Università degli studi di Pavia

Facoltà di scienze matematiche, fisiche e naturali

CORSO DI LAUREA MAGISTRALE IN SCIENZE FISICHE

Universalità in teorie probabilistiche

Relatore

Chiarissimo Prof. Giacomo Mauro D'Ariano

Correlatore

Dott. Paolo Perinotti

Tesi di laurea di

Alessio Belenchia

Anno Accademico 2011/2012

Indice

Introduzione **3**

1 Computazione Quantistica **8**
1.1 Introduzione 8
1.2 Il Formalismo dei Circuiti Quantistici 10
1.2.1 Circuiti Classici 10
1.2.2 Circuiti quantistici 17
1.2.3 Gate di singolo qubit e gate locali 19
1.2.4 Control NOT 21
1.2.5 Universalità esatta e approssimata 23
1.3 Universalità del CNOT 24
1.3.1 Prima parte: universalità delle unitarie a due livelli . . . 24
1.3.2 Seconda parte: controlled gate 27
1.3.3 Terza parte: conclusione della dimostrazione 29
1.4 Universalità dei gate entanglanti 29
1.4.1 Dimostrazione di Brylinsky e RQT 31

2 Teorie Operazionali **33**
2.1 Introduzione 33
2.2 Formalismo delle OPT 34
2.3 Teoria Quantistica in dimensione finita 37
2.3.1 Discriminabilità Locale 40
2.4 Teoria quantistica su spazi reali 41
2.4.1 Bit, Rebit e Qubit 41
2.4.2 Equivalenza con la formulazione operazionale 43
2.4.3 Bilocal tomography 48

3 Dimostrazione per Induzione **51**
3.1 Dimostrazione: caso standard 51
3.1.1 Risultati preliminari 53
3.1.2 Induzione 56

3.1.3 Conclusione della dimostrazione 57
3.2 Dimostrazione:caso della RQT 57
3.2.1 Induzione 59
3.2.2 Universalità debole 60

Conclusioni **61**

A **64**

64
A.1 Elementi di Teoria dei Gruppi 64
A.2 Gruppi e algebre di Lie 65
A.2.1 Gruppi di Lie: caso generale 66
A.2.2 Gruppi Classici 69
A.2.3 Algebre di Lie e mappa esponenziale 71

B **76**

76
B.1 Gruppi Ortogonale e Unitario 76

C **83**
C.1 Un risultato importante 83

Bibliografia **85**

Introduzione

L'assiomatizzazione della Teoria Quantistica, a partire da assiomi di carattere fisico, è stato un problema aperto sin dalla nascita della meccanica quantistica negli anni '20. Dal punto di vista matematico la teoria ha solide fondamenta, come descritte nel lavoro fondamentale di von Neumann del 1932. Nei libri standard di meccanica quantistica la teoria è introdotta dicendo che ad ogni sistema fisico è associato uno spazio di Hilbert separabile, che gli stati di un sistema fisico sono raggi unitari in questo spazio e che le osservabili sono rappresentate da operatori autoaggiunti. Questo tipo di formulazione, per quanto matematicamente consistente e predittivamente potente, si basa sull'assunzione a priori di una struttura matematica che non è giustificata sulla base di principi fisici. Lo stesso von Neumann si dichiarò avverso alla sua stessa formulazione matematica arrivando a dire: *I don't belive in Hilbert space anymore*, come riportato da Birkhoff nel 1961. La situazione della Teoria Quantistica, fino a pochi anni fa, era quella di una teoria con postulati aventi una traduzione matematica ben precisa ma che non si riuscivano a ritradurre nel linguaggio della fisica. L'obbiettivo principale dei vari tentativi di assiomatizzazione che si sono susseguiti è quindi sempre stato di riuscire a derivare la struttura matematica della teoria quantistica (matematica degli spazi di Hilbert o $C^* - algebre$) a partire da postulati di natura fisica, con ovviamente una precisa traduzione in termini matematici. Resisi conto dell'importanza di una assiomatizzazione della teoria quantistica, von Neumann e Birkhoff inaugurarono un filone di ricerca ancora attivo che è quello della Quantum Logic. In questa direzione sono notevoli i lavori di Mackey, Jauch e Piron degli anni '60. In seguito, negli anni '80, Ludwig inizio un programma di assiomatizzazione attraverso un approcio operazionale basato sui concetti di preparzione e apparato misuratore la cui combinazione, nei modi dettati dai postulati, dava le probabilità degli outcome di esperimenti. Tuttavia Ludwig non riuscì nell'impresa di derivare la struttura dello spazio di Hilbert a partire da soli assiomi di carattere operazionale.

Negli ultimi dieci anni il progetto di ricostruire la Teoria Quantistica a partire da assiomi fisicamente fondati ha ripreso vigore grazie, tra i vari, al lavoro di Hardy[25]. In particolare l'attenzione di una grossa parte della comunità scien-

tifica interessata ai fondamenti della teoria quantistica si è concentrata sulla Quantum Information.

La Quantum Information nasce sostanzialemente negli anni '80 del secolo scorso dall'incontro di due comunità, quella dei computer scientist e quella dei fisici interessati ai fondamenti. Di particolare rilievo in questo ambito sono i lavori di Deutsch [13], [14], che mettono in risalto i possibili vantaggi emergenti dall'utilizzare un paradigma quantistico per la computazione. Da qui in poi i lavori teorici per trovare algoritmi quantistici più efficienti di quelli classici e gli sforzi sperimentali per la realizzazione di questi ultimi non sono mai cessati. La ricaduta pratica delle ricerche, passate e future, in Quantum Information è impressionante, si va dalla crittografia quantistica alla possibilità del teletrasporto (quantistico), dalla fattorizzazione di numeri in tempi polinomiali alla error correction. Attualmente molti gruppi in tutto il mondo sono attivi nel ricercare sistemi adatti a svolgere il ruolo di qubit per una futura realizzazione di un quantum computer.

Risulta quindi chiaro che il formalismo astratto della teoria quantistica ha forti conseguenze sulle modalità con cui può essere processata l'informazione. Con un ragionamento inverso si è sviluppato il tentativo di derivare la teoria quantistica a partire da soli assiomi di natura informazionale ispirati dalla idea di Wheeler *it from bit*. Ci sono stati vari tentativi di assiomatizzazione, tra cui quello di D'Ariano [24], Hardy [25] e Masanes e Muller [28], in cui la teoria quantistica veniva derivata, all'interno di una classe molto ampia di teorie, attraverso postulati di carattere fisico. Tuttavia in questi lavori rimaneva sempre una qualche assunzione matematica non traducibile in termini fisici elementari. In un lavoro del 2011 D'Ariano, Perinotti e Chiribella, [32], sono riusciti, a partire da assiomi operazionali, a derivare la teoria quantistica in dimensione finita.

Questi ultimi lavori si basano sul framework delle teorie probabilistiche operazionali (OPT). Data la semplicità concettuale di questo framework, che pure ha come fondamento matematico la teoria delle categorie monoidali simmetriche, è possibile che le teorie operazionali siano una classe molto ampia. Alcune di queste teorie mostrano che la non-località non è una caratteristica esclusiva della teoria quantistica. Vi sono ad esempio teorie, ad esempio quella delle box di Popescu e Rohrlich, che mostrano una non-località più forte della QT senza tuttavia ammettere trasmissione di informazione superluminale. Questo semplice esempio ci mostra come delle caratteristiche ritenute proprie e caratterizzanti la QT siano in realtà condivise anche da altre teorie probabilistiche. Risulta quindi interessante indagare OPT che differiscono in qualche modo dalla QT. Infatti in questo modo si possono mettere in luce quali siano le caratteristiche effettivamente peculiari della teoria quantistica e si può quindi arrivare ad una maggiore comprensione di questa teoria. Inoltre si pongono le basi a possibili

generalizzazioni della teoria quantistica. Infatti data una assiomatizzazione su basi fisiche della QT quello che rimane da fare è cercare di indebolire qualche assunzione e studiare le caratteristiche della teoria modificata che ne risulta. Come sostenuto da Hardy, [27], lo studio di teorie probabilistiche generalizzate, diverse dalla QT, nell'ambito operazionale potrebbe essere il giusto modo per superare le difficoltà che si incontrano nel formulare una teoria quantistica della gravità.

Nel lavoro [32] gli autori derivano la teoria quantistica a partire da cinque assiomi, che caratterizzano sia la QT che la teoria probabilistica classica, con l'aggiunta di quello che è il postulato di purificazione. La QT risulta essere una teoria causale, cioè tale che la probabilità degli outcome di un esperimento eseguito ad un certo tempo non dipende da quali esperimenti si decide di fare a tempi successivi. Inoltre soddisfa anche l'assioma di discriminabilità locale. Quest'ultimo implica che se due stati bipartiti sono differenti allora è possibile discriminarli (con probabilità di errore inferiore ad 1/2) attraverso misure locali sulle componenti. Questo assioma è di fondamentale importanza e permette di riconciliare il riduzionismo con l'olismo della teoria quantistica. Se si indebolisce questo principio si vengono a presentare teorie che hanno un grado di olismo maggiore di quello della QT senza peraltro cadere in teorie con olismo illimitato. In particolare Hardy e Wootters in [21] hanno mostrato come la teoria quantistica su spazi vettoriali reali (RQT) non abbia la discriminabilità locale ma sia invece *bilocal tomographic*, ovvero lo stato di ogni sistema composto sia determinabile dalla statistica di misurazioni fatte su coppie di sistemi componenti.

In questo lavoro, ispirati dall'analisi del problema svolta da D'Ariano in [6] sulla base dei lavori di Deutsch, studieremo una caratteristica importante della teoria quantistica provando che la stessa continua a valere nell'ambito della RQT anche se con una piccola differenza. Questa caratteristica è l'universalità del gate entanglante Control-NOT (CNOT) assieme ai gate locali per la computazione. L'universalità di un set di gate sta a significare che qualsiasi altra trasformazione reversibile della teoria può essere ottenuta applicando i soli gate del set. In particolare il fatto che, oltre ai gate locali, l'unico gate richiesto per l'universalità sia un gate bipartito è significativo in quanto viene a coinvolgere solo due qubit alla volta che entrano in interazione unitaria. Lo stimolo iniziale per questo lavoro proviene dal risultato di Masanes *et al.*, [8], che dimostrano che l'unica teoria con discriminabilità locale in cui i sistemi elementari siano qubit e che ammetta un gate reversibile bipartito entanglante è la teoria quantistica. La dimostrazione di tale risultato si avvale in maniera sostanziale dei risultati sull'universalità. Questo ci porta a sospettare che il principio che esista un solo gate bipartito che insieme a quelli locali sia universale per la computazione potrebbe essere un candidato molto forte per individuare la teoria quantistica

nell'ambito delle possibili teorie dell'informazione. Dai risultati trovati si vedrà tuttavia che indebolendo il requisito di discriminabiltà locale e la richiesta che i sistemi elementari siano i qubit si trovano altre teorie soddisfacenti lo stesso principio. Il risultato non dà quindi risposte conclusive in questa prospettiva, in quanto da un lato esso suggerisce che il principio di esistenza di un solo gate entanglente universale non sia strettamente quantistico, dall'altro esso è stato ottenuto per una teoria che di quella quantistica è stretta parente, ovvero la teoria quantistica reale. Resta pertanto aperta la domanda se la teoria quantistica, reale o complessa, non sia comunque l'unica teoria che ammette un siffatto set di gate universali per la computazione.

Il problema dell'universalità nella computazione quantistica ha una lunga storia. La teoria della computazione classica ebbe inizio con i lavori pioneristici di Church e Turing degli anni '30, i quali formalizzarono dal punto di vista matematico il concetto di algoritmo e tra gli altri introdussero il modello computazionale più popolare che è la macchina di Turing. Un secondo modello di computazione, per certi versi più realistico delle macchine di Turing, è quello dei circuiti logici. Questo modello è intrinsecamente irreversibile e quindi non compatibile con l'analogo quantistico che produce una computazione reversibile (i gate sono operatori unitari). Tuttavia negli anni '70 Charles Bennet, ispirato dai lavori di Landauer sulla dissipazione di energia nella computazione, dimostrò che la computazione classica irreversibile è equivalente alla computazione classica reversibile. Quest'ultima è infine un caso (molto) particolare di computazione quantistica. Negli anni '80 Tommaso Toffoli dimostrò che per la computazione classica reversibile esiste un gate a tre bit universale che va sotto il nome di gate di Toffoli mentre non sono sufficienti i gate a due bit per implementare qualsiasi circuito reversibile. Negli stessi anni numerosi fisici si stavano interrogando sulle possibilità che la teoria quantistica poteva offrire se applicata alla teoria della computazione, tra i tanti lo stesso Feynman si interrogava sulle possibilità di un eventuale computer quantistico. Nel 1985 Deutsch [13] propose il primo modello di computer quantistico universale estendendo al caso quantistico il modello della macchina di Turing universale. Successivamente lo stesso Deutsch [14], sviluppò il modello delle reti computazionali quantistiche che sono alla base dell'attuale formalismo dei circuiti quantistici. In questo lavoro Deutsch si interrogò sull'esistenza di un gate quantistico universale per la computazione in analogia al caso classico, e dimostrò che una variante quantistica del gate di Toffoli è universale. Seguirono molti altri lavori sull'universalità nella teoria della computazione quantistica, [18] [15] [16] [19] [20] [7] [12]. In particolare Barenco *et al.* in [18] dimostrarono che l'insieme dei gate locali più il CNOT è un insieme esattamente universale, risultato che si può ora trovare in ogni libro di quantum computation, [9] [10]. In seguito J. Brylinski e R. Bry-

linski in [7], dimostrarono[1] che è sufficiente un gate entanglante qualsiasi per avere l'universalità esatta (ovviamente sempre assieme ai locali).

Ispirati da quest'ultimo lavoro abbiamo cercato una generalizzazione al caso della RQT. Quello che si è visto è che la dimostrazione così come è fatta non è valida nel caso della RQT. Tuttavia si è riusciti ad elaborare un metodo, partendo dai risultati di [6], che permette di dimostrare induttivamente l'universalità esatta del CNOT più gate locali sia nel caso della QT che nel caso della RQT. Per la QT il risultato trovato è già noto, tuttavia il metodo utilizzato è originale e più semplice di quelli presenti in letteratura, mentre per la RQT il risultato è nuovo.

Il presente lavoro è così strutturato. Nel primo capitolo si introduce la teoria della computazione quantistica, facendo una breve introduzione storica seguita dall'introduzione del formalismo dei circuiti. Per prima cosa si analizzano i circuiti classici reversibili e non evidenziandone l'equivalenza. Poi si introduce il formalismo dei circuiti quantistici in dettaglio e si analizza il concetto di universalità esatta e approssimata. Infine si illustrano le dimostrazioni dell'universalità del CNOT e di un gate entanglante bipartito qualsiasi così come da letteratura. Particolare enfasi viene posta nell'evidenziare il passaggio della dimostrazione di [7] che non risulta valido in RQT.

Nel secondo capitolo si introduce il formalismo delle OPT. Ci soffermiamo sui postulati da cui deriva la QT ponendo particolare enfasi sulla discriminabilità locale. Segue l'introduzione della RQT, in particolare si mostra come la teoria quantistica su spazi reali sia equivalente alla OPT in cui gli stati sono rappresentati da matrici densità reali. Infine si analizza il grado di olismo di questa teoria mostrando che possiede la proprietà di *bilocal tomography*.

Il terzo capitolo contiene i risultati originali del lavoro di tesi. Da una parte viene dimostrata l'universalità del CNOT e gate locali per la QT con una dimostrazione semplificata rispetto alla letteratura. Dall'altra parte si ottiene un risultato di universalità debole per la RQT con una dimostrazione analoga. Viene infine posta evidenza sulla differenza tra la proprietà di universalità della teoria standard e quella trovata per la RQT che giustifica l'appellativo *debole* per quest'ultima. Quest'ultimo capitolo è basato sull'articolo di D'Ariano, Perinotti e Belenchia [35].

In appendice A è riportata una breve introduzione alla teoria dei gruppi e algebre di Lie, con particolare attenzione ai gruppi classici e alle definizioni di interesse. In appendice B si fa riferimento ai gruppi unitario e ortogonale presentando i risultati utili ai fini del lavoro. Infine in appendice C è riportato il lemma chiave per i risultati ottenuti assieme alla sua dimostrazione.

[1] Complemento essenziale alla dimostrazione viene dal lavoro di Harrow [12].

Capitolo 1

Computazione Quantistica

In questo capitolo introdurremo il concetto di computazione quantistica. Inoltre faremo cenno a due possibili approcci alla teoria della computazione. Da un lato abbiamo infatti il modello della macchina di Turing e dall'altro il modello a circuiti logici. Questi due modelli per quanto diversi risultano essere equivalenti (in senso opportuno)per quanto riguarda il potere computazionale. In particolare quello che svilupperemo in dettaglio sarà il formalismo dei circuiti quantistici facendo inoltre cenno all'analogo classico dei circuiti logici reversibili. Esploreremo infine il concetto di universalità, esatta ed approssimata, per un set di gate quantistici e dimostreremo che il CNOT insieme a gate locali costituiscono un set universale.

In particolare nella prima parte del capitolo, dopo alcune note storiche sulla nascita della teoria della computazione, ci concentreremo sui quantum circuits, descrivendone il formalismo e arrivando a dare la definizione di set esattamente universale e universale, in accordo con [7],[12]. Nella seconda parte riporteremo la dimostrazione dell'universalità esatta di CNOT e gate locali come da letteratura e infine la dimostrazione, più generale della prima, che ogni gate entanglante insieme ai gate locali costituisce un set esattamente universale per la *quantum computation*.

1.1 Introduzione

Un algoritmo è, informalmente, un insieme di istruzioni che applicate ad un certo input danno in uscita un certo output. Per quanto la nozione di algoritmo possa sembrare di per se intuitiva la sua formalizzazione matematica si è avuta solo dopo gli anni '30 grazie ai lavori di Turing e Church. La formalizzazione del concetto di algoritmo era necessaria per la risoluzione di uno dei problemi di Hilbert e portò alla nascita della moderna teoria della computazione. Il problema

in questione era se ci fosse un algoritmo usabile, almeno in linea di principio, per risolvere tutti i problemi della matematica e la risposta che fu trovata è che un tale algoritmo non esiste.

Turing per formalizzare il concetto di algoritmo definì la classe di macchine computazionali che oggi vanno sotto il nome di *macchine di Turing*. Esistono svariate varianti di macchine di Turing, tra cui quelle probabilistiche, e risultano uno degli approcci più esplorati alla teoria della computazione classica. Va sottolineato che la macchina di Turing è un modello di computazione basato su una descrizione classica e come tale presenta delle limitazioni. Inoltre la macchina di Turing presenta delle idealizzazioni, come l'avere una memoria illimitata, che la rendono poco realistica.

Più realistico ed utile ai nostri scopi sarà il modello dei circuiti aciclici per la computazione. Questo modello risulta essere equivalente a quello della macchina di Turing dal punto di vista della potenza computazionale ma più utile in vista della generalizzazione al caso quantistico. Un circuito è costituito da *wires* che trasportano i bit, alcuni di essi sono di input e altri di output, e da *logic gate* che eseguono determinate operazioni logiche. Più formalmente un gate logico è una funzione

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

I modelli ora citati sono entrambi classici. Una delle domande che emerse negli anni ottanta nell'ambito della teoria della computazione, si vedano ad esempio i lavori di Feynman del '82, è se modelli di computazione che sfruttino le caratteristiche della teoria quantistica potessero portare ad algoritmi più efficienti di quelli classici. La risposta a questa domanda fu affermativa, come mostrato da Deutsch e Jozsa(1992), Shor(1994) ed altri. Ad esempio algoritmi quantistici basati sulla trasformata di Fourier quantistica di Shor per problemi di fattorizzazione permettono di ottenere uno speedup esponenziale sui migliori algoritmi classici noti, mentre l'algoritmo di ricerca quantistica di Grover permette di ottenere uno speedup quadratico rispetto ad algoritmi classici. Inoltre risultò che i computer quantistici avrebbero permesso di fare compiti computazionali impossibili per i computer classici, come ad esempio la crittografia quantistica. In particolare la classe delle funzioni computabili quantisticamente risulta essere la stessa di quelle computabili classicamente.

Nel 1985 Deutsch in [13], propose una variante (più forte) della famosa congettura di Churh-Turing. Secondo la congettura originale: *Every function which would naturally be regarded as computable can be computed by the universal Turing machine.* Questa congettura venne riformulata in [13] con il nome di principio di Church-Turing asserendo che: *Every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means.* Nello stesso lavoro Deutsch introdusse una variante quantistica

della macchina di Turing universale, il computer quantistico universale. Infine mostrò come la teoria classica basata sulla macchina di Turing universale non rispetti il principio sopra enunciato mentre lo rispetti il computer quantistico universale, sancendo così la superiorità della computazione quantistica su quella classica.

In seguito nel 1989 Deutsch propose il modello computazionale denominato *quantum computational networks* che è l'analogo quantistico dei circuiti logici convenzionali. Questo modello fu poi sviluppato da Yao in [23], in cui viene anche mostrata l'equivalenza del modello dei circuiti quantistici con quello della macchina di Turing quantistica.

1.2 Il Formalismo dei Circuiti Quantistici

Introduciamo ora il formalismo dei circuiti quantistici riportando anche i principali gate per la computazione quantistica. Prima però facciamo una breve digressione sui circuiti classici e in particolare sull'universalità per i circuiti classici reversibili.

1.2.1 Circuiti Classici

Iniziamo con una breve introduzione ai circuiti logici classici. Un circuito logico è costituito da wires e gate. Ricordiamo che un gate è una funzione

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

da n bit di input a m bit di output. Ad esempio il NOT logico è implementato da un gate con un input ed un output:

$$NOT(x) = 1 \oplus x,$$

dove $\oplus$ è l'addizione modulo due.

Più formalmente, una funzione Booleana è una funzione

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

e un circuito Booleano è una rappresentazione di una funzione Booleana come la composizione di altre funzioni Booleane. In particolare sia $\mathfrak{A}$ un insieme di funzioni booleane fissate, allora un circuito $\mathfrak{C}$ sulla base $\mathfrak{A}$ è una sequenza di assegnazioni che coinvolgono n variabili di input $x_1, \cdots, x_n$ e varie variabili ausiliarie $y_1, \cdots, y_r$ in modo che la j-esima assegnazione sia del tipo $y_j = f_j(u_1, ..., u_l)$, $f_j \in \mathfrak{A}$, dove le variabili u_i sono o variabili di input o variabili

ausiliarie che precedono y_j, come chiarito in Fig.1.1. Il valore dell'ultima variabile ausiliaria è il risultato della computazione. Il circuito $\mathfrak{C}$ è detto computare la funzione booleana F se il risultato della computazione è uguale a $F(x_1, ..., x_n)$ per ogni $x_1, ..., x_n$. Se si selezionano m variabili ausiliare come variabili di output allora il circuito computerà una funzione $F : \{0,1\}^n \to \{0,1\}^m$. Ogni circuito può essere rappresentato da un grafo aciclico a cui vertici sono situati i gate della base, da cui il nome stesso di circuito.

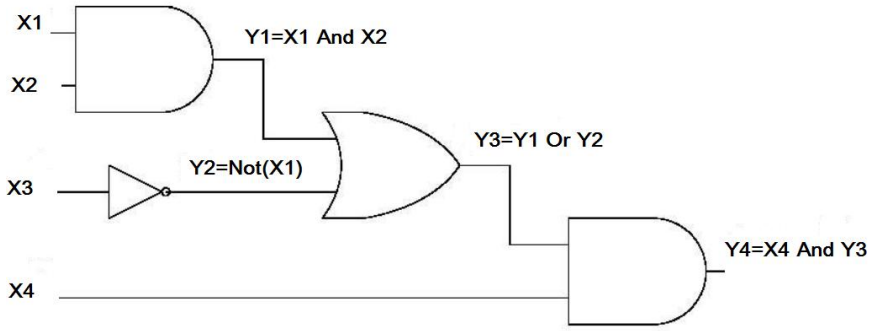


Figura 1.1: Esempio di circuito booleano con una sola variabile di output.

Quello che si dimostra è che la base $\mathfrak{A} = \{NOT, OR, AND\}$, dove gli elementi OR e AND sono gate a due input e un output, è completa, ovvero che per ogni funzione $F : \{0,1\}^n \to \{0,1\}^m$ esiste un circuito su $\mathfrak{A}$ che la computa. Nella terminologia che introdurremo dopo questa base è detta universale per la computazione classica *irreversibile*.

Mostriamo, rifacendoci a [10], che la base sopra citata permette di ottenere qualsiasi funzione booleana[1]. Indichiamo i gate della base nel seguente modo:

$$NOT(x) = \neg x,\ OR(x,y) = x \vee y,\ AND(x,y) = x \wedge y. \tag{1.1}$$

Teorema 1.2.1. *La base $\{\neg, \wedge, \vee\}$ è completa. In particolare il solo sottoinsieme $\{\neg, \wedge\}$ è ancora una base completa.*

Dimostrazione. Una qualsiasi funzione booleana a n argomenti è determinata dalla sua tabella dei valori che contiene 2^n righe, in ognuna delle quali vi è il valore degli argomenti ed il corrispondente valore della funzione. Se la funzione assume valore 1 solo una volta allora può essere ottenuta da una congiunzione di variabili o variabili negate. Ad esempio se $f(x,y,z) = 1 \Leftrightarrow (x,y,z) = (1,0,1)$ allora

$$f(x,y,z) = x \wedge \neg y \wedge z.$$

[1]Da qui è poi facile vedere che ogni funzione del tipo $f : \{0,1\}^n \to \{0,1\}^m$ può essere computata da un circuito appropriato sulla stessa base.

Nel caso generale una funzione potrà quindi essere rappresentata nel seguente modo

$$f(x) = \bigvee_{\{u:f(u)=1\}} \chi_u(x), \tag{1.2}$$

dove $u = (u_1, ..., u_n)$ e χ_u è tale che

$$\chi_u = \begin{cases} 1, & \text{se } x = u \\ 0, & \text{altrimenti} \end{cases} \tag{1.3}$$

L'ultimo punto del teorema ci dice che la base considerata è ridondante. Questo è mostrato dalle identità di De Morgan che riportiamo di seguito

$$x \wedge y = \neg(\neg x \vee \neg y), \quad x \vee y = \neg(\neg x \wedge \neg y). \tag{1.4}$$

■

Una ulteriore semplificazione al teorema esposto è che il solo gate logico NAND, definito da

$$NAND(x, y) \equiv x \uparrow y = \neg(x \wedge y), \tag{1.5}$$

è un gate universale[2]. Questo deriva direttamente dalle seguenti identità

$$NOT(x) = x \uparrow x \tag{1.6}$$

$$x \wedge y = (x \uparrow y) \uparrow (x \uparrow y). \tag{1.7}$$

Siccome la computazione quantistica, che introdurremo nel prossimo paragrafo, è reversibile non include come caso particolare i circuiti booleani che sono invece irreversibili. Tuttavia agli inizi degli anni '70 Charles Bennet, spinto dai precedenti lavori di Landauer, dimostrò l'equivalenza della computazione classica irreversibile e reversibile. Successivamente, negli anni '80, Toffoli e Fredkin introdussero il modello dei circuiti reversibili per la computazione. In questo contesto i circuiti classici reversibili, che andiamo ora ad introdurre, sono il sottoinsieme classico dei più generali circuiti quantistici[3] e sono computazionalmente equivalenti ai circuiti irreversibili prima esaminati.

Una mappa reversibile su un insieme finito non è altro che una permutazione $G : \{0,1\}^n \to \{0,1\}^n$.

[2]In quanto fatto precedentemente nel teorema ed anche in questo punto si sta assumendo tacitamente che sia possibile effettuare l'operazione COPY che manda un bit in due copie di se stesso, [29].

[3]Le permutazioni possono essere viste come matrici unitarie che mandano elementi della base computazionale in elementi della base computazionale. Ovvero matrici unitarie con un solo 1 in ogni colonna e riga.

Definizione 1.1 (Circuito classico reversibile)**.**
Sia $\mathfrak{A}$ un insieme di permutazioni della forma $G : \{0,1\}^k \to \{0,1\}^k$, che chiamiamo base. Un circuito reversibile sulla base $\mathfrak{A}$ è una sequenza di permutazioni $G_1[A_1], \ldots, G_l[A_l]$ dove A_j è un insieme di bit e $G_j \in \mathfrak{A}$. La permutazione realizzata dal circuito sarà il prodotto di permutazioni

$$W = G_1[A_1] \cdots G_l[A_l]$$

.

Più in generale si può considerare l'utilizzo di bit ancillari, nel qual caso la permutazione realizzata dal circuito è la permutazione G tale che il prodotto W agente su N bit ($N \geq n$) soddisfa alla condizione $W\left(x, 0^{N-n}\right) = \left(Gx, 0^{N-n}\right), \forall x \in \{0,1\}^n$.

A questo punto per computare una generica funzione $F : \{0,1\}^n \to \{0,1\}^m$ attraverso un circuito reversibile, si computa la permutazione $F_\oplus : \{0,1\}^{n+m} \to \{0,1\}^{n+m}$ definita da

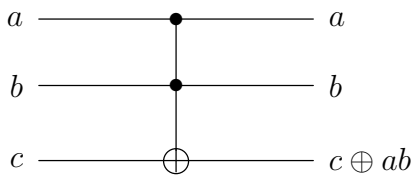
$$F_\oplus(x, 0) = (x, F(x)).$$

Questa semplice considerazione rende l'idea dell'equivalenza tra computazione irreversibile e reversibile.

Universalità nella teoria reversibile classica

Si verifica facilmente che nel caso classico reversibile i gate a due bit non sono universali. Infatti le permutazioni su due bit risultano essere funzioni lineari[4] e quindi non permettono di realizzare tutte le funzioni della forma $F_\oplus$ ma solo quelle lineari, [10]. Questo significa che per la computazione classica non esiste un insieme di gate a uno e due bit che sia universale. Nel 1980 Tommaso Toffoli dimostrò che un gate, adesso noto come gate di Toffoli, a tre input e tre output è universale per i circuiti reversibili, ovvero ogni circuito può essere ottenuto componendo solo gate di Toffoli a patto di avere almeno un bit ancillare.

Il gate di Toffoli è dato da $\Lambda_\oplus : (x, y, z) \to (x, y, z \oplus xy)$ e la sua rappresentazione circuitale è la seguente



Prima di illustrare l'universalità del gate di Toffoli richiamiamo brevemente le ragioni che portarono alla ricerca di schemi di computazione reversibile e

[4]Con l'identificazione naturale di $\{0,1\}$ con $\mathbb{F}^2$, campo a due elementi.

mostriamo che un altro gate a tre bit, il gate di Fredkin, è universale. Questo gate, al contrario di quello di Toffoli, presenta una implementazione fisica intuitiva che è quella del *billiard ball computer*, [11], che andremo brevemente ad illustrare.

Come già citato i lavori che spinsero Bennet ed altri ad interessarsi a schemi di computazione reversibili furono quelli di Landauer del '61 e '67. Landauer indagò la connessione tra dissipazione di energia e computazione arrivando a formulare il famoso *principio di Landauer*

Se un computer cancella un singolo bit di informazione allora l'entropia dell'ambiente deve aumentare di almeno $k_B \ln 2$.

Questo principio[5] quindi pone un limite inferiore all'energia che deve essere dissipata durante una computazione. Tuttavia la cancellazione di bit di informazione avviene solamente in una computazione irreversibile. Nel caso reversibile non viene persa alcuna informazione e quindi in questo caso il principio di Landauer non pone alcun vincolo all'energia che deve essere dissipata durante la computazione.

Siccome le leggi della fisica sono fondamentalmente reversibili (dato un sistema isolato, sia le leggi della dinamica classica che l'evoluzione temporale della meccanica quantistica sono reversibili), i fisici iniziarono ad indagare l'equivalenza tra computazione reversibile e irreversibile. Come già detto Bennet dimostrò che questa equivalenza esiste e che la computazione reversibile può essere eseguita senza dissipazione di energia ad ogni step. In seguito Toffoli e Fredkin mostrarono l'esistenza di gate reversibili universali. Questi permettono di simulare reversibilmente qualunque computazione irreversibile.

Il modello del billiard ball computer è un modello computazionale basato su processi fisici banali (seppur idealizzati). In particolare è un modello di computazione composto solo da palle da biliardo che urtano elasticamente dei pannelli riflettori o le altre palle. Quello che Fredkin e Toffoli mostrano in [11] è che data una precisa geometria al contenitore delle palle e appropriate condizioni iniziali alle palle stesse si può fare una qualsiasi computazione[6]. In questo senso il modello è universale.

La presenza o meno di una palla ad un possibile sito di input sta ad indicare un 1 o 0 rispettivamente e allo stesso modo nei siti di output. L'importanza di questo modello sta nel fatto che permette di collegare la computazione con

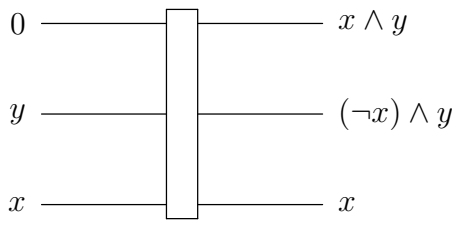
Input			Output		
a	b	c	a′	b′	c′
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	1	1	1

Figura 1.2: Tavola dei valori del gate di Fredkin.

fenomeni fisici elementari. Inoltre questo modello è manifestamente reversibile, in quanto basato sulle leggi degli urti elastici della meccanica classica.

Attraverso questo modello è possibile implementare in maniera semplice il gate di Fredkin (Fig.1.3), che è un gate a tre bit. Tale gate oltre ad essere reversibile è anche conservativo, dove questo sta a significare che il numero di 1 in input e pari a quello in output. Dal punto di vista del modello fisico del biliardo questo corrisponde alla conservazione della massa. Oltre a queste proprietà il gate di Fredkin è anche universale. Quanto appena detto ci permette di fare una osservazione interessante. Sembra che, al contrario del caso quantistico, nel caso classico la computazione richieda interazioni a tre corpi per avere un gate universale. Tuttavia questa affermazione non è corretta proprio alla luce del modello billiard ball che mostra come un gate universale, gate di Fredkin, possa essere implementato attraverso un modello in cui le interazioni fondamentali sono a due corpi, ovvero quelle tra le palle da biliardo.

Per mostrare che il gate di Fredkin è universale basta che da esso si possano ottenere, ad esempio, i gate AND, NOT e COPY. Il gate di Fredkin può essere configurato in modo tale da simulare questi gate configurando opportunamente i bit ancillari. Ad esempio, dalla tavola di valori del gate in Fig.1.2 si vede subito che la seguente configurazione del gate da il gate AND



(1.8)

[5]Il suddetto principio è stato recentemente validato sperimentalmente ed è alla base della risoluzione del paradosso del demone di Maxell.

[6]In realtà costruire un computer di questo tipo presenterebbe difficoltà insormontabili dovute alla instabilità del sistema stesso e alla impossibilità di isolarlo dall'ambiente.

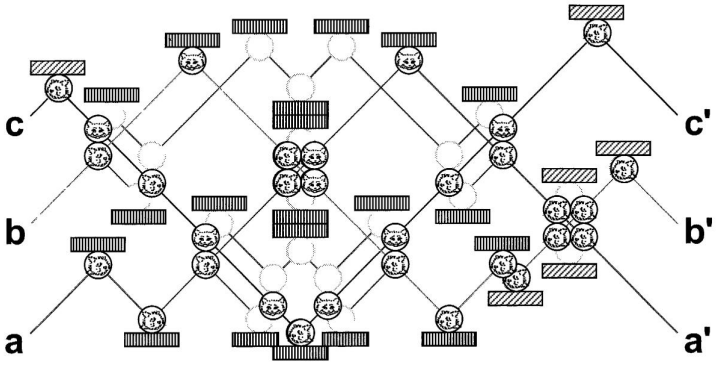
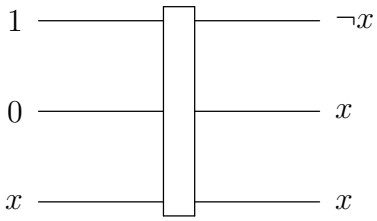


Figura 1.3: Billiard ball computer che implementa il gate di Fredkin. Le sfere vuote indicano possibili cammini della palle a causa delle collisioni. Immagine tratta da [9].

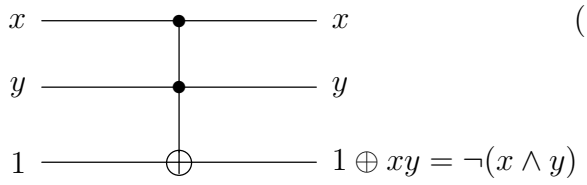
Risulta chiaro che dei tre bit uno è ancillare mentre un altro contiene del garbage inutile ai fini della computazione[7]. Si hanno poi le seguenti implementazioni del NOT e COPY



(1.9)

dove il gate simula il NOT se si trascurano gli ultimi due bit mentre simula il COPY trascurando il primo bit.

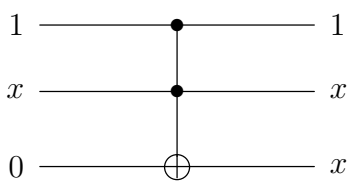
In modo del tutto analogo si dimostra l'universalità del gate di Toffoli, ad esempio dimostrando che esso permette di ottenere il gate NAND



(1.10)

e COPY

[7]Risulta possibile effettuare la computazione reversibile in maniera tale che tutti i bit spazzatura risultino in fine in uno stato standard. Questa tecnica va sotto il nome di *uncomputing*.



(1.11)

Osservazione

L'universalità del gate di Toffoli è una universalità *debole*[8], nel senso che perchè il gate sia universale è necessario assumere di avere un bit ancillare, [29]. Questo è dovuto al fatto che il gate di Toffoli rappresenta una permutazione pari quando agisce su $n > 3$ bit, ovvero quando si considera ad esempio $I \otimes T$, dove T è la rappresentazione matriciale del gate di Toffoli, per $n = 4$. Il prodotto di permutazioni pari è ancora una permutazione pari e quindi attraverso gate di Toffoli non si potrà mai ottenere una permutazione dispari di $n = 4$ bit. Però se, chiamata A la rappresentazione matriciale di una permutazione dispari su $n = 4$ bit, si considera un bit ancillare allora si ha la permutazione $I \otimes A$ su $n = 5$ bit che è pari e può essere ottenuta attraverso un circuito di soli gate di Toffoli. Un ragionamento analogo varrà anche per la teoria quantistica reale, come sarà esposto alla fine dell'ultimo capitolo.
Passiamo ora all'analisi del formalismo dei circuiti quantistici sul quale sarà poi basato tutto il resto del lavoro.

1.2.2 Circuiti quantistici

Introduciamo ora la definizione di circuito quantistico e i principali gate quantistici. I computer classici operano su insiemi finiti di bit classici i quali possono esistere solo in due stati distinti 0 e 1. Lo stato del sistema complessivo di n bit è dato specificando il valore di tutti i bit. Quindi l'insieme degli stati è

$$\mathbb{B}^n = \{0, 1\}^n ,$$

cioè un insieme finito con cardinalità 2^n.

Un computer quantistico opera invece sull'analogo quantistico del bit, ossia il *qubit*. Il qubit è di per se il sistema quantistico più semplice e fisicamente è dato da un qualsiasi sistema quantistico a due livelli, come ad esempio lo spin di una particella a spin 1/2 o la polarizzazione di un fotone. Nel resto della trattazione il qubit è considerato come un oggetto matematico astratto, il che permette di sviluppare la teoria della computazione indipendentemente dal particolare sistema che realizza il qubit. Il qubit ha ancora due stati perfettamente

[8]Termine che useremo anche nell'ultimo capitolo per la teoria quantistica reale.

discriminabili che chiamiamo 0 e 1 (spin up e spin down nell'esempio di uno spin 1/2) ma, grazie al principio di sovrapposizione, può assumere uno stato che è sovrapposizione lineare a coefficienti complessi di questi. Lo spazio degli stati per un singolo qubit è lo spazio di Hilbert due dimensionale $\mathbb{C}^2$ e i due stati $\{|0\rangle, |1\rangle\}$[9] ne costituiscono una base ortonormale che prende il nome di *base computazionale*. Lo stato di un qubit è quindi un vettore (o meglio un raggio[10]) unitario in uno spazio di Hilbert due dimensionale[11].

Dato un sistema composto di n qubit lo spazio degli stati sarà il prodotto tensore degli spazi di singolo qubit e quindi

$$\underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n} = \mathbb{C}^{2^n}. \tag{1.12}$$

Chiamiamo gli stati della base computazionale di tale spazio

$$|x_1, ..., x_n\rangle, x_i \in \mathbb{B}, \tag{1.13}$$

uno stato arbitrario del sistema sarà dato da

$$|\psi\rangle = \sum_{(x_1,...,x_n)\in\mathbb{B}^n} a_{x_1,...,x_n}|x_1, ..., x_n\rangle, \quad \sum_{(x_1,...,x_n)\in\mathbb{B}^n} |a_{x_1,...,x_n}|^2 = 1. \tag{1.14}$$

Da quanto detto si ha che un sistema di n qubit, al contrario del caso classico, può assumere un continuo si stati diversi. La computazione quantistica può essere pensata come una sequenza di trasformazioni sullo stato del sistema. Le trasformazioni ammesse sono quelle che preservano la norma dello stato ovvero le trasformazioni unitarie. Il gruppo delle trasformazioni reversibili di un sistema di n qubit è quindi il gruppo di Lie $U(2^n)$ e le trasformazioni di questo gruppo sono i gate quantistici. Va notato che quanto detto presuppone che si stia considerando un quantum computer come un sistema isolato[12], infatti è solo in questo caso che la dinamica del sistema è puramente unitaria. Essendo i gate operatori unitari è ovvio che la computazione quantistica sia reversibile ed è anche ovvio che comprenda come sottoinsieme la computazione classica reversibile. Infatti i gate che possiamo definire classici sono quelli che evolvono stati della base computazionale in stati della base computazionale e rappresentano delle permutazioni. Dal punto di vista matriciale sono matrici i qui elementi sono o 0 o 1 con esattamente un 1 per ogni riga e colonna, [14].

[9] Da ora useremo la notazione di Dirac, questa è perfettamente legittima dato che lavoreremo sempre con sistemi quantistici di dimensione finita.

[10] Dato che moltiplicare lo stato per un fattore di fase globale da uno stato fisicamente equivalente.

[11] Nel prossimo capitolo ritorneremo sul concetto di qubit specificando la struttura del suo spazio degli stati e confrontandolo con il rebit della computazione reale.

[12] Chiaramente questa è una idealizzazione perchè è noto che nessun sistema è effettivamente isolato.

Definizione 1.2 (Circuito quantistico)**.**
Sia $\mathfrak{A}$ un insieme di operatori unitari, che chiamiamo base. Un circuito quantistico sulla base $\mathfrak{A}$ è una sequenza di gate $U_1[A_1], \ldots, U_l[A_l]$ dove A_j è un insieme ordinato di qubit e $U_j \in \mathfrak{A}$. L'operatore realizzato dal circuito sarà il prodotto degli operatori

$$W = U_l[A_l] \cdots U_1[A_1],$$

con $W : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$.

Se si considera la possibilità di avere dei bit ancillari allora l'operatore realizzato dal circuito è l'operatore $U : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ tale che il prodotto W agente su N ($N \geq n$) soddisfi alla condizione

$$W\left(|\xi\rangle \otimes |0^{N-n}\rangle\right) = \left(U|\xi\rangle \otimes |0^{N-n}\rangle\right), \forall |\xi\rangle \in \mathbb{C}^{2^n}.$$

1.2.3 Gate di singolo qubit e gate locali

Introduciamo ora i principali gate di singolo qubit, dandone la rappresentazione matriciale nella base computazionale, e il concetto connesso di gate locali. Prendiamo in considerazione il gruppo delle trasformazioni del singolo qubit, ovvero $U(2)$. Questo è il gruppo delle matrici unitarie 2×2. Tra queste le più importanti sono sicuramente le matrici di Pauli[13]:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{1.15}$$

Altri gate a singolo qubit importanti sono l'Hadamard gate, il phase gate e il gate $\pi/8$, rispettivamente

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} T = \begin{bmatrix} 1 & 0 \\ 0 & exp^{(i\pi/4)} \end{bmatrix} \tag{1.16}$$

In particolare nell'ultimo capitolo useremo una variante a determinante uno dell'Hadamard

$$\tilde{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}. \tag{1.17}$$

Le tre matrici di Pauli oltre ad essere elementi del gruppo sono anche matrici hermitiane a traccia nulla e quindi elementi dell'algebra di $SU(2)$[14]. Questo fatto

[13] Queste matrici oltre ad essere unitarie e a traccia nulla sono anche hermitiane.

[14] Secondo le convenzioni usate in appendice i generatori del gruppo sono $i\sigma_k$,cioè i volte le matrici di Pauli, che sono matrici anti-hermitiane a traccia nulla.

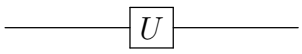
sarà ripreso ed utilizzato estesamente nell'ultimo capitolo. Osserviamo fin da ora che esponenziando le matrici di Pauli si ottengono quelli che sono gli operatori di rotazione attorno agli assi x, y, z, che hanno la seguente rappresentazione matriciale.

$$R_x(\vartheta) = e^{-i\vartheta X/2} = \begin{bmatrix} \cos\frac{\vartheta}{2} & -i\sin\frac{\vartheta}{2} \\ -i\sin\frac{\vartheta}{2} & \cos\frac{\vartheta}{2} \end{bmatrix} \tag{1.18}$$

$$R_y(\vartheta) = e^{-i\vartheta Y/2} = \begin{bmatrix} \cos\frac{\vartheta}{2} & \sin\frac{\vartheta}{2} \\ \sin\frac{\vartheta}{2} & \cos\frac{\vartheta}{2} \end{bmatrix} \tag{1.19}$$

$$R_z(\vartheta) = e^{-i\vartheta Z/2} = \begin{bmatrix} e^{-i\frac{\vartheta}{2}} & 0 \\ 0 & e^{i\frac{\vartheta}{2}} \end{bmatrix} \tag{1.20}$$

Tali operatori sono detti di rotazione perchè se si considera la rappresentazione di Bloch[15] lo stato del qubit è rappresentato da un punto su una 2-sfera e l'applicazione di questi operatori porta ad una rotazione spaziale attorno all'opportuno asse della sfera. I gate finora introdotti hanno un bit in input e uno in output e la loro rappresentazione circuitale è del tipo:

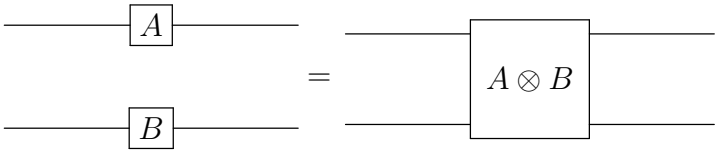


Se ora consideriamo un sistema di due qubit e pensiamo di agire sul primo qubit con il gate A e sul secondo con il gate B, dove $A, B \in U(2)$, allora la matrice 4×4 che descrive il processo non è altro che

$$(A \otimes I)(I \otimes B) = A \otimes B, \tag{1.21}$$

ovvero il prodotto tensore dei due gate elementari. Abbiamo che il prodotto tensore di due operatori è un operatore agente sul prodotto tensore degli spazi sui quali agiscono i fattori ed è definito dalla relazione

$$(A \otimes B)|\xi\rangle \otimes |\mu\rangle = A|\xi\rangle \otimes B|\mu\rangle. \tag{1.22}$$



(1.23)

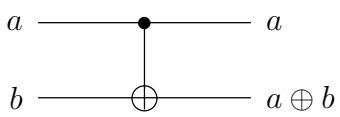
In quanto detto sopra si è ottenuto il gate $A \otimes B \in U(2) \otimes U(2) \subset U(4)$, questo è un gate locale. Più in generale, considerato un sistema di n-qubit un *gate locale* è un elemento di $\bigotimes_n U(2)$, ovvero corrisponde all'applicazione separata di gate ad un bit ad ogni qubit[16].

[15] Vedremo questa rappresentazione nel secondo capitolo.

[16] Ricordiamo che anche l'identità, rappresentata da i fili stessi, è un gate quantistico.

1.2.4 Control NOT

Introduciamo ora il gate più importante per tutto quello che segue. Questo gate è il Control NOT (CNOT) ed è un gate a due bit. La sua importanza nel nostro caso risiede nel fatto che questo gate assieme a quelli locali risulterà formare un set esattamente universale. La sua rappresentazione circuitale è data da



(1.24)

mentre la sua rappresentazione matriciale la seguente:

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

Il primo qubit è il qubit di controllo mentre il secondo è il target. L'azione del CNOT, nella base computazionale, è di lasciare inalterato il target se il controllo è in 0 mentre se il controllo è in 1 il target cambia stato (da 0 a 1 o viceversa). Osserviamo da subito una caratteristica fondamentale del CNOT: è un gate *entanglante*.

Definizione 1.3.
Uno stato di un sistema quantistico composto $|\psi\rangle_{AB} \in H_{AB}$ è detto **separabile** se è della forma

$$|\psi\rangle_{AB} = |\varphi\rangle \otimes |\eta\rangle,$$

dove $|\varphi\rangle \in H_A$ e $|\eta\rangle \in H_B$. Uno stato non separabile è detto **entangled**.

Definizione 1.4.
Diremo che un gate è **primitivo** se mappa stati separabili in stati separabili. Un gate è **entanglante** se non è primitivo. Più precisamente un gate è entanglante se esiste almeno uno stato separabile che viene mappato in uno stato entangled.

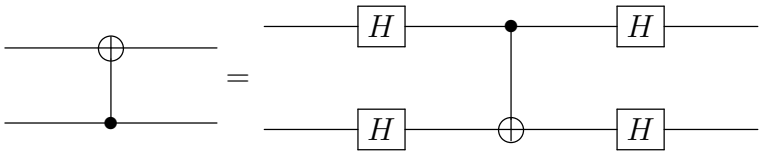
Verifichiamo subito che il CNOT è un gate entanglante. Infatti si ha

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |0\rangle \overset{CNOT}{\rightarrow} \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \tag{1.26}$$

lo stato a destra della freccia è uno stato di Bell ed è uno stato massimamente entangled.

Mostriamo ora come dal CNOT più gate Hadamard locali si possa ottenere un gate CNOT con target e controllo scambiati ed anche come con questo nuovo gate si possa ottenere il gate SWAP che scambia due qubit. Il gate CNOT con

controllo e target scambiati è indicato come $V(2,1)$ ed è ottenuto attraverso il seguente circuito



(1.27)

La verifica è banale. Infatti la rappresentazione matriciale di $V(2,1)$ è la seguente

$$V(2,1) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \tag{1.28}$$

detto questo basta verificare che il seguente prodotto di matrici dia proprio (1.28):

$$(H \otimes H)V(H \otimes H) = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 \end{bmatrix}$$

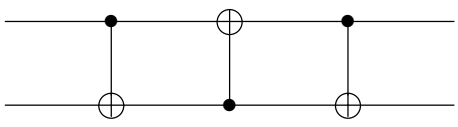
Per quanto riguarda lo swap questo verrà indicato nel seguito come P, l'azione di questo gate è

$$P|ab\rangle = |ba\rangle$$

e la sua rappresentazione matriciale nella base computazionale è la seguente

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{1.29}$$

Lo SWAP può essere ottenuto attraverso il seguente circuito



(1.30)

dove il gate centrale è $V(2,1)$. Anche in questo caso la verifica è banale, basta infatti svolgere il seguente prodotto di matrici e verificare che da luogo a (1.29)

$$VV(2,1)V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{1.31}$$

Infine l'azione dello SWAP su prodotti tensore di matrici 2×2 è la seguente

$$P(A \otimes B)P = B \otimes A \tag{1.32}$$

1.2.5 Universalità esatta e approssimata

Veniamo ora a precisare cosa si intende per set di gate esattamente universale e universale seguendo [7] e [12]. Consideriamo un gate A di singolo qubit, questo da luogo a n diversi gate locali su n qubit,

$$A(i)|x_1, \ldots, x_n\rangle = |x_1\rangle \otimes \cdots |x_{i-1}\rangle \otimes A|x_i\rangle \otimes \cdots \otimes |x_n\rangle$$

$A(i)$ è quindi il gate che applica A al qubit i-esimo e l'identità a tutti gli altri, cioè in altre parole

$$A(i) = I \otimes \cdots \otimes A \otimes \cdots I.$$

In maniera analoga un gate a due qubit da luogo a $n(n-1)$ gate a n qubit.

Dato un set di gate a uno e due qubit diremo che questo set è **universale** se , per ogni $n \geq 2$, ogni gate a n qubit può essere approssimato con precisione arbitraria da un circuito costituito solo dai gate del set[17]. Diremo invece che il set è **esattamente universale** se ogni gate a n qubit può essere ottenuto esattamente da un circuito costituito solo dai gate del set.

In termini matematicamente più precisi, chiamato $\mathfrak{S}$ l'insieme dei gate che si considerano si ha che:

- $\mathfrak{S}$ è universale se $\forall n$, $\forall W \in U(2^n)$ e $\forall \epsilon > 0$ esistono $U_1, ..., U_k \in \mathfrak{S}$ tali che[18]
$$d(W, \underbrace{U_k \cdots U_2 U_1}_{U}) := 1 - \inf_{|\psi\rangle \neq 0} \frac{\langle\psi|W^\dagger U|\psi\rangle}{\langle\psi|\psi\rangle} < \epsilon$$
- $\mathfrak{S}$ è esattamente universale se $\forall W \in U(2^n)$ esistono $U_1, ..., U_k \in \mathfrak{S}$ tali che
$$W = U_k \cdots U_2 U_1.$$

[17] Per essere precisi, dai gate a n qubit generati dai gate del set.

[18] La metrica scelta non è importante, $d(\cdot, \cdot)$ può essere una metrica qualsiasi.

Condizioni equivalenti si possono formulare in termini di $\langle \mathfrak{S} \rangle$. Chiamato $\langle \mathfrak{S} \rangle$ il gruppo generato da $\mathfrak{S}$, ovvero l'insieme di tutti i prodotti di un numero finito di elementi di $\mathfrak{S}$ o loro inverse, si ha che:

- $\mathfrak{S}$ è universale $\Leftrightarrow$ $\langle \mathfrak{S} \rangle$ è denso in $U(2^n), \forall n \in \mathbb{N}$.
- Se[19] $\mathfrak{S} = \mathfrak{S}^{-1}$: $\mathfrak{S}$ è esattamente universale $\Leftrightarrow$ $\langle \mathfrak{S} \rangle = U(2^n), \forall n \in \mathbb{N}$.

Da notare che un set finito di gate può essere universale ma non esattamente universale, in quanto il gruppo che genera sarà numerabile mentre il gruppo unitario è un gruppo continuo (non numerabile).

1.3 Universalità del CNOT

In questo paragrafo ripercorriamo la dimostrazione dell'universalità esatta del CNOT insieme ai gate locali come presentata in letteratura. Ci rifacciamo a [9],[10] e [18]. La dimostrazione può essere suddivisa in tre parti:

1. Si dimostra che le unitarie a due livelli sono un set esattamente universale
2. Si dimostra che CNOT e gate locali sono sufficienti a generare qualsiasi *controlled gate*
3. Si dimostra che attraverso i *controlled gate* si genera una qualsiasi unitaria a due livelli

1.3.1 Prima parte: universalità delle unitarie a due livelli

Con matrice unitaria a due livelli si intende una matrice unitaria agente su uno spazio di Hilbert d-dimensionale che è non banale solo su un sottospazio di dimensione minore o uguale a due. Ad esempio la seguente matrice unitaria 4×4 è a due livelli:

$$\begin{bmatrix} a & 0 & 0 & b \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ c & 0 & 0 & d \end{bmatrix}$$

$a, b, c, d \in \mathbb{C}$ tali che $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ sia unitaria.

[19] Per quanto ci riguarderà la seguente condizione è soddisfatta perchè il nostro set sarà formato da tutti i gate locali più il CNOT che ha la proprietà $V = V^\dagger$.

Diamo ora la procedura per ottenere una qualsiasi unitaria come prodotto di unitarie a due livelli. Iniziamo illustrando il caso 3×3. Segue una generalizzazione qualitativa della procedura al caso generico. Infine presentiamo il risultato con una dimostrazione formale.

Riportiamo la procedura per una generica matrice unitaria 3×3

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}.$$

Mostreremo che è possibile trovare tre matrici unitarie a due livelli U_1, U_2, U_3 tali che

$$U_3 U_2 U_1 U = I$$

e quindi

$$U = U_3^\dagger U_2^\dagger U_1^\dagger.$$

Se $d = 0$ si prende $U_1 = I$ mentre, se $d \neq 0$, si sceglie U_1 di modo che sia a due livelli e che, moltiplicata per U dia

$$U_1 U = \begin{bmatrix} a' & b' & c' \\ 0 & e' & f' \\ g' & h' & i' \end{bmatrix}$$

cioè porti ad azzerare la componente $(2, 1)$. Per arrivare a questo risultato si sceglie

$$U_1 = \begin{bmatrix} \frac{a^*}{\sqrt{|a|^2+|d|^2}} & \frac{d^*}{\sqrt{|a|^2+|d|^2}} & 0 \\ \frac{d}{\sqrt{|a|^2+|d|^2}} & \frac{-a}{\sqrt{|a|^2+|d|^2}} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

come si può facilmente verificare questo garantisce il risultato voluto. Ora se $g' = 0$ si prende

$$U_2 = \begin{bmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

altrimenti

$$U_2 = \begin{bmatrix} \frac{a'^*}{\sqrt{|a'|^2+|g'|^2}} & 0 & \frac{g'^*}{\sqrt{|a|^2+|d|^2}} \\ 0 & 0 & 1 \\ \frac{g'}{\sqrt{|a'|^2+|g'|^2}} & 0 & \frac{-a'}{\sqrt{|a'|^2+|g'|^2}} \end{bmatrix}$$

In questo modo si ha

$$U_2U_1U = \begin{bmatrix} 1 & b'' & c'' \\ 0 & e'' & f'' \\ 0 & h'' & i'' \end{bmatrix}. \tag{1.33}$$

Dalla unitarietà del prodotto delle matrici segue che $b'', c'' = 0$. Infine scelta

$$U_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & i''^* \end{bmatrix},$$

si verifica subito che $U_3U_2U_1U = I$ che è il risultato cercato. Data ora una generica unitaria U $d \times d$ è possibile trovare matrici unitarie a due livelli $U_1, ..., U_{d-1}$ tali che

$$U_{d-1} \cdots U_1U$$

abbia un uno in posizione $(1, 1)$ e zero altrove sulla prima riga e colonna, ossia

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & u_{22} & \cdots \\ 0 & \cdots & u_{dd} \end{bmatrix}.$$

Si ripercorre poi la stessa procedura per la sottomatrice unitaria $d-1 \times d-1$ fino ad arrivare ad avere[20]

$$U_kU_{k-1} \cdots U_1U = I \Rightarrow U = U_k^\dagger \cdots U_1^\dagger, \tag{1.34}$$

dove $k \leq (d-1) + (d-2) + \cdots + 1 = d(d-1)/2$.

Teorema 1.3.1.
Una qualsiasi unitaria U agente su $\mathbb{C}^M$ può essere scritta come prodotto di $M(M-1)/2$ matrici unitarie a due livelli.

Dimostrazione. Si ha che per ogni coppia di numeri complessi c_1, c_2 esiste una matrice unitaria 2×2 V tale che

$$V \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} \sqrt{|c_1|^2 + |c_2|^2} \\ 0 \end{pmatrix} \tag{1.35}$$

Da questo ne discende che per ogni vettore unitario $|\xi\rangle \in \mathbb{C}^M$ esistono $(M-1)$ matrici unitarie a due livelli $V^1, ..., V^{M-1}$ tali che

$$V^1 \cdots V^{M-1}|\xi\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \end{pmatrix}, \tag{1.36}$$

[20]Si vede facilmente che l'inversa di una matrice unitaria a due livelli è ancora a due livelli.

dove V^s agisce[21] sul sottospazio generato da $\{|s\rangle, |s+1\rangle\}$. Allora data una matrice unitaria U $M \times M$ abbiamo che moltiplicando U^{-1} a sinistra per opportune matrici $U_1^1, ..., U_1^{M-1}$ possiamo trasformare la prima colonna nel vettore $|1\rangle$. Data l'unitarietà la prima riga diviene il vettore $\langle 1|$. Agendo in maniera analoga sulle rimanenti colonne si ottiene un set di matrici U_j^i, $1 \leq j \leq i \leq M-1$ tali che

$$U_{M-1}^{M-1} \left(U_{M-2}^{M-2} U_{M-2}^{M-1}\right) \cdots \left(U_1^1 \cdots U_1^{M-1}\right) U^{-1} = I \tag{1.37}$$

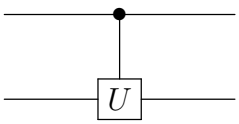
e quindi

$$U = U_{M-1}^{M-1} \left(U_{M-2}^{M-2} U_{M-2}^{M-1}\right) \cdots \left(U_1^1 \cdots U_1^{M-1}\right). \tag{1.38}$$

■

1.3.2 Seconda parte: controlled gate

Un *controlled gate* è un gate con un certo numero di bit di controllo e un certo numero di bit target. Un particolare esempio è lo stesso CNOT. Più in generale saremo interessati a gate Control-U



(1.39)

la cui azione è data da $|a = 1\rangle|b\rangle \to |1\rangle U|b\rangle$ o $|a = 0\rangle|b\rangle \to |0\rangle|b\rangle$.

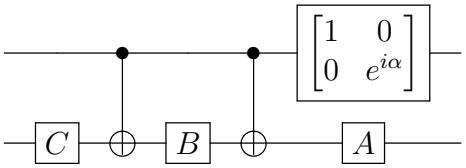
Mostriamo ora come, attraverso solo locali e CNOT, si possa ottenere un qualsiasi controlled gate con un solo bit target. Per raggiungere l'obbiettivo ci serviamo del seguente lemma di cui omettiamo la dimostrazione

Lemma 1.3.2.
Data una qualsiasi matrice $U \in U(2)$, esistono tre matrici unitarie A, B, C tali che $ABC = I$ e

$$U = e^{i\alpha} AXBXC,$$

dove α è un fattore di fase e X è la matrice di Pauli.

Grazie a questo lemma è immediato verificare che il circuito (1.39) è equivalente al seguente



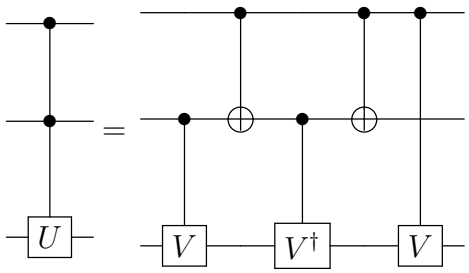
(1.40)

[21] Anche nel seguito della dimostrazione l'indice in alto indicherà il sottospazio su cui agiscono le matrici.

Ora siamo interessati ad implementare con solo CNOT e locali un controlled gate con un numero arbitrario di bit di controllo. Formalmente un gate di questo tipo è indicato come

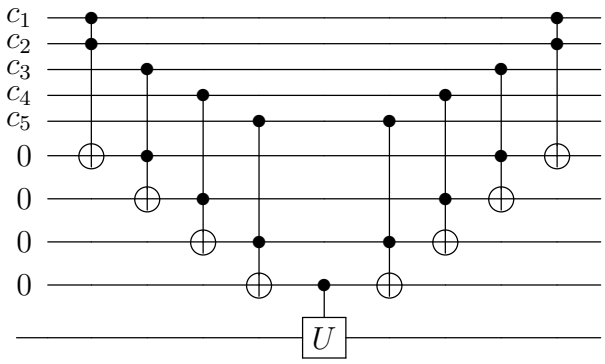
$$C^n(U)|x_1, ..., x_n\rangle|\psi\rangle = |x_1, ..., x_n\rangle U^{(x_1 \cdots x_n)}|\psi\rangle,$$

dove l'esponente di U sta ad indicare che l'operazione viene eseguita quando tutti i qubit di controllo sono uguali[22] a $|1\rangle$. Per il caso $n = 2$ la soluzione è semplice, si verifica infatti che vale la seguente equivalenza



dove $V^2 = U$. In particolare se $U = X$ il gate a primo membro è il gate di Toffoli.

Esiste un modo per implementare un qualsiasi control gate con un solo target[23] attraverso il gate di Toffoli, di seguito riportiamo il circuito nel caso $n = 5$. Da notare che vengono usati quattro bit ancillari:



Detto questo abbiamo che ogni control gate con un solo gate di target è ottenuto con CNOT e gate locali. Possiamo ora passare all'ultima parte della dimostrazione.

[22]Non è difficile considerare dei contolled gate che agiscono nel momento in cui il bit di controllo è 0. In questo caso la notazione grafica è la stessa con al posto di un pallino pieno uno vuoto sul quantum wire del bit di controllo.

[23]Per approfondimenti si rinvia a [9].

1.3.3 Terza parte: conclusione della dimostrazione

Mostriamo infine come, attraverso solo controlled gate, si possa ottenere una qualsiasi matrice unitaria a due livelli agente sullo spazio degli stati di n qubit. Per fare ciò necessitiamo del concetto di *Gray Code*. Dati due numeri binari a, b un gray code che li unisce è una sequenza di numeri binari che inizia da a e termina in b tale che elementi vicini differiscono in un solo bit.

Ora data un'unitaria $2^n \times 2^n$ a due livelli, supponiamo che agisca non banalmente sul sottospazio generato dai vettori della base computazionale $|s\rangle$ e $|t\rangle$ e indichiamo gli elementi del gray code congiungenti s, t con g_j dove $g_1 = s$ e $g_m = t$[24]. Il circuito che implementa U si ottiene nel seguente modo. Per prima cosa si fa un bit flip per scambiare $|g_1\rangle$ con $|g_2\rangle$ usando come target il bit in cui i due differiscono e condizionato dall'avere tutti gli altri bit nello stesso stato. Si prosegue con controlled gate analoghi scambiando $|g_2\rangle$ con $|g_3\rangle$ e via fino ad arrivare a scambiare $|g_{m-2}\rangle$ con $|g_{m-1}\rangle$. A questo punto si fa un control-$\tilde{U}$, dove $\tilde{U}$ è la sottomatrice 2×2 di U non banale, sul bit in cui differiscono $|g_{m-1}\rangle$ e $|g_m\rangle$. Infine si ripetono i controlled gate iniziali al contrario per eliminare gli scambi fatti.

Quanto detto conclude la dimostrazione. Infatti abbiamo dimostrato che ogni unitaria su n qubit può essere ottenuta dalle sole unitarie a due livelli, queste a loro volta possono essere ottenute da circuiti con solo control gate con un solo bit target e infine questi ultimi si ottengono da circuiti contenenti solo CNOT e gate locali. Da qui l'universalità del set dei gate locali più il CNOT. Come si vede la dimostrazione, anche se non complessa, è abbastanza laboriosa.

1.4 Universalità dei gate entanglanti

In quest'ultimo paragrafo riportiamo la dimostrazione di [7] dell'universalità esatta dei gate locali assieme ad un qualsiasi gate entanglante[25]. Il punto in cui questa dimostrazione non funziona per il caso della RQT verrà messo in evidenza.

Il teorema principale è il seguente:

Teorema 1.4.1. *Dato un gate a due qubit V, sono equivalenti le seguenti affermazioni:*

1. *l'insieme di tutti i gate locali assieme a V è universale*
2. *l'insieme di tutti i gate locali assieme a V è esattamente universale*

[24] Chiaramente $m \leq n + 1$ dalla definizione di gray code.

[25] La dimostrazione in [7] è ancora più generale di quella qui riportata a causa del fatto che come sistemi elementari vengano considerati qudit, ovvero sistemi quantistici a d-livelli.

3. V è entanglante

Evidentemente l'implicazione $2 \Rightarrow 1$ è ovvia per le definizioni prima date di universalità di un set di gate. La dimostrazione dell'implicazione $1 \Leftrightarrow 3$ è non banale ma anch'essa non molto complessa, tuttavia non ci interessa ai fini del nostro lavoro. La parte interessante, che è anche la più complessa, è la dimostrazione dell'implicazione $3 \Rightarrow 2$. Come sottolineato da Harrow, [12], perchè la dimostrazione in [7] sia completa in linea di principio è necessario assumere di avere a disposizione non solo V ma anche[26] V^{-1}. Nel suo articolo Harrow mostra come il risultato in [7] rimanga valido senza dover assumere di avere anche $V^\dagger$ e colma quindi, con il suo teorema, il passo mancante nella dimostrazione.

Nel seguito della nostra trattazione non ci cureremo del problema evidenziato da Harrow supponendo quindi di aver accesso anche a V^{-1}. Tuttavia ai fini della generalità della dimostrazione si rimanda al lavoro di Harrow per lo step mancante.

La dimostrazione dell'implicazione procede per step diversi. In quanto segue non riportiamo le dimostrazioni dettagliate che possono essere trovate in [7].

1. Riduzione al caso n=2

Per poterci ridurre al caso n=2 è necessario dimostrare che l'insieme di tutti i gate a due qubit è esattamente universale. In questo caso si hanno $\binom{n}{k}$ sottogruppi $H(p,q) = \{A(p,q) : A \in U(4)\}$ di $U(2^n)$, dove $A(p,q)$ indica che il gate a due qubit A è fatto agire sui qubit q-esimo e p-esimo. Ogni $H(p,q)$ è un sottogruppo chiuso e connesso, quindi essendo $U(2^n)$ un gruppo di Lie compatto si può utilizzare il Lemma C.1.1. Quello che è sufficiente mostrare è che tali sottogruppi generano un sottogruppo denso di $U(2^n)$. Questo è dimostrato da Di Vincenzo in [19], quindi grazie a LemmaC.1.1 abbiamo il risultato cercato. Ovviamente una dimostrazione alternativa di questo punto è quella del paragrafo precedente, ovvero dell'universalità esatta del CNOT con i gate locali.

Adesso che ci siamo ridotti al caso $n = 2$ non resta che dimostrare che V assieme alle locali, cioè $H = U(2) \otimes U(2)$, genera tutto $U(4)$. Definiamo

$$H' = VHV^\dagger,$$

dove V è un gate entanglante. Siccome H è un sottogruppo chiuso e connesso così è anche H'. Allora, da LemmaC.1.1, sappiamo che se questi due sottogruppi generano un sottogruppo denso di $U(4)$ allora generano tutto $U(4)$ e quindi avremmo il nostro risultato di universalità.

Quindi si vuole mostrare che H e H' generano un sottogruppo denso di $U(4)$.

[26] Ovvero che $V^\dagger$ sia nel set di gate considerati.

2. Analisi delle algebre di Lie I:

Chiamiamo $\mathfrak{h}$ e $\mathfrak{h}^{'}$ le algebre di H e $H^{'}$ rispettivamente. Sia ora ξ l'algebra di Lie generata da $\mathfrak{h}$ e $\mathfrak{h}^{'}$, abbiamo $\mathfrak{h} \subseteq \xi \subseteq \mathfrak{g}$, dove $\mathfrak{g} = \mathfrak{u}(4)$. Il primo risultato che si dimostra è che

Lemma 1.4.2.
Non ci sono algebre di Lie contenute strettamente tra $\mathfrak{h}$ *e* $\mathfrak{g}$*. Cioè risulta che* $\xi = \mathfrak{h}$ *oppure* $\xi = \mathfrak{g}$*.*

La dimostrazione di questo lemma, come anche quella della proposizione che segue, può essere trovata in [7]. Detto questo si ha che valgono le seguenti implicazioni:

$$\xi = \mathfrak{h} \Leftrightarrow \mathfrak{h} = \mathfrak{h}^{'} \Leftrightarrow H = H^{'} \tag{1.41}$$

3. Analisi delle algebre di Lie II:

Dalla definizione di *normalizer*, data in appendice, si ha che l'ultima uguaglianza è vera se e soltante se $V \in N_{U(4)}H$. Tuttavia si può dimostrare la seguente

Proposizione 1.4.3.
$N_{U(4)}H$ *è il gruppo dei gate non-entanglanti*[27] *.*

Quindi abbiamo che $V \notin N_{U(4)}H$ e quindi $\xi = \mathfrak{g}$. Questo ci dice che H ed $H^{'}$ generano un sottogruppo denso di $U(4)$ e quindi, dal LemmaC.1.1, generano tutto il gruppo. Ma allora ne segue che l'insieme dei gate $H \cup \{V\}$, cioè i locali più un generico entanglante, genera tutto il gruppo, il che è il risultato di universalità esatta che cercavamo.

1.4.1 Dimostrazione di Brylinsky e RQT

In questo breve paragrafo osserviamo dove la dimostrazione appena illustrata, che è stata l'impulso d'avvio per ricavare i risultati originali di questo lavoro di tesi, viene a non valere nel caso della teoria quantistica sugli spazi reali. La teoria quantistica su spazi reali verrà ripresa in maggior dettaglio nel prossimo capitolo e i risultati di universalità verranno illustrati nell'ultimo. Per il momento ci è sufficiente dire che per il caso $n = 2$ il gruppo delle trasformazioni locali sarà assunto essere $SO(2) \otimes SO(2)$ la cui algebra è costituita da

$$\mathfrak{h} = span\{I \otimes Y, Y \otimes I\} = span\{v_1, v_2\}. \tag{1.42}$$

[27]Tra i gate non entanglanti non vi sono solo i gate locali. Infatti i gate non-entanglanti vengono caratterizzati in [7] come tutti e soli i gate del tipo $A \otimes B$ o $(A \otimes B)P$, dove $A, B \in U(2)$ e P è lo SWAP, formando il gruppo L. Quindi si ha $H \subset L \subset U(4)$.

Detto questo si consideri l'algebra del gruppo $SO(4)$:

$$\mathfrak{so}(4) = span\{I \otimes Y, Y \otimes I, X \otimes Y, Z \otimes Y, Y \otimes Z, Y \otimes X\} = span\{v_1, v_2, v_3, v_4, v_5, v_6\}, \tag{1.43}$$

vogliamo mostrare che in questo caso esiste un'algebra ξ strettamente inclusa tra $\mathfrak{h}$ e $\mathfrak{so}(4)$. Per fare questo basta osservare che valgono le seguenti regole di commutazione:

$$[v_1, v_2] = 0 \tag{1.44}$$
$$[v_1, v_3] = 0 \tag{1.45}$$
$$[v_1, v_4] = 0 \tag{1.46}$$
$$[v_2, v_3] = 2v_4 \tag{1.47}$$
$$[v_2, v_4] = -2v_3 \tag{1.48}$$

ottenute mediante la relazione

$$[A \otimes B, C \otimes D] = [A, C] \otimes BD + CA \otimes [B, D]. \tag{1.49}$$

Quindi $\xi = span\{v_1, v_2, v_3, v_4\}$ è un'algebra dato che il sistema di generatori citati è chiuso per commutazione, ed è tale che $\mathfrak{h} \subset \xi \subset \mathfrak{so}(4)$. Quindi in questo caso l'analogo del Lemma1.4.2 non vale.

Capitolo 2

Teorie Operazionali

2.1 Introduzione

L'assiomatizzazione della Teoria Quantistica, a partire da assiomi di carattere fisico, è stato un problema aperto sin dalla nascita della meccanica quantistica negli anni '20. Dal punto di vista matematico la teoria ha solide fondamenta, come descritte nel lavoro fondamentale di von Neumann *Mathematical Foundations of Quantum Mechanics* del 1932. Tuttavia manca una chiara traduzione degli assiomi matematici nel linguaggio della fisica. In questo capitolo introdurremo il formalismo delle teorie probabilistiche operazionali (OPT) e rifacendoci ai lavori [33] e [32] mostreremo quali sono gli assiomi di natura informazionale da cui deriva la teoria quantistica[1].

Fatto questo ci concentreremo sull'assioma di discriminabilità locale che permette di riconciliare il riduzionismo con il carattere olistico della teoria quantistica. Introdurremo poi la teoria quantistica su spazi vettoriali reali (RQT) mostrando come essa possa essere formulata come OPT in cui gli stati sono descritti da matrici densità reali. Mostreremo infine, rifacendoci a [21], che la RQT non possiede la discriminabilità locale senza tuttavia avere un olismo illimitato.

Nel precedente capitolo abbiamo sviluppato il formalismo dei circuiti quantistici. Questo stesso formalismo trova anche una naturale applicazione nella descrizione di teorie probabilistiche generalizzate venendo a costituire una notazione grafica che si sostituisce alle formule.

[1] In dimensione finita.

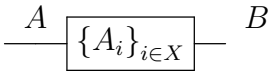
2.2 Formalismo delle OPT

Una teoria probabilistica operazionale è una teoria che descrive un set di esperimenti che possono essere realizzati attraverso dispositivi fisici e da predizioni circa le probabilità dei risultati in questi esperimenti.

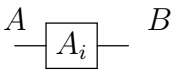
Iniziamo introducendo i concetti fondamentali di sistema e test per arrivare a definire cosa si intende per teoria operazionale. Poi introdurremo la probabilità arrivando alla definizione di OPT.

Test e sistemi sono le nozioni primitive del framework operazionale. Un test è pensabile come un singolo uso di un device fisico[2]. Il device deve avere un sistema in input e uno di output, che verranno indicati con lettere maiuscole, e una volta usato produce un outcome $i \in X$, dove X è un qualche insieme. Il fatto che il dispositivo abbia prodotto un outcome, che sia un rumore o una luce che si accende o un numero su un display, indica che un qualche *evento* è accaduto. Un evento è un concetto primitivo, è qualcosa che accade. Formalmente abbiamo la seguente

Definizione 2.1.
Un test con sistema in input A e in output B è una collezione di eventi $\{A_i\}_{i\in X}$, dove X è un qualche insieme di outcome. Un test verrà rappresentato come



mentre un singolo evento

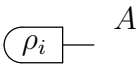


Chiaramente un test può avere più di input e più di un output. Un esperimento è dato dall'applicazione di diversi dispositivi su sistemi fisici, questo viene descritto attraverso un grafo aciclico diretto (le loop sono proibite) dove le box rappresentano test mentre i fili sono i sistemi fisici. Qui c'è un punto importante del formalismo. I fili nei circuiti rappresentano i sistemi ed hanno solo la funzione di determinare come i vari test (o eventi) sono tra loro connessi. Infatti è possibile connettere tra loro solo test tali che un output del primo coincida con un input del secondo. Quindi i sistemi sono le connessioni causali tra eventi differenti. Da notare che i fili, per quanto detto, non rappresentano l'evoluzione libera che è invece un particolare tipo di test. Tra i vari tipi di sistemi vi è anche quello banale, che rappresenta l'assenza di una connessione causale e pertanto è indicato dall'assenza di un filo e arrotondando la corrispondente parte della box a cui è connesso. L'insieme degli eventi di un test è chiuso rispetto alle operazioni di unione, intersezione e complementazione, quindi gli eventi formano un'algebra Booleana.

[2]Tuttavia un test non descrive per forza un dispositivo costruito dall'uomo ma può benissimo descrivere un fenomeno naturale come l'interazione tra particelle.

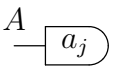
Definizione 2.2.
Un test con un singolo outcome, cioè $|X| = 1$, è detto **deterministico**. Un test con il sistema banale come input è detto **test di preparazione** e indicato con

$$|\rho_i)_A$$



Un test con sistema banale come output è detto **test di osservazione** e indicato con

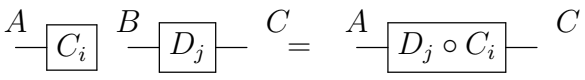
$$(a_j|_A$$



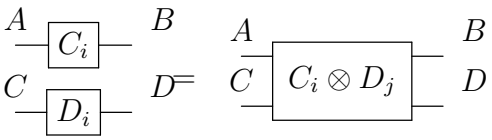
In QT un test di preparazione è detto *random source of quantum states* mentre un test di osservazione è una misurazione quantistica rappresentata da una POVM (Positive Operator Valued Measure).

Nelle precedenti definizioni abbiamo introdotto, affianco alla rappresentazione circuitale, una notazione alla Dirac (per quelli che a breve saranno identificati come stati ed effetti della teoria) che risulta più familiare a chi conosca la meccanica quantistica.

I test si possono comporre in serie ed in parallelo, dando ancora dei test. I sistemi si possono comporre in parallelo dando un sistema composto. In particolare si ha per la composizione in serie



e per quella in parallelo



Possiamo ora definire una teoria operazionale:

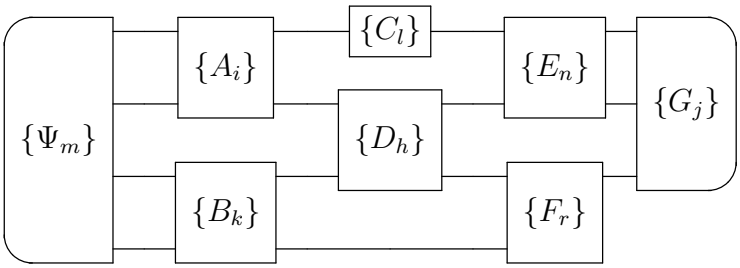
Definizione 2.3.
Una teoria operazionale è data da un insieme di sistemi chiuso sotto composizione e da un insieme di test chiuso sotto composizione in serie e in parallelo.

In una teoria operazionale un circuito può rappresentare come sono connessi i dispositivi fisici in un esperimento oppure l'insieme degli eventi che accadono nello stesso.

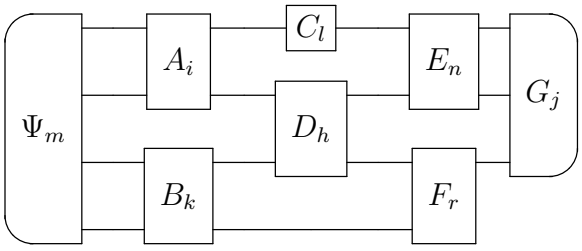
Facciamo ora un passo successivo. La teoria fin qui esposta può descrivere esperimenti o processi naturali, tuttavia vogliamo ora poter dare previsioni probabilistiche sui possibili outcome di un esperimento. Per avere una struttura probabilistica si deve imporre che i test dal sistema banale in se stesso siano *probabilità*. In questo modo si ha

Definizione 2.4.
Una teoria operazionale è **probabilistica** (OPT) se ogni test $\{p_i\}_{i\in X}$ dal sistema banale in se stesso è associato ad una distribuzione di probabilità per gli outcome, ovvero si ha che $p_i \in [0,1]$ e $\sum_{i\in X} p_i = 1$ e la composizione di due test dal sistema banale in se è data dal prodotto delle probabilità.

Quindi ora un circuito chiuso (da un test di preparazione all'inizio e uno di osservazione alla fine) rappresenta una distribuzione di probabilità, Fig.(2.1). Se sono specificati gli eventi per ogni test, Fig.(2.2), rappresenta la probabilità congiunta di tali eventi.



(2.1)



(2.2)

In una OPT un evento di preparazione per il sistema A definisce una funzione che manda un evento di osservazione in una probabilità $\rho_i : (a_j| \mapsto (a_j|\rho_i)$ ed allo stesso modo un evento di osservazione definisce una funzione che manda un evento di preparazione in una probabilità $a_j : |\rho_i) \mapsto (a_j|\rho_i)$. Dal punto di vista probabilistico due eventi di preparazione (o osservazione) che danno luogo alla stessa funzione sono equivalenti e questo fatto porta alla definizione di stati ed effetti della teoria.

Definizione 2.5.
Gli **stati** sono classi di equivalenza di eventi di preparazione mentre gli **effetti** sono classi di equivalenza di eventi di osservazione.

Prendendo combinazioni lineari a coefficienti reali di stati o di effetti si ottengono due spazi vettoriali reali uno duale dell'altro. Chiamati $St(A)$ e $Eff(A)$ l'insieme degli stati e effetti, rispettivamente, del sistema A gli spazi vettoriali saranno indicati con $St_{\mathbb{R}}(A)$ e $Eff_{\mathbb{R}}(A)$. A questo punto ogni evento da un sistema A ad un sistema B induce una mappa lineare $C_i : St_{\mathbb{R}}(A) \to St_{\mathbb{R}}(B)$. Due eventi da A a B sono equivalenti se per ogni sistema C i due eventi composti in parallelo con la mappa identità su C inducono la stessa mappa.

Definizione 2.6.
Le **trasformazioni**, da A a B, sono classi di equivalenza di eventi.

Una trasformazione deterministica è detta **canale**. Un canale da A a B è reversibile se esiste un'altro canale da B a A tale che la composizione in serie dei due dia il canale identico. Le trasformazioni reversibili da un sistema in se stesso formano un gruppo. Diamo ora due ultime definizioni prima di passare ad esporre gli assiomi da cui si deriva la QT in dimensione finita.

Definizione 2.7.
Un *refinement* di un evento C è dato da un test $\{D_j\}_{j\in X}$ e un sottoinsieme $Y \subseteq X$ tali che $C = \sum_{i\in Y} D_i$. Un evento $D \in \{D_j\}_{j\in X}$ raffina C. Se inoltre C ammette solo refinement banali allora è detto **atomico**.

Definizione 2.8. Uno stato atomico è detto **puro**. Uno stato che non sia atomico è detto **mixed**. Uno stato mixed che può essere raffinato da ogni altro stato è detto **completely mixed**.

2.3 Teoria Quantistica in dimensione finita

Avendo introdotto le nozioni fondamentali delle OPT possiamo riportare gli assiomi da cui è possibile derivare la teoria quantistica, [32]. Va sottolineato che questi sono tutti principi di natura operazionale, dove con questo si intende che sono principi che possono essere espressi usando solo i concetti delle teorie operazionali probabilistiche (come stato, effetto, trasformazione e loro derivati).

Riportiamo ora di seguito i cinque assiomi più il postulato di purificazione. Di seguito faremo dei brevi commenti sull'assioma di causalità e il postulato di purificazione, rimandando l'analisi della discriminabilità locale ad un paragrafo a parte.

Assioma 1 (Causalità)**.**
La probabilità degli eventi di preparazione è indipendente dalla scelta dei test osservazionali. Ovvero dato un test di preparazione $\{\rho_i\}$ la probabilità dell'evento ρ_i data la scelta del test osservazionale $\{a_j\}_{j\in Y}$, $p(i|a_j) = \sum_{j\in Y}(a_j|\rho_i)$, è indipendente dalla scelta del test osservazionale.

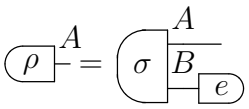
Una OPT che soddisfa questo assioma è detta *causale*. Lo stesso assioma si può riformulare in maniera equivalente richiedendo che dati due test $\{A_i\}, \{B_j\}$ connessi da almeno un sistema, la probabilità marginale di un evento del primo non dipenda dalla scelta del secondo test, mentre la probabilità marginale di un evento del secondo test in generale dipende dalla scelta del primo. Questa asimmetria delle marginali corrisponde al *no signaling from the future* ed è la causalità stessa. L'assioma di causalità può essere quasi pensato come parte del framework data la sua natura fondamentale e la sua fondatezza fisica.

Una OPT causale è caratterizzata dal fatto che, per ogni sistema, l'effetto deterministico è unico e ogni stato è proporzionale ad uno deterministico. In QT l'effetto deterministico non è altro che l'operatore identità sullo spazio di Hilbert del sistema mentre uno stato deterministico non è altro che una matrice densità a traccia unitaria. L'effetto deterministico per un sistema A è indicato da $(e|_A$.

Il fatto che l'effetto deterministico sia unico per ogni sistema porta a poter definire il concetto di stato marginale. Dato uno stato di un sistema composto $|\sigma)_{AB}$, il suo marginale sul sistema A è lo stato

$$|\rho)_A = (e|_B|\sigma)_{AB}, \tag{2.3}$$

o in circuiti



(2.4)

Passiamo ora al secondo assioma introducendo prima il concetto di stati perfettamente distinguibili. Dato un insieme di stati deterministici $\{\rho_i\}_{i\in X}$, questi sono perfettamente distinguibili se esiste un test osservazionale $\{a_j\}_{j\in X}$ tale che

$$(a_j|\rho_i) = \delta_{ij}. \tag{2.5}$$

Assioma 2 (Perfect distinguishability)**.**
Ogni stato non completely mixed può essere perfettamente distinto da un qualche altro stato.

Il terzo assioma riguarda la compressione dell'informazione e necessita di un breve preambolo per poterne capire il significato. Dato un test di preparazione $\{\rho_i\}_{i\in X}$, con $\rho_i \in St(A)$ tale che $\sum_{i\in X}(e|\rho_i) = 1$, questo è detto sorgente di informazione. Uno schema di compressione è dato da una operazione di codifica $\mathfrak{E}$ da A ad un sistema C tale che $dim(St(C)) \leq dim(St(A))$. Diremo che uno schema di compressione è *lossless* per la sorgente se esiste una operazione di decodifica $\mathfrak{D}$ tale che

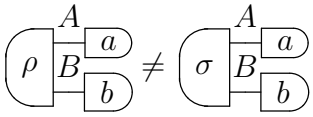
$$\mathfrak{D}\mathfrak{E}|\rho_i) = |\rho_i), \forall i \in X \tag{2.6}$$

e diremo che lo schema è lossless per uno stato ρ se lo è per ogni sorgente $\{\rho_i\}_{i\in X}$ tale che $\sum_{i\in X} |\rho_i) = |\rho)$. Uno schema di compressione è detto *ideale* se è lossless e la dimensione del sistema C è la minore possibile.

Assioma 3 (Ideal compression)**.**
Per ogni stato esiste uno schema di compressione ideale.

Enunciamo ora l'assioma di discriminabilità locale che analizzeremo in seguito.

Assioma 4 (Discriminabilità locale)**.**
Per ogni coppia di stati differenti $|\rho), |\sigma) \in St(AB)$ esistono due effetti $a \in Eff(A)$ e $b \in Eff(B)$ tali che



(2.7)

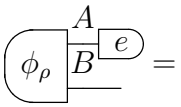
Ovvero i due stati danno diverse probabilità per almeno un esperimento locale.

Riportiamo ora l'ultimo assioma, in questo si fa uso del concetto di misura atomica, che consiste in una misura in cui ogni effetto è atomico.

Assioma 5 (Pure conditioning)**.**
Se un sistema bipartito è in uno stato puro allora ogni outcome di una misura atomica su un sottosistema induce uno stato puro sull'altro.

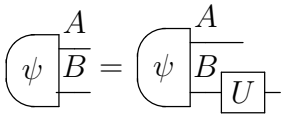
Gli assiomi elencati fino a questo momento sono soddisfatti sia dalla teoria quantistica che dalla teoria probabilistica classica e a meno dell'assioma di discriminabilità locale anche dalla RQT. Ora introduciamo il postulato di purificazione che viene a caratterizzare la teoria quantistica tra tutte le OPT che soddisfano gli assiomi precedenti.

Dato uno stato deterministico ρ di un sistema A una sua **purificazione** è uno stato puro $\phi_\rho \in St(AB)$, per un qualche B[3], tale che il suo marginale sul sistema A sia proprio ρ. Ovvero



(2.8)

Postulato 1.
Ogni stato ha una purificazione. Fissato il sistema purificante la purificazione è unica a meno di canali reversibili sul sistema purificante, cioè



(2.9)

[3]Detto sistema purificante.

Questo postulato intuitivamente dice che l'ignoranza su una parte (stato non puro di un sottosistema) è sempre compatibile con la massima conoscenza del tutto (stato puro del sistema composto). Inoltre la richiesta di unicità è la chiave che permette di derivare a partire da questo postulato numerose caratteristiche della QT. Conseguenze dirette del postulato sono ad esempio la transitività del gruppo delle trasformazioni reversibili sugli stati puri, l'unicità dello stato invariante sotto l'azione di tale gruppo e molti altri. Riportiamo infine per completezza quello che è il teorema chiave, dimostrato in [33], utilizzato in [32] per derivare la QT dagli assiomi più il postulato di purificazione.

Teorema 2.3.1 (State specify the theory)**.**
Date due OPT Θ_1 *e* Θ_2 *che soddisfano il postulato di purificazione, se hanno lo stesso insieme di stati deterministici allora* $\Theta_1 = \Theta_2$.

Grazie a questo teorema per derivare dai principi esposti la QT è sufficiente dimostrare che per ogni sistema A gli stati deterministici possono essere descritti come matrici Hermitiane positive con traccia unitaria.

Passiamo ora ad analizzare il postulato di principale interesse per il nostro lavoro, la discriminabilità locale. Come vedremo alla fine del capitolo questo assioma non è soddisfatto dalla teoria quantistica su spazi reali di cui ci interesserà studiare la proprietà di universalità della computazione.

2.3.1 Discriminabilità Locale

Analizziamo l'assioma di discriminabilità locale (LD) e le sue conseguenze. Innanzi tutto la LD per stati bipartiti implica quella per stati multipartiti in generale. La LD permette quindi di rinconciliare il riduzionismo scientifico con l'olismo della teoria quantistica, nel senso che per discriminare uno stato congiunto di N sistemi non è necessario fare un test congiunto a N sistemi ma è sufficiente usare N test di singolo sistema. La LD permette cioè di ottenere lo stato di un sistema composto andando ad operare sui singoli sottosistemi, processo che prende il nome di tomografia di uno stato e che nell'ambito della QT è noto come **tomografia quantistica**.

L'assioma LD è equivalente all'assioma di *local tomography* introdotto in [34], il quale può essere formulato come

Assioma 6 (Local tomography)**.**
Lo stato di un sistema composto AB è completamente caratterizzato dalla statistica delle misure sui sottosistemi A e B.

Vediamo che dalla LD discende il seguente fatto. Ogni stato $\rho \in St(AB)$ ed ogni effetto $E \in Eff(AB)$ possono essere scritti nel seguente modo

$$|\rho)_{AB} = \sum_{i=1}^{D_A} \sum_{j=1}^{D_B} A_{ij} |\alpha_i)_A |\beta_j)_B \tag{2.10}$$

$$(E|_{AB} = \sum_{i,j} B_{ij} (a_i|_A (b_j|_B, \tag{2.11}$$

dove $\{\alpha_i\}, \{\beta_j\}$ e $\{a_i\}, \{b_j\}$ sono basi degli spazi vettoriali $St_{\mathbb{R}}(A)$ $St_{\mathbb{R}}(B)$ e $Eff_{\mathbb{R}}(A)$ $Eff_{\mathbb{R}}(A)$ rispettivamente, (A_{ij}) e (B_{ij}) sono opportune matrici reali e $D_A = dim(St_{\mathbb{R}}(A))$. La dimostrazione di quanto detto è banale anche se si basa su un concetto che non è stato ancora introdotto. Diciamo che un insieme di stati (effetti) è **separante** per gli effetti (stati) se per ogni coppia di effetti (stati) esiste almeno uno stato (effetto) nell'insieme tale che dia probabilità diverse con gli effetti (stati) delle coppia. Si dimostra che un insieme di effetti separanti per tutti gli stati genera tutto $Eff_{\mathbb{R}}(A)$. La LD implica ora che gli effetti fattorizzati siano separanti per gli stati e quindi che questi generino tutto $Eff_{\mathbb{R}}(AB)$. Analogamente siccome lo spazio vettoriale degli stati è il duale di quello degli effetti si ha che gli stati fattorizzati generano tutto $St_{\mathbb{R}}(AB)$. Da quanto detto seguono (2.10) ed (2.11). Quello che si è dimostrato ci dice che

$$St_{\mathbb{R}}(AB) = St_{\mathbb{R}}(A) \otimes St_{\mathbb{R}}(B) \Rightarrow D_{AB} = D_A D_B \tag{2.12}$$

che è la richiesta introdotta da Hardy in [25], come quarto assioma. Vedremo, attraverso l'analisi fatta in [21], che una tale relazione non è valida nella RQT.

2.4 Teoria quantistica su spazi reali

Veniamo ora ad analizzare la RQT della quale saremo interessati a dimostrare la proprietà di universalità per la computazione. Iniziamo con confrontare i sistemi più semplici per la QT, la RQT ed anche la teoria classica. Poi passiamo a mostrare che la RQT intesa come la teoria quantistica ristretta a spazi reali è equivalente alla OPT in cui gli stati sono rappresentati da matrici densità reali. Infine analizziamo il grado di olismo della RQT mostrando che soddisfa ad una richiesta più debole della LD.

2.4.1 Bit, Rebit e Qubit

Come già precedentemente detto il qubit è il sistema quantistico non banale più semplice. Lo spazio di Hilbert associato a tale sistema ha dimensione 2, cioè è

$\mathbb{C}^2$. Quello che vogliamo determinare ora è la struttura del convesso degli stati deterministici per il sistema qubit.

Gli stati di un sistema in QT sono rappresentati da matrici densità, che sono operatori hermitiani positivi, a traccia minore o uguale ad uno[4], sullo spazio di Hilbert del sistema. Nel caso del qubit avremo quindi matrici densità 2×2. Vale il seguente teorema

Teorema 2.4.1 (Sfera di Bloch)**.**
Gli operatori densità a traccia unitaria su $\mathbb{C}^2$ sono in corrispondenza biunivoca con i punti di una 3-palla unitaria B_3. In particolare ogni operatore densità può essere scritto in maniera univoca nella forma seguente

$$\rho = \frac{1}{2}(I + \underline{n} \cdot \underline{\sigma}), \underline{n} \in B_3, \tag{2.13}$$

dove $\underline{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. Gli stati puri corrispondono alla 2-sfera unitaria mentre gli stati mixed sono interni. Lo stato maximally mixed corrisponde al centro della sfera.

Dimostrazione. Le matrici di Pauli più l'identita costituiscono una base ortonormale dello spazio vettoriale reale delle matrici hermitiane 2×2, quindi ogni operatore densità è scrivibile, in maniera unica, come combinazione lineare di queste. Siccome poi vogliamo che la traccia di ogni ρ sia unitaria abbiamo che il coefficiente dell'identità deve essere $1/2$, infatti tutte le matrici di Pauli hanno traccia nulla. Inoltre il fatto che ρ sia hermitiana implica che i coefficienti che moltiplicano le matrici di Pauli debbano essere reali. Infine dalla positività di ρ

$$1 + \langle v|\underline{n} \cdot \underline{\sigma}|v\rangle \geq 0, \forall |v\rangle \in \mathbb{C}^2. \tag{2.14}$$

La relazione precedente implica, come è facile verificare, che $\|n\| \leq 1$. Ricordiamo ora che in QT una matrice densità descrive uno stato puro se e soltanto se è idempotente, cioè $\rho^2 = \rho$, questo implica[5] che

$$Tr(\rho^2) = Tr(\rho) = 1.$$

Siccome si verifica che

$$Tr[\rho^2] = \frac{1}{2}(1 + \|n\|^2), \tag{2.15}$$

[4]Il fatto che uno stato abbia traccia minore di 1 indica il fatto che non sia uno stato deterministico, ovvero che la probabilità di preparazione dello stato sia minore dell'unità. Stato deterministico è sinonimo di stato normalizzato.

[5]La traccia del quadrato della matrice densità è una misura del grado di purezza di uno stato, ed è detta *purity*.

si ha che lo stato è puro se e solo se $\|n\| = 1$, ovvero sta sulla superficie della sfera. Gli stati interni saranno quindi necessariamente mixed e il centro della palla sarà $\rho = \frac{1}{2}I$ che è lo stato maximally mixed (è il massimamente caotico). ■

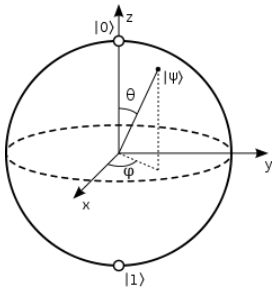


Figura 2.1: La Sfera di Bloch è il convesso degli stati normalizzati per il qubit.

In Fig.2.1 sono riportati i due stati puri perfettamente discriminabili $|0\rangle, |1\rangle$ che costituiscono una base ortonormale dello spazio di Hilbert del qubit. Se volessimo considerare il convesso degli stati per il bit classico questo corrisponderebbe al segmento congiungente i due stati sopra citati, Fig.2.2. Ovvero il convesso degli stati per il bit classico è un simplesso. Questa è una caratteristica di tutti i sistemi classici all'interno del framework operazionale. Il fatto che il convesso classico sia un segmento è dovuto al fatto che il bit classico si può trovare o in $|0\rangle$ o in $|1\rangle$ e non in sovrapposizioni lineari di questi. Ovviamente anche a livello classico sono ammesse delle miscele statistiche dei due stati puri. Come si vede da (2.13) per il caso reale le matrici densità sono diagonali nella base $|0\rangle, |1\rangle$ di autostati di σ_z.

Se invece si considera il convesso degli stati per la RQT, pensata come la OPT in cui gli stati sono rappresentati da matrici densità reali, si ha da (2.13) che il convesso dei normalizzati consiste in un cerchio contenente l'origine nel piano xOz. Ovvero tale convesso non contiene ad esempio il punto corrispondente allo stato $\rho = \frac{1}{2}(I + a\sigma_y)$ dato che questa non è una matrice reale.

2.4.2 Equivalenza con la formulazione operazionale

Per dimostrare l'equivalenza della meccanica quantistica con spazi di Hilbert reali e la OPT in cui gli stati sono matrici densità reali partiamo analizzando la seconda. In quanto segue ci rifacciamo al formalismo sviluppato in [30]. La nostra teoria è quindi una OPT, senza LD, in cui gli stati sono rappresentati da

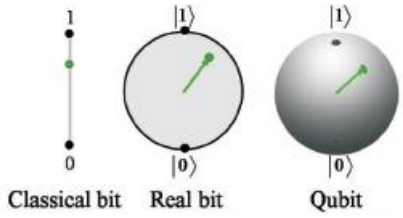


Figura 2.2: Rappresentazione geometrica del convesso degli stati normalizzati per teoria classica, RQT e QT, rispettivamente.

matrici densità reali, ovvero matrici reali simmetriche e positive. Le trasformazioni di questa teoria assumiamo che siano tutte quelle trasformazioni lineari che mandano stati in stati, ovvero che preservano il cono degli stati. Per quanto riguarda gli effetti questi devono essere funzionali lineari sugli stati in $[0, 1]$. In particolare gli effetti saranno rappresentati da matrici A tali che

$$0 \leq Tr[\rho A] \leq 1, \forall \rho. \tag{2.16}$$

Essendo gli stati matrici densità reali simmetriche $\{\rho_{ij}\}$ $d \times d$, ad ogni stato ρ della teoria è possibile associare un vettore v_ρ in uno spazio vettoriale reale di dimensione $\frac{d(d+1)}{2}$ nel seguente modo

$$v_k = \begin{cases} \rho_{1,k}, & \text{se } k \leq d \\ \rho_{2,[k-(d-1)]}, & \text{se } d < k \leq 2d-1 \\ \rho_{2,[k-(2d-3)]}, & \text{se } 2d-1 < k \leq 3d-2 \\ \rho_{2,[k-(3d-6)]}, & \text{se } 3d-2 < k \leq 4d-3 \\ \cdots & \\ \rho_{d,d}, & \text{se } k = d(d+1)/2 \end{cases} \tag{2.17}$$

Lo spazio duale ad $\mathbb{R}^{\frac{d(d+1)}{2}}$ è ancora lo stesso spazio vettoriale. Quindi un effetto è dato da un vettore reale in questo spazio e corrisponde quindi ad una matrice reale $d \times d$ simmetrica.
Una matrice simmetrica è diagonale sulla base dei suoi autovettori ed ha autovalori reali, quindi può essere scritta come

$$A = \sum_i \lambda_i |\alpha_i\rangle\langle\alpha_i|, \tag{2.18}$$

dove gli $|\alpha_i\rangle$ sono gli autovettori (reali) di A. Allora dalla condizione (2.16) si ha che

$$0 \leq A \leq I. \tag{2.19}$$

Infatti scelto $\rho = |\alpha_k\rangle\langle\alpha_k|$ risulta che

$$0 \leq Tr[\rho A] \leq 1 \Rightarrow 0 \leq \lambda_k \leq 1 \ \forall k. \tag{2.20}$$

In quanto segue faremo uso di un formalismo a doppio ket per stati bipartiti introdotto in [30] e [31] che andiamo brevemente ad illustrare. Consideriamo due basi ortonormali $\{|h_i\rangle\}$ e $\{|k_j\rangle\}$ di due spazi di Hilbert H e K di dimensione M ed N rispettivamente. Quello che si può dimostrare è che la mappa dagli operatori lineari da H in K e $K \otimes H$

$$\begin{aligned} &Lin(H,K) \to K \otimes H \\ &M = \sum_{ij} M_{ij}|k_j\rangle\langle h_i| \mapsto |M\rangle\rangle = \sum_{ij} M_{ij}|k_j\rangle|h_i\rangle, \end{aligned} \tag{2.21}$$

è un isomorfismo tra spazi di Hilbert. Relazioni utili che discendono da quanto appena esposto sono le seguenti

$$A \otimes B|C\rangle\rangle = |ACB^T\rangle\rangle, \quad |A\rangle\rangle = A \otimes I|I\rangle\rangle \tag{2.22}$$

$$\langle\langle A|B\rangle\rangle = Tr[A^\dagger B] \tag{2.23}$$

$$Tr_1\left[|A\rangle\rangle\langle\langle B|\right] = AB^\dagger \tag{2.24}$$

$$Tr_2\left[|A\rangle\rangle\langle\langle B|\right] = A^T B^*. \tag{2.25}$$

Consideriamo ora le trasformazioni. Se C è una trasformazione della teoria allora deve mandare stati in stati, anche quando applicata ad un sottosistema di un sistema composto. Quindi avremo

$$(C \otimes \mathfrak{I})|I\rangle\rangle\langle\langle I| = \sum_i p_i |A_i\rangle\rangle\langle\langle A_i|, \tag{2.26}$$

dove $\sum_i p_i = 1$ e gli $|A_i\rangle\rangle$ sono vettori reali[6].
Ora vediamo che la relazione tra stato bipartito e mappa ammissibile è uno ad uno, ovvero avremo un isomorfismo tra il cono delle mappe ammissibili e quello degli stati della teoria. Supponiamo che

$$((C-D) \otimes \mathfrak{I})|I\rangle\rangle\langle\langle I| = 0, \tag{2.27}$$

vogliamo dimostrare che allora $C = D$. Uno stato puro bipartito generico è della forma

$$|B\rangle\rangle\langle\langle B| = (I \otimes B^T)|I\rangle\rangle\langle\langle I|(I \otimes B) = (\mathfrak{I} \otimes F)(|I\rangle\rangle\langle\langle I|), \tag{2.28}$$

[6]Si ricordi che per il teorema spettrale le matrici simmetriche possono essere diagonalizzate sulla base dei propri autovettori attraverso matrici ortogonali.

dove $(\mathfrak{I} \otimes F)$ è la mappa $(I \otimes B^T) \bullet (I \otimes B)$. Detto questo abbiamo che noto il secondo membro di (2.26) abbiamo l'azione di $(C \otimes \mathfrak{I})$ su ogni stato bipartito, infatti

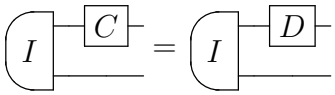
$$(C \otimes \mathfrak{I})|B\rangle\rangle\langle\langle B| = (C \otimes \mathfrak{I})[(I \otimes B^T)|I\rangle\rangle\langle\langle I|(I \otimes B)] \tag{2.29}$$

$$= (I \otimes B^T) \sum_i p_i |A_i\rangle\rangle\langle\langle A_i|(I \otimes B) \tag{2.30}$$

$$= \sum_i p_i |A_i B\rangle\rangle\langle\langle A_i B| \tag{2.31}$$

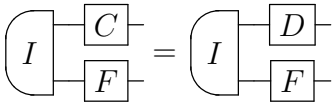
$$= \sum_i p_i (A_i \otimes I)|B\rangle\rangle\langle\langle B|(A_i^T \otimes I). \tag{2.32}$$

Detto questo è facile convincersi che $C = D$ infatti



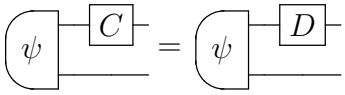
(2.33)

implica



(2.34)

e quindi



(2.35)

questo per ogni stato puro ψ. Dato che la teoria ha la LD sui puri[7] ne discende che $C = D$.

Mostriamo ora che ogni mappa del tipo $(A_i \otimes I) \bullet (A_i^T \otimes I)$ la si può ottenere da una isometrica reale e che quest'ultima la si può a sua volta ottenere a partire da una ortogonale.
Definiamo

$$V = \sum_i \sqrt{p_i} \left(A_i \otimes I_2 \otimes |e_i\rangle_3\right), \tag{2.36}$$

dove gli $|e_i\rangle$ sono vettori di base di un qualche $\mathbb{R}^{d_{out}}$. Questa mappa va da uno spazio a dimensione d_{in} ad uno di dimensione $d_{in}d_{out}$. Si verifica subito che la mappa è isometrica, infatti

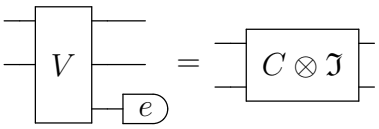
$$V^T V = \sum_{ij} \sqrt{p_i} \left(A_i^T \otimes I_2 \otimes \langle e_i|\right) \left(A_i \otimes I_2 \otimes |e_i\rangle_3\right) = \sum_i p_i \left(A_i^T A_i \otimes I_2\right) = I_{12}. \tag{2.37}$$

[7] Vedi [33].

Ora vale la seguente relazione

$$Tr_3\left[V \bullet V^T\right] = \sum_i p_i \left(A_i \otimes I_2\right) \bullet \left(A_i^T \otimes I_2\right). \tag{2.38}$$

In circuiti



(2.39)

A questo punto consideriamo il seguente operatore

$$O = V \otimes \langle e_0| + \sum_i P_i \otimes \langle e_i|, \tag{2.40}$$

dove gli $|e_k\rangle$ sono una base ortonormale di un qualche $\mathbb{R}^n$ e i P_i e V hanno supporti ortogonali. In particolare valgono le seguenti proprietà

$$V^T P_i = P_i^T V = 0 \tag{2.41}$$
$$V^T V = I \tag{2.42}$$
$$P_i^T P_j = \delta_{ij} I \tag{2.43}$$
$$P_i P_j^T = \delta_{ij} \Pi_i \tag{2.44}$$
$$V V^T = \Pi_{\mathfrak{R}(V)}, \tag{2.45}$$

dove $\mathfrak{R}(V)$ è il range di V e gli operatori Π_k sono proiettori sui range dei P_k. Date queste proprietà si ha

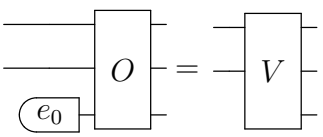
$$O^T O = V^T V \otimes |e_0\rangle\langle e_0| + \sum_i P_i^T P_i \otimes |e_i\rangle\langle e_i| = I \otimes \left(|e_0\rangle\langle e_0| + \sum_i |e_i\rangle\langle e_i| \right) = I, \tag{2.46}$$

e grazie alla ortonormalità dei $|e_k\rangle$

$$O O^T = V V^T + \sum_i P_i P_i^T = \Pi_{\mathfrak{R}(V)} + \sum_i \Pi_i = I. \tag{2.47}$$

Quindi abbiamo infine che

$$O \left(\bullet \otimes |e_0\rangle\langle e_0|\right) O^T = V \bullet V^T \tag{2.48}$$



(2.49)

Abbiamo quindi che la teoria su spazi di Hilbert reali, dove le trasformazioni reversibili sono quelle ortogonali ha, considerando sistemi aperti, le stesse trasformazioni, gli stessi stati ed effetti della OPT prima analizzata e quindi le due sono equivalenti.

2.4.3 Bilocal tomography

Veniamo infine a mostrare in cosa la QT e la RQT differiscono apertamente. La RQT non soddisfa all'assioma di discriminabilità locale. Tuttavia soddisfa a tutti gli altri compreso il postulato di purificazione. Il fatto che non soddisfi al postulato di LD è semplice da provare, infatti dato un singolo re-bit il suo stato è rappresentato da una matrice reale simmetrica, lo spazio vettoriale reale di tali matrici ha dimensione 3 ed ammette come base ortonormale I, σ_x, σ_y. Consideriamo ora un sistema di due re-bit, in questo caso lo spazio vettoriale delle matrici simmetriche ha dimensione 10 ed ammette come base ortogonale $\{I \otimes I, \sigma_\alpha \otimes I, I \otimes \sigma_\alpha, \sigma_i \otimes \sigma_j, \alpha = x, z, i, j = x, y, z\}$. Da quanto detto si osserva subito che la condizione (2.12) non è soddisfatta in quanto $10 \neq 9$ e si capisce anche il motivo. Il fatto è che, pensando in termini di effetti, l'effetto σ_y non fa parte della teoria, tuttavia nel caso di due sistemi $\sigma_y \otimes \sigma_y$ risulta essere un effetto. Questo mostra anche che quello che in QT era un effetto locale in RQT diviene una misura globale.

Mostriamo ora che la RQT sebbene non abbia la LD non è una teoria con un grado di olismo illimitato. Vedremo infatti che sono sufficenti misure uno e due-locali per determinare lo stato di un sistema n-partito[8].

Introduciamo ora il concetto di *bilocal tomography* (BT) e mostriamo che la RQT la possiede. In quanto segue ci inspiriamo a [21]. Una teoria è detta *bilocal tomographic* se lo stato di un sistema composto può essere determinato dalle statistiche di misure che agiscono su uno o al massimo due sottosistemi. Si osservi che se si restringe il campo a sole misure su un sottosistema (locali) si recupera la LD. Per una teoria con BT gli effetti fattorizzati non sono più separanti per gli stati e quindi deve valere, per un sistema bipartito,

$$D_{AB} \geq D_A D_B. \tag{2.50}$$

La dimensione dello spazio degli stati in una OPT è pari al numero di parametri reali necessari ad individuare univocamente uno stato. Assumendo che valga la BT e ricordando la dualità tra spazio degli stati e spazio degli effetti è possibile determinare un limite superiore al numero di parametri che individuano uno stato di un sistema tripartito. Dato il sistema composto ABC

[8]Tutto il ragionamento verrà fatto considerando una particolare partizione di un sistema in sottosistemi ma è indipendente dalla scelta della particolare partizione.

se eseguiamo misure locali sui tre sistemi possiamo ottenere al più un numero di parametri indipendenti pari al numero di misure di questo tipo, ovvero $D_A D_B D_C$. Se ora pensiamo di eseguire, ad esempio, una misura congiunta su AB assieme ad una locale su C possiamo ottenere al più $[D_{AB} - D_A D_B]D_C$, questa espressione è ben definita dato che vale (2.50). Data ora l'ipotesi che valga la BT abbiamo la seguente disuguaglianza

$$\begin{aligned} D_{ABC} &\leq D_A[D_{BC} - D_B D_C] + D_B[D_{AC} - D_A D_C] \\ &+ D_A[D_{BC} - D_C D_C] + D_A D_B D_C \\ &= D_A D_{BC} + D_B D_{AC} + D_C D_{AB} - 2D_A D_B D_C. \end{aligned} \tag{2.51}$$

In RQT lo spazio vettoriale degli stati è lo spazio vettoriale delle matrici reali simmetriche sullo spazio reale associato ad ogni sistema, quindi chiamata n_i la dimensione dello spazio dei vettori di stato per il sistema i-esimo si ha

$$D_i = \frac{n_i(n_i+1)}{2}, \tag{2.52}$$

e dato un sistema composto da m sottosistemi si ha

$$D_{A_1 A_2 \ldots A_m} = \frac{n(n+1)}{2}, \tag{2.53}$$

dove $n = n_1 n_2 \cdots n_m$. Da questa relazione è chiaro che la disuguaglianza (2.51) è soddisfatta dalla RQT, tuttavia questa non è ancora la dimostrazione della BT. Dobbiamo infatti dimostrare che sono sufficienti solo misure uno e due-locali per ottenere tutti i parametri che individuano uno stato. Per fare ciò basta considerare i seguenti n^2 operatori Hermitiani linearmente indipendenti

$$P_v = |v\rangle\langle v|, v = 1, ..., n \tag{2.54}$$

$$P_{uvx} = |u\rangle\langle v| + |v\rangle\langle u|, v > u \tag{2.55}$$

$$P_{uvy} = -i(|u\rangle\langle v| - |v\rangle\langle u|), v > u \tag{2.56}$$

di questi operatori gli ultimi sono $\frac{n(n-1)}{2}$ operatori immaginari che non possono essere considerati nelle combinazioni lineari che rappresentano stati di un singolo sottosistema. Tuttavia entrano in gioco quando si considerano sistemi composti. Chiamiamo ora gli operatori introdotti Q_k con $k \in \{v, uvx, uvy : v > u\}$, sappiamo che operatori del tipo

$$Q_{k_1 \ldots k_m} = Q_{k_1}^{A_1} \otimes Q_{k_2}^{A_2} \otimes \cdots \otimes Q_{k_m}^{A_m}, \tag{2.57}$$

quando considerati come operatori sullo spazio di Hilbert complesso sono indipendenti, tuttavia alcuni di essi sono immaginari e quindi non possono rappresentare stati della RQT. Gli operatori reali sono tutti quelli con al più un numero pari di elementi con $k \in \{uvy, v > u\}$ e si può dimostrare che questi sono esattamente $n(n+1)/2$, con $n = n_1 n_2 \cdots n_m$. Quindi gli operatori reali della forma (2.57) costituiscono una base completa per lo spazio degli stati in RQT. Detto questo si può concludere notando che per ottenere questi operatori, che sono osservabili legittime del sistema, è sufficiente avere i $Q_{k_j}^{A_j}$ reali e ogni coppia di immaginari $Q_{k_i}^{A_i} \otimes Q_{k_j}^{A_j}$, ma i primi rappresentano misure locali mentre i secondi misure a due componenti. Abbiamo quindi dimostrato che la RQT ha la BT e quindi, seppur non abbia la LD, ha olismo limitato dalla Bilocal Tomography. Va citato che un altro modo per indebolire il postulato di LD perchè rimanga valido in RQT è quello di introdurre la discriminabilità locale sui puri, per questo fatto si rimanda a [33].

Detto questo risulta interessante studiare le proprietà di una teoria come la RQT in vista di meglio comprendere quali sono le caratteristiche peculiari della QT e quali invece sono condivise da teorie diverse, ed anche cosa ci si debba aspettare dall'indebolimento dei postulati da cui deriva la QT in vista di possibili generalizzazioni della stessa.

Nel prossimo capitolo analizzeremo il quesito centrale di questo lavoro, ovvero se la RQT abbia una proprietà di universalità della computazione analoga a quella della QT.

Capitolo 3

Dimostrazione per Induzione

In questo capitolo sono presentati i risultati originali di questo lavoro. Si è studiata l'universalità esatta dell'insieme di CNOT e gate locali per la teoria quantistica e per la sua variante con spazi reali. Per fare questo si è preso spunto dal lavoro di J. Brylinsky e R. Brylinski [7] e dal lavoro di DiVincenzo [19] nonchè dall'analisi del problema svolta in [6] da D'Ariano. L'approccio ideato utilizza il fatto che le trasformazioni reversibili nelle due teorie esaminate formano dei gruppi di Lie. Si studiano quindi le algebre di tali gruppi per arrivare al risultato di universalità.
Nella prima parte viene dimostrata l'universalità esatta dell'insieme di CNOT e gate locali per la teoria quantistica attraverso una dimostrazione per induzione. La dimostrazione ideata risulta essere molto più semplice di quelle presenti in letteratura.
Nella seconda parte, con una tecnica analoga, viene dimostrata l'universalità di CNOT e gate locali per la teoria quantistica su spazi vettoriali reali, enfatizzando la differenza con il caso quantistico standard. Quest'ultimo è il risultato originale del lavoro.
Questo capitolo si rifà al lavoro [35] di D'Ariano, Perinotti e Belenchia.

3.1 Dimostrazione: caso standard

Iniziamo con il caso della teoria quantistica. Lo spazio di Hilbert di un singolo qubit è $\mathbb{C}^2$ mentre per un sistema di n-qubit è $\mathbb{C}^{2^n}$. Le trasformazioni reversibili per un sistema di n-qubit formano un gruppo di Lie e sono le trasformazioni unitarie sullo spazio degli stati. Quindi il gruppo in questione è $U(2^n)$. Quello che si vuole dimostrare è che dati CNOT e gate locali si possono generare tutti i gate del gruppo, ovvero si può generare una generica unitaria sul sistema di

n-qubit. Per fare questo la dimostrazione sarà per induzione e farà riferimento all'algebra del gruppo.

Prima di procedere osserviamo che considerare come gruppo $U(2^n)$ oppure $SU(2^n)$ è irrilevante ai fini della dimostrazione. Per vedere questo si consideri una matrice densità arbitraria ρ e un gate quantistico $A \in U(2^n)$ tale che

$$\det A = e^{i\delta} \neq 1. \tag{3.1}$$

L'azione del gate sullo stato del sistema è

$$\rho \to A\rho A^\dagger. \tag{3.2}$$

Si consideri ora il seguente gate quantistico

$$G = e^{i\theta I} = \begin{bmatrix} e^{i\theta} & \cdots & \cdots \\ & \ddots & \\ \cdots & \cdots & e^{i\theta} \end{bmatrix} = e^{i\theta} I, \tag{3.3}$$

questo gate ha, per $\theta = \delta/2n$, determinante pari a $e^{i\delta}$. Ora basta osservare che vale la seguente uguaglianza

$$A\rho A^\dagger = G_\delta A' \rho A'^\dagger G_\delta^\dagger = A' \rho A'^\dagger, \forall \rho, \tag{3.4}$$

dove $A' = G_\delta^\dagger A \in SU(2^n)$. Quindi se ne conclude che ogni gate quantistico in $U(2^n)$ lo si ottiene da un gate speciale attraverso la moltiplicazione per una diagonale di fasi. Quest'ultima, essendo $e^{i\theta} I$, è sempre un gate locale che abbiamo a disposizione per ipotesi. Questo fatto, sebbene banale nel caso del gruppo unitario, non è più vero nel caso del gruppo ortogonale e sarà proprio questo a portare alla differenza tra universalità nel caso quantistico e universalità nel caso della RQT.

Data ora la suriettività[1] della mappa esponenziale per $SU(2^n)$ (e anche $U(2^n)$) si ha che ogni matrice di $SU(2^n)$ può essere scritta come

$$U = e^{iH}, \tag{3.5}$$

dove H è una matrice hermitiana. Per il caso di un singolo qubit il gruppo che si deve considerare è $SU(2)$, i cui generatori infinitesimi[2] sono

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} Y = -\sigma_y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}, \tag{3.6}$$

[1] Vedi Appendice B.

[2] Base dell'algebra del gruppo.

ovvero le tre matrici sigma di Pauli[3].

Nel caso di due qubit i quindici generatori dell'algebra $\mathfrak{su}(4)$ sono dati da:

$$\sigma_i \otimes \sigma_j, \ i,j = 0,1,2,3, \tag{3.7}$$

dove $\sigma_0 = I$ e non si deve considerare il caso $i = j = 0$.
In generale, per n-qubit, una base di $\mathfrak{su}(2^n)$ è data da tutte le stringhe di lunghezza n di sigma di Pauli e identità senza alcuna restrizione[4]. L'accento sulla assenza di vincoli è dovuto al fatto che nel caso della RQT saranno invece presenti.
Enunciamo ora il teorema che vogliamo dimostrare.

Teorema 3.1.1. *Dati i generatori dei gate locali per un sistema di n-qubit, agendo per coniugazione con il gate CNOT si può ottenere una qualunque stringa di lunghezza n di sigma di Pauli. Più precisamente, coniugando con il CNOT i generatori dei gate locali è possibile ottenere tutti i restanti generatori dell'algebra* $\mathfrak{su}(2^n)$.

La dimostrazione del teorema, che sarà per induzione, sarà il primo passo verso la dimostrazione dell'universalità di CNOT e gate locali. Prima di procedere alla dimostrazione richiamiamo alcuni risultati preliminari, validi anche nel caso della RQT.

3.1.1 Risultati preliminari

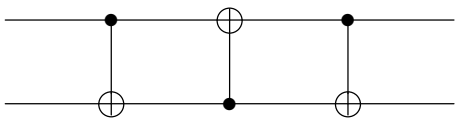
In quanto segue indicheremo con V e P rispettivamente il gate CNOT con primo bit come control-bit e il gate di SWAP. Questi gate sono già stati analizzati nel primo capitolo, qui ne riportiamo le rappresentazioni matriciali

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \tag{3.8}$$

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{3.9}$$

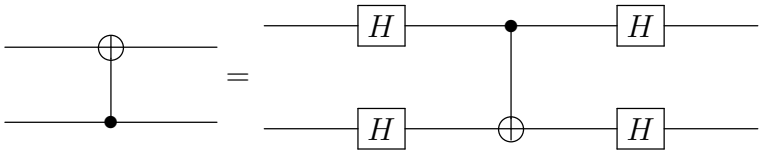
Ricordiamo inoltre che il secondo può essere ottenuto dal primo più gate locali nel seguente modo:

[3]Il generatore mancante per avere tutta l'algebra $\mathfrak{u}(2)$ è semplicemente l'identità 2×2.
[4]A parte il fatto di non considerare $\bigotimes_n I$, che darebbe luogo a tutta l'algebra $\mathfrak{u}(2^n)$.



(3.10)

dove



(3.11)

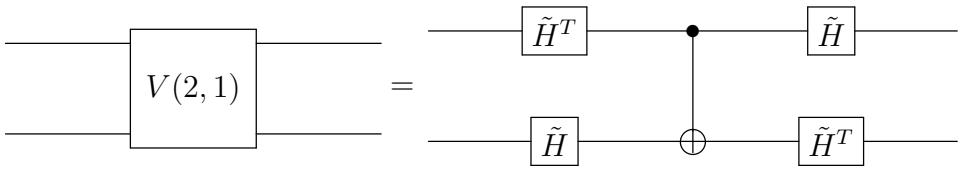
Osserviamo tuttavia che il gate H ha determinante meno uno. Per poter usare questo risultato nel caso della RQT facciamo ora vedere che il gate $V(2,1)$, e quindi anche P, può essere ottenuto dal solo CNOT e gate in $SO(2) \otimes SO(2)$. Per fare questo introduciamo il seguente gate

$$\tilde{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \tag{3.12}$$

Questo gate appartiene a $SO(2)$ ed si verifica facilmente che vale la seguente uguaglianza

$$V(2,1) = (\tilde{H}^T \otimes \tilde{H}) V (\tilde{H} \otimes \tilde{H}^T), \tag{3.13}$$

cioè in circuiti



(3.14)

Veniamo ora a mostrare qual'è l'azione per coniugazione del CNOT su elementi del tipo $\sigma_i \otimes \sigma_j$, dove $i, j = 0, 1, 2, 3$. Ricordiamo[5] che dato un gruppo di Lie G con algebra $\mathfrak{g}$ e dati un elemento $U \in G$ e $H \in \mathfrak{g}$ allora

$$U e^{iH} U^{-1} = e^{iUHU^{-1}}. \tag{3.15}$$

Siccome $V = V^{-1}$ si ha che la coniugazione con il CNOT è data da

$$\sigma_i \otimes \sigma_j \to V \left(\sigma_i \otimes \sigma_j \right) V. \tag{3.16}$$

[5]La dimostrazione può essere trovata in appendice.

Per svolgere i calcoli si sono usate le seguenti espressioni per il CNOT

$$V = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X = I \otimes |+\rangle\langle +| + Z \otimes |-\rangle\langle -|, \tag{3.17}$$

dove $|0\rangle, |1\rangle$ sono gli elementi della base computazionale mentre

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

Valgono allora le seguenti relazioni[6]:

$$I \otimes Y \xrightarrow{V} Z \otimes Y \tag{3.18}$$
$$Y \otimes I \xrightarrow{V} Y \otimes X \tag{3.19}$$
$$I \otimes X \xrightarrow{V} I \otimes X \tag{3.20}$$
$$I \otimes Z \xrightarrow{V} Z \otimes Z \tag{3.21}$$
$$X \otimes I \xrightarrow{V} X \otimes X \tag{3.22}$$
$$Z \otimes I \xrightarrow{V} Z \otimes I \tag{3.23}$$
$$X \otimes X \xrightarrow{V} X \otimes I \tag{3.24}$$
$$Z \otimes Z \xrightarrow{V} I \otimes Z \tag{3.25}$$
$$Y \otimes Y \xrightarrow{V} X \otimes Z \tag{3.26}$$
$$X \otimes Z \xrightarrow{V} Y \otimes Y \tag{3.27}$$
$$X \otimes Y \xrightarrow{V} Y \otimes Z \tag{3.28}$$
$$Z \otimes X \xrightarrow{V} Z \otimes X \tag{3.29}$$
$$Z \otimes Y \xrightarrow{V} I \otimes Y \tag{3.30}$$
$$Y \otimes Z \xrightarrow{V} X \otimes Y \tag{3.31}$$
$$Y \otimes X \xrightarrow{V} Y \otimes I \tag{3.32}$$

Ultima considerazione da fare è la seguente. Nelle dimostrazioni che seguono, quando si parla di applicare il CNOT nel caso di un sistema di n-bit si intende l'applicazione del gate $I \otimes \cdots \otimes V \otimes \cdots \otimes I$, dove il CNOT è applicato sulla desiderata coppia di bit[7]. Questo non pone nessun problema in quanto si ricordi che

$$(A \otimes B)(C \otimes D) = AC \otimes BD. \tag{3.33}$$

[6]La freccia con la sovrascritta indica la coniugazione attraverso il CNOT.

[7]Stesso ragionamento per il gate P, e ragionamento analogo per i gate locali.

3.1.2 Induzione

Dimostriamo ora il teorema 3.1.1 per induzione. Il primo passo consiste nel dimostrare che, a partire dai generatori locali per $n = 2$ qubit si ottengono, mediante coniugazione con CNOT o gate locali, i restanti generatori di $\mathfrak{su}(4)$. I generatori dei gate locali hanno la forma

$$A \otimes I + I \otimes B, A, B \in \mathfrak{su}(2). \tag{3.34}$$

Per quanto ci interessa consideriamo i sei generatori linearmente indipendenti $I \otimes \sigma_i, i = 1, 2, 3$. Coniugando con il CNOT, dalle relazioni precedentemente ottenute, si ottengono:

$$Z \otimes Y \quad Z \otimes Z \quad Y \otimes X \quad X \otimes X \tag{3.35}$$

In particolare l'ultimo generatore ottenuto ci permette di ottenere tutti gli altri ed anche i generatori mancanti semplicemente coniugandolo con rotazioni locali. Infatti risulta che:

$$e^{iZ\pi/4} X e^{-iZ\pi/4} = Y \tag{3.36}$$

$$\tilde{H} X \tilde{H}^\dagger = Z \tag{3.37}$$

Questo conclude il caso $n = 2$. Facciamo ora il passo induttivo, assumiamo di poter generare stringhe arbitrarie di $n - 1$ sigma di Pauli ovvero tutta la base di generatori di $\mathfrak{su}(2^n)$. Vogliamo dimostrare di poter generare, attraverso il CNOT e gate locali, tutte le stringhe di lunghezza n a partire da stringhe del tipo $I \otimes C$, dove C è una stringa arbitraria di lunghezza $n - 1$ che abbiamo a disposizione per ipotesi induttiva. A livello di gate quello che si sta dicendo è che, dato il gate a $n - 1$ qubit e^{itC} possiamo considerare di aggiungere un ulteriore qubit ed avere il gate $I \otimes e^{itC} = e^{itI \otimes C}$. Tutto quello che ci serve dimostrare è che, a partire dalla stringa

$$I \otimes \underbrace{X \otimes X \cdots \otimes X}_{n-1} \tag{3.38}$$

che è nel nostro repertorio per ipotesi, è possibile ottenere la stringa di sole n matrici X. Fatto questo coniugando con gate locali si ottiene una qualunque stringa di matrici sigma. Va fatta una precisazione importante, le stringhe con una o più identità non si ottengono da quella di tutte X, tuttavia sono presenti nel nostro repertorio per ipotesi. Infatti le si ottiene partendo da stringhe del tipo $I \otimes C$, dove C è una stringa arbitraria di lunghezza $n - 1$ con un numero appropriato di I, attraverso l'azione ripetuta del gate P.

Mostriamo quindi come si ottiene la stringa di sole X:

$$I \otimes X^{\otimes_{n-1}} \xrightarrow{P} X \otimes I \otimes X^{\otimes_{n-2}} \xrightarrow{V^{12}} X \otimes X \cdots \otimes X, \tag{3.39}$$

dove con V^{12} intendiamo il CNOT applicato ai primi due bit, ovvero il gate $V \bigotimes_{n-2} I$.

3.1.3 Conclusione della dimostrazione

Abbiamo quindi concluso la dimostrazione del teorema 3.1.1. Ora quello che rimane da mostrare per concludere la dimostrazione dell'universalità dell'insieme di CNOT e gate locali è che aver ottenuto tutti i generatori dell'algebra $\mathfrak{su}(2^n)$ è sufficiente per avere tutto il gruppo $SU(2^n)$ (e quindi per i ragionamenti precedenti tutto $U(2^n)$).
Per far questo notiamo che, detto Λ un generatore dell'algebra, $e^{it\Lambda}, t \in \mathbb{R}$ è un sottogruppo ad un parametro chiuso e connesso di $SU(2^n)$. Notiamo inoltre che grazie alla formula di Lie, Eq.A.2.9, i sottogruppi ad un parametro che abbiamo a disposizione generano un sottogruppo denso di $SU(2^n)$. Allora possiamo applicare il LemmaC.1.1, che riportiamo qui per chiarezza:

Lemma 3.1.2.
Sia $\mathfrak{G}$ un gruppo di Lie compatto. Se $\mathfrak{H}_1, \cdots, \mathfrak{H}_k$ sono sottogruppi chiusi connessi e generano un sottogruppo denso di $\mathfrak{G}$, allora essi generano $\mathfrak{G}$.

Questo conclude la nostra dimostrazione.
Poniamo l'accento sul fatto che una dimostrazione di questo tipo, per quanto ne sappiamo, risulta molto meno laboriosa di quelle presenti in letteratura.

3.2 Dimostrazione:caso della RQT

Passiamo ora al caso della RQT. Nel capitolo precedente abbiamo visto come la OPT in cui gli stati sono descritti da matrici densità reali sia equivalente alla teoria quantistica formulata con spazi vettoriali reali.
Abbiamo ora che lo spazio degli stati del singolo re-bit è $\mathbb{R}^2$e per un sistema di n-rebit è $\mathbb{R}^{2^n}$. Il gruppo dei gate reversibili è il gruppo ortogonale $O(2^n)$ che è un gruppo di Lie compatto ma non connesso[8]. Dato che in questo caso non si ha la libertà di moltiplicare per delle diagonali di fasi non è possibile trascurare le matrici a determinante -1 del gruppo. Sarà proprio questo fatto a portare alla differenza nella prova di Universalità della RQT rispetto alla QT.

[8]Si veda Appendice B.

In questo caso ci concentreremo, per prima cosa, nell'ottenere tutto $SO(2^n)$, che è un gruppo di Lie compatto e connesso, da CNOT e gate locali per poi passare a considerare la componente non connessa all'identità del gruppo ortogonale. Una matrice ortogonale speciale, data la suriettività della mappa esponenziale[9] $exp : \mathfrak{so}(\mathfrak{n}) \to \mathfrak{SO}(\mathfrak{n})$, può sempre essere scritta come

$$A = e^{\xi}, \tag{3.40}$$

dove ξ è una matrice antisimmetrica reale. Il generatore dell'algebra $\mathfrak{so}(2)$ che consideriamo è quindi

$$Y = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \tag{3.41}$$

Invece per quanto riguarda due rebit i sei generatori di $\mathfrak{so}(4)$ saranno:

$$I \otimes Y \quad Y \otimes I \quad Y \otimes X \quad Y \otimes Z \quad X \otimes Y \quad Z \otimes Y. \tag{3.42}$$

Si noti che il numero di Y in ogni generatore è sempre dispari (cioè uno in questo caso) e che questo garantisce l'antisimmetria delle matrici.

Nel caso generale di n-rebit i generatori di $\mathfrak{so}(2^n)$ saranno tutte le stringhe di lunghezza n di matrici X, Y, Z, I con il vincolo di avere un numero dispari di Y. Per il caso di due rebit abbiamo che i gate locali sono gate del tipo

$$A \otimes B, A, B \in SO(2), \tag{3.43}$$

e quindi i generatori a cui siamo interessati sono

$$I \otimes Y \quad Y \otimes X. \tag{3.44}$$

Procediamo ora alla dimostrazione di un teorema analogo a quello esposto prima:

Teorema 3.2.1. *Dati i generatori dei gate locali per un sistema di n-rebit, agendo per coniugazione con il gate CNOT si può ottenere una qualunque stringa di lunghezza n di matrici X,Y,Z,I con un numero dispari di Y . Più precisamente, coniugando con il CNOT i generatori dei gate locali è possibile ottenere tutti i restanti generatori dell'algebra* $\mathfrak{so}(2^n)$.

[9] Vedi Appendice B.

3.2.1 Induzione

Dimostriamo ora il teorema 3.2.1 per induzione in maniera analogo a prima. Il primo passo consiste nel dimostrare che, a partire dai generatori locali per $n = 2$ rebit si ottengono, mediante coniugazione con CNOT o gate locali, i restanti generatori di $\mathfrak{so}(4)$. I generatori dei gate locali sono dati in (3.44). Coniugando con il CNOT, dalle relazioni precedentemente ottenute, si ottengono:

$$Z \otimes Y \quad Y \otimes X, \tag{3.45}$$

e agendo su questi con gate locali[10] si ha:

$$(\tilde{H}^T \otimes I)(Z \otimes Y)(\tilde{H} \otimes I) = X \otimes Y, \tag{3.46}$$

$$(I \otimes \tilde{H})(Y \otimes X)(I \otimes \tilde{H}^T) = Y \otimes Z. \tag{3.47}$$

Abbiamo quindi i sei generatori di $\mathfrak{so}(4)$. Supponiamo adesso di poter generare stringhe arbitrarie, con numero dispari di Y, di $n-1$ matrici X, Y, Z, I. Ovvero tutta la base di generatori di $\mathfrak{so}(2^{n-1})$. Vogliamo dimostrare di poter generare, attraverso il CNOT e gate locali, tutte le stringhe di lunghezza n a partire da stringhe del tipo $I \otimes C$, dove C è una stringa arbitraria di lunghezza $n-1$, con numero dispari di Y, che abbiamo a disposizione per ipotesi induttiva. Riscriviamo i generatori che abbiamo nel seguente modo

$$I \otimes Y \otimes B \quad I \otimes X \otimes A \quad I \otimes Z \otimes A, \tag{3.48}$$

dove A, B sono stringhe di lunghezza $n-2$ con rispettivamente un numero dispari e un numero pari di Y.
Da questi possiamo ora ottenere:

$$I \otimes Y \otimes B \overset{V^{12}}{\to} Z \otimes Y \otimes B, \tag{3.49}$$

$$I \otimes X \otimes A \overset{P^{12}}{\to} X \otimes I \otimes A \overset{V^{12}}{\to} X \otimes X \otimes A. \tag{3.50}$$

A questo punto agendo con il gate locale $\tilde{H}$ possiamo scambiare X con Z e viceversa. Infine agendo con il CNOT su $X \otimes Z \otimes A$ otteniamo

$$Y \otimes Y \otimes A. \tag{3.51}$$

Questo conclude la dimostrazione per induzione del teorema 3.2.1. Esattamente come nel caso della QT possiamo utilizzare il LemmaC.1.1 per dimostrare che tutto il gruppo $SO(2^n)$ viene generato.

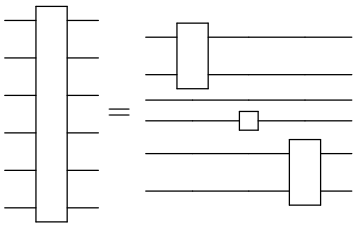
[10] Ho anche semplicemente con il gate SWAP.

3.2.2 Universalità debole

Abbiamo visto che attraverso CNOT e gate locali di $SO(2) \otimes SO(2)$ si può generare un qualsiasi gate ortogonale speciale su n-rebit. Tuttavia è immediato rendersi conto che i gate a determinante -1 non si possono ottenere. Per vedere questo basta considerare le proprietà del prodotto di Kronecker. In particolare date $A \in O(2^n)$ e $B \in O(2^p)$, dove n e p sono interi positivi, si ha

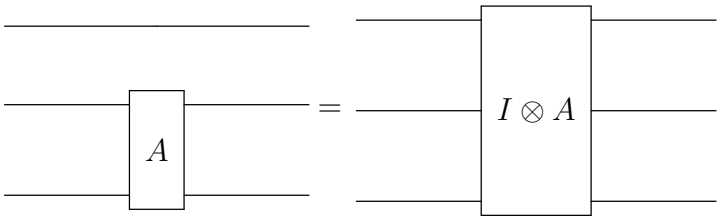
$$\det(A \otimes B) = (\det A)^{2^p} (\det B)^{2^n}. \tag{3.52}$$

Quindi è chiaro che dati $n > 2$ rebit e CNOT e gate locali non si potrà mai ottenere un gate a determinante -1. Il circuito riportato di seguito chiarifica ulteriormente questo punto.



(3.53)

Potrebbe sembrare che per ogni n sia necessario un gate n-partito a determinante -1 per poter ottenere tutti gli altri a determinate -1 sul sistema di n-rebit. Se questo fosse vero starebbe a significare che la teoria non ammette l'universalità in alcun modo e che inoltre richiede in generale l'interazione di tutti i sottosistemi per la computazione. In realtà abbiamo trovato che non è questo il caso. Per risolvere il problema basta aggiungere un rebit ancillare (un registro locale).
Infatti dato un gate $A \in O(2^n)$ con determinante -1, per quanto detto prima, il gate su $n+1$-rebit $I \otimes A$ ha determinate $+1$ e quindi è ottenibile attraverso CNOT e gate locali come dimostrato precedentemente. Quindi aggiungendo a n-rebit un solo rebit ancillare, il cui stato iniziale e finale coincidono, è possibile implementare un qualunque gate su n-rebit a determinante -1 usando solo CNOT e gate locali.



(3.54)

Questo risultato ci mostra che la RQT possiede una proprietà di universalità *debole*, dove l'appellativo debole evidenzia la differenza rispetto alla teoria standard che non necessità di alcun qubit ancillare, come sottolineato in [18].

Conclusioni

In questo lavoro abbiamo affrontato il problema dell'universalità della computazione per la teoria quantistica standard (con spazi di Hilbert complessi) e per quella su spazi reali. Nel primo capitolo abbiamo descritto la teoria della computazione, sia classica che quantistica, soffermandoci sull'equivalenza della computazione classica reversibile e irreversibile. Abbiamo richiamato il fatto che per la computazione classica reversibile, sottoclasse di quella quantistica, il gate di Toffoli tripartito è universale ma che la teoria non ammette gate bipartiti universali. Introducendo però il gate di Fredkin e la sua realizzazione attraverso il *billiard ball computer* si è mostrato che questo fatto non è indice della necessità di interazioni fisiche a tre corpi per la computazione classica reversibile. Ci siamo poi concentrati sulla computazione quantistica mostrando che, al contrario del caso classico, la teoria quantistica della computazione ammette come universale un set (continuo) di gate al più bipartiti. In particolare abbiamo visto che basta, assieme ai gate locali, un solo gate entanglante, il CNOT. Nello stesso capitolo abbiamo introdotto il formalismo dei quantum circuit per la computazione e abbiamo formalizzato i concetti di insieme universale ed esattamente universale. Concentrandoci su quest'ultimo aspetto abbiamo ripercorso quella che è la dimostrazione dell'universalità esatta dell'insieme dei gate locali assieme al CNOT come presentata in letteratura. Abbiamo presentato anche una dimostrazione più generale che mostra come i gate locali più un qualsiasi gate bipartito entanglante siano un set esattamente universale.

Lo studio della teoria dell'informazione e computazione quantistica ha portato ad importanti passi avanti nella comprensione della teoria quantistica stessa, facendo emergere la convinzione che la teoria possa essere caratterizzata completamente dal punto di vista di come viene processata l'informazione e mettendo enfasi sull'importanza dei sistemi a dimensione finita. Sulla scia di queste idee sono emersi negli ultimi anni diversi tentativi di assiomatizzare la teoria quantistica all'interno di un framework molto generale che è quello delle teorie operazionali probabilistiche (OPT). In particolare D'Ariano, Perinotti e Chiribella sono riusciti a derivare completamente la teoria quantistica (in dimensione finita) a partire da assiomi di natura puramente operazionale. Con lo

sviluppo di questi studi si è capito che la teoria quantistica fa parte di un'ampia classe di teorie probabilistiche generalizzate assieme anche alla teoria classica che viene a distinguersi dalla prima per il fatto di non soddisfare al postulato di purificazione. Per cercare di capire meglio la teoria quantistica si è quindi cercato, e si cerca tuttora, di analizzare altre teorie probabilistiche che differiscono dalla QT in qualche aspetto. Questi studi dei fondamenti della teoria quantistica hanno almeno un duplice obbiettivo. Da una parte si vuole capire a livello elementare la natura della teoria quantistica che ad oggi è la teoria con il maggior numero di verificazioni sperimentali che possediamo. Secondariamente, una volta raggiunta un'assiomatizzazione basata su concetti fisici della teoria, è possibile studiare cosa accade modificando gli assiomi per sondare quali generalizzazioni della teoria siano ancora consistenti con ciò che osserviamo. Sulla linea (ma non solo) di questi quesiti è stata studiata la meccanica quantistica con spazi vettoriali reali al posto dell'usuale spazio di Hilbert. I primi studi risalgono addirittura agli anni '60 con i lavori di Stuecklberg e hanno interessato più recentemente studiosi come Wootters e Hardy. Nel secondo capitolo di questo lavoro, dopo aver introdotto il formalismo delle OPT, abbiamo riportato gli assiomi da cui, in [32], è stata derivata tutta la struttura matematica della teoria quantistica. Abbiamo enfatizzato l'assioma di LD e abbiamo visto come la teoria con spazi reali non soddisfi questo assioma ma una sua versione più debole.

Ci siamo poi interessati allo studio di un aspetto particolare della RQT, ovvero abbiamo cercato di capire se la RQT abbia una proprietà di universalità della computazione analoga a quella della QT. Il lavoro fatto ha preso stimolo dal recente lavoro di Masanes *et al.* in cui si mostra come la teoria quantistica sia l'unica teoria operazionale con discriminabilità locale ad avere come sistemi elementari i qubit e tra le trasformazioni reversibili di due qubit almeno una entanglante. La RQT viola l'assioma di discriminabilità locale e costituisce quindi un buon esempio per verificare se indebolendo le ipotesi sulla teoria l'universalità si venga a perdere. Resta però aperta la domanda se la teoria quantistica, reale o complessa, non sia comunque l'unica teoria che ammette un set di gate universale con un solo gate bipartito. I risultati originali che abbiamo trovato, a partire dall'analisi svolta in [6], sono stati esposti nel terzo capitolo e si rifanno a [35]. Siamo riusciti per prima cosa a ritrovare il risultato di universalità del CNOT per la QT con una dimostrazione per induzione che risulta più semplice di quelle presenti in letteratura. Con la stessa tecnica sviluppata per il caso reale abbiamo poi dimostrato che il CNOT assieme ai gate locali di $SO(2) \otimes SO(2)$ è universale per la RQT. Tuttavia in questo caso appare la necessità di avere un bit reale aggiuntivo a causa del fatto che il gruppo ortogonale non è connesso ed è per questo che l'universalità di CNOT e locali per la RQT è stata definita *debole*. Risulta interessante notare che un analogo problema sorgeva nella

computazione classica reversibile. In quel caso un gate universale era il gate di Toffoli da solo, ma era comunque indispensabile un bit ancillare per avere l'universalità. Da questo risulta che la teoria quantistica, rispetto a quella classica e alla RQT, ha la proprietà di avere i gate a due qubit come gate universali senza necessitare di alcun bit ancillare.

Sembra che l'universalità esatta dei gate locali e il gate entanglante CNOT per la computazione non sia appannaggio della sola teoria quantistica ma una proprietà condivisa anche da altre teorie o almeno dalla RQT, anche se in modo leggermente diverso. Un problema che rimane aperto per sviluppi futuri è se un postulato di universalità della computazione ben formulato, assieme ai cinque assiomi del secondo capitolo, sia sufficiente per individuare tra le varie teorie probabilistiche la teoria quantistica. Se fosse così si avrebbe un nuovo postulato per la teoria quantistica intimamente connesso alla teoria della computazione.

Appendice A

In questa appendice richiamiamo alcuni concetti di teoria dei gruppi usati in questo lavoro, rifacendoci per lo più a [1] e [2]. In particolare introdurremo il concetto di gruppo di Lie e algebra di Lie facendo attenzione ai legami tra questi.

A.1 Elementi di Teoria dei Gruppi

Iniziamo dando alcune definizioni basilari di teoria dei gruppi.

Definizione A.1.
Un **gruppo** è un insieme non vuoto G con una mappa $\circ : G \times G \to G$ con le seguenti proprietà:

1. Chiusura: $\forall g, h \in G,\ g \circ h \in G$
2. Associatività: $\forall\, a, b, c \in G,\ a \circ (b \circ c) = (a \circ b) \circ c$.
3. Elemento neutro: $\exists e \in G$ t.c. $\forall\ g \in$ G risulta $g \circ e = e \circ g = g$.
4. Elemento inverso: $\forall g \in G\ \exists h \in G$ t.c. $g \circ h = h \circ g = e$.

Se inoltre $g \circ h = h \circ g\ \forall g, h \in G$ allora il gruppo si dice abeliano.

Quindi dato un insieme ed una operazione su di esso, per verificare se è o meno un gruppo è necessario verificare la chiusura, associatività e l'esistenza dell'identità e delle inverse. Nel seguito l'inversa di un elemento g verrà indicata con g^{-1}. Veniamo ora ad altre definizioni basilari per quanto riguarda i gruppi e le operazioni tra essi.

Definizione A.2.
Un **sottogruppo** di un gruppo G è un sottoinsieme H di G con le seguenti proprietà:

1. $e \in G$
2. Se $h \in H$ allora $h^{-1} \in H$
3. Se $h, g \in H$ allora $h \circ g \in H$

Un sottogruppo H di G è detto **normale** se $\forall g \in G$ e $\forall h \in H$ si ha $ghg^{-1} \in G$.

In questo lavoro particolare rilevanza avranno i sottogruppi speciale unitario $SU(2n)$ e speciale ortogonale $SO(2n)$ di cui ci occuperemo in seguito.

Definizione A.3.
Il **normalizer** di un sottoinsieme S del gruppo G è dato da

$$N_G(S) = \{g \in G | gS = Sg\} \tag{A.1}$$

Si verifica facilmente che il normalizer di un sottoinsieme S di G è un sottogruppo di G.

Definizione A.4.
Siano G e H due gruppi. Una mappa $\phi : G \to H$ è un **omomorfismo** se $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ $\forall g_1 g_2 \in G$. Un omomorfismo biettivo è un **isomorfismo**.

Chiudiamo questa carrellata di definizioni elementari con quella di gruppo prodotto diretto.

Definizione A.5.
Siano G e H due gruppi, se ne consideri il prodotto cartesiano $G \times H$ e si definisca su questo insieme l'operazione prodotto seguente:

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2).$$

Questa operazione rende il prodotto cartesiano un gruppo che prende il nome di **gruppo prodotto diretto** dei due gruppi G e H.

A.2 Gruppi e algebre di Lie

In questo paragrafo introdurremo le nozioni di gruppo ed algebra di Lie e le relazioni che intercorrono tra questi oggetti matematici. Infine dimostreremo la formula del prodotto di Lie, che è utilizzata nel lavoro.

A.2.1 Gruppi di Lie: caso generale

Un gruppo di Lie è un oggetto matematico che è sia un gruppo che una varietà differenziabile liscia. L'algebra di Lie associata ad un gruppo può essere pensata come lo spazio tangente nell'identità al gruppo. In quanto segue formalizzeremo queste definizioni. Partiamo dai concetti di varietà differenziabile e spazio tangente in un punto alla varietà.

Definizione A.6.
Una varietà differenziabile di classe k, C^k, è data da una varietà topologica e un atlante $\{X; U_i, \varphi_i\}$ tale che i cambiamenti di carta $\varphi_{ij} \doteq \varphi_i \varphi_j^{-1}$ sono funzioni differenziabili di classe C^k.

Per quanto riguarda lo spazio tangente diamo una definizione geometrica basata su una relazione di equivalenza tra curve sulle varietà.

Definizione A.7.
Data una varietà differenziabile M liscia di dimensione m consideriamo due curve lisce su di essa, γ_1 e γ_2, tali che $\gamma_1(0) = \gamma_2(0) = p$. Diremo che le due curve sono tangenti in p se, scelta una carta coordinata $\{U, \varphi\}$ con $p \in U$, risulta che $\frac{d}{ds}\left(\varphi\left(\gamma_1\left(s\right)\right)\right)\Big|_{s=0} = \frac{d}{ds}\left(\varphi\left(\gamma_2\left(s\right)\right)\right)\Big|_{s=0}$. La relazione di tangenzialità è una relazione di equivalenza nell'insieme di tutte le curve di $\mathbb{R}^m$ passanti per $\varphi(p)$ e le classi di equivalenza di curve sono i vettori tangenti a M in p. Lo spazio tangente in p alla varietà, T_pM, è definito come l'insieme di tutti i vettori tangenti a M in p ed ha la struttura di spazio vettoriale.

Arriviamo ora alla definizione di gruppo di Lie. Questi sono dei gruppi che hanno anche una struttura di varietà differenziabile e l'algebra di Lie corrispondente risulta essere lo spazio tangente nell'identità. Dopo aver richiamato le definizioni generali passeremo a considerare i gruppi classici ovvero gruppi di Lie di matrici.

Definizione A.8.
Un **gruppo di Lie** G è una varietà differenziabile con una struttura di gruppo tale che il prodotto gruppale $G \times G \to G$ e la mappa inversa $g \to g^{-1}$ sono liscie.

Si dimostra che la componente connessa all'identità di un gruppo di Lie è ancora un gruppo di Lie e che le diverse componenti connesse di un gruppo di Lie sono diffeomorfe tra loro. Esempi di gruppi di Lie sono:

- Il gruppo $GL(n; \mathbb{R})$ con il prodotto matriciale.
- Lo spazio Euclideo $\mathbb{R}^n$ con la somma vettoriale.

- $\mathbb{C} - \{0\}$ con la moltiplicazione.
- Il prodotto $G \times H$ di due gruppi di Lie con la struttura di gruppo prodotto diretto e quella di varietà prodotto.

Definizione A.9.
Un **sottogruppo di Lie** H di G è un sottogruppo di G che è anche una sottovarietà.

In questo caso un omomorfismo tra gruppi di Lie è una mappa di classe C^∞ che preserva la struttura di gruppo. Se tale mappa è un diffeomorfismo prende il nome di isomorfismo(tra gruppi di Lie).

Definizione A.10.
Una **algebra di Lie** finito dimensionale reale (complessa) è uno spazio vettoriale reale (complesso) finito dimensionale $\mathfrak{g}$, con una mappa $[,] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ con le seguenti proprietà:

1. Bilineare
2. Antisimmetrica, $[X, Y] = -[Y, X]\ \forall X, Y \in \mathfrak{g}$
3. Identità di Jacobi: $[X, [Y, Z]] + [Z, [X, Y]] + [Y, [Z, X]] = 0\ \forall X, Y \in \mathfrak{g}$

Come si vede un'algebra di Lie non è ne associativa ne commutativa e soddisfa l'identità di Jacobi.

Definizione A.11.
Una sottoalgebra di un'algebra di Lie $\mathfrak{g}$ è un sottospazio $\mathfrak{h}$ di $\mathfrak{g}$ tale che $[H_1, H_2] \in \mathfrak{h}, \forall H_1, H_2 \in \mathfrak{h}$. Se $\mathfrak{g}$ è un'algebra complessa ed $\mathfrak{h}$ è un sottospazio reale chiuso sotto commutazione allora $\mathfrak{h}$ è detta sottoalgebra reale di $\mathfrak{g}$.

Si possono poi definire gli omomorfismi tra algebre di Lie semplicemente come applicazioni lineari che preservano la struttura di algebra. Si dimostra che una sottoalgebra di un'algebra di Lie è ancora un'algebra di Lie e che una sottoalgebra reale di un'algebra di Lie complessa è un'algebra di Lie reale.
Esempi di algebre di Lie sono:

- Lo spazio vettoriale di tutti i campi vettoriali lisci su una varietà M, $\mathfrak{C}^\infty(M, TM)$, con la derivata di Lie tra campi vettoriali.
- Lo spazio vettoriale $\mathfrak{gl}(n, \mathfrak{R})$ delle matrici $n \times n$ reali con il commutatore tra matrici definito come $[A, B] = AB - BA$.
- $\mathbb{R}^3$ con il prodotto vettoriale.

Concludiamo con due risultati astratti dando la definizione di algebra di Lie associata ad un gruppo di Lie. Un campo vettoriale X (a priori non necessariamente liscio) su un gruppo di Lie G è detto *left invariant* se vale la seguente relazione:

$$dl_v \circ X = X \circ l_v, \forall v \in G$$

dove $l_v : G \to G$ è un diffeomorfismo definito da $l_v(g) = vg, \forall g \in G$. L'insieme dei campi vettoriali su G *left invariant* è indicato con $\mathfrak{g}$. Si dimostra la seguente proposizione[1]

Proposizione A.2.1.
Sia G un gruppo di Lie e $\mathfrak{g}$ l'insieme dei campi vettoriali left invariant su G. Allora valgono le seguenti proprietà:

1. *$\mathfrak{g}$ è uno spazio vettoriale reale e la mappa $\alpha : \mathfrak{g} \to T_eG$ definita da $\alpha(X) = X(e)$, dove e è l'identità di G, è un isomorfismio di $\mathfrak{g}$ con lo spazio tangente a G nell'identità. Di conseguenza $dim\mathfrak{g} = dimT_eG = dimG$.*

2. *Campi vettoriali left invariant sono lisci.*

3. *La parentesi di Lie di campi vettoriali left invariant è ancora un campo vettoriale left invariant.*

4. *$\mathfrak{g}$ forma un'algebra di Lie con l'operazione di parentesi di Lie tra campi vettoriali.*

Dimostrazione. Dimostriamo solamente il punto (1) (il (4) è automatico dati gli altri). Il fatto che $\mathfrak{g}$ sia spazio vettoriale e che α sia lineare è ovvio. Se $\alpha(X) = \alpha(Y)$ allora per ogni $g \in G$ risulta

$$X(g) = X(l_g(e)) = dl_g(X(e)) = dl_g(Y(e)) = Y(g)$$

e quindi $X = Y$, i.e. la mappa α è iniettiva.
Ora dato $x \in T_eG$ consideriamo $X(g) = dl_g(x)$ per ogni $g \in G$. Allora $\alpha(X) = x$ e il campo X è left invariant dato che

$$X(gh) = dl_{gh}(x) = dl_g dl_h(x) = dl_g(X(h)), \forall g, h \in G.$$

Questo conclude la dimostrazione del primo punto.
Per quanto riguarda il punto (4), una volta dimostrati il punto (2) e (3), risulta automaticamente dimostrato dato che le parentesi di Lie soddisfano le condizioni di antisimmetria e Jacobi. ■

[1]La dimostrazione completa può essere trovata in [1].

Questa proposizione ci mostra come i campi left invariant costituiscano l'algebra di Lie relativa al gruppo G e come questa sia isomorfa allo spazio tangente nell'identità a G. Nel seguito identificheremo sempre l'algebra di Lie del gruppo con lo spazio tangente nell'identità.

A.2.2 Gruppi Classici

I gruppi classici sono sottogruppi del gruppo generale lineare $GL(n;\mathbb{K})$, ovvero l'insieme delle matrici $n \times n$, con entrate nel campo $\mathbb{K}$, invertibili. In particolare ci concentreremo sui sottogruppi di $GL(n;\mathbb{C})$.

Definizione A.12.
Chiamiamo **gruppo di Lie di matrici** un sottogruppo chiuso di $GL(n;\mathbb{C})$.

Vale il seguente teorema che enunciamo senza dimostrare.

Teorema A.2.2. *Ogni gruppo di Lie di matrici è un gruppo di Lie.*

Esempi di sottogruppi chiusi di $GL(n;\mathbb{C})$ sono:

- $GL(n;\mathbb{R})$
- $SL(n;\mathbb{R})$
- $O(n;\mathbb{R})$, $SO(n;\mathbb{R})$
- $U(n)$, $SU(n)$
- $SO(p,q;\mathbb{R})$

Da questo momento avremo a che fare sempre con gruppi di Lie di matrici. Diamo ora le definizioni di gruppo compatto, connesso e semplicemente conneso.

Definizione A.13.
Un gruppo di Lie G è **compatto** se sono soddisfatte le due condizioni seguenti:

1. Se A_n è una sequenza di matrici di G convergente ad A, allora $A \in G$.
2. Esiste una costante c tale che per ogni $A \in G$, $|A_{ij}| \leq c \; \forall 1 \leq i,j \leq n$.

Questa definizione non è quella topologica legata all'esistenza di un sottoricoprimento finito, tuttavia è equivalente ad essa grazie ad un teorema di analisi elementare dato che l'insieme delle matrici complesse $n \times n$ è isomorfo a $\mathbb{C}^{n^2}$ e la definizione richiede che G ne sia un sottoinsieme chiuso e limitato.

Definizione A.14.
Un gruppo di Lie G è **connesso** se date due matrici $A, B \in G$ esiste un cammino continuo $A(t), t \in [a,b] \subseteq \mathbb{R}$ tale che $A(t) \in G, \forall t \in [a,b]$ e $A(a) = A$, $A(b) = B$.

La definizione di connettezza data risulta essere equivalente, per i gruppi di Lie, alla definizione topologica. Un gruppo di Lie non connesso è decomponibile, in maniera unica, in componenti connesse. In particolare risulta che la componente contenente l'identità è un sottogruppo.

Definizione A.15.
Un gruppo di Lie connesso è detto **semplicemente connesso** se ogni circuito chiuso in G può essere deformato con continuità ad un punto in G. In altri termini G è semplicemente connesso se dato un qualsiasi cammino chiuso $A(t), t \in [0,1] : A(0) = A(1)$ in G, esiste una famiglia parametrizzata di circuiti chiusi $A(t,s), t, s \in [0,1]$ in G tali che:

1. A(s,0)=A(s,1), $\forall s$.
2. A(0,t)=A(t).
3. A(1,t)=A(1,0), $\forall t$.

Mostriamo ora alcuni risultati riguardo le proprietà enunciate per gruppi di Lie di interesse. Iniziamo dal fatto che i gruppi $O(n)$, $SO(n)$, $U(n)$ e $SU(n)$ sono compatti. Questo è facile da verificare perchè il limite di matrici ortogonali (unitarie) è una matrice ortogonale (unitaria) ed il limite di matrici a determinante uno è una matrice a determinante uno. Inoltre le colonne di una matrice ortogonale (unitaria) hanno norma uno e quindi gli elementi di matrice hanno modulo minore o al più uguale ad uno. Veniamo ora alla connettezza.

Proposizione A.2.3.
Il gruppo U(n) è connesso.

Dimostrazione. Consideriamo $U(n)$. Dal teorema spettrale sappiamo che ogni matrice unitaria A è diagonalizzata mediante una matrice unitaria le cui colonne sono gli autovettori di A

$$A = B\, Diag(e^{i\theta_j})\, B^\dagger.$$

Allora si consideri

$$A(t) = B \begin{bmatrix} e^{i(1-t)\theta_1} & \cdots & 0 \\ & \ddots & \\ 0 & & e^{i(1-t)\theta_n} \end{bmatrix} B^\dagger$$

con $t \in [0,1]$, questo definisce un cammino continuo in $U(n)$ che congiunge ogni $A \in U(n)$ con l'identità. ■

Con una dimostrazione analoga si può dimostrare che anche il gruppo speciale unitario è connesso per ogni n. Si dimostra che il gruppo $GL(n;\mathbb{R})$ non è connesso, infatti un cammino continuo che connettesse due matrici del gruppo una a determinante positivo e l'altra con determinate negativo dovrebbe passare forzatamente per una matrice a determinante zero che non appartiene al gruppo. Le matrici a determinate positivo e negativo di $GL(n;\mathbb{R})$ costituiscono le due componenti connesse del gruppo. Risultato analogo vale per il gruppo $O(n)$ che non è connesso. In particolare la componente connessa contenete l'identità è in questo caso il gruppo $SO(n)$. Come si vedrà in seguito il fatto che il gruppo ortogonale non sia connesso ha importanti implicazioni nello studio dell'universalità di gate bipartiti per la computazione nella teoria quantistica su spazi reali. Tra i gruppi sopra citati solo $SU(n)$ risulta essere semplicemente connesso.

Veniamo ora a definire un gruppo ad un parametro, concetto che verrà utilizzato nel seguito.

Definizione A.16.
Una funzione $A : \mathbb{R} \to GL(n;\mathbb{C})$ è detta gruppo ad un parametro se:

1. A è continua.
2. $A(0) = I$.
3. $A(t+s) = A(t)A(s), \forall t, s \in \mathbb{R}$.

A.2.3 Algebre di Lie e mappa esponenziale

Iniziamo con il richiamare la definizione di esponenziale di una matrice. Sia X una matrice reale o complessa $n \times n$, l'esponziale è definito tramite la seguente serie di potenze

$$e^X = \sum_{m=0}^{\infty} \frac{X^m}{m!} \tag{A.2}$$

.

Proposizione A.2.4.
Per ogni matrice X la serie in (A.2) *converge. L'esponenziale di una matrice è una funzione continua di X.*

Dimostrazione. Dalle proprietà della norma sappiamo che

$$\|X^m\| \leq \|X\|^m ,$$

e quindi

$$\left\| \sum_{m=0}^{\infty} \frac{X^m}{m!} \right\| \leq \sum_{m=0}^{\infty} \frac{\|X^m\|}{m!} = e^{\|X\|} < \infty$$

allora la serie in (A.2) converge assolutamente e quindi converge. ■

Raccogliamo nella seguente proposizione alcune proprietà dell'esponenziale di matrici.

Proposizione A.2.5.
Siano X, Y matrici $n \times n$ arbitrarie. Allora valgono:

- $e^0 = I$.
- $(e^X)^{-1} = e^{-X}$.
- $e^{(a+b)X} = e^{aX} e^{bY}, \forall a, b \in \mathbb{C}$.
- *Se XY=YX allora* $e^{X+Y} = e^X e^Y = e^Y e^X$.
- $det(e^X) = e^{TrX}$.
- *Se C è invertibile allora* $Ce^X C^{-1} = e^{CXC^{-1}}$.

Dimostrazione. Ci interessa dimostrare solo l'ultimo punto di questa proposizione dato che questa proprietà sarà usata nella prossima proposizione. La dimostrazione è immediata osservando che

$$(CXC^{-1})^m = CX^m C^{-1}$$

e quindi i due membri dell'uguaglianza sono uguali termine a termine. ■

Veniamo ora a dare una nuova definizione di algebra di Lie per un gruppo di Lie di matrici.

Definizione A.17.
L'algebra di Lie $\mathfrak{g}$ del gruppo G è l'insieme di tutte le matrici X tali che $e^{tX} \in G, \forall t \in \mathbb{R}$

Riassumiamo nella seguente proposizione delle proprietà basilari delle algebre di Lie per gruppi di matrici.

Proposizione A.2.6.
Siano G un gruppo di Lie, $\mathfrak{g}$ la sua algebra e $X, Y \in \mathfrak{g}$. Allora valgono:

1. *e^X è un elemento della componente connessa con l'identità.*

2. *Sia* $A \in G$ *allora* $AXA^{-1} \in \mathfrak{g}$.

3. $sX \in \mathfrak{g}, \forall s \in \mathbb{R}$.

4. $X + Y \in \mathfrak{g}$.

5. $[X, Y] \doteq XY - YX \in \mathfrak{g}$.

Si noti che i punti (3),(4) mostrano che $\mathfrak{g}$ è uno spazio vettoriale reale.

Dimostrazione. Dimostriamo punto per punto.

1. Dato $e^{tX} = \gamma(t)$ questo appartine a G per ogni $t \in \mathbb{R}$ per definizione di algebra di Lie ed è un cammino continuo in G. Quindi essendo $\gamma(0) = I$ e $\gamma(1) = e^X$ concludiamo.

2. Grazie all'ultimo punto della proposizione A.2.5 abbiamo che

$$Ae^{tX}A^{-1} = e^{t(AXA^{-1})}$$

e siccome $Ae^{tX}A^{-1} \in G$ concludiamo.

3. $e^{t(sX)} = e^{(ts)X}$, deve essere in G se $X \in \mathfrak{g}$.

4. La dimostrazione è ovvia se X,Y commutano. Se non commutano dobbiamo ricorrere alla formula del prodotto di Lie, che dimostreremo alla fine del paragrafo,

$$e^{t(X+Y)} = \lim_{m\to\infty} \left(e^{\frac{tX}{m}} e^{\frac{tY}{m}}\right)^m.$$

Allora dal fatto che G è un gruppo ne segue che $\left(e^{\frac{tX}{m}} e^{\frac{tY}{m}}\right)^m \in G$ e siccome è un gruppo di Lie di matrici il limite di successioni in G deve ancora essere in G a patto che il limite sia invertibile, il che è il nostro caso. Quindi $e^{t(X+Y)} \in G, \forall t \in \mathbb{R}$ e questo mostra che $X + Y \in \mathfrak{g}$.

5. Differenziando termine a termine e^{tX} si ottine

$$\frac{d}{dt}(e^{tX})_{t=0} = X$$

e quindi

$$\frac{d}{dt}\left(e^{tX}Ye^{-tX}\right)_{t=0} = XY - YX.$$

Ora dal punto (2) segue che $e^{tX}Ye^{-tX} \in \mathfrak{g}, \forall t \in \mathbb{R}$ e siccome $\mathfrak{g}$ è uno spazio vettoriale reale ne segue che la derivata di ogni curva liscia in $\mathfrak{g}$ deve ancora essere in $\mathfrak{g}$. Quindi $XY - YX \in \mathfrak{g}$.

■

L'ultimo punto mostra che l'algebra di Lie come definita in eq.(A.17) è chiusa rispetto al commutatore di matrici. Il commutatore è chiaramente antisimmetrico e per ispezione diretta si verifica che $gl(n;\mathbb{R})$ con il commutatore soddisfa l'identità di Jacobi mostrando quindi l'equivalenza tra le due definizioni di algebra di Lie date nel caso del gruppo generale lineare. Anche $gl(n;\mathbb{C})$, con l'analoga operazione di commutazione, si verifica essere un'algebra di Lie, in questo caso complessa. Essendo poi ogni algebra di Lie di un gruppo di Lie di matrici una sottoalgebra reale di $gl(n;\mathbb{C})$, grazie alla proposizione precedente, si ha che le due definizioni di algebra di Lie date sono equivalenti per tutti i gruppi di Lie di matrici.

Definizione A.18.
Dato un gruppo di Lie G e la sua algebra $\mathfrak{g}$, la **mappa esponenziale** è la mappa

$$exp : \mathfrak{g} \to G$$

tale che ad ogni $X \in \mathfrak{g}$ associa e^X.

Torneremo nella prossima appendice ad illustrare delle proprietà della mappa esponenziale, nel caso dei gruppi ortogonale e unitario, che ci saranno utili nel seguito del lavoro. Ora definiamo il logaritmo di una matrice che ci servirà nella dimostrazione della formula di Lie.

Proposizione A.2.7.
La funzione

$$\log A \doteq \sum_{m=1}^{\infty} (-1)^{m+1} \frac{(A-I)^m}{m}, \tag{A.3}$$

è definita e continua per ogni matrice complessa A $n \times n$ con $\|A - I\| < 1$, inoltre $\log A$ *è reale se A è reale. Risulta infine che nel dominio di definizione*

$$e^{\log A} = A.$$

Citiamo, senza dimostrare, una proprietà del logaritmo che useremo subito.

Proposizione A.2.8.
Per ogni A $n \times n$ con $\|A\| < \frac{1}{2}$ esiste una costante c tale che

$$\|\log(I + A) - A\| \leq c \|A\|^2$$

Teorema A.2.9 (Formula di Lie)**.**
Siano X, Y matrici complesse $n \times n$. Allora

$$e^{X+Y} = \lim_{m\to\infty} \left(e^{\frac{X}{m}} e^{\frac{Y}{m}} \right)^m. \tag{A.4}$$

Dimostrazione. Dalla serie di potenze per l'esponenziale si ha

$$e^{\frac{X}{m}} e^{\frac{Y}{m}} = I + \frac{X}{m} + \frac{Y}{m} + C_m,$$

dove $\|C_m\| \leq \frac{cost.}{m^2}$. Il membro di sinistra appartiene al dominio del logaritmo per m sufficientemente grandi, dato che converge all'identità per m che tende all'infinito. Adesso

$$\log\left(e^{\frac{X}{m}} e^{\frac{Y}{m}}\right) = \log\left(I + \frac{X}{m} + \frac{Y}{m} + C_m\right) = \frac{X}{m} + \frac{Y}{m} + C_m + E_m,$$

dove, dalla proposizione precedente, $\|E_m\| \leq c\left\|\frac{X}{m} + \frac{Y}{m} + C_m\right\|^2 \leq \frac{cost.}{m^2}$. Esponenziando il logaritmo abbiano

$$e^{\frac{X}{m}} e^{\frac{Y}{m}} = exp\left(\frac{X}{m} + \frac{Y}{m} + C_m + E_m\right) \Rightarrow \left(e^{\frac{X}{m}} e^{\frac{Y}{m}}\right)^m = exp\left(X + Y + mC_m + mE_m\right)$$

e siccome C_m, E_m sono di ordine $\frac{1}{m^2}$ possiamo concludere usando la continuità dell'esponenziale. ■

Appendice B

B.1 Gruppi Ortogonale e Unitario

In questa appendice descriviamo i gruppi unitario e ortogonale che sono usati nelle discussioni sull'universalità. In particolare discuteremo quali siano le proprietà di questi gruppi di Lie nonchè le loro algebre dimostrando una proprietà importante della mappa esponenziale per questi gruppi.

Gruppo Ortogonale

Iniziamo con il gruppo ortogonale e ortogonale speciale.
Una matrice reale $n \times n$ è detta **ortogonale**, $A \in O(n)$, se preserva il prodotto scalare standard di $\mathbb{R}^n$ o equivalentemente se[1]

$$AA^T = A^T A = I. \tag{B.1}$$

In particolare vale la seguente

Proposizione B.1.1.
Sia A una matrice reale $n \times n$, sono equivalenti:

1. $A^T = A^{-1}$
2. *Le colonne (righe) di A son una base ortonormale di $\mathbb{R}^n$.*
3. $\langle Av, Aw \rangle = \langle v, w \rangle, \forall v, w \in \mathbb{R}^n$.
4. $\|Av\| = \|v\|, \forall v \in \mathbb{R}^n$.

Dimostrazione.
1. $\Leftrightarrow$ 2.
Il determinante di una matrice che soddisfa 1. può essere ± 1 e quindi le colonne

[1] Indichiamo con A^T la trasposta della matrice A.

(righe) sono n vettori linearmente indipendenti. Inoltre osserviamo che il punto 1. è equivalente alla richiesta (B.1). Da questo si ha banalmente che le colonne (righe) sono ortonormali, e quindi abbiamo il punto 2. Viceversa è banale verificare che se è soddisfatto il punto 2. allora si ha (B.1).
1. $\Leftrightarrow$ 3.
Se vale (B.1) allora

$$\langle Av, Aw\rangle = v^T A^T A w = v^T w = \langle v, w\rangle .$$

Se vale 3. allora

$$v^T w = v^T \left(A^T A\right) w \Rightarrow v^T \left(A^T A - I\right) w = v^T B w, \forall v, w \in \mathbb{R}^n \Rightarrow B = 0.$$

3. $\Rightarrow$ 4.
Ovvia, dato che per definizione $\|v\| = \sqrt{\langle v, v\rangle}$.
4. $\Rightarrow$ 3.
Da 4. abbiamo che $\|A(v+w)\| = \|v+w\|$; $\|Av\| = \|v\|$; $\|Aw\| = \|w\|$ e quindi

$$\langle v+w, v+w\rangle = \langle v, v\rangle + 2\langle v, w\rangle + \langle w, w\rangle = \langle Av, Av\rangle + 2\langle Av, Aw\rangle + \langle Aw, Aw\rangle$$
$$\Rightarrow \langle v, w\rangle = \langle Av, Aw\rangle$$

■

Risulta facile convincersi che le matrici ortogonali formano un gruppo in quanto l'inversa di una ortogonale è ancora ortogonale ed anche il prodotto di due ortogonali è ancora ortogonale. Inoltre la relazione (B.1) è preservata sotto limite e quindi il gruppo ortogonale è un gruppo di Lie di matrici. Dal punto di vista geometrico gli elementi di $O(n)$ sono rotazioni e combinazioni di rotazioni e riflessioni. Come abbiamo già detto il determinante di una matrice ortogonale può essere ± 1. Se si considerano solo le matrici ortogonali a determinate $+1$ si ottiene un sottogruppo di Lie del gruppo ortogonale che è il gruppo speciale ortogonale $SO(n)$, che è la componente connessa dell'identità[2].

Si dimostra che sia $O(n)$ che $SO(n)$ sono gruppi **compatti**, il primo non è connesso mentre il secondo si. Il fatto che $O(n)$ non sia connesso è semplice da capire data la continuità della funzione determinante e il fatto che questo può assumere solo i valori ± 1. Nessuno dei due gruppi è invece semplicemente connesso. Geometricamente gli elementi si $SO(n)$ sono le sole rotazioni, quindi preservano l'orientazione dello spazio vettoriale.
Vale anche la seguente

[2]Essendo la componente connessa contenente l'identità è automaticamente un gruppo di Lie.

Proposizione B.1.2.
Sia $A \in O(n)$ e $\lambda \in \mathbb{R}$ un autovalore di A, allora $|\lambda| = 1$.

Dimostrazione. Se $Av = \lambda v$, con $v \neq 0$, allora:

$$\|Av\| = \|v\| = |\lambda| \, \|v\|$$

Quindi $(|\lambda| - 1) \, \|v\| = 0 \Rightarrow |\lambda| = 1$. ■

Veniamo ora all'algebra del gruppo ortogonale. Dalla A.2.6 sappiamo che l'algbra di $O(n)$ coincide con quella della componente dell'identità ossia $SO(n)$. Tale algebra è indicata con $\mathfrak{so}(\mathfrak{n})$. Questo fatto ci dice che i due gruppi hanno la stessa dimensione. Considerando il punto (1) di B.1.1 abbiamo che data una matrice reale $n \times n$ X, la matrice e^{tX} è ortogonale se e soltanto se

$$X = -X^T \tag{B.2}$$

ovvero X è antisimmetrica. Quindi l'algebra di Lie $\mathfrak{so}(\mathfrak{n})$ è lo spazio reale delle matrici $n \times n$ antisimmetriche. Notare che la richiesta (B.2) garantisce che $Tr(X) = 0$ e più precisamente che la diagonale di queste matrici sia una diagonale di zeri. La dimensione di quest'algebra è

$$\frac{n}{2}(n-1).$$

Vale la seguente importante proprietà, [5]:

Proposizione B.1.3.
La mappa esponenziale $exp : so(n) \to SO(n)$ è suriettiva.

Prima di dimostrare questa proposizione richiamiamo, senza dimostrare, due teoremi che serviranno allo scopo.

Teorema B.1.4.
Per ogni matrice antisimmetrica A esistono una matrice ortogonale P e una matrice diagonale a blocchi D tali che $A = PDP^T$, dove

$$D = \begin{bmatrix} D_1 & & \cdots & \cdots \\ & D_2 & \cdots & \\ \vdots & \vdots & \ddots & \vdots \\ & & \cdots & D_p \end{bmatrix}$$

tale che ogni blocco è o zero o una matrice 2×2 della forma

$$D_i = \begin{bmatrix} 0 & -d_i \\ d_i & 0 \end{bmatrix},$$

dove $d_i \in \mathbb{R}^+/0$. In particolare gli autovalori di A sono o 0 o immaginari puri del tipo $\pm d_i$.

Teorema B.1.5.
Per ogni matrice ortogonale R esistono una matrice ortogonale P e una matrice diagonale a blocchi E tali che $R = PEP^T$, dove

$$E = \begin{bmatrix} E_1 & & \cdots & \cdots \\ & E_2 & \cdots & \\ \vdots & \vdots & \ddots & \vdots \\ & & \cdots & E_p \end{bmatrix}$$

tale che ogni blocco è ± 1 o una matrice 2×2 della forma

$$E_i = \begin{bmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{bmatrix},$$

dove $0 < \theta_i < \pi$. In particolare gli autovalori di R sono del tipo $\cos\theta_i \pm i\sin\theta_i$ o ± 1.

Veniamo ora alla dimostrazione della ProposizioneB.1.3.

Dimostrazione. Sia $R \in SO(n)$, allora avremo un numero pari di autovalori uguali a -1 e questi possono essere raggruppati in blocchi di dimensione due corrispondenti a $\theta = \pi$. Sia ora D una diagonale a blocchi del tipo di Teorema B.1.4. Possiamo calcolare e^D. Se $D_i = 0$ abbiamo $e^{D_i} = e^0 = 1$ mentre se

$$D_i = \begin{bmatrix} 0 & -d_i \\ d_i & 0 \end{bmatrix}$$

abbiamo

$$e^{D_i} = \begin{bmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{bmatrix}$$

Quindi abbiamo visto che per ogni matrice E del tipo di Teorema B.1.5 troviamo una matrice D diagonale a blocchi del tipo di Teorema B.1.4 tale che $e^D = E$. Come conseguenza si ha

$$R = PEP^T = Pe^D P^T = Pe^D P^{-1} = e^{PDP^T} = e^A$$

per una opportuna $A \in \mathfrak{so}(\mathfrak{n})$, questo conclude la dimostrazione. ■

Gruppo Unitario

Veniamo ora al gruppo unitario e speciale unitario. Questi gruppi hanno una grande rilevanza in molti ambiti della fisica, basti pensare ad esempio alla fisica delle particelle. In particolare le trasformazioni unitarie nella teoria quantistica

descrivono l'evoluzione unitaria di uno stato nello spazio di Hilbert del sistema (isolato).
Una matrice complessa $n \times n$ è detta unitaria se

$$AA^\dagger = A^\dagger A = I, \tag{B.3}$$

dove con $A^\dagger$ indichiamo l'aggiunto di A, in particolare $A^\dagger = \left(A^T\right)^*$.

Proposizione B.1.6.
Sia A una matrice complessa $n \times n$, sono equivalenti:

1. $A^\dagger = A^{-1}$
2. *Le colonne (righe) di A son una base ortonormale*[3] *di $\mathbb{C}^n$.*
3. $\langle Av, Aw \rangle = \langle v, w \rangle, \forall v, w \in \mathbb{C}^n$.
4. $\|Av\| = \|v\|, \forall v \in \mathbb{C}^n$.

Dalla condizione (B.3) risulta che

$$|detA|^2 = 1,$$

quindi il determinante di una matrice unitaria è un fattore di fase $e^{i\theta}$. Analogamente al caso del gruppo ortogonale è facile convincersi che l'insieme di tutte le matrici unitarie assieme al prodotto matricile formi un gruppo di Lie di matrici, chiamato $U(n)$, e che restringendosi alle matrici a determinante uguale ad 1 si ottenga un sottogruppo di Lie, chiamato $SU(n)$.

Si dimostra che sia $U(n)$ che $SU(n)$ sono gruppi **compatti** e **connessi**, mentre solo $SU(n)$ è semplicemente connesso. Risulta chiaro che una matrice unitaria reale è una matrice ortogonale. Riportiamo di seguito il seguente risultato senza dimostrazione

Teorema B.1.7 (Teorema Spettrale)**.**
Una matrice A è diagonalizzabile mediante matrici unitarie se e soltanto se è normale.

Osservazione 1.
Una matrice si dice normale se $AA^\dagger = A^\dagger A$. Chiaramente matrici ortogonali e unitarie sono casi particolari di matrici normali.

Osservazione 2.
Il teorema afferma che se A è normale allora esistono U unitaria ed D diagonale tali che $A = UDU^\dagger$. Si può inoltre dimostrare che

[3]Rispetto al prodotto hermitiano standard.

- Se A è anti-hermitiana allora le entrate di D sono nulle o immaginari puri.
- Se A è hermitiana allora le entrate di D sono reali.
- Se A è unitaria allora le entrate di D hanno valore assoluto 1.

Veniamo ora a considerare l'algebra del gruppo unitario.
Abbiamo che

$$e^{tX} \in U(n) \Leftrightarrow \left(e^{tX}\right)^{\dagger} = e^{-tX} \Leftrightarrow X^{\dagger} = -X,$$

cioè l'algebra di Lie del gruppo $U(n)$, chiamata $\mathfrak{u}(\mathfrak{n})$, è lo spazio reale di tutte le matrici complesse $n \times n$ anti-hermitiane[4]. Quindi si ha che

$$dim U(n) = dim(u(n)) = 2n^2 - (n^2 - n) - n = n^2.$$

Se si considera $SU(n)$, utilizzando il fatto che

$$det\left(e^{A}\right) = e^{Tr(A)},$$

si ha che $\mathfrak{su}(\mathfrak{n})$ è il sottospazio di $\mathfrak{u}(\mathfrak{n})$ delle matrici a traccia nulla ($Tr(X) = 0$). La dimensione di $\mathfrak{su}(\mathfrak{n})$, e quindi del gruppo, è pari a quella di $\mathfrak{u}(\mathfrak{n})$ meno uno (dato dalla condizione aggiuntiva sulla traccia), quindi è $n^2 - 1$.
Come nel caso del gruppo ortogonale vale un risultato di suriettività della mappa esponenziale.

Teorema B.1.8.
Le mappe esponenziali

$$exp : u(n) \to U(n) \ , \ exp : su(n) \to SU(n)$$

sono suriettive.

Dimostrazione. Consideriamo $A \in U(n)$. Da Osservazione 2 abbiamo che $A = UDU^{\dagger}$ dove D è una matrice diagonale con entrate del tipo $e^{i\theta}$

$$D = \begin{bmatrix} e^{i\theta_1} & & \cdots & \cdots \\ & e^{i\theta_2} & \cdots & \\ \vdots & \vdots & \ddots & \vdots \\ & & \cdots & e^{i\theta_n} \end{bmatrix}$$

Ora consideriamo la matrice anti-simmetrica

[4]Se si considera la scrittura e^{iY} allora i generatori del gruppo, Y, sono hermitiani.

$$E = \begin{bmatrix} i\theta_1 & & \cdots & \cdots \\ & i\theta_2 & \cdots & \\ \vdots & \vdots & \ddots & \vdots \\ & & \cdots & i\theta_n \end{bmatrix}$$

si ha banalmente che $e^E = D$. Quindi presa $B = UEU^\dagger$ abbiamo che

$$e^B = A.$$

Nel caso di una matrice $A \in SU(n)$ la dimostrazione è inalterata a parte il fatto che ora si deve avere $e^{\theta_1} e^{\theta_2} \cdots e^{\theta_n} = e^{\theta_1 + \theta_2 + \cdots + \theta_n} = 1$ e quindi

$$\theta_1 + \theta_2 + \cdots + \theta_n = 0.$$

Cioè ora la matrice E è a traccia nulla e quindi per l'invarianza per permutazioni della traccia anche B è a traccia nulla, cioè $B \in \mathfrak{su}(\mathfrak{n})$. ■

Appendice C

C.1 Un risultato importante

Veniamo ora a riportare un lemma, da [7], che è di fondamentale importanza.

Lemma C.1.1. *Sia $\mathfrak{G}$ un gruppo di Lie compatto. Se $\mathfrak{H}_1, \cdots, \mathfrak{H}_k$ sono sottogruppi chiusi connessi e generano un sottogruppo denso di $\mathfrak{G}$, allora essi generano $\mathfrak{G}$.*

Riportiamo di seguito, a puro titolo informativo, la dimostrazione notevolmente tecnica, data in [7], del lemma. Una dimostrazione dettagliata va oltre gli scopi di questo lavoro.

Dimostrazione. Consideriamo $k = 2$ dato che il caso generale si riduce facilmente a questo. Consideriamo il sottoinsieme $\Sigma = \mathfrak{H}_1\mathfrak{H}_2$ di $\mathfrak{G}$ e il suo prodotto n-volte $\Sigma^n = \Sigma \cdots \Sigma$. Allora $\Sigma, \Sigma^2, \ldots$ è una sequenza crescente di sottoinsiemi la cui unione, detta Σ^∞, è densa in $\mathfrak{G}$. Si vuole mostrare che esiste un m tale che $\Sigma^m = \mathfrak{G}$.

Si osservi per prima cosa che Σ^n è compatto e connesso. Questo discende dal fatto che Σ^n è l'immagine della mappa continua di moltiplicazione μ dall'insieme compatto e connesso $(\mathfrak{H}_1 \times \mathfrak{H}_2)^{\times n}$ in $\mathfrak{G}$. Quindi Σ^∞ e $\mathfrak{G}$ sono connessi. Siccome è possibile rappresentare fedelmente $\mathfrak{G}$ in un qualche $\mathbb{C}^N$, $\mathfrak{G}$ è una varietà algebrica reale irriducibile dello spazio delle matrici di dimensione N. Cioè $\mathfrak{G}$ ha una struttura aggiuntiva compatibile con quella di gruppo di Lie che è quella di varietà algebrica liscia irriducibile. Grazie alle ipotesi fatte i sottogruppi considerati sono delle sottovarietà chiuse irriducibili. La mappa μ è un morfismo di varietà algebriche reali irriducibili. Ne segue usando il teorema di Tarski-Seindenberg che Σ^n è un insieme semialgebrico in $\mathfrak{G}$ e la sua chiusura algebrica[1] Z_n è irriducibile. Quindi $Z_1, Z_2, \ldots$ è una sequenza crescente di sottovarietà chiuse irriducibili la cui unione è densa in $\mathfrak{G}$. Ne segue che $Z_p = \mathfrak{G}$ per qualche p e, siccome Σ^p è semialgebrica, questo implica che Σ^p contiene un

[1] L'unica più piccola sottovarietà algebrica reale chiusa di $\mathfrak{G}$ che contiene Σ^n.

intorno aperto $\mathfrak{O}$ di uno dei suoi punti g. Ora ne segue che Σ^{2p+1} contiene un intorno $\mathfrak{U}$ dell'identità. Allora Σ^{2p+1+k} contiene l'intorno aperto $\Omega_k = \mathfrak{U}\Sigma_k$ di Σ_k e quindi Σ^∞ e aperto in $\mathfrak{G}$. D'altra parte Σ^∞ è un sottogruppo di $\mathfrak{G}$, ma $\mathfrak{G}$ è connesso e quindi non ha sottogruppi aperti diversi da se stesso, quindi $\Sigma^\infty = \mathfrak{G}$.

Abbiamo mostrato che $\mathfrak{G}$ è l'unione di una sequenza crescente di insiemi aperti Ω_k, ma $\mathfrak{G}$ è compatto e quindi $\mathfrak{G} = \Omega_q$ per un qualche q. Quindi $\mathfrak{G} = \Sigma^{2p+1+q}$. ■

Bibliografia

[1] F.W. Warner, *Foundations of differential manifolds and Lie groups*, Springer (1983).

[2] B.C. Hall, *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*, Springer (2000).

[3] A. Kirillov, *An Introduction to Lie Groups and Lie Algebras*, Cambridge University Press (2008).

[4] M. Gourdin, *Basics of Lie groups*, èditions Frontières (1982).

[5] J. Gallier, *Geometric Methods and Applications: For Computer Science and Engineering*, Springer (2001).

[6] G.M. D'Ariano, Unpublished Notes.

[7] J. Brylinski, R. Brylinski, in *Mathematics of Quantum Computation*, Computational Mathematics Series, Chapman& Hall(2002).

[8] G. de la Torre, L. Masanes, A.J. Short, M.P. Muller *Deriving quantum theory from its local structure and reversibility*, arXiv:1110.5482 (2011).

[9] M.A. Nielsen, I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

[10] A.Y. Kitaev, A.H. Shen, M.N. Vyalyi, *Classical and Quantum Computation*, American Mathematical Society (2002).

[11] E. Fredkin, T. Toffoli, *Conservative Logic*, International Journal of Theoretical Physics **21** (1982).

[12] A.W. Harrow, *Exact universality from any entangling gate without inverses*,Q. Inf. Comp. Vol.8 (2008).

[13] D. Deutsch, *Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer*, Proceedings of the Royal Society of London A(1985).

[14] D. Deutsch, *Quantum Computational Networks*, Proceedings of the Royal Society of London A(1989).

[15] D. Deutsch, A. Barenco, A. Ekert, *Universality in Quantum Computation*, Proceedings of the Royal Society of London A(1995).

[16] S. Lloyd, *Almost any Quantum Logic Gate is Universal*, Physical Review Letters **75** (1995).

[17] A. Muthukrishnan, *Classical and Quantum Logic Gates: An Introduction to Quantum Computing*, Quantum Information Seminar, Rochester Center for Quantum Information (RCQI), (1999).

[18] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, H. Weinfurter, *Elementay gates for quantum computation*, Physical Review A**52**(1995).

[19] D.P. DiVincenzo, *Two-bit gates are universal for quantum computation*, Phys. Rev. A **51** (1995).

[20] D.P. DiVincenzo, *Quantum Gates and Circuits*, Proc. R. Soc. Lond. A (1998).

[21] L. Hardy, W. Wootters, *Limited Holism and Real-Vector-Space Quantum Theory*, Foundations of Physics Vol. 42 (2012).

[22] W.K. Wootters, *Entanglement Sharing in Real-Vector-Space Quantum Theory*, (2010).

[23] A.C. Yao, *Quantum Circuit Complexity*, Foundations of Computer Science (1993).

[24] G.M. D'Ariano, *Probabilistic theories: What is special about Quantum Mechanics?*, Philosophy of Quantum Information and Entanglement 85 (2010).

[25] L. Hardy, *Quantum Theory From Five Reasonable Axioms*, arXiv:quant-ph/0101012v4 (2001).

[26] L. Hardy, R. Spekkens, *Why Physics Needs Quantum Foundations?*, arXiv:1003.5008v1 (2010).

[27] L. Hardy, *Foliable Operational Structures for General Probabilistic Theories*, arXiv:0912.4740v1 (2009).

[28] L. Masanes, M.P. Muller, *A derivation of quantum theory from physical requirements*, New Journal of Physics Vol.13 (2011).

[29] J. Preskill, *Lecture Notes* del corso di Quantum Computation, Caltech (1998).

[30] G.M. D'Ariano, *Note del corso di Fondamenti della Meccanica Quantistica*.

[31] G.M. D'Ariano, P. Lo Presti, M.F. Sacchi, *Bell Measurements and Observables*, Phys. Lett. A **272** (2000).

[32] G.M. D'Ariano, P. Perinotti, G. Chiribella, *Informational derivation of quantum theory*, Phys. Rev. A **84** (2011).

[33] G.M. D'Ariano, P. Perinotti, G. Chiribella, *Probabilistic theories with purification*, Phys. Rev. A **81** (2010).

[34] J. Barrett, *Information processing in generalized probabilistic theories*, arXiv:quant-ph/0508211v3 (2006).

[35] G.M. D'Ariano, P. Perinotti, A. Belenchia, in preparation.