questa espressione se $l + m$ è pari sono:

$$S^k_{0,0} \longrightarrow \triangle(x_1, \cdots, x_k) = 0 \pmod 2 \text{ e } \triangle(x_1, \cdots, x_n) = 0 \pmod 4$$
$$S^k_{1,1} \longrightarrow \triangle(x_1, \cdots, x_k) = 1 \pmod 2 \text{ e } \triangle(x_1, \cdots, x_n) = 2 \pmod 4$$

mentre se $l + m$ è dispari:

$$S^k_{0,1} \longrightarrow \triangle(x_1, \cdots, x_k) = 0 \pmod 2 \text{ e } \triangle(x_1, \cdots, x_n) = 2 \pmod 4$$
$$S^k_{1,0} \longrightarrow \triangle(x_1, \cdots, x_k) = 1 \pmod 2 \text{ e } \triangle(x_1, \cdots, x_n) = 0 \pmod 4$$

Dopo queste riflessioni, abbiamo i quattro insiemi per tutte le possibili domande; il risultato che viene fuori è l'espressione seguente:

$$|S^k_{0,0}| + |S^k_{1,1}| + |S^k_{1,0}| + |S^k_{0,1}| = 2^{n-1} \tag{4.7}$$

dove 2^{n-1} è il numero di stringhe di input che hanno un numero pari di $x_i = 1$, coincide con al metà di tutte le possibili stringhe.

Da questo punto la dimostrazione del teorema segue ciò che viene affrontato nel Lemma 2. Prima di continuare con la dimostrazione è necessario definire il Lemma successivo:

Lemma 1 *[8, eqn. 1.54]*

$$\sum_{\substack{i \equiv a \\ (mod\ 4)}} \binom{n}{i} = \begin{cases} 2^{n-2} + 2^{\frac{n}{2}-1} & se\ n - 2a \equiv 0 (mod\ 8) \\ 2^{n-2} - 2^{\frac{n}{2}-1} & se\ n - 2a \equiv 4 (mod\ 8) \\ 2^{n-2} & se\ n - 2a \equiv 2, 6 (mod\ 8) \\ 2^{n-2} + 2^{\frac{n-3}{2}} & se\ n - 2a \equiv 1, 7 (mod\ 8) \\ 2^{n-2} - 2^{\frac{n-3}{2}} & se\ n - 2a \equiv 3, 5 (mod\ 8) \end{cases}$$

Lemma 2 *Se n è un numero dispari, allora:*

$$|S^k_{0,0}| + |S^k_{1,1}| = \begin{cases} 2^{n-2} + 2^{\frac{n-3}{2}} & se\ \frac{(n-1)}{2} + 3(n-k) \equiv 0, 3 (mod\ 4) \\ 2^{n-2} - 2^{\frac{n-3}{2}} & se\ \frac{(n-1)}{2} + 3(n-k) \equiv 1, 2 (mod\ 4) \end{cases}$$

D'altra parte, se n è un numero pari, avremo:

$$|S^k_{0,0}| + |S^k_{1,1}| = \begin{cases} 2^{n-2} & se\ \frac{n}{2} + 3(n-k) \equiv 1, 3 (mod\ 4) \\ 2^{n-2} + 2^{\frac{n}{2}-1} & se\ \frac{n}{2} + 3(n-k) \equiv 0 (mod\ 4) \\ 2^{n-2} - 2^{\frac{n}{2}-1} & se\ \frac{n}{2} + 3(n-k) \equiv 2 (mod\ 4) \end{cases}$$

Continuando la dimostrazione, si definiscono due funzioni che descrivono la probabilità di vincere data dal rapporto del numero di stringhe vincenti per il numero di stringhe che hanno un numero pari di $x_i = 1$:

$$\frac{S^k_{0,0} + S^k_{1,1}}{2^{n-1}} \text{ è la probabilità di vincere se } l + m \text{ è un pari} \tag{4.8}$$

$$\frac{S^k_{0,1} + S^k_{1,0}}{2^{n-1}} \text{ è la probabilità di vincere se } l + m \text{ è un dispari} \tag{4.9}$$

Queste due funzioni vengono ulteriormente scomposte in diversi casi attraverso l'utilizzo del lemma 2; osservando la 4.8 le probabilità saranno diverse in base al numero di partecipanti n:

- $\frac{2^{n-2} \pm 2^{\frac{n-3}{2}}}{2^{n-1}} \equiv \frac{1}{2} \pm 2^{-\frac{n+1}{2}}$ se n è un numero dispari;
- $\frac{2^{n-2} \pm 2^{\frac{n}{2}-1}}{2^{n-1}} \equiv \frac{1}{2} \pm 2^{-\frac{n}{2}}$ se n è un numero pari e se $\frac{n}{2} + 3(n-k) \equiv 0, 2 (\text{mod } 4)$
- $\frac{2^{n-2}}{2^{n-1}} \equiv \frac{1}{2}$ se n è un numero pari e se $\frac{n}{2} + 3(n-k) \equiv 1, 3 (\text{mod } 4)$

Mentre osservando la 4.9 e sapendo che $\left(S^k_{0,1} + S^k_{1,0}\right) \equiv \left(1 - S^k_{0,0} + S^k_{1,1}\right)$ le probabilità di vincita saranno:

- $\frac{1-\left(2^{n-2}\pm 2^{\frac{n-3}{2}}\right)}{2^{n-1}}$ se n è un numero dispari;
- $\frac{1-\left(2^{n-2}\pm 2^{\frac{n}{2}-1}\right)}{2^{n-1}}$ se n è un numero pari e se $\frac{n}{2}+3(n-k)\equiv 0,2(\text{mod } 4)$
- $\frac{1-\left(2^{n-2}\right)}{2^{n-1}}$ se n è un numero pari e se $\frac{n}{2}+3(n-k)\equiv 1,3(\text{mod } 4)$

Teorema 3 *Alcuni semplici protocolli deterministici hanno raggiunto il limite superiore imposto dal teorema 2.*

Dimostrazione.

Le seguenti strategie, che dipendono dal numero di giocatori n (mod 8), riescono a vincere il gioco in esatta proporzione $\frac{1}{2}+2^{-[n/2]}$. Le seguenti strategie risultano essere le possibilità migliori tra tutte le strategie classiche:

n (mod 8)	giocatore 1	giocatori dal 2 a n
0	00	00
1	00	00
2	01	00
3	11	11
4	11	00
5	00	00
6	10	00
7	11	11

Esempio di una Strategia Classica con 6 Partecipanti

Per riuscire a capire meglio la strategia classica, analizzerò nel dettaglio il caso in cui partecipino al gioco 5 persone.

Ogni partecipante deve scegliere una strategia prima dell'inizio del gioco; facendo riferimento alla tabella precedente si nota che ogni partecipante, per riuscire a vincere il gioco, dovrà utilizzare la strategia [00].

Quindi la stringa s che definisce la strategia collettiva ha lunghezza 5 ed è:

$$s = 00, 00, 00, 00, 00$$

il numero che indica i giocatori che utilizzeranno una delle strategie $[01, 10]$ è $k = 0$.

Dato che la somma dei partecipanti che hanno scelto come strategia una delle stringhe $[10, 11]$ è pari, gli insiemi, contenenti le stringhe che soddisfano la 4.1, sono $S^k_{0,0}$ e $S^k_{1,1}$.

Dopo aver calcolato tutte le variabili interessate e sapendo che il numero dei giocatori che ha scelto una delle strategie $[10, 11]$ è pari, faccio riferimento alla 4.8; per questo motivo la probabilità di vincere è data dalla seguente espressione:

$$\frac{2^{n-2} + 2^{\frac{n-3}{2}}}{2^{n-1}} \equiv \frac{1}{2} + 2^{-\frac{n+1}{2}}$$

proprio come afferma il teorema 3.

4.3.2 Strategia Probabilistica

Il termine strategia probabilistica si riferisce ad una distribuzione di probabilità su un insieme di strategie deterministiche.

Le variabile casuali che vengono condivise dai partecipanti durante la fase iniziale del gioco corrispondono alla decisione di quale strategia deterministica verrà utilizzata durante l'esecuzione del protocollo.

Nonostante l'aggiunta, al modello classico, di una condivisione illimitata di variabili casuali, verrà dimostrato che non esiste nessun protocollo probabilistico che abbia una possibilità di successo superiore a $\frac{1}{2}$ nel peggior caso.

Lemma 3 *Consideriamo un gioco a più partecipanti (come quello definito nelle pagine precedenti); per ogni protocollo probabilistico che ha successo con probabilità p, esiste un protocollo deterministico che ha successo con proporzione p.*

Dimostrazione.

Questo è un caso speciale di un teorema formalizzato dallo scienziato cinese Andrew Yao [9]. Si consideri qualsiasi strategia probabilistica che abbia successo con una probabilità p, cioè un protocollo è in grado di vincere il gioco con probabilità minima p per ogni istanza del problema che soddisfa la premessa.

Si considerino le strategie deterministiche che rientrano nella definizione di strategia probabilistica: per assurdo, si assuma che la strategia migliore tra quelle presenti abbia una proporzione di successo $q < p$.

A questo punto, qualsiasi strategia deterministica mischiata con strategie probabilistiche avrà come risultato una proporzione al massimo come q. Questa affermazione è in contraddizione con l'esistenza di una strategia probabilistica, la quale vince con una proporzione di almeno p.

Da ciò si evince che $p \leq q$, ma questo è in contrapposizione con l'assunzione iniziale. Per questa ragione si dimostra che deve esistere una strategia deterministica che abbia successo con almeno una proporzione p.

Il risultato appena ottenuto pone le basi del seguente teorema:

Teorema 4 *Non esiste nessuna strategia classica per il gioco G_n che vinca con una probabilità maggiore di $\frac{1}{2} + 2^{-[n/2]}$.*

Dimostrazione.

Qualsiasi strategia vincente per il gioco G_n che abbia successo con probabilità $p > \frac{1}{2} + 2^{-[n/2]}$ implica l'esistenza di una strategia deterministica, in accordo con il Lemma 3, la quale avrà una probabilità di vincita almeno p. Questo contraddice il teorema iniziale.

4.4 Dispositivi Quantistici Imperfetti

I dispositivi quantistici, nella maggior parte dei casi, sono inaffidabili e non ci si può aspettare il risultato perfetto previsto dalla meccanica quantistica. Tuttavia è possibile ritenersi soddisfatti dato che la strategia quantistica presentata, ed in generale qualsiasi protocollo quantistico, è in grado di vincere questa determinata tipologia di gioco con una probabilità che è sempre e comunque superiore rispetto a qualsiasi strategia classica.

Infatti prendendo in esame il seguente modello imperfetto, si ipotizzi che il bit classico y_i, output di ogni giocatore A_i, corrisponda alla previsione di un meccanismo quantistico con una certa probabilità p e che gli errori sono indipendenti da giocatore a giocatore. Ciò equivale ad aggiungere alla fine della procedura perfetta seguita da ogni giocatore, un ulteriore passo random: il partecipante produce l'opposto del risultato corretto con probabilità $1 - p$.

Teorema 5 *Per ogni $p > \frac{1}{2} + \frac{\sqrt{2}}{4} \approx 85\%$ e per un numero sufficientemente grande di giocatori, la probabilità di far uscire l'output previsto dalla meccanica quantistica per ogni giocatore è almeno p. La probabilità di successo per il gioco G_n è strettamente maggiore di qualsiasi altra ottenibile classicamente.*

Dimostrazione.

La probabilità p_n di vincere il gioco è data dalla probabilità di avere un numero pari di errori:

$$p_n = \sum_{\substack{i \equiv 0 \\ (\mathrm{mod}\ 2)}} \binom{n}{i} p^{n-i}(1-p)^i = \frac{1}{2} + \frac{(2p-1)^n}{2} \tag{4.10}$$

Questo risultato è stato ricavato grazie al principio di induzione: per $n = 1$ la probabilità risulta essere p che equivale proprio a $\frac{1}{2} + \frac{(2p-1)}{2}$. Ammettendo la validità della funzione per n, si continua la dimostrazione per induzione. Per $n+1$, con $n \geq 1$ si avrà la seguente espressione:

$$p_{n+1} = p^{n+1} + \binom{n+1}{2} p^{n+1-2}(1-p)^2$$

dove p_{n+1} è dato dalla formula 4.10 con $i = 0, 2$; il risultato è il seguente, dove X corrisponde al valore che assume $\binom{n}{i}$:

$$p_{n+1} \equiv p^{n+1} + Xp^{n+1-2}(1-p)^2 \equiv Xp^{n-1}(2p^2 - 2p + 1)$$

che ci porta proprio alla deduzione corretta poiché, sapendo che $n + 1 \equiv 2$, i termini vengono sostituiti:

$$p_{n+1} = Xp^{n-1}\left(\frac{1}{2} + \frac{(2p-1)^2}{2}\right) \equiv Xp^0\left(\frac{1}{2} + \frac{(2p-1)^{n+1}}{2}\right)$$

che è proprio il risultato atteso, quindi viene dimostrata la validità della 4.10.

Analizzando il caso il cui il numero di partecipanti n sia dispari, per il teorema 4, sappiamo che la probabilità di successo di un qualsiasi protocollo classico è limitata superiormente dall'espressione:

$$p'_n = \frac{1}{2} + 2^{-[n/2]}$$

Per un qualsiasi n fissato, si definisce un valore di soglia e_n:

$$e_n = \frac{1}{2} + \frac{(\sqrt{2})^{1+\frac{1}{n}}}{4}$$

Da cui si deduce che:

$$p > e_n \Longrightarrow p_n > p'_n$$

In altre parole, il protocollo quantistico con n giocatori supera qualsiasi strategia classica a condizione che $p > e_n$. Per esempio $e_3 \approx 89.7\%$ e $e_5 \approx 87.9\%$.

Nel momento in cui n incrementa, e_n diminuisce; infatti il limite di e_n per n che tende a infinito, è dato da:

$$\lim_{n\to\infty} e_n = \frac{1}{2} + \frac{\sqrt{2}}{4} \approx 85\%$$

Lo stesso limite viene ottenuto nel caso in cui n sia un numero pari.

Un'ulteriore modo di interpretare il dispositivo quantistico imperfetto è quello di assumere che nella maggior parte del tempo esso produca una risposta corretta, ma qualche volta il dispositivo fallisce e non produce alcuna risposta.

Quando questo succede, il giocatore a cui non arriva nessuna risposta capisce che tutte le informazioni sono andate perdute; la migliore e anche unica soluzione che gli rimane è quella di scegliere un bit in maniera casuale per l'output.

Con l'utilizzo di questa strategia è possibile percorrere due strade: o ogni giocatore ha la fortuna di ricevere una risposta corretta, nel qual caso il gioco è certamente vinto; oppure almeno un partecipante produce una risposta in modo casuale; in questo caso il gioco può essere vinto con probabilità $\frac{1}{2}$ indipendentemente da cosa succeda agli altri giocatori.

Corollario 1 *Per tutti i* $q > \frac{1}{\sqrt{2}} \approx 71\%$ *e per tutti gli* n *sufficientemente grandi, i dati raccolti partecipando al gioco* G_n *non possono essere spiegati da nessuna teoria classica, se ogni giocatore emette in output ciò che è previsto dalla meccanica quantistica quando riceve una risposta con almeno una probabilità* q *o in caso contrario, il giocatore produce una risposta casuale.*

Dimostrazione. Se il partecipante al gioco ottiene una risposta corretta con una probabilità q oppure produce una risposta casuale, la probabilità che il risultato in output sia corretto è $p = q + \frac{1}{2}(1 - q) \equiv \frac{(1+q)}{2}$. Sappiamo dal teorema 5 che un dispositivo quantistico imperfetto è più affidabile rispetto a qualsiasi dispositivo classico, se n è grande abbastanza e $p > \frac{1}{2} + \frac{\sqrt{2}}{4}$. Questo porta direttamente ad avere che $q > \frac{1}{\sqrt{2}}$.

Capitolo 5

Conclusioni

In questa tesi è stato dimostrato che la pseudo-telepatia quantistica può risolvere semplici problemi che non possono essere gestiti e risolti in maniera uniforme dai protocolli classici.

Attraverso un semplice esempio di gioco (si poteva scegliere un altro gioco qualsiasi che rispettasse i vincoli iniziali), è stata dimostrata l'efficienza della pseudo-telepatia quantistica rispetto a qualsiasi altra teoria classica, indipendentemente dal numero di partecipanti.

L'utilizzo delle pseudo-telepatia quantistica non è ancora definibile a livello pratico per via delle limitazioni dovute alle difficoltà nella creazione di un computer quantistico; tuttavia la dimostrazione fatta in questa tesi e, soprattutto, i lavori svolti da scienziati di tutto il mondo a favore della teoria quantistica, stanno avendo un gran risvolto pratico. Nel corso degli anni ci stiamo avvicinando sempre di più alla meccanica quantistica poiché la maggior parte degli esperimenti teorici ha portato alla luce un fatto fondamentale: la computazione quantistica è una teoria in grado di risolvere in un ordine di tempo polinomiale, problemi classici che vengono risolti nel miglior caso in un ordine di tempo esponenziale o addirittura non vengono risolti.

Ancora siamo lontani dal poter utilizzare la meccanica quantistica in campo pratico e a livelli accettabili, anche se ci sono stati degli esperimenti che fanno ipotizzare l'utilizzo di questa teoria in tempi non lontani. Si stanno facendo enormi passi avanti nella comprensione di questa teoria, la quale è una pietra fondamentale per una miglior conoscenza del nostro universo.

Bibliografia

[1] Benioff, P. (1982). "Quantum mechanical hamiltonian models of turing machines". Journal of Statistical Physics (29), 515-546.

[2] Bennett, C. H. (1973). "Logical Reversibility of Computation". IBM Journal of Research and Development (17), 535-532.

[3] Feynman, R. P. (1982). "Simulating physics with computers". International Journal of Theoretical Physics (21), 467-488.

[4] Main, M., Rozenberg, G. (2010). "Quantum Pseudo-Telepathy Saves the World". Bulletin of the European Association for Theoretical Computer Science (99).

[5] Deutsch, D. (1985). "Quantum theory, the Church-Turing principle and the universal quantum computer in Proceedings of the Royal Society of London". The Royal Society (400), 97-117.

[6] Brassard, G., Broadbent, A., Tapp, A. (2003). "Multi-Party Pseudo-Telepathy".In: Algorithms and Data Structures, 1-11.

[7] Dirac, P. A. M. (1939). "A new notation for quantum mechanics". Mathematical Proceedings of the Cambridge Philosophical Society 35 (3), 416-418.

[8] Gould, H. W. (1972). "Combinatorial Identities, A Standardized Set of Tables Listing 500 Binomial Coefficient Summations". Morgantown Printing and Binding Co.

[9] Yao, A. C. C. (1977). "Probabilistic computations: Toward a unified measure of complexity" Proceeding of 18th IEEE Symposium on Foundations of Computer Science, 222-227.

[10] Turing, A. (1936/7). "On computable numbers, with an application to the Entscheidungsproblem", Proceedings of the London Mathematical Society, Series 2 (42), 230-265.

[11] Holevo, A. S. (1973). "Bounds for the quantity of information transmitted by a quantum communication channel". Problems of Information Transmission 9 (3), 177-183.

[12] Brassard, G., Broadbent, A., Tapp, A. (1999). "The cost of exactly simulating quantum entanglement with classical communication". Physical Review Letters (83), 1874-1877.

[13] von Neumann, J. (1945). "First Draft of a Report on the EDVAC", retrieved August 24, 2011

[14] Schrödinger, E. (1935). "Die gegenwärtige Situation in der Quantenmechanik". Naturwissenschaften 23, 807-812; 823-828; 844-849.

[15] Schrödinger, E. (1936). "Probability relations between separated systems". Mathematical Proceedings of the Cambridge Philosophical Society 32, 446-452.

[16] Einstein, A. (1948). "Quanten-Mechanik und Wirklichkeit". Dialectica (2), 320-324.

[17] Lee, K. C. (2011). "Entangling Macroscopic Diamonds at Room Temperature". Science Magazine (334), 1253-1256.

[18] Behbood, N. (2014). "Generation of Macroscopic Singlet States in a Cold Atomic Ensemble". Physical Review Letters (113).

[19] Shor, P. W. (1994). "Algorithms for quantum computation: Discrete log and factoring". Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, 124-134.