UNIVERSITÀ DEGLI STUDI DI CAMERINO

SCUOLA DI SCIENZE E TECNOLOGIE

Corso di Laurea in Matematica e Applicazioni Classe 32

GLI OPERATORI TRECCIA SONO PORTE QUANTISTICHE UNIVERSALI

Tesi di Laurea in Topologia (S.S.D MAT/03)

Relatore:
Prof. *Riccardo Piergallini*

Laureando:
Gabriele Montecchiari

Anno Accademico 2009 - 2010

Indice

Capitolo 1

Introduzione

La meccanica quantistica è una teoria fisica che inizia a svilupparsi nella seconda metà del XX secolo ed è considerata fino ad oggi la più completa.
Poiché l'informazione si codifica e si elabora con mezzi fisici, negli ultimi vent'anni si è ricercato un modo per applicare i risultati ottenuti nel campo della fisica quantistica alla computazione, ottenendo risultati molto promettenti.
Nella teoria della computazione e della complessità si è mostrato che l'approccio quantistico risulta molto efficace ed innovativo rispetto a quello classico, tanto da ottenere una diminuzione esponenziale del numero di operazioni da compiere per risolvere alcuni problemi.
La computazione quantistica si presenta come una teoria che va contro l'intuizione e, dunque, difficilmente comprensibile (*"nessuna spiegazione concreta dei computer quantistici è possibile"* – Michel Nielsen [10]), tuttavia con il formalismo matematico è possibile spiegare ogni caratteristica della computazione quantistica in maniera chiara e precisa.

Le difficoltà fondamentali in cui si incorre nella progettazione di computer quantistici sono di natura fisica: uno dei principali ostacoli è costituito dall'interazione del sistema con l'ambiente circostante. Questo processo è chiamato "*decoherence*" o " rumore quantistico" ed è una delle fonti principali di errori. Risulta, dunque, fondamentale capire come costruire circuiti *fault tolerant*, cioè nei quali gli errori si ripercuotano in maniera limitata sul risultato. Nel 1977 da un gruppo di fisici guidato da Jon Leinaas e Jan Myrheim, presso l'Università di Oslo, sono state teorizzate alcune particelle, chiamate *anyons*, il cui comportamento può essere ben descritto sfruttando elementi topologici come il gruppo delle trecce. Come scrivono Gavin K. Brennen e Jiannis K. Pachos in

[5], "la più importante struttura matematica dietro l'evoluzione degli *anyons* è il gruppo delle trecce".
Nel 1997 Alexei Kitaev mostrò che gli *anyons* possono essere implementati in computazioni che si possono dimostrare essere "fault tolerant" proprio in virtù delle proprietà topologiche di tali particelle [9] .
L'interesse verso le possibili applicazioni degli *anyons* per la costruzione di computer quantistici è aumentato quando nel 2005 è stato scoperto da Vladimir Goldman e dai suoi colleghi presso l'Università di Stony Brook che gli *anyons* possono essere prodotti in laboratorio (nonostante questo risultato sia ancora controverso). Per eventuali approfondimenti si fa riferimento alle pubblicazioni dello stesso Vladimir Goldman, come ad esempio [3] e [4].

Negli ultimi anni, diversi fisici e matematici si sono occupati di studiare le sorprendenti connessioni tra la teoria di nodi, link e trecce (su cui si basa principalmente la natura degli *anyons*) e numerosi aspetti chiave della computazione quantistica come l'*entanglement* e l'universalità delle porte logiche quantistiche.
Le teorie che si sono sviluppate ed i risultati che si sono ottenuti in tale campo hanno dato origine ad una nuova branca della Topologia, denominata *Topologia quantistica*, che ha per esempio portato all'introduzione di molti nuovi invarianti quantistici utili per la classificazione dei link.

D'altra parte, la meccanica quantistica rappresenta sicuramente la risorsa maggiore nel campo dello sviluppo di computer innovativi e, forse, la Topologia costituirà la chiave che permetterà finalmente una sua efficace applicazione attraverso gli *anyons*.
Per questo motivo è importante analizzare a fondo il formalismo matematico su cui si basa la natura degli *anyons*, cioè la teoria delle trecce, e ricercare connessioni con la computazione quantistica.

Questa breve trattazione si concentra sulla relazione tra il gruppo di Artin delle trecce ed il gruppo delle trasformazioni unitarie enucleandone alcuni degli aspetti più semplici.
Il lavoro è strutturato in modo tale da essere accessibile anche a coloro che non conoscono la computazione quantistica e la teoria delle trecce.
Nella prima parte saranno, infatti, sintetizzati i principali concetti della computazione quantistica, con particolare attenzione a quelli impiegati nei capitoli a seguire.

Nella seconda parte si parlerà del gruppo delle trecce e delle proprietà ad esso relative, definendo anche gli strumenti di algebra che vengono impiegati nelle successive dimostrazioni.
La terza parte costituisce il vero e proprio nucleo della trattazione e si basa principalmente sugli articoli [6] e [8].
Nell'ultima parte si discuterà sommariamente la natura degli *anyons* fornendone alcune semplici rappresentazioni sempre sfruttando la teoria delle trecce.

Capitolo 2

Cenni di meccanica quantistica e computazione quantistica

In questo capitolo si presenteranno i concetti principali della computazione quantistica e del modello circuitale quantistico, fornendo le nozioni per comprendere la trattazione che segue.

2.1 I postulati della meccanica quantistica

La teoria formale della meccanica quantistica si basa su alcuni concetti fondamentali che possono essere sintetizzati nei quattro postulati che qui elenchiamo, una spiegazione più dettagliata può essere trovata in [2] ed in [11].

Postulato 1. *Ad ogni sistema fisico è associato uno spazio di Hilbert chiamato spazio degli stati del sistema. In ogni istante il sistema è completamente caratterizzato dal suo stato, che corrisponde ad un versore dello spazio degli stati associato.*

Il sistema quantistico più semplice è definito *qubit* (quantum bit) ed è descritto da uno spazio di Hilbert isomorfo a $\mathbb{C}^2$.
In $\mathbb{C}^2$ si può considerare la base canonica computazionale, che nella notazione di Dirac si scrive:

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

Allora lo stato generico di un *qubit* sarà descritto dalla sovrapposizione lineare degli stati della base:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \quad con \quad c_0, c_1 \in \mathbb{C} \;\; e \;\; |c_0|^2 + |c_1|^2 = 1$$

Si hanno, dunque, 4 parametri reali soggetti ad un vincolo. Usando la forma polare dei numeri complessi si ottiene:

$$|\psi\rangle = r_0 e^{i\phi_0}|0\rangle + r_1 e^{i\phi_1}|1\rangle = e^{i\phi_0}(r_0|0\rangle + r_1 e^{i\phi_1 - \phi_0}|1\rangle)$$

Il fattore di fase $e^{i\phi_0}$ comune a tutte le componenti non ha rilevanza fisica, come seguirà dal postulato 4, quindi può essere trascurato. Sfruttando poi la condizione di normalizzazione già imposta sopra si ottiene :

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$$

dove lo stato è parametrizzato dagli angoli θ e $\phi = \phi_1 - \phi_0$.
Tali angoli rappresentano le coordinate sferiche di un punto appartenente ad una sfera bidimensionale di raggio unitario, chiamata sfera di Bloch, nella quale gli stati contrassegnati da $|0\rangle$ e da $|1\rangle$ sono rispettivamente polo nord e sud (figura 2.1).

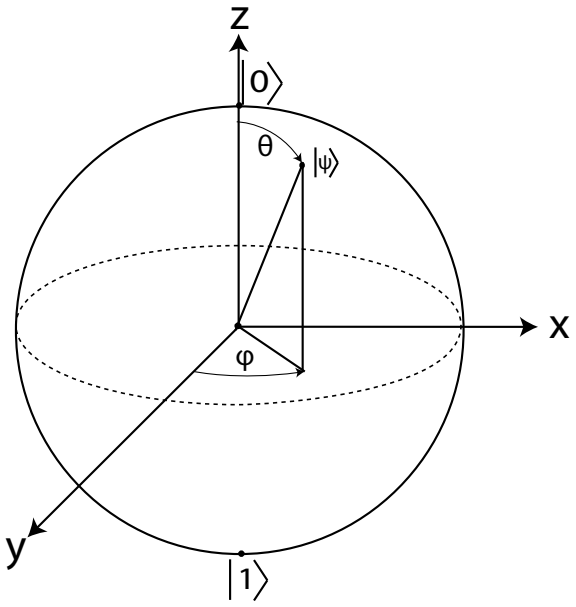

Figura 2.1: Sfera di Bloch

Postulato 2. *Lo spazio associato agli stati di un sistema composito è il prodotto tensoriale degli spazi dei singoli sottosistemi che lo costituiscono.*

Se consideriamo un sistema composto da n *qubits*, ad esso sarà associato lo spazio di Hilbert

$$(\mathbb{C}^2)^{\otimes n} = \overbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}^{n-volte}$$

Una base naturale di questo prodotto tensore è data da tutti i possibili prodotti tensoriali di n vettori che possono essere o $|0\rangle$ o $|1\rangle$ cioè da elementi del tipo:

$$|\psi_1\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle \qquad \text{con} \qquad |\psi_i\rangle = |0\rangle \text{ o } |1\rangle$$

e possono anche essere scritti come $|\psi_1\psi_2 \ldots \psi_n\rangle$.
Tale base è detta base computazionale.

Postulato 3. *Ogni processo fisico che avviene in un sistema isolato è descritto in modo completo da una trasformazione unitaria che opera sullo spazio degli stati.*

Ciò vuol dire che se consideriamo uno stato $|\psi\rangle$ di un sistema in un tempo t e lo stato $|\psi'\rangle$ in un tempo t' questi saranno legati dalla relazione $|\psi'\rangle = U|\psi\rangle$ dove U è una trasformazione unitaria, cioè una trasformazione che conserva il prodotto scalare. In formule, usando la notazione di Dirac per il prodotto scalare, si hanno le seguenti uguaglianze, valide per tutti i vettori $|\phi\rangle$, $|\psi\rangle$ dello spazio degli stati:

$$\langle U\phi|U\psi\rangle = \langle \phi|U^\dagger U|\psi\rangle = \langle \phi|\psi\rangle$$

dove la prima uguaglianza deriva direttamente dalla definizione di prodotto scalare, la seconda dalla unitarietà di U. Si può, inoltre, scrivere equivalentemente:

$$U^\dagger U = I.$$

Relativamente ad un *qubit* gli operatori unitari fondamentali sono l'identità, che lascia invariato il sistema, e gli operatori di Pauli rappresentati dalle seguenti matrici:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Vale inoltre la seguente proposizione

Proposizione 1. *Qualunque trasformazione a singolo qubit può essere ottenuta come prodotto di trasformazioni originate dalle matrici di Pauli e dalla matrice identica, a meno di un fattore di fase che, comunque, non è misurabile* [11].

Postulato 4. *Ad ogni osservabile (una qualsiasi grandezza fisica misurabile) può essere associato un operatore hermitiano M sullo spazio degli stati. Considerando la decomposizione spettrale di M:*

$$M = \sum_{m=1} \lambda_m P_m$$

dove con P_m si indicano i proiettori sugli autospazi di M, allora i possibili risultati della misura saranno i corrispondenti autovalori di M.

Consideriamo ora di misurare l'osservabile M quando il sistema si trova in uno stato $|\psi\rangle$; la probabilità di ottenere come risultato λ_m è data da:

$$P(m) = \|P_m|\psi\rangle\|^2 = \langle\psi|P_m|\psi\rangle$$

essendo

$$\langle\psi|P_m^\dagger P_m|\psi\rangle = \langle\psi|P_m P_m|\psi\rangle = \langle\psi|P_m|\psi\rangle.$$

Inoltre ogni volta che si effettua una misura ottenendo come risultato λ_m lo stato del sistema collassa sull'autovettore relativo normalizzato, cioè diventa:

$$|\psi'\rangle = \frac{P_m|\psi\rangle}{\sqrt{P(m)}}$$

In genere per effettuare le misurazioni la matrice standard usata è l'operatore di Pauli Z denotando per comodità gli autovalori con la stessa etichetta dei suoi autovettori $|0\rangle, |1\rangle$. In tal modo il risultato della misura sarà 0 se lo stato è proiettato sull'autovettore $|0\rangle$ ed 1 se lo stato viene proiettato su $|1\rangle$.
Se un sistema di un *qubit* si trova nello stato :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

misurando l'osservabile Z si otterrà il risultato 0 con probabilità α^2 ed il risultato 1 con probabilità β^2.
Il discorso può essere generalizzato ad n *qubits*, considerando l'operatore $Z^{\otimes n}$; in tal caso i possibili risultati saranno 2^n.

2.2 Circuiti e porte quantistiche

Modello circuitale classico e quantistico

Nella computazione classica un algoritmo può essere modellizzato tramite un circuito.
Un circuito è composto da porte logiche, che eseguono computazioni elementari, e da connessioni, che trasferiscono le informazioni all'interno del circuito.
Una porta logica realizza una applicazione

$$f : \{0,1\}^n \to \{0,1\}^m$$

Ricordiamo che nella computazione classica ciascun bit può assumere solo lo stato $|0\rangle$ o $|1\rangle$, lo stato di un sistema composto da n bit può essere formalizzato come:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \cdots \otimes |\psi_n\rangle, \text{ con } |\psi_i\rangle = |0\rangle \text{ o } |1\rangle.$$

Ipotizziamo ora di associare a questa porta una trasformazione lineare unitaria che agisca sui vettori che rappresentano gli stati del sistema. Per far questo è necessario che sia $m = n$. In particolare, se consideriamo lo spazio $(\mathbb{C}^2)^{\otimes n} = \overbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}^{n \quad volte}$ ed in esso la base naturale del prodotto tensore, si osserva che l'applicazione descritta manda elementi di questa base in elementi di questa base, non essendo permessi stati sovrapposti.
La trasformazione agisce, dunque, come una permutazione sugli elementi della base; pertanto la matrice associata sarà una matrice di permutazione: avrà tutti zeri tranne un unico 1 in corrispondenza di ciascuna riga e di ciascuna colonna.

Il modello circuitale può essere applicato anche alla computazione quantistica. Questa volta le unità di informazioni diventano i *qubits* e ad ogni porta logica quantistica può essere associata una qualunque matrice unitaria, non necessariamente di permutazione.

In primo luogo si osserva che, poiché ogni computazione quantistica è sempre rappresentata da una matrice unitaria, dunque si avrà sempre $m = n$. La differenza principale fra il circuito quantistico e quello classico è nella sovrapposizione di stati del sistema e nell'accessibilità alle informazioni. In un modello classico, un bit si può trovare solo negli stati della base $|0\rangle$ e $|1\rangle$, che possono essere misurati con esattezza; nel modello quantistico, invece, durante

la computazione si possono ottenere stati sovrapposti (combinazioni lineari di $|0\rangle$ e $|1\rangle$) ma il risultato della misura sarà non deterministico e, comunque, sempre o 0 o 1); l'accesso, dunque, alle informazioni è fortemente limitato.

Nei circuiti quantistici rivestono particolare importanza le porte *qubits* definite "controllate". Una porta "controllata", indicata con CU, (dove U è una porta a singolo qubit) ha la caratteristica di applicare al secondo *qubit* la porta U se il primo *qubit* si trova nello stato $|1\rangle$, mentre lascia il sistema invariato nel caso in cui lo stato del primo *qubit* sia $|0\rangle$. In questo caso il primo *qubit* è chiamato "di controllo". Se i *qubit* di controllo sono più di uno la porta si indica con CnU; in tal caso la porta U sarà applicata all'ultimo *qubit* se e solo se i primi $n-1$ si trovano nello stato $|1\rangle$.

Risulta molto utile, per comprendere il funzionamento di un circuito quantistico, la sua rappresentazione grafica. Se ne fornisce un esempio in figura 2.2 dove sono rappresentate la porta U a singolo *qubit*, che agisce solo sul secondo *qubit*, ed una porta "controllata" CU, che agisce sul secondo *qubit* ed ha il primo come *qubit* di controllo .

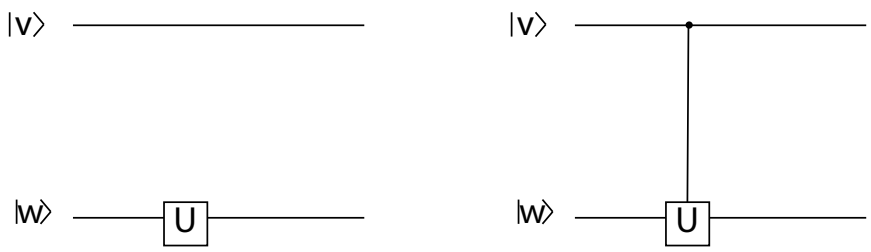

Figura 2.2: A sinistra è raffigurata la porta U, a destra la porta CU.

Universalità di una porta quantistica a due *qubits*

Definizione 1 (Insieme universale esatto di porte logiche quantistiche)**.** *Sia* $G \equiv \{G_{1,n_1}, \ldots, G_{r,n_r}\}$ *un insieme di porte quantistiche, tali che* G_{j,n_j} *agisce su* n_j *qubits per ogni* $j = 1, \ldots, r$*. Tale insieme è detto* universale esatto *se ogni trasformazione unitaria* U_N *a* n *qubits può essere decomposta nel prodotto di successive azioni delle trasformazioni* G_{j,n_j} *su differenti sottoinsiemi dei qubits in input.*

Si ha il seguente risultato:

Teorema 1 (Universalità delle porte logiche quantistiche)**.** *L'insieme* $G \equiv \{U \in U(2), CNOT\}$ *è universale, dove U(2) è il gruppo delle porte a singolo qubit, costituito, quindi, dalle trasformazioni unitarie che agiscono su uno spazio di Hilbert di dimensione 2, mentre CNOT è la porta a due qubits a cui è associata la seguente trasformazione* [2] [11].

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

La porta $CNOT$ in particolare applica al secondo *qubit* la porta NOT (rappresentata dalla matrice di Pauli X) se il primo *qubit* si trova nello stato $|1\rangle$, altrimenti lascia il sistema invariato.

Si fornisce un accenno del percorso da fare per dimostrare questo risultato. Inizialmente si mostra che ogni operazione controllata che agisce su due *qubits* può essere implementata sfruttando solo le porte di G.
In seguito si prova che la porta C_2NOT o porta Toffoli può essere costruita sfruttando solo porte $CNOT$ ed operazioni controllate agenti su due *qubits*, tramite il circuito in figura 2.3, dove $A = (1-i)/2(I+iX)$ e vale che $A^2 = X$, (X è uno degli operatori di Pauli, I la matrice identica), si indica inoltre con B la matrice aggiunta di A e si osserva che $AB = BA = I$.

In seguito si mostra che è possibile implementare con queste porte tutte le porte con n *qubits* di controllo, quindi si arriva a costruire ogni porta con gli elementi dell'insieme G.

Per costruire in maniera precisa una qualunque porta quantistica è necessario un numero infinito di porte a singolo *qubit* in aggiunta ad una specifica porta a due *qubits* (ad esempio la porta $CNOT$).
Tuttavia è possibile simulare con un grado di precisione arbitrario l'azione di una qualunque porta quantistica con un numero finito di porte quantistiche. Per valutare l'errore di approssimazione di una determinata porta quantistica è necessario definire una funzione di distanza:

Definizione 2 (Distanza tra due porte logiche quantistiche)**.** *Date due porte logiche quantistiche, rappresentate dagli operatori* D *e* D' *si definisce distanza*

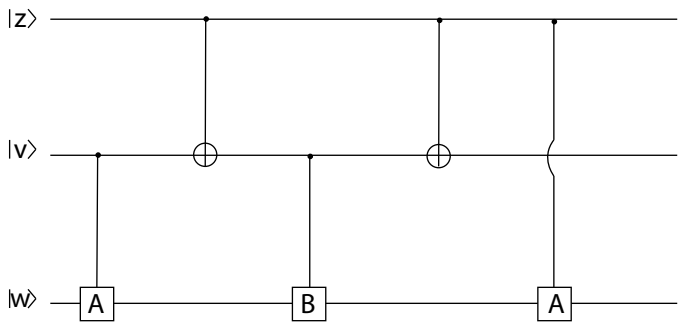

Figura 2.3: Rappresentazione della costruzione di una porta Toffoli con la porta $CNOT$e porte a singolo *qubit*. La porta NOT è rappresentata graficamente con il simbolo $\oplus$.

tra D e D' il numero reale associato alla coppia di operatori dall'applicazione $d : U(n) \times U(n) \to \mathbb{R}$:

$$d(D, D') = \max_{\langle\psi|\psi\rangle=1} \|(D - D')|\psi\rangle\|$$

Una porta quantistica U è detta approssimabile con altre porte quantistiche $U_1, \ldots, U_n$ se è possibile ottenere operatori U' arbitrariamente vicini ad U mediante circuiti finiti realizzati con le porte $U_1, \ldots, U_n$.
Si può, allora, dare la seguente definizione:

Definizione 3 (Insieme di porte quantistiche universale)**.** *Un insieme di porte quantistiche è detto universale se ogni operazione unitaria può essere approssimata con accuratezza arbitraria tramite un circuito costruito sfruttando solo le porte contenute nell'insieme stesso* [2] [11].

In particolare è possibile dimostrare ([2] e [11]) che ciascuna porta a singolo *qubit* può essere approssimata tramite le matrici seguenti:

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \quad W = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

Corollario del teorema 1 può essere considerato, quindi, il seguente asserto:

Corollario 1. *L'insieme $\{H, W, P, CNOT\}$ è universale.*

Si può osservare che per implementare una qualunque trasformazione, anche approssimata, è, comunque, sempre necessaria una porta a due *qubits* con

alcune caratteristiche fondamentali.
Non tutte le porte a due *qubits* costituiscono un insieme universale con quelle a singolo *qubit*.

2.3 Stati *entangled* e porte *entangling*

Definizione 4 (Stato *entangled*)**.** *Sia S un sistema di due qubits con base canonica $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ e sia*

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

uno stato del sistema, tale stato è entangled se e solo se non può essere scritto come prodotto tensore di singoli qubits cioè come

$$|\psi\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$$

Possiamo, ad esempio, dire che lo stato $|\psi\rangle = 1/\sqrt{2}\,(|00\rangle+|11\rangle)$ è *entangled* mentre non lo è lo stato $|\phi\rangle = 1/\sqrt{2}\,(|00\rangle+|01\rangle)$, poiché quest'ultimo può essere scritto come $|\phi\rangle = 1/\sqrt{2}\;|0\rangle \otimes (|0\rangle + |1\rangle)$.
La seguente proposizione fornisce un criterio utile per determinare se uno stato di un sistema a due *qubits* è *entangled*.

Proposizione 2 (Condizioni per uno stato *entangled*)**.** *Sia S un sistema a due qubits e sia $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ uno stato di tale sistema, allora lo stato è entangled se e solo se si ha la seguente relazione tra le componenti con cui è espresso lo stato nella base canonica:*

$$\alpha\delta \neq \beta\gamma$$

Dimostrazione. Supponiamo che lo stato $|\psi\rangle$ non sia *entangled*; allora può essere scritto come

$$|\psi\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$$

da cui calcolando i prodotti tensoriali si ottiene:

$$|\psi\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

Ne consegue che $\alpha = ac, \beta = ad, \gamma = bc, \delta = bd$ e dunque $\alpha/\beta = \gamma/\delta$; segue la tesi.

Supponiamo invece che valga

$$\alpha/\gamma = \beta/\delta = r$$

Si ha la seguente catena di uguaglianze:

$$\begin{aligned} |\psi\rangle &= \gamma(\alpha/\gamma(|00\rangle + |10\rangle) + \delta(\beta/\delta(|01\rangle + |11\rangle) = \\ &= \gamma(\alpha/\gamma(|0\rangle + |1\rangle) \otimes |0\rangle + \delta(\beta/\delta(|0\rangle + |1\rangle) \otimes |1\rangle = \\ &= \gamma(r(|0\rangle + |1\rangle) \otimes |0\rangle + \delta(r(|0\rangle + |1\rangle) \otimes |1\rangle = \\ &= (r|0\rangle + |1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) \end{aligned}$$

Da tali uguaglianze deriva che lo stato non è *entangled*. □

Si osserverà in seguito che la proprietà di una porta logica di originare stati *entangled* risulta fondamentale. In tale situazione la porta è definita *entangling*.

Definizione 5 (porta *entangling*)**.** *Sia A una porta a due qubits, allora A è definita* entangling *se e solo se esiste un vettore $|\alpha\beta\rangle = |\alpha\rangle \otimes |\beta\rangle$ tale che $A|\alpha\beta\rangle$ è uno stato* entangled.

Possiamo ora enunciare il teorema di Briylinski che lega la proprietà di una porta logica di creare stati *entangled* alla sua universalità:

Teorema 2 (di Brylinski)**.** *Una porta a due qubits unitamente a tutte le porte a singolo qubit costituisce un insieme universale se e solo se è* entangling.

Tale risultato non è banale, la dimostrazione può essere trovata in [1].

Capitolo 3

Elementi di algebra

In questo capitolo si forniscono alcune nozioni di algebra, che verranno impiegate in seguito, tra cui quelle di presentazione e rappresentazione di un gruppo.

3.1 Gruppi liberi

Definizione 6 (Monoide delle parole su un alfabeto A)**.** *Dato un insieme A sia W=$\{a_1 \dots a_n$ tale che $a_i \in A$ e $n \geq 0\}$ l'insieme delle parole su A e sia $*$ l'operazione di concatenazione, definita*

$$a_1 \dots a_n * a'_1 \dots a'_n = a_1 \dots a_n a'_1 \dots a'_n.$$

Allora $W(A) = (W(A), *)$ è un monoide, chiamato monoide delle parole sull'alfabeto A, nel quale l'elemento neutro è costituito dalla parola vuota, di lunghezza nulla.

Definizione 7 (Gruppo libero)**.** *Dato un insieme di elementi $\{a_1, \dots, a_n\}$ si definisce gruppo libero generato da $a_1, \dots, a_n$ e si indica con $\langle a_1, \dots, a_n \rangle$ il gruppo $G = (G, *)$ definito come segue. Consideriamo il monoide delle parole $W(a_1, a_1^{-1}, \dots, a_n, a_n^{-1})$, usando inoltre a_i^j come abbreviazione di $a \dots a$, j volte, se $j \geq 0$ e di $a^{-1} \dots a^{-1}$, $-j$ volte, se $j < 0$. Allora G è il gruppo che si ottiene quozientando W :*

- $w_1 a_i^j a_i^k w_2 = w_1 a_i^{j+k} w_2 \quad \forall\ i = 0 \dots n; \quad \forall\ j, k \in \mathbb{Z}, \quad \forall\ w_1, w_2 \in W$
- $w_1 a_i^0 w_2 = w_1 w_2 \qquad\qquad \forall\ i = 0 \dots n, \quad \forall\ w_1, w_2 \in W$

Relativamente ai gruppi liberi vale inoltre la seguente proposizione:

Proposizione 3. *Dato un gruppo libero su n generatori* $\langle a_1, \ldots, a_n \rangle$ *e un gruppo* G *e dati n elementi arbitrari* $g_1 \ldots g_n \in G$*, esiste ed è unico un omomorfismo*

$$\phi\langle a_1 \ldots a_n \rangle \to G$$

tale che $\phi(a_i) = g_i$*. In particolare se* $g_1, \ldots, g_n$ *generano* G*, allora* ϕ *è suriettivo.*

3.2 Presentazioni di gruppi

Definizione 8. *Si definisce presentazione di un gruppo* G *con generatori* $a_1, \ldots, a_n$ *e relazioni* $w_1, \ldots, w_l \in W(a_1, a_1^{-1}, \ldots, a_n, a_n^{-1})$ *la scrittura*

$$\langle a_1, \ldots, a_n | w_1, \ldots, w_l \rangle$$

a condizione che G *sia isomorfo al gruppo* $\langle a_1 \ldots a_n \rangle / \langle\langle w_1 \ldots w_l \rangle\rangle$*, cioè il gruppo generato dagli elementi* $a_1, \ldots, a_n$ *quozientato con il più piccolo sottogruppo normale contenente le parole* $w_1, \ldots, w_l$*.*

Sia ϕ l'omomorfismo definito nella proposizione 3 con $g_1, \ldots, g_n$ generatori di G e sia $\langle a_1 \ldots a_n \rangle / ker(\phi)$ il gruppo libero quozientato con il nucleo dell'applicazione ϕ, allora per il teorema degli omomorfismi esiste un isomorfismo ψ fra $\langle a_1 \ldots a_n \rangle / ker(\phi)$ e G.
Se $ker(\phi) = \langle\langle w_1, \ldots, w_l \rangle\rangle$ dall'isomorfismo si ottiene nuovamente la presentazione del gruppo G (figura 3.1).

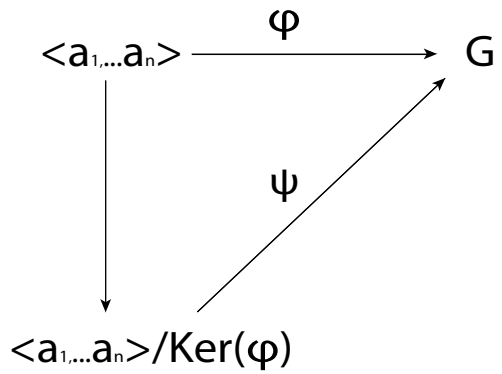

Figura 3.1: L'isomorfismo ψ.

Vale il seguente teorema:

Teorema 3. *Per ogni gruppo* $G \cong \langle a_1 \dots a_n | w_1 \dots w_l \rangle$*, per ogni gruppo* H *e per ogni collezione di elementi* $h_1 \dots h_n \in H$ *esiste ed è unico un omomorfismo* $\phi : G \to H$ *tale che* $\phi(a_i) = h_i$ *(dove si lascia implicito l'isomorfismo definito sopra tra* G *e* $\langle a_1 \dots a_n \rangle / \langle\langle w_1 \dots w_l \rangle\rangle$*) se e solo se per ogni relazione* w_j *vale la seguente proprietà:*

$$w_j = a_{i_1}^{k_1} \dots a_{i_m}^{k_m} \Longrightarrow h_{i_1}^{k_1} \dots h_{i_m}^{k_m} = id_H$$

Dimostrazione. Si osserva che, per la proposizione 3, esiste un unico omomorfismo

$$\psi : \langle a_1 \dots a_n \rangle \to \ H$$

tale che $\psi(a_i) = h_i$ per ogni scelta di $h_1 \dots h_n \in H$. L'applicazione ψ può passare a quoziente dando così origine ad un omomorfismo

$$\phi : \langle a_1 \dots a_n \rangle / \langle\langle w_1 \dots w_l \rangle\rangle \to H$$

se e solo se $\langle\langle w_1 \dots w_l \rangle\rangle \subseteq ker(\psi)$, se cioè $\psi(w_i) = id_H$ per ogni relazione w_i (figura 3.2). □

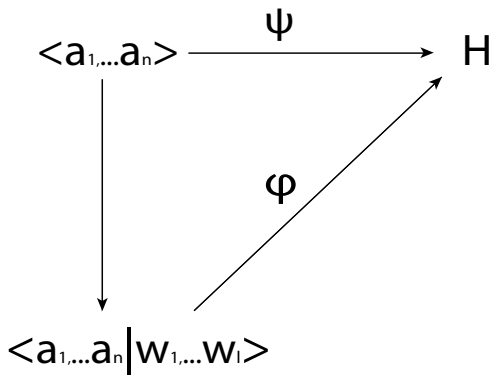

Figura 3.2: Gli omomorfismi ψ e ϕ del teorema 3.

3.3 Rappresentazioni di gruppi

Definizione 9 (Rappresentazione di un gruppo G)**.** *Si definisce* rappresentazione *di un gruppo (G,*) un omomorfismo* $p : G \to GL(V)$ *dove* $GL(V)$ *è il gruppo delle trasformazioni lineari dello spazio vettoriale* V *in se stesso.*

In particolare vale il seguente risultato che può essere considerato un corollario del teorema 3:

Corollario 2. *Dato un gruppo G ed una sua presentazione, allora una rappresentazione di G $p : G \to GL(V)$ può essere costruita definendo in modo arbitrario la sua azione su un insieme di generatori di G a condizione che le relazioni vengano rispettate.*

Dimostrazione. Il corollario segue immediatamente dal teorema 3 ponendo $H = GL(V)$. □

Capitolo 4

Il gruppo delle trecce di Artin

In questo capitolo verrà fornita la definizione di treccia e di gruppo delle trecce con particolare attenzione alle relazioni che lo caratterizzano. Approfondimenti relativi a questi argomenti possono essere trovati in [12].

4.1 Le trecce

Definizione geometrica di treccia

Definizione 10 (Treccia)**.** *Nello spazio* $\mathbb{R}^3$ *consideriamo le collezioni di punti* $A_i = (i, 0, 1)$ *e* $B_i = (i, 0, 0)$ *con i=1... n. Una curva continua che collega i punti* A_i *ai punti* B_i *è definita* monotona *rispetto alla quota se percorrendola da* A_i *a* B_i *la coordinata lungo l'asse z decresce in maniera monotona.*
Definiamo allora treccia *un insieme di curve continue monotone rispetto alla quota che non si intersecano a due a due e che collegano i punti* A_i *ai punti* B_i*. Queste sono chiamate le stringhe della treccia.*

In particolare se si chiamano le stringhe che costituiscono la treccia $s_1 \dots s_n$, una parametrizzazione generica di una treccia è una applicazione:

$$\phi : [0, 1] \times \{s_1, s_2 \dots s_n\} \to \mathbb{R}^3$$

che associa ad una coppia (z, s_i) un punto di $\mathbb{R}^3$ con le seguenti limitazioni:

- $\phi(z, s_i) = (x, y, z)\ \forall i = 1, \dots, n$ garantisce che la quota cresca in maniera monotona per ogni i.

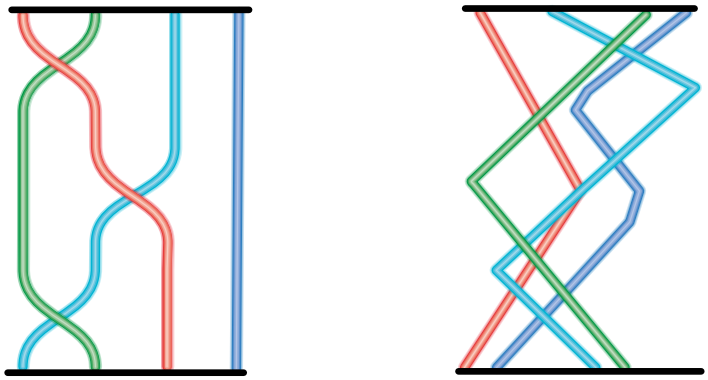

Figura 4.1: Esempi di trecce

- $\phi(z, s_i) \neq \phi(z, s_j) \quad \forall i \neq j$ garantisce che le curve siano disgiunte.

Definizione 11 (Equivalenza di trecce)**.** *Due trecce sono dette* equivalenti *se esiste una deformazione continua che porta una treccia nell'altra.*

Con deformazione continua si intende un'applicazione

$$\psi : [0, 1] \times \{s_1, s_2 \dots s_n\} \times [0, 1] \to \mathbb{R}^3$$

che associa alla terna (z, s_i, t) un punto in $\mathbb{R}^3$ in maniera continua e tale per cui per ogni t l'applicazione $\psi_t(z, s_i) = \psi(z, s_i, t)$ rispetti le due proprietà elencate sopra, cioè parametrizzi una treccia.

Trecce poligonali

Si può dimostrare che ogni treccia è equivalente ad una treccia formata da linee poligonali. Vale inoltre la seguente proposizione:

Proposizione 4. *Due trecce formate da linee poligonali sono equivalenti se e solo se sono collegate tra loro da una sequenza di trecce nella quale ciascuna è ottenuta dalla precedente attraverso il movimento elementare descritto in figura 4.2.*

La dimostrazione di questa proposizione si basa sul fatto che ogni equivalenza tra trecce poligonali può essere descritta mediante una successione finita di equivalenze elementari del seguente tipo.
Siano i lati AB e BC del triangolo ABC due segmenti della linea spezzata che costituisce una stringa di una treccia che non interseca ABC in nessun altro

punto oltre quelli di AB e BC; allora i segmenti AB e BC possono essere sostituiti con il solo segmento AB ottenendo così una treccia diversa ma equivalente a quella data (figura 4.2).
La spezzata ottenuta deve essere sempre ascendente; il movimento in figura 4.3 è, dunque, proibito.

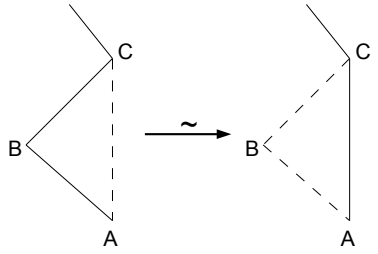

Figura 4.2: Equivalenza di trecce

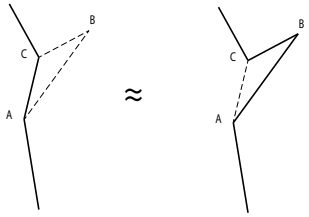

Figura 4.3: Movimento proibito

Esiste una rappresentazione bidimensionale molto intuitiva delle classi di equivalenza delle trecce tramite una proiezione sul piano xz; infatti ciascuna classe di equivalenza contiene almeno una treccia formata da linee poligonali con le seguenti proprietà:

1. Ciascun vertice è proiettato in un punto che non è proiezione di altri punti della treccia.

2. Ciascun punto del piano è proiezione al massimo di due punti interni ai segmenti le cui proiezioni si incontrano trasversalmente.

3. Le quote dei punti doppi sono tutte distinte.

Tale rappresentazione verrà sfruttata in tutte le raffigurazioni di trecce che seguono ed è stata implicitamente impiegata nella figura 4.1. D'ora in avanti,

inoltre, si parlerà indistintamente di treccia sia per denotare una classe di equivalenza, sia per denotare un particolare elemento rappresentante della stessa classe.

4.2 Il gruppo delle trecce

La struttura del gruppo delle trecce

L'insieme delle trecce con n stringhe, quozientato con la relazione di equivalenza precedentemente definita, ha una naturale struttura di gruppo. Tale gruppo è chiamato gruppo delle trecce di Artin e si indica brevemente con B_n.

Il prodotto tra due trecce a e b si ottiene comprimendo la treccia a e la treccia b a metà della loro lunghezza, lasciando fissi i punti con quota uguale ad 1 quando si contrae a e uguale a 0 quando si contrae b: l'unione delle due trecce contratte è una treccia di lunghezza uguale a quella di a e b e costituisce per definizione il prodotto tra le due trecce. Nella figura 4.4 si fornisce una rappresentazione bidimensionale del prodotto di due trecce sfruttando la proiezione sul piano xz.

Deriva facilmente dalla definizione che tale prodotto è associativo.
L'elemento neutro del gruppo è la treccia formata da n stringhe parallele, l'elemento inverso di una treccia a, denotato con a^{-1}, corrisponde all'immagine speculare della treccia a, rispetto al piano $z = 1/2$. Osserviamo a questo proposito che l'inverso dell'elemento A in figura è proprio l'elemento B, infatti la treccia AB risulta essere equivalente all'elemento neutro.

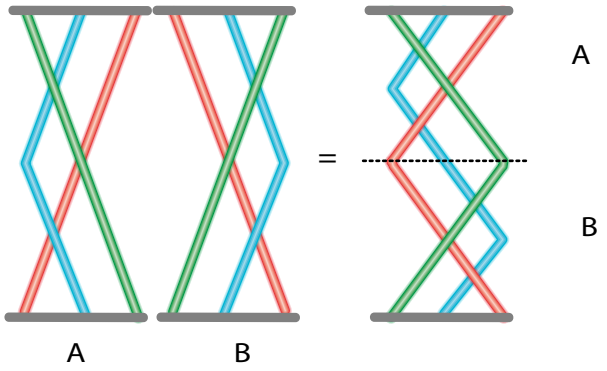

Figura 4.4: Prodotto di trecce

Presentazione di B_n

Il gruppo delle trecce può essere descritto mediante una presentazione basata su un insieme di generatori e alcune relazioni tra questi.
Si osserva che ogni elemento di B_n può essere ottenuto come prodotto di elementi del tipo b_i o b_i^{-1}, dove b_i è la treccia in cui la stringa $i-$esima incrocia una sola volta la stringa $(i+1)-$esima passandole sopra, mentre le altre stringhe non formano incroci (figura 4.5). Si ottiene così che $b_1, \ldots, b_n$ generano il

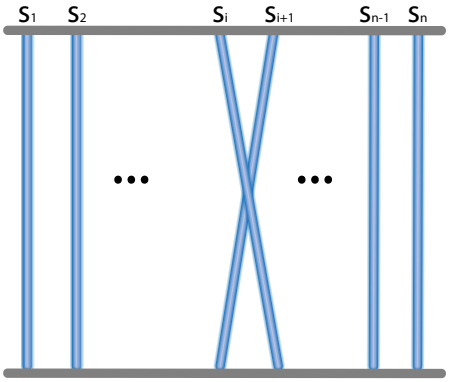

Figura 4.5: Elemento generatore b_i

gruppo delle trecce B_n.

Per comprendere quali relazioni debbano intercorrere fra i generatori $b_1 \ldots b_n$ affinché il gruppo astratto generato sia isomorfo a quello delle trecce, si devono considerare le trasformazioni per le quali non è possibile fornire una rappresentazione continua sfruttando la proiezione.
Si devono, dunque, considerare tutte le trasformazioni di trecce per le quali in un certo istante una delle tre proprietà elencate in precedenza non viene rispettata.

La proprietà (1) non è più presente se si considerano, prendendo in esame il gruppo B_2 (1), le trasformazioni in figura 4.6.
La relazione $b_i b_i^{-1} = 1$ che si ottiene è già rispettata banalmente in ogni gruppo.
Esistono numerose trasformazioni sotto la cui azione la proprietà (2) non vale, un esempio di queste è mostrato in figura 4.7.

La relazione descritta in questo caso è detta *relazione delle trecce*:

$$b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1}$$

Si può osservare che tutte le altre trasformazioni che generano situazioni in cui la (2) non è rispettata portano a relazioni riconducibili a quella descritta.

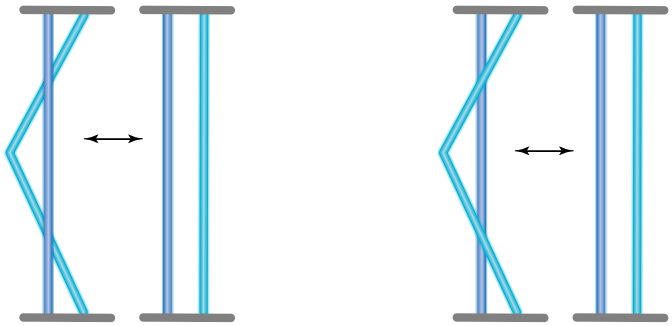

Figura 4.6: Trasformazioni che portano alla relazione banale

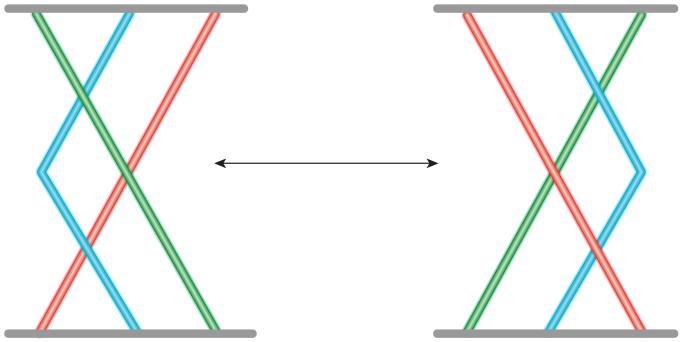

Figura 4.7: Trasformazione che porta alla relazione delle trecce

In figura 4.8 è infine mostrata la trasformazione in cui non vale più la proprietà (3). Tale trasformazione porta alla relazione

$$b_i b_j = b_j b_i \qquad \forall i, j | i - j| \geq 2$$

detta anche *commutatività lontana*.

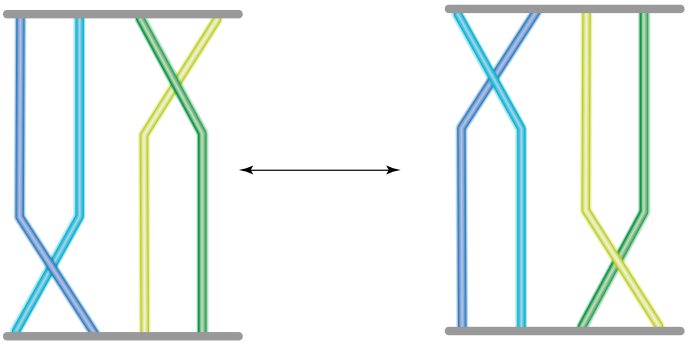

Figura 4.8: Trasformazione da cui deriva la commutatività lontana

Le relazioni trovate sono sufficienti per caratterizzare algebricamente B_n. Si può, quindi, enunciare il seguente teorema:

Teorema 4 (di Artin)**.** *Il gruppo delle trecce B_n ammette la seguente presentazione* [12]*:*

$$\langle b_1, \ldots, b_n \mid b_i b_j b_i^{-1} b_j^{-1} \ \forall i, j \text{ tali che } |i-j| \geq 2,\ b_i b_{i+1} b_i b_{i+1}^{-1} b_i^{-1} b_{i+1}^{-1} \ \forall i = 1 \ldots n \rangle$$

.

Capitolo 5

Operatori treccia unitari e porte quantistiche

In tale capitolo sarà data la definizione di operatore treccia, quindi saranno presentati gli operatori treccia unitari e verranno discusse alcune delle loro proprietà. Approfondimenti in relazione a tali argomenti possono essere trovati in [8] ed in [6].

5.1 Operatori treccia

Consideriamo uno spazio vettoriale V ed il suo n-uplo prodotto tensore $V^{\otimes n}$, sia poi $End(V^{\otimes n})$ l'insieme di tutti gli operatori lineari $A : V^{\otimes n} \to V^{\otimes n}$.
Tale insieme costituisce un gruppo con l'usuale operazione di composizione.

Proposizione 5. *Per ogni elemento R operatore su $V \otimes V$ vale che:*

$$(R \otimes I \otimes I)(I \otimes I \otimes R) = (I \otimes I \otimes R)(R \otimes I \otimes I)$$

Dove I è la matrice identità 2×2.

Dimostrazione. Osserviamo che $I \otimes I = I_4$ (la matrice identica 4×4). Si ottiene dunque

$$(R \otimes I_4)(I_4 \otimes R) = R \otimes R = (I_4 \otimes R)(R \otimes I_4)$$

□

Tale proprietà può essere generalizzata. Si ha infatti che $\forall i, j | i-j| \geq 2$:

$$\begin{aligned}(I^{\otimes i-1} \otimes \mathcal{R} \otimes I^{\otimes n-i-1})(I^{\otimes j-1} \otimes \mathcal{R} \otimes I^{\otimes n-j-1}) \quad = \\ = (I^{\otimes j-1} \otimes \mathcal{R} \otimes I^{\otimes n-j-1})(I^{\otimes i-1} \otimes \mathcal{R} \otimes I^{\otimes n-i-1})\end{aligned}$$

5.2 L'equazione di Yang-Baxter

Sia R un operatore su $V \otimes V$ allora l'equazione operatoriale

$$(\mathcal{R} \otimes I)(I \otimes \mathcal{R})(\mathcal{R} \otimes I) = (I \otimes \mathcal{R})(\mathcal{R} \otimes I)(I \otimes \mathcal{R})$$

è detta equazione di Yang-Baxter; non tutti gli operatori su $V \otimes V$ sono soluzioni dell'equazione di Yang-Baxter.
Si può ora dare la seguente definizione:

Definizione 12 (Operatore treccia)**.** *Un operatore lineare $R : V \otimes V \to V \otimes V$ è chiamato operatore treccia se soddisfa l'equazione di Yang-Baxter.*

Dye nel suo articolo [6] raggiunge i seguenti risultati relativamente alle soluzioni dell'equazione di Yang-Baxter:

Proposizione 6. *Se R è soluzione dell'equazione di Yang-Baxter allora :*

- *Se $\alpha \in \mathbb{C}$ ed ha norma unitaria allora anche αR è soluzione.*
- *Se Q è una matrice invertibile $Q : V \to V$ allora anche*

  $$A = (Q \otimes Q)R(Q \otimes Q)$$

  è una soluzione.
- *Se R è invertibile allora R^{-1} è una soluzione.*

5.3 Soluzioni unitarie all'equazione di Yang-Baxter

Si ricorda che le porte quantistiche sono rappresentate solo da operatori unitari; se si vogliono, dunque, considerare operatori treccia come porte quantistiche sarà necessario che siano anche unitari.

Su questo problema verte la seconda parte dell'articolo [6] di Dye da cui si evincono i seguenti risultati:

Teorema 5 (Soluzioni unitarie dell'equazione di Yang-Baxter)**.** *Le matrici* 4×4 *che rappresentano gli operatori soluzioni unitarie dell'equazione di Yang-Baxter si dividono in 4 famiglie. Ogni soluzione ha la forma:*

$$kARA^{-1}T$$

dove k *è un qualunque complesso di norma unitaria,* $A = Q \otimes Q$*, dove* $Q = \begin{pmatrix} w & x \\ y & z \end{pmatrix}$ *è una matrice invertibile soggetta alle limitazioni descritte sotto, inoltre*

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

e R *ha una delle seguenti forme:*

Famiglia 1 *:*

$$R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & q & 0 \\ 0 & 0 & 0 & r \end{pmatrix}$$

con la restrizione che $1 = p\overline{p} = q\overline{q} = r\overline{r}$*.*

Per gli elementi della matrice Q *vale la restrizione:*

$$y = -\frac{w\overline{x}}{\overline{z}}$$

Famiglia 2 *:*

$$R = \begin{pmatrix} 0 & 0 & 0 & p \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ q & 0 & 0 & 0 \end{pmatrix}$$

con la restrizione che $|pq| = 1$*. Inoltre vi devono essere le seguenti relazioni fra gli elementi di* R *e* Q*:*

$$p = \frac{(x\overline{x} + z\overline{z})(\overline{w}x + \overline{y}z)}{(w\overline{w} + y\overline{y})(w\overline{x} + y\overline{z})}$$

$$q = \frac{(w\overline{w} + y\overline{y})(w\overline{x} + y\overline{z})}{(x\overline{x} + z\overline{z})(\overline{w}x + \overline{y}z)}$$

Famiglia 3 *:*

$$R = \begin{pmatrix} 0 & 0 & 0 & p \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ q & 0 & 0 & 0 \end{pmatrix}$$

sempre con la restrizione che $|pq| = 1$*. Per gli elementi della matrice* Q *vale la restrizione:*

$$y = -\frac{w\overline{x}}{\overline{z}}$$

Inoltre fra gli elementi di Q *e* R *devono valere le seguenti relazioni:*

$$p\overline{p} = \frac{(z\overline{z})^2}{(w\overline{w})^2}$$

$$q\overline{q} = \frac{(w\overline{w})^2}{(z\overline{z})^2}$$

Famiglia 4 *:*

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

Non vi sono restrizioni sulla matrice Q*.*

Dalla classificazione di Dye si possono ricavare alcune soluzioni unitarie particolari che saranno utili di seguito, inoltre si può provare che tutte le altre soluzioni unitarie sono simili a questi tipi di matrici:

$$R = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 1 \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$R' = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & 0 & d \end{pmatrix} \qquad R'' = \begin{pmatrix} 0 & 0 & 0 & a \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ d & 0 & 0 & 0 \end{pmatrix}$$

dove a,b,c e d sono numeri complessi di norma unitaria.
In particolare dalla prima famiglia del teorema di Dye è facile ottenere matrici del tipo di R' prendendo come Q la matrice identica e ponendo $k = a$, $kp = b$, $kq = c$ e $kr = d$.

5.4 Operatori treccia e porte logiche quantistiche

Considerando le matrici R,R',R'' viste prima si osserva che queste costituiscono porte logiche quantistiche a due *qubits*.

Analizziamo in primo luogo l'azione di R sugli elementi della base canonica:

$$R|00\rangle = (1/\sqrt{2})|00\rangle - (1/\sqrt{2})|11\rangle \qquad R|01\rangle = (1/\sqrt{2})|01\rangle + (1/\sqrt{2})|10\rangle$$

$$R|10\rangle = -(1/\sqrt{2})|01\rangle + (1/\sqrt{2})|10\rangle \quad R|11\rangle = (1/\sqrt{2})|00\rangle + (1/\sqrt{2})|11\rangle$$

Si osserva che la matrice costituisce proprio il cambiamento di base dalla canonica alla base di Bell per gli stati *entangled*.
Analizziamo ora l'azione delle matrici R' e R'' sugli elementi della base: tale calcolo sarà utile in seguito:

$$R'|00\rangle = a|00\rangle, \quad R'|01\rangle = c|10\rangle, \quad R'|10\rangle = b|01\rangle, \quad R'|11\rangle = d|11\rangle.$$

$$R''|00\rangle = d|11\rangle, \quad R''|01\rangle = b|01\rangle, \quad R''|10\rangle = c|10\rangle, \quad R''|11\rangle = a|00\rangle.$$

Capitolo 6

Gli operatori treccia sono porte quantistiche universali

In questo capitolo sarà affrontata la dimostrazione dell'universalità degli operatori trovati nel capitolo precedente ed analizzate alcune loro caratteristiche.

Teorema 6 (universalità della porta R)**.** *Sia R la porta logica quantistica espresse in base canonica dalla matrice:*

$$R = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 1 \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}$$

Tale porta è universale.

Dimostrazione. La tesi deriva immediatamente dal teorema di Brylinski (teorema 2 cap.2) poiché si ottengono stati *entangled* applicandola a tutti gli elementi della base canonica. □

Tuttavia è degna di menzione la dimostrazione diretta computazionale fornita in [8] che mira a costruire la porta $CNOT$ per mezzo di porte a singolo *qubit* e della porta R. Infatti si ha

$$CNOT = (A \otimes B)R(C \otimes D)$$

dove:

$$A = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \qquad B = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$$

$$C = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} \qquad D = \begin{pmatrix} -1 & 0 \\ 0 & -i \end{pmatrix}$$

Teorema 7 (Condizioni per l'universalità di R' ed R'')**.** *Le matrici R' ed R'' costituiscono porte quantistiche universali se e solo se vale fra i termini non nulli di ciascuna delle due matrici la relazione:*

$$ad - bc \neq 0$$

Dimostrazione. Consideriamo un generico stato che non sia *entangled*. Dalla proposizione 2 (cap.2) si ha che lo stato può essere scritto come

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \quad con \quad \alpha\delta = \beta\gamma$$

Sfruttando la proprietà di linearità ed il calcolo fatto in precedenza dell'azione delle due matrici sulla base canonica si ottiene:

- $R'|\psi\rangle = \alpha R'|00\rangle + \beta R'|01\rangle + \gamma R'|10\rangle + \delta R'|11\rangle =$

  $\alpha a|00\rangle + \beta c|01\rangle + \gamma b|10\rangle + \delta d|11\rangle$

- $R''|\psi\rangle = \alpha R''|00\rangle + \beta R''|01\rangle + \gamma R''|10\rangle + \delta R''|11\rangle =$

  $\alpha d|00\rangle + \beta b|01\rangle + \gamma c|10\rangle + \delta a|11\rangle$

Deriva da ciò che la matrice R' non è *entangling* solo nel caso in cui si verifichi la relazione:

$$\alpha a \delta d = \beta c \gamma b$$

Tuttavia nella relazione possono essere semplificati i termini $\alpha, \beta, \gamma, \delta$ sfruttando il fatto che per ipotesi $\alpha\delta = \beta\gamma$, dunque si ottiene la condizione cercata.
Lo stesso vale per la matrice R''.
Ora è possibile applicare il teorema di Brylinski per ottenere la tesi. □

Capitolo 7

Generalizzazione e rappresentazione del gruppo delle trecce

In questo capitolo sarà data una rappresentazione unitaria del gruppo delle trecce sfruttando gli oggetti definiti in precedenza ed una sua generalizzazione.

7.1 Una rappresentazione del gruppo delle trecce

Consideriamo il gruppo delle trecce di Artin ed il gruppo degli automorfismi dell' n-simo prodotto tensore di uno spazio vettoriale V.
Sia poi R una soluzione invertibile dell'equazione di Yang-Baxter. Vale allora il seguente teorema:

Teorema 8. *Esiste una rappresentazione:*

$$rep_n : B_n \to Aut(V^{\otimes n}) \quad tale \quad che \quad rep_n(b_i) = I^{\otimes i-1} \otimes \mathcal{R} \otimes I^{\otimes n-i-1}$$

Dimostrazione. Dal corollario 2 (Cap.2) si ottiene che la rappresentazione rep_n esiste B_n se sono rispettate le relazioni, cioè:

- $rep_n(b_i)rep_n(b_{i+1})rep_n(b_i) = rep_n(b_{i+1})rep_n(b_i)rep_n(b_{i+1}) \quad \forall i \in \mathbb{N}$

- $rep_n(b_i)rep_n(b_j) = rep_n(b_j)rep_n(b_i) \qquad \text{con } |i-j| \geq 2$

Dalla prima relazione esplicitamente è:

$$\overbrace{(I^{\otimes i-1} \otimes R \otimes I^{\otimes n-i-1})}^{rep_n(b_i)}\overbrace{(I^{\otimes i} \otimes R \otimes I^{\otimes n-i-2})}^{rep_n(b_{i+1})}\overbrace{(I^{\otimes i-1} \otimes R \otimes I^{\otimes n-i-1})}^{rep_n(b_i)} =$$

$$= \overbrace{(I^{\otimes i} \otimes R \otimes I^{\otimes n-i-2})}^{rep_n(b_{i+1})}\overbrace{(I^{\otimes i-1} \otimes R \otimes I^{\otimes n-i-1})}^{rep_n(b_i)}\overbrace{(I^{\otimes i} \otimes R \otimes I^{\otimes n-i-2})}^{rep_n(b_{i+1})}$$

A questo punto si osserva che la relazione è soddisfatta se R è soluzione dell'equazione di Yang-Baxter, proprietà facilmente verificabile.
La seconda relazione diventa:

$$(I^{\otimes i-1} \otimes \mathcal{R} \otimes I^{\otimes n-i-1})(I^{\otimes j-1} \otimes \mathcal{R} \otimes I^{\otimes n-j-1}) \quad =$$
$$= (I^{\otimes j-1} \otimes \mathcal{R} \otimes I^{\otimes n-j-1})(I^{\otimes i-1} \otimes \mathcal{R} \otimes I^{\otimes n-i-1})$$

che risulta soddisfatta per ogni operatore su $V \otimes V$ grazie alla Proposizione 5 (cap.5). □

Nella figura 7.1 che segue si fornisce una rappresentazione grafica dell'equazione di Yang-Baxter per l'operatore R, mediante il gruppo delle trecce.

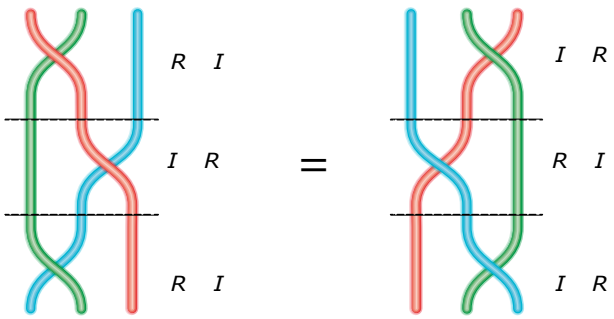

Figura 7.1: Rappresentazione grafica dell'equazione di Yang-Baxter

7.2 Il gruppo delle trecce esteso

Al fine di costruire una relazione fra porte quantistiche ed il gruppo delle trecce è necessario rendere quest'ultimo più generico aggiungendovi degli elementi che nella rappresentazione possano corrispondere alle porte a singolo *qubit*.

Per far questo consideriamo un generico gruppo G con elemento neutro e ed il suo prodotto diretto $n-$volte, G^n
Siano poi

$$h_i : G \to G^n$$

funzioni definite nel seguente modo:

$$h_i(g) \longmapsto (\overbrace{e, e \ldots, e}^{i-1 \ volte}, g \overbrace{e, e, e \ldots, e}^{n-i \ \ volte})$$

Si può allora osservare che G^n è generato dagli elementi del tipo $h_i(g)$ con $g \in G$ e $i = 1 \ldots n$, inoltre vale la proprietà che se $i \neq j$ allora

$$h_i(g)h_j(g') = h_i(g)h_j(g')$$

Possiamo ora definire una estensione del gruppo delle trecce di Artin: GB_n è formato da tutti i prodotti formali fra gli elementi di B_n e quelli di G, modulo le relazioni:

$$h_i(g)b_j = b_j h_i(g) \qquad\qquad \forall i < j \text{ o } i > j + 1$$

dove con $h_i(g)$ e b_j si indicano i generatori rispettivamente di G^n e di B_n.

Si noti che nel gruppo appena definito continuano a valere le relazioni presenti in B_n (l'equazione di Yang-Baxter e la commutatività lontana) solo se nel prodotto non sono presenti elementi di G; tali proprietà, invece, non sono rispettate in presenza di elementi di G.

Si può fornire una rappresentazione grafica di GB_n come per il gruppo delle trecce di Artin.
Un generatore di B_n, b_i, viene rappresentato come di consuetudine con la sovrapposizione della i-sima stringa sulla i+1-sima.
Un generatore di G^n, $h_i(g)$ viene rappresentato con un punto posto sulla i-sima stringa etichettato con g (l'elemento di G ad esso relativo).

La proprietà del gruppo GB_n sopra enunciata indica che nella rappresentazione i punti possono essere mossi lungo le stringhe a cui appartengono se queste non si sovrappongono fra loro.
Si osserva che nella rappresentazione non è possibile che un punto possa essere mosso lungo una stringa se questa passa sopra o sotto ad un'altra.
Se invece non sono presenti punti etichettati valgono le usuali relazioni delle trecce.
Si forniscono alcuni esempi per comprendere quali relazioni valgono all'interno

di questo gruppo, sfruttando anche la rappresentazione grafica. In tali esempi A sarà un generico elemento di G.

Es. 1 Consideriamo il gruppo GB_2, in esso vale l'uguaglianza:

$$h_1(A)b_2 = b_2h_1(A)$$

Tale uguaglianza deriva dalla relazione scritta sopra, poiché in questo caso $i < j$ (Figura 7.2).

Es. 2 Sempre nel gruppo GB_2 si ha:

$$h_1(A)s_1 \neq s_1h_1(A)$$

In tal caso si ha che $i = j$: la relazione non sussiste più. (Figura 7.3)

Es. 3 Consideriamo il gruppo GB_4, in esso vale l'uguaglianza:

$$h_1(A)b_2b_3b_2 = h_1(A)b_3b_2b_3 = b_3b_2b_3(h_1(A))$$

Tale uguaglianza è dovuta alla relazione delle trecce che viene rispettata in questo caso. (Figura 7.4)

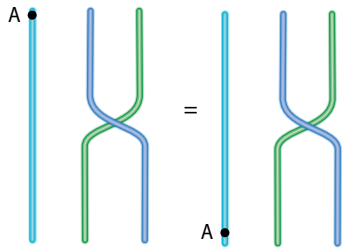

Figura 7.2: Rappresentazione grafica del primo esempio

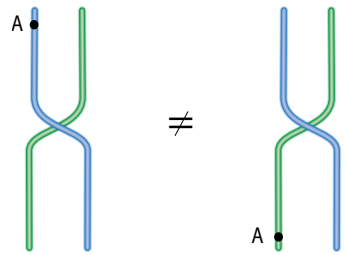

Figura 7.3: Rappresentazione grafica del secondo esempio

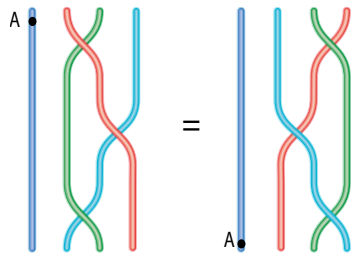

Figura 7.4: Rappresentazione grafica del terzo esempio

Consideriamo ora ψ rappresentazione del gruppo G:

$$\psi : G \to Aut(V)$$

Esso induce una naturale rappresentazione del gruppo G^n:

$$\psi^{\otimes n} : G^n \to Aut(V^{\otimes n}),$$

in modo tale che

$$\psi^{\otimes n}(g_1, g_2 \ldots, g_n) = \psi(g_1) \otimes \psi(g_2) \otimes \cdots \otimes \psi(g_n)$$

Se il gruppo G è un sottogruppo di $Aut(V)$ la rappresentazione ψ diventa l'inclusione di G in $Aut(V)$ e di conseguenza la rappresentazione $\psi^{\otimes n}$ risulta definita nel seguente modo:

$$\psi^{\otimes n}(g_1, g_2 \ldots, g_n) = g_1 \otimes g_2 \otimes \cdots \otimes g_n$$

Cioè, se i singoli elementi di G sono matrici allora gli elementi di G^n saranno associati ai prodotti tensoriali di tali matrici.
Prendendo in particolare G = U(2), dove U(2) è il gruppo delle matrici unitarie 2×2, che può esser visto come il gruppo delle porte a singolo *qubit* e sfruttando la descrizione formale del gruppo GB_n, si può definire la rappresentazione:

$$\Gamma : U(2)B_n \to Aut(V^{\otimes n})$$

tale che:

- $\Gamma(h_i(g)) = h_i(g) = \overbrace{I \otimes I \cdots \otimes I}^{i-1 \quad volte} \otimes g \otimes \overbrace{I \otimes I \otimes I \cdots \otimes I}^{n-i \quad volte}$
- $\Gamma(b_i) = \overbrace{I \otimes I \cdots \otimes I}^{i-1 \quad volte} \otimes R \otimes \overbrace{I \otimes I \otimes I \cdots \otimes I}^{n-i-1 \quad volte}$

Naturalmente tutte le proprietà dimostrate per il gruppo GB_n continuano a valere per $U(2)B_n$; inoltre anche la rappresentazione grafica definita per GB_n si applica a $U(2)B_n$.
Si deve osservare che in questo caso il prodotto diretto diviene il prodotto tensore e che i punti etichettati rappresentano matrici appartenenti a $U(2)$.

In particolare relativamente agli esempi di cui si è discusso in precedenza, l'elemento A di G, diventa in questo caso una matrice unitaria 2×2 e le identità o disuguaglianze possono essere riscritte sfruttando la notazione con il prodotto tensore:

Es. 1

$$(A \otimes I \otimes I)(I \otimes R) = A \otimes R = (I \otimes R)(A \otimes I \otimes I)$$

Es. 2

$$(A \otimes I)R \neq R(A \otimes I)$$

Es. 3

$$\begin{aligned}
& (A \otimes I \otimes I \otimes I)(I \otimes R \otimes I)(I \otimes I \otimes R)(I \otimes R \otimes I) = \\
= \; & (A \otimes I_6)(I \otimes ((R \otimes I)(I \otimes R)(R \otimes I))) = \\
= \; & (A \cdot I) \otimes I_6(R \otimes I)(I \otimes R)(R \otimes I) = \\
= \; & (I \cdot A) \otimes (I \otimes R)(R \otimes I)(I \otimes R) \cdot I_6 = \\
= \; & (I \otimes ((I \otimes R) \otimes (R \otimes I)(I \otimes R)) \cdot (A \otimes I_6) = \\
= \; & (I \otimes I \otimes R)(I \otimes R \otimes I)(I \otimes I \otimes R)(A \otimes I \otimes I \otimes I)
\end{aligned}$$

Si può allora enunciare il seguente teorema:

Teorema 9. *Ogni computer quantistico ha le sue trasformazioni unitarie base nell'immagine di* Γ.

Dimostrazione. Le tesi segue direttamente dall'universalità della matrice R (Teorema (6)). □

Il teorema implica che in linea teorica un qualunque circuito può essere scritto sfruttando il gruppo delle trecce esteso ed in particolare la sua rappresentazione grafica.
Si ha inoltre che in tutti i tratti del circuito in cui non vi sono trasformazioni a singolo *qubit* valgono le relazioni delle trecce.

In figura 7.5 sono date rappresentazioni delle porte R e $CNOT$.
ISi osserva che, per la rappresentare la porta $CNOT$, si usa la fattorizzazione

$$CNOT = (A \otimes B)R(C \otimes D)$$

presentata nel teorema 6 (cap.6).
Si osserva inoltre che la rappresentazione della porta $CNOT$ costituisce la chiave per rappresentare ogni circuito: sarà sufficiente, a questo scopo, decomporre l'azione del circuito in porte $CNOT$ e porte a singolo qubit.

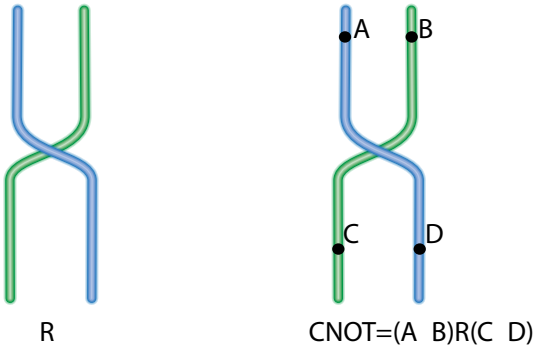

Figura 7.5: Rappresentazione della costruzione della porta $CNOT$ con la porta R e porte a singolo *qubit*

Capitolo 8

Breve introduzione agli anyons

In questo capitolo si darà un cenno del concetto *anyon* e delle sue relazioni con il gruppo delle trecce.
Per approfondire ci si può ricondurre a [5].

8.1 Bosoni e fermioni

Nello spazio tridimensionale le particelle puntiformi possono essere *bosoni* o *fermioni* a seconda del comportamento delle loro funzioni d'onda: se due particelle identiche permutano scambiandosi di posto la funzione d'onda può acquisire segno negativo (*fermioni*) o positivo (*bosoni*).

Una interpretazione topologica di questo fatto può essere data assumendo che ogni singolo scambio risulta in un fattore di fase del tipo $e^{i\phi}$.
Si osserva che lo spazio tridimensionale meno un numero finito di punti ha gruppo fondamentale banale, cioè ogni percorso può essere deformato fino al percorso banale, ciò implica che la funzione d'onda di una particella dopo una circuitazione completa attorno ad un'altra risulti identica a quella di partenza. In questo caso,dunque, deve essere $e^{i\phi}e^{i\phi} = 1$ da cui $\phi = 0$ o π.

8.2 *Anyons*

La situazione cambia se si considera uno spazio bidimensionale, poiché il piano meno un numero finito di punti non ha gruppo fondamentale nullo. In questo caso una particella che circuita attorno ad un'altra uguale acquisisce un fattore di fase che può non essere banale. Risulta conveniente sfruttare le

world lines per stabilire la posizione spazio-temporale degli *anyons*; in questo modo gli scambi di *anyons* possono facilmente essere descritti intrecciando le loro *world lines* .

Si ipotizza che gli *anyons* siano intrappolati in un piano e che, dunque, le *world lines* relative abbiano 2 dimensioni spaziali ed una temporale.
In particolare nell'esempio in figura 8.1 sono generate dal vuoto due coppie di *anyons* e anti-*anyons* $(a, \overline{a})$ e $(b, \overline{b})$ con un processo fisico locale.
In seguito l'*anyon* a e l'*anyon* b sono fatti circolare uno attorno all'altro; dunque le loro *world lines* si intrecciano. Infine le coppie corrispondenti vengono fuse. La fusione della coppia di stati c e $\bar{c}$ potrebbe non risultare nel vuoto, perché il processo di intreccio potrebbe aver avuto l'effetto di modificare lo stato interno di uno degli *anyons*. I risultati della fusione sono gli *anyons* c e $\overline{c}$ che possono essere fusi di nuovo ottenendo il vuoto.

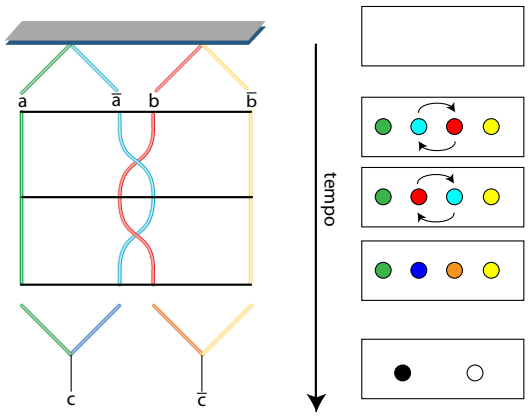

Figura 8.1: Le *world lines* di *anyons* in 2+1 dimensioni. A destra si fornisce la rappresentazione nelle due dimensioni spaziali relativa ad ogni fase del processo.

Bibliografia

[1] Brylinski J L e Brylinski R, *Mathematics of Quantum Computation*, Boca Raton, FL:Chapman and Hall/CRC,2002.

[2] C. Toffalori, F. Corradini, S. Leonesi, S. Mancini, *Teoria della commutabilità e della complessità*, Mc Graw-Hill, 2005.

[3] F. E. Camino, W. Zhou e V. J. Goldman, *Realization of a Laughlin quasiparticle interferometer: Observation of fractional statistics* , Phys. Rev. B 72, 075342, 2005.

[4] F. E. Camino, W. Zhou e V. J. Goldman, *Transport in the Laughlin quasiparticle interferometer: Evidence for topological protection in an anyonic qubit* , Phys. Rev. B 74, 115301, 2006.

[5] G. K. Brennen e J.K. Pachos, *Why should anyone care about computing with anyone*, preprint on line: arXiv:quant-ph/0704.2241v2, settembre 2007.

[6] H. A. Dye, *Unitary Solution to the Yang-Baxter equation*, Quantum Information Processing 2 117(preprint online: arXiv: preprint quant-ph/0211050v3), agosto 2003.

[7] J. Preskill *Lecture Notes for Physics 219: Quantum Computation*, California Institute of Technology, Giugno 2004.

[8] L. H Kauffman e S. J Lomonaco Jr, *Braiding operatore are universal quantum gates*, New Journal of Physics 6 134, ottobre 2004.

[9] M. H.Freedman, A. Kitaev, M. J. Larsen e Z. Wang, *Topological Quantum Computation* . Bullettin of the American Mathematical Society, Volume 40, pubblicato elettronicamente il 10 ottobre 2002.

[10] M. A. Nielsen, *Quantum computing for everyone*, Online:http://michaelnielsen.org/blog/quantum-computing-for-everyone, agosto 2008.

[11] M. A. Nielsen e I. L.Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press,1999.

[12] V.V. Prasolov e A.B. Sossinsky, *Knots, Links, Braids and 3-Manifolds-An Introduction to the New Invariants in Low-Dimensional Topology*, American Mathematical Society (Providence, Rhode Island),1997.