Introduzione alla Teoria dell'Informazione Quantistica*†

11 aprile 2019

Indice

*Ver. 9; Questi appunti si trovano sul sito http://www.unibo.it/docenti/cristian.degliesposti nella sezione 'Contenuti utili'. Alcune parti sono mutuate dagli appunti del corso precedente tenuto da Lorenzo Campos Venuti e Marco Roncaglia. Si ringraziano anche Mario Maffei, Florian Shtini, Andrea Rondelli e Luigi Tizzano per la segnalazione di alcune sviste. E' gradita la segnalazione di altri eventuali errori a degliesposti@bo.imm.cnr.it

†*In july 2018, for the incoming new course on "Quantum States of Matter and Radiation", some parts of these notes have been translated in English, to be used as a guide for the lectures. Far from being complete and exhaustive, the parts in English are provided only when* ***not*** *available in Nielsen and Chuang's book [23] or other references quoted part by part. Observations about possible errors are welcome at* degliesposti@bo.imm.cnr.it

1 Informazione quantistica

Ossia l'informazione immagazzinata, elaborata e trasmessa in sistemi fisici descritti (necessariamente) dalla meccanica quantistica. Parliamo di **comunicazione quantistica** quando due o più sottosistemi si scambiano informazione attraverso un canale che preserva il carattere quantistico dell'informazione. In particolare, il fronte attualmente più concreto dell'informazione quantistica è quello della **crittografia quantistica**, in cui esistono protocolli di trasmissione intrinsecamente sicuri nel senso che se un intruso cerca di carpire il segnale trasmesso da un mittente ad un destinatario, questi sono in grado di accorgersene. Esistono dispositivi a fibre ottiche di questo tipo già funzionanti e commercializzati.

Parliamo poi di **computazione quantistica** quando è possibile immagazzinare, leggere e scrivere l'informazione in supporti (memorie) costituiti da sistemi fisici con proprietà genuinamente quantistiche. Inoltre dovremo poter elaborare l'informazione quantistica con opportuni circuiti o porte logiche che sfruttino al pieno le caratteristiche non classiche di tali sistemi. Per chiarire meglio l'idea enunciamo qui i **criteri di DiVincenzo** [13], individuati nel 2000 come punti fondamentali da affrontare per la realizzazione di un elaboratore quantistico:

- Possibilità di inizializzare e leggere gli elementi fondamentali in cui viene immessa l'informazione quantistica (si veda la sottosezione 1.1 successiva).
- Esistenza di un insieme universale di porte logiche quantistiche per l'elaborazione (in analogia e per estensione alle porte logiche classiche fondamentali NOT, OR, AND).

[1] Parte non svolta e non richiesta.

- E' inoltre importante che i tempi su cui operano le porte siano sufficientemente piccoli rispetto a quelli di decoerenza, ossia i tempi su cui un tipico stato perde le proprietà essenziali quantistiche con le quali era stato preparato. Allo stesso modo le memorie dovranno mantenere fedelmente lo stato per i tempi necessari all'elaborazione.

- Scalabilità, per integrare il maggior numero possibile di memorie, canali e porte in uno spazio limitato.

I costituenti fondamentali a cui si fa riferimento nel primo punto dei criteri di DiVincenzo godono, in quanto sistemi quantistici, di due proprietà che risulteranno fondamentali:

- Il principio di sovrapposizione.

- L'**entanglement** (interlacciamento), che discuteremo diffusamente più avanti.

In qualche modo nei criteri di DiVincenzo risulta implicito il fatto che, a livello concettuale, esistano anche degli algoritmi quantistici che trattino l'informazioni in modo efficiente. In effetti, non è detto che sia sufficiente estendere per analogia gli algoritmi classici già noti; la formulazione di **algoritmi quantistici** radicalmente nuovi che sfruttino il principio di sovrapposizione e/o l'entanglement è un passaggio fondamentale della compuazione quantistica (vedremo un esempio più avanti). L'esperienza, almeno nella prima decade del XXI secolo, mostra che ciò che possiamo chiamare computazione quantistica non soppianta la computazione e la informatica tradizionale nella maggior parte degli scopi ma si rivolge piuttosto alla possibile soluzione di probemi di enormi difficoltà che non sono trattabili dai calcolatori classici o lo sono solo per dimensioni di input molto ridotte. Senza entrare nei dettagli della articolata classificazione della complessità dei problemi da un punto di vista algoritmico (introdotta ad es. nel Cap. 3 di [23]), ci limitiamo qua a sottolineare che ciò che fa la differenza tra quello che qualitativamente chiamiamo un "problema facile" ed uno "difficile" sta nel modo in cui crescono le risorse computazionali (tempo e memoria) necessarie per la soluzione. Come spesso accade anche in Fisica si individua il passaggio sostanziale da un regime all'altro quando si passa da un andamento polinomiale ad uno più che polinomiale, che per brevità a volte si indica come esponenziale. Quindi, dato il migliore algoritmo classico conosciuto per la soluzione di un problema logico-matematico, se le risorse impiegate da questo algoritmo seguono una legge al più polinomiale nella dimensione di input allora potremmo dire che quel problema è "facile" o a complessità computazionale "bassa" mentre se la legge è più che polinomiale lo definiamo "difficile" o ad "alta" complessità computazionale. Qua ci basterà dire che nella ricerca algoritmica attuale la computazione quantistica si rivolge alla seconda classe di problemi, perché (almeno in assenza di un algoritmo migliore) la crescita esponenziale in molti casi specifici significa una impossibilità pratica nel risolvere il problema su scala umana.

In questo senso la computazione quantistica potrebbe diventare decisiva perché con un algoritmo sostanzialmente nuovo di tipo quantistico, cioè che può avvalersi della struttura matematica presente nello spazio di Hilbert, il problema potrebbe ricadere nella classe polinomiale. Ne è un esempio rilevante la fattorizzazione di un numero nei suoi fattori primi, che se può sembrare banale per numeri di poche cifre diventa rapidamente ingestibile per numeri lunghi. In effetti, dati due numeri interi primi p_1 e p_2 ed il loro prodotto $p = p_1 p_2$, la ricerca di p_1 o p_2 (unici) dato p si dimostra essere un problema che con il miglior algoritmo conosciuto per macchine classice richiede risorse esponenzialmente crescenti rispetto ai bit necessari per esprimere p. Non a caso, su questa idea è fondato uno dei sistemi di crittografia più diffusi (RSA a chiave pubblica). Se il messaggio è cifrato allora un eventuale intruso per decifrare il messaggio necessita di una parte della chiave che è nota solo se si conoscono i fattori di partenza, e se questa è abbastanza lunga la decifratura non è fattibile in tempi utili per l'intruso. Se però questo avesse a disposizione un computer quantistico le sue possibilità aumenterebbero in maniera drastica usando ad esempio l'algoritmo quantistico di Shor che permette la fattorizzazione in un tempo polinomiale anzichè esponenziale (si veda anche la sezione successiva sugli algoritmi).

Infine è opportuno completare questa panoramica parlando anche di **simulazione quantistica**. Come in elettrotecnica, specialmente prima dell'avvento del digitale, si usavano circuiti analogici da banco per simulare attraverso un sistema di componenti elettrici attivi e passivi il comportamento effettivo di un altro sistema (ad es. i canali di conduzione di una membrana fisiologica) retto dallo stesso sistema di equazioni differenziali tensione/corrente, così Feynman [17] nel 1981 alla I Conferenza su Fisica e Computazione affermò che l'unica via promettente per simulare in tutta la sua complessità un sistema quantistico fosse quella di avvalersi del comportamento, o del "funzionamento" di un altro sistema quantistico poichè le risorse computazionali dei sistemi fisici classici non risulteranno in generale sufficienti. Questa idea generale oggigiorno trova sempre più applicazione grazie a modelli intermedi, per cui si descrive il comportamento fisico di un sistema quantistico $\mathcal{Q}_A$ tramite un modello $\mathcal{M}$ e si cerca un secondo sistema pure quantistico $\mathcal{Q}_B$ che risulti più facile da studiare (teoricamente e/o sperimentalmente) e che in determinate condizioni di lavoro sia anch'esso descritto dal modello $\mathcal{M}$. Il campo di simulazione quantistica forse più fervido è quello in cui $\mathcal{Q}_B$ è rappresentato da un gruppo di atomi freddi in un reticolo ottico, in cui le interazioni effettive tra i gradi di libertà si possono regolare in laboratorio con una ampia variabilità, e attraverso una serie di modelli quantistici paradigmatici (Heisenberg, Hubbard, sine-Gordon, Lieb-Liniger, ecc.) si affrontano problemi di base ancora aperti nella fisica dei corpi fortemente correlati nella materia condensata o nella materia nucleare.

Quantum Information

In the following we will use this term to describe the information that is stored, processed and transmitted in physical systems (necessarily) described by quantum mechanics. We will speak of ***quantum communication*** *when two or more subsystems exchange information on a channel that preserves the quantun nature of the information. In particular, the topic that is currently more de-*

veloped from the practical point of view is ***quantum cryptography****, where there exist intrinsically safe transmission protocols, in the sense that if an eavesdropper tries to catch the signal transmitted from a sender to a receiver then these are able to recognise the interference. There exist working optical fibers-based devices of this kind already available on the market.*

We will speak instead of ***quantum computation*** *when it is possible to store, read and write quantum information in memories built from physical systems with genuine quantum features. Moreover, we will need to process quantum information with suitable circuits or gates that fully exploit the non-classical features of such systems. In order to clarify better this idea, let us summarise here* ***DiVincenzo criteria****, put forth in 2000 as fundamental elements to face, having some technology at hand, in order to arrive at a quantum computer:*

- *Possibility to initialise and read the fundamental blocks in which quantum information "lives" (see next subsection 1.1).*
- *Existence of a universal set of quantum gates for processing (in analogy and by extension of classical fundamental logic gates NOT, OR, AND).*
- *Moreover, it is important that the characteristic times on which the gates do operate are sufficiently small with respect to decoherence times, that is, the timescale on which a typical state looses the essential quantum features with which it was prepared. In the same fashion memories should maintain faithfully the state over the times required for processing.*
- *Scalability, in order to integrate the maximum possible number of memories, channels and gates in a limited amount of space.*

The fundamental blocks of the first point of DiVincenzo criteria enjoy, due to their quantum nature, of two features that will turn to be essential:

- *Superposition principle*
- ***Entanglement****, that we will treat in detail in following sections.*

In DiVincenzo criteria it is somehow implicit the fact that, at least conceptually, there exist also ***quantum algorithms*** *that allow for an efficient treatment of the information. In fact, it is not guaranteed that it is sufficient to extend by analogy the known classical algorithms; the formulation of radically new quantum algorithms that exploit the superposition principle and/or entanglement is a fundamental step towards quantum computation (an example will be given later on). Experience, at least in the first decade of XXI century, shows that what we can call quantum computation does not suppress traditional computer science and computation for the majority of tasks but rather focuses on the possible solution of problems of enormous difficulty that are not affordable on classical computers or they are affordable only for very small input dimension. Without entering here the detailed classification of problems complexity from the algorithmic point of view (introduced for instance in Chap. 3 of [23]), here we will limit ourselves to note that what makes the difference between an "easy problem"*

and a "hard" one lies in the way the computational resources (time and storage) required for a solution grow with respect to the input size. As customary also in Physics a substantial passage is marked when one passes from a polynomial trend to an exponential one. Hence, give the best known classical algorithm for the solution of logical-mathematical problem, if the resources taken by such an algorithm follow at most a polynomial law as a function of some input dimension then we could say that the problem is "easy" or with "low" computational complexity, while if the law is more than polynomial we will term it as "hard" or with "high" computational complexity. Here it will suffice to say that in current algorithmic research quantum computation is devoted to the second class, because (at least until a better algorithm is found) the exponential growth in many specific cases means a practical impossibility in solving the problem on a human scale.

In this sense quantum computation could become decisive because with a substantially new algorithm of quantum kind (meaning that it can handle the mathematical structure of Hilbert space) the same problem could fall in the polynomial class. A relevant and celebrated example is prime numbers factoring, that could seem trivial for integer numbers of a few digits but becomes rapidly untractable for long numbers. In fact, given two prime numbers p_1 and p_2 and their product $p = p_1 p_2$, the search of p_1 or p_2 (that are unique) given p turns out to be a problem that using the best known algorithm on classical machines requires exponentially growing resources with respect to the number of bits used to express p. Not incidentally on this idea lies one of the most used cryptographic systems (public key RSA). If the message is crypted then a possible eavesdropper that wants to de-crypt it will need a part of the key that is known only if the initial two factors p_1 and p_2 are known, so if the key is sufficiently long (1024 in many current applications) de-cryption is not feasible in times useful for the eavesdropper. However, if the latter would have a quantum computer at disposal the possibilities would increase dramatically using for istance Shor's algorithm since it allows for prime factorisation in polynomial time (instead of exponential, see also following section on algorithms).

Finally, it is worth to complete this overview speaking also of ***quantum simulation****. Like in traditional electrotechnics, especially before the digital advent, analogic circuits were used to simulate through a series of active and passive electrical elements the effective behaviour of a totally different system (say the conduction channels in physiological membrane) because they share the common underlying structure of current/voltage differential equations, in the same spirit Feynman [17] in 1981 at the First Conference on Physics and Computation argued that the only promising way to simulate a quantum system in all its complexity is to employ the behaviour, or the "functioning", of another quantum system because the computational resources of classical physical systems will not be sufficient in general. This general idea nowadays sees an increasing number of applications thanks to intermediate models, for which one describes the physical behaviour of a quantum system $\mathcal{Q}_A$ through a model $\mathcal{M}$ and then one looks for a second system $\mathcal{Q}_B$, quantum as well, that for some reason is easier to study (theoretically and/or experimentally) and that under certain working*

conditions is described by the same model $\mathcal{M}$. The realm of quantum simulation that is currently perhaps more vivid is $\mathcal{Q}_B$ implemented by a group of cold atoms in an optical lattice, where effective interactions among degrees of freedom can be tuned in laboratories within wide ranges, and on the hand of paradigmatic quantum models (Heisenberg, Hubbard, sine-Gordon, Lieb-Liniger, etc.) one can afford the solution of still-open, fundamental problems in the physics of strongly-correlated particles in condensed matter or nuclear matter.

1.1 Il *qubit*

Come esistono gli elaboratori classici analogici e digitali, possiamo immaginare di trattare l'informazione quantistica in sistemi descritti da uno spazio di Hilbert infinito o finito dimensionale. Attualmente nella ricerca possiamo distinguere due filoni principali:

- Computazione quantistica a variabili continue ed in particolare in sistemi descritti da oscillatori armonici.
- Computazioni quantistica in **sistemi a due livelli**, che chiameremo **qubit**.

In questo contesto ci concentreremo essenzialmente solo sul secondo caso, quando non specificato diversamente. Va comunque detto che esistono alcuni approcci, principalmente teorici, all'informazione quantistica con sistemi finito dimensionali a più di due livelli che vengono genericamente indicati come *qudit*. Mutuando la usuale notazione "0" ed "1" per i due livelli logici classici, per un qubit scriveremo allora il generico stato (puro) come:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

avendo in mente che ora $|0\rangle$ e $|1\rangle$ rappresenteranno, a livello fisico, due stati ortogonali di un sistema fisico quali ad esempio le proiezioni lungo un asse dello spin di una particella a spin $1/2$ $|m = -1/2\rangle$ e $|m = +1a/2\rangle$. Le combinazioni lineari della forma (1) al variare di $\alpha, \beta \in \mathbb{C}$ individuano uno spazio di Hilbert $\mathcal{H}$ di dimensione (complessa) 2. Solitamente si considerano stati normalizzati all'unità, ossia $\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$.

Elenchiamo di seguito i sistemi fisici che attualmente permettono l'implementazione effettiva di qubit ([14] per una panoramica):

- Risonanza magnetica nucleare (7.7 in [23] e 1.9.3 in [1], [26] e 5.4 in [8] per ulteriori approfondimenti).
- Atomi in cavità elettromagnetiche (7.5 in [23] e 1.9.2 in [1], [30] e 5.2 in [8] per ulteriori approfondimenti).
- Fotoni (7.4 in [23], [30] per ulteriori approfondimenti), ad esempio nei gradi di libertà di polarizzazione trasversa orizzontale e verticale rispetto ad un sistema di riferimento.
- Punti quantici (*quantum dots* - sez. 4 in [4] e [27, 18, 12]).

- Sistemi superconduttivi ([32] per ulteriori approfondimenti).
- Trappole elettromagnetiche (7.6 in [23] e 1.9.1 in [1], [31, 19] e 5.3 in [8] per ulteriori approfondimenti) e reticoli ottici.

1.2 Operazioni ad un qubit

I fondamenti della meccanica quantistica permettono sostanzialmente due tipi di evoluzione (o trasformazione) per un dato sistema fisico isolato: il **collasso della funzione d'onda** nel caso di misura di un'osservabile oppure l'**evoluzione unitaria**. Il caso tipico e più importante è quello dell'evoluzione temporale governata dall'equazione di Schrödinger; in rappresentazione di Schrödinger gli stati evolvono temporalmente da un tempo t_0 ad un tempo t attraverso un operatore unitario $U^{-1} = U^\dagger$:

$$|\psi(t)\rangle = U(t;t_0)|\psi(t_0)\rangle$$

Più in generale ammetteremo che, in assenza di processi di misura, uno stato $|\psi\rangle$ all'interno di un elaboratore quantistico si trasformi secondo trasformazioni unitarie:

$$|\psi\rangle \to U|\psi\rangle.$$

La fuoriuscita dall'ambito di tali trasformazioni infatti potrebbe dar luogo alla violazione di alcune richieste fisiche come la causalità o l'esistenza di una velocità limite nel trasferimento di informazione, e l'analisi di tali questioni di fondamento ci porterebbe ampiamente fuori dallo scopo di questi appunti.

Ora, nel caso di un singolo qubit, le trasformazioni lineari ed unitarie complesse 2×2 si possono tutte esprimere come combinazioni lineari opportune delle matrici

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \sigma^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma^y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2}$$

dove abbiamo identificato la prima componente come quella sullo stato $|0\rangle$ e la seconda quella sullo stato $|1\rangle$. Riconosciamo nelle tre matrici σ^a , $a = x, y, z$ le matrici di Pauli, consistentemente con il fatto che la rappresentazione di spin $1/2$ del momento angolare, con le due proiezioni $|m = \pm 1/2\rangle$ lungo un asse di quantizzazione, è appunto il tipico esempio di sistema a due livelli. Quindi, almeno in linea di principio, in un certo procedimento di calcolo - o algoritmo - quantistico possiamo pensare di utilizzare le infinite matrici U(2) per manipolare il singolo qubit. Notiamo anche che la matrice σ^x ha l'effetto di scambiare il ruolo di $|0\rangle$ e $|1\rangle$, che è quello che classicamente chiameremmo come porta logica NOT. Un'altra matrice molto usata negli algoritmi quantistici è la cosiddetta **porta logica di Hadamard**:

$$U_H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(\sigma^x + \sigma^z\right).$$

L'effetto di tale porta su uno stato $|0\rangle$, per cui la probabilità di osservare in una misura il valore 0 è del 100%, è quello di generare lo stato $(|0\rangle + |1\rangle)/\sqrt{2}$ che

invece ha una probabilità del 50% di restituire 0 e una probabilità del 50% di restituire 1. L'effetto è simile sullo stato di ingresso $|1\rangle$ ma in tal caso lo stato di uscita è $(|0\rangle - |1\rangle)/\sqrt{2}$, con le stesse probabilità di uscita per 0 ed 1, ma con una diversa fase sulla componente di $|1\rangle$. Vedremo più avanti le conseguenze di una tale differenza di fase.

1.3 Operazioni a due qubit: CNOT e insieme universale di porte logiche

Da un punto di vista matematico gli stati possibili di due qubit, che per il momento indicheremo con A e B, appartengono ad uno spazio di Hilbert $\mathcal{H}_{AB}$ costruito a partire dagli spazi $\mathcal{H}_A$ e $\mathcal{H}_B$ e detto **prodotto tensore**: $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Per ogni scelta possibile di uno stato $|\psi\rangle_A$ in $\mathcal{H}_A$ possiamo liberamente scegliere uno stato $|\psi\rangle_B$ in $\mathcal{H}_B$ ed indicheremo lo stato complessivo del sistema AB come $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$. Quando il contesto non determina un'ambiguità useremo anche le notazioni equivalenti $|\psi\rangle_A|\psi\rangle_B$, $|\psi_A, \psi_B\rangle$ o ancora più semplicemente $|\psi_A\psi_B\rangle$. Gli operatori lineari L_A e L_B costruiti a partire da operatori su A e B agiscono come:

$$(L_A \otimes L_B)\,|\psi\rangle_{AB} = (L_A|\psi\rangle_A) \otimes (L_B|\psi\rangle_B)$$

mentre per i prodotti scalari avremo semplicemente:

$$({}_A\langle\phi|\otimes_B\langle\phi|)(|\psi\rangle_A \otimes |\psi\rangle_B) =_A \langle\phi|\psi\rangle_A \;{}_B\langle\phi|\psi\rangle_B.$$

Un'operazione meno banale sul sistema AB di due qubit è la proiezione parziale del qubit A su un dato stato $|\phi\rangle_A$ mentre il qubit B non viene preso in considerazione:

$${}_A\langle\phi|(|\psi\rangle_A \otimes |\psi\rangle_B) = \alpha|\psi\rangle_B \in \mathcal{H}_B$$

con $\alpha =_A \langle\phi|\psi\rangle_A$.

Una base di $\mathcal{H}_{AB}$ è data da tutte le possibili combinazioni degli elementi di base di A e di B ossia:

$$|0\rangle_A|0\rangle_B\ ,\ \ |0\rangle_A|1\rangle_B\ ,\ \ |1\rangle_A|0\rangle_B\ ,\ \ |1\rangle_A|1\rangle_B$$

e viene detta **base computazionale**. In generale la dimensione dello spazio di Hilbert che è il prodotto tensore di due spazi è data da $\dim\mathcal{H}_A \dim\mathcal{H}_B$, che dà appunto 4 per due qubit. Ora, è possibile far vedere [23] che p**er costruire un insieme universale di porte logiche quantistiche nello spirito dei criteri di DiVincenzo, è sufficiente combinare ripetutamente porte logiche ad un qubit (matrici unitarie U(2) ad elementi arbitari) ed una sola particolare porta logica a due qubit che li accoppia.** L'aspetto da rimarcare è che questo risultato è vero **per un qualsiasi numero di qubit** L. Il loro spazio di Hilbert globale ha dimensione 2^L ed una qualunque porta logica dell'insieme universale è di fatto una qualunque trasformazione unitaria del gruppo $U(N)$ con $N = 2^L$. La dimensione (numero di parametri continui reali indipendenti da specificare) di tale gruppo è $N^2 = 2^{2L}$, e l'affermazione di sopra sull'universalità di porte

A	B	A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

Tabella 1: Tavola di verità della funzione binaria CNOT.

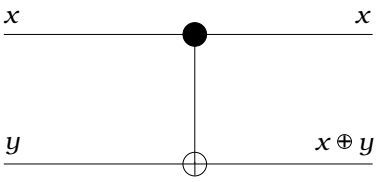

Figura 1: Rappresentazione grafica della porta logica CNOT. Il bit in corrispondenza del simbolo • è di controllo, mentre quello in corrispondenza di ⊕ contiene il dato in uscita.

logiche arbitrarie a un qubit combinata con una particolare a due qubit è di portata molto ampia perchè scarica la ricchezza di informazione di una simile infinità di trasformazioni nelle infinite combinazioni che si possono fare di L qubit, accoppiati a due a due e singolarmente trasformati in modo desiderato. A livello grafico vedremo che questi accoppiamenti e queste unitarie di singolo qubit, in tutte le sequenze desiderate, corrispondono a costruire un **circuito quantistico** (che estende con trasformazioni unitarie l'idea di circuiti a porte logiche classiche).

La porta essenziale che costituisce l'accoppiamento non può essere qualsiasi (non potrebbe essere ad esempio l'identità!) ma solitamente viene scelta tra alcune porte a due qubit notevoli. In particolare vediamo il NOT controllato (CNOT), che serve al nostro scopo. Tale porta agisce nel modo seguente: lascia inalterato il bit B se il bit A è 0, mentre lo inverte se A è 1. Con bit classici la tavola di verità del CNOT (indicato dal simbolo ⊕) è quella riportata in tabella 1. Si noti che A⊕B=B⊕A. Intesa come porta logica a due ingressi e due uscite, il CNOT lascia invariato il bit di controllo A. Così se x e y indicano, rispettivamente, i valori classici 0 o 1 del bit A e del bit B indicheremo l'azione classica del CNOT come: $(x, y) \rightarrow (x, x \oplus y)$. La rappresentazione grafica di tale porta è data in fig. 1.

A livello quantistico quantistico possiamo rappresentare il CNOT nella base computazionale attraverso la matrice unitaria 4×4

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{3}$$

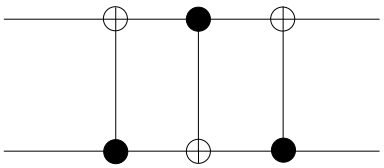

Figura 2:

Esercizio: Dimostrare che lo schema di fig. 2 scambia la configurazione dei bit di ingresso, quale che sia.

In ingresso la linea superiore (x) funge da dati e quella inferiore (y) da controllo. Al passaggio successivo la linea superiore porta il bit di controllo $x \oplus y$ e quella inferiore il bit di dati y: $(x, y) \to (y \oplus x, y) \to (y \oplus x, y \oplus (y \oplus x))$. Ma poiché vale $y \oplus (y \oplus x) = x$ (lo si verifichi con una tabella di verità) allora all'ultimo passaggio avremo $(y \oplus x, y \oplus (y \oplus x)) = (y \oplus x, x) \to (x \oplus (y \oplus x), x) = (y, x)$.

Dato che quando il bit di dati viene posto a 0 in ingresso, sia il bit di controllo x e quello di dati in uscita vengono posti uguali al valore x ($x \oplus 0 = x$), ci si può chiedere se agendo su una combinazione lineare $|x\rangle = \alpha|0\rangle + \beta|1\rangle$ l'azione sia ancora quella di copiare il qubit per α e β generici. Per linearità di U_{CNOT} abbiamo

$$|x\rangle|y = 0\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|0\rangle \to \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle$$

che corrisponde ad una copia del bit di controllo solo quando questo è 0 ($\alpha = 1$, $\beta = 0$) o 1 ($\alpha = 0$, $\beta = 1$) ma non nel caso generale. In effetti l'impossibilità di duplicare uno stato arbitrario di un qubit per mezzo del CNOT non è altro che la manifestazione di una proprietà molto più generale della meccanica quantistica:

> **Teorema di non-clonabilità (no-cloning)**: Non può esistere un dispositivo che produce due copie esatte di un generico stato quantistico incognito $|\psi\rangle$.
>
> *Dimostrazione*: Supponiamo per assurdo che per un qualunque stato $|\psi\rangle$ il dispositivo prenda in ingresso tale stato ed uno stato "vergine" $|v\rangle$ su cui viene copiato appunto $|\psi\rangle$
>
> $$|\psi\rangle|v\rangle \to |\psi\rangle|\psi\rangle.$$
>
> La trasformazione espressa sinteticamente come una freccia sarà una unitaria in meccanica quantistica; essendo $|\psi\rangle$ generico e incognito la unitaria non potrà però dipendere da come è fatto specificatamente lo stato di ingresso. Se ora ripetiamo la medesima operazione (unitaria) per un altro stato di ingresso $|\psi'\rangle$ avremo $|\psi'\rangle|v\rangle \to |\psi'\rangle|\psi'\rangle$. Quindi prendendo il prodotto scalare di queste due espressioni ed assumendo senza perdita di generalità $\langle v|v\rangle = 1$ si avrebbe $\langle\psi|\psi'\rangle = \langle\psi|\psi'\rangle^2$, cioè $\langle\psi|\psi'\rangle = 0$ oppure $\langle\psi|\psi'\rangle = 1$ il

che contraddice l'ipotesi che $|\psi\rangle$ e $|\psi'\rangle$ si potessero scegliere in modo arbitario.□

Notiamo tuttavia come l'argomentazione appena esposta lasci aperto il caso di due stati mutuamente ortogonali. In effetti nella corrispondenza classica due istanze mutuamente escludentesi (ad es. 0 o 1) sono associate a stati ortogonali e per l'appunto non esiste a priori una non clonabilità per stati classici.

1.4 Algoritmi quantistici

Se abbiamo a disposizione un registro classico a L bit sappiamo che il numero massimo che possiamo rappresentare in una memoria di un elaboratore è $N = 2^L$. Tale numero è anche il numero di stati di base su cui si può espandere il generico stato quantistico $|\psi\rangle$ a L qubit. In un certo senso, un registro quantistico nel quale è immagazzinato $|\psi\rangle$ contiene informazione sui 2^L numeri complessi che definiscono l'espansione sulla base (ad es. quella computazionale a L qubit). Se κ è il numero di bit classici che servono su una data macchina per rappresentare (in modo approssimato) un numero complesso, allora l'insieme dei coefficienti di espansione di $|\psi\rangle$ necessiterà di $\kappa 2^L$ bit classici per essere memorizzato. Ad esempio quindi l'informazione codificata in $L = 100$ qubit con $\kappa = 64$ occupa 64×2^{100} bit $= 8 \times 2^{90}$KBytes $\cong 10^{18}$TBytes. Il divario tra la capacità classica e quella quantistica (nominale) aumenta esponenzialmente con L. Da un punto di vista sperimentale non è ancora possibile manipolare in modo soddisfacente un tale numero di qubit ma, a parte l'ostacolo di natura tecnologica, esiste comunque un problema di natura concettuale: quale procedura o algoritmo ci permette di accedere **simultaneamente** a tale informazione? E' come se gli stati quantistici avessero una sorta di **parallelismo intrinseco** per la codifica e l'elaborazione dell'informazione. Non va dimenticato però che l'azione di misura (o lettura in un elaboratore) di per sè distrugge la sovrapposizione lineare che permette un tale parallelismo, facendo collassare la funzione d'onda in uno stato della sovrapposizione in cui si trovava prima della misura. Pertanto, rimane aperta la questione di come sfruttare questa potenza nominale. In questo senso, il concepimento di algoritmi genuinamente quantistici è uno dei settori più importanti dell'informazione quantistica. Vediamo ora in dettaglio l'esempio forse più semplice.

1.4.1 Sfruttare il parallelismo intrinseco: L'algoritmo di Deutsch-Josza

Consideriamo una funzione f dall'insieme dei possibili numeri binari a L bit all'insieme $0, 1$ e supponiamo di sapere a priori che vale la seguente proprietà: la funzione è costante, ossia assume lo stesso valore per ogni possibile argomento, oppure è bilanciata nel senso che per metà dei 2^L possibili argomenti vale 0 e per l'altra metà vale invece 1. Il problema che viene posto è quello di stabilire se f è bilanciata o costante con il numero minimo di valutazioni della funzione. Tale problema ha un carattere accademico più che una reale utilità pratica, ma

ci permetterà appunto di vedere in che modo l'elaborazione a livello quantistico dell'informazione contenuta in un registro di qubit possa sfruttare in modo decisivo il principio di sovrapposizione degli stati. Anche la scelta del tipo di funzione è stata fatta ad-hoc; infatti per ognuno dei 2^L argomenti della tavola di verità a L bit possiamo assegnare in modo indipendente due valori alla funzione in uscita, generando così 2^{2^L} possibili funzioni binarie, e molte di queste non saranno nè costanti nè bilanciate.

Vediamo innanzi tutto il caso classico. Nella migliore delle ipotesi potremo valutare la funzione in metà dei possibili argomenti, cioè $2^L/2$, ed ottenere sempre lo stesso valore. A questo punto basta un'ulteriore valutazione per scoprire se siamo nel caso bilanciato o costante. Quindi il numero minimo di valutazioni di f da effetturare nel caso classico è $2^{L-1}+1$. Dovendo confrontare l'efficenza di un algoritmo classico con quella di uno quantistico, stiamo implicitamente assumendo che il calcolo dei valori assunti da f sia essenzialmente classico ed implementabile con un opportuno dispositivo. A livello quantistico, in generale non sappiamo che significato dare ad espressioni del tipo $f(\alpha|0\rangle + \beta|1\rangle)$ quindi sarà necessario individuare una strategia per valutare f su ciascuno dei suoi possibili argomenti preservando al tempo stesso le sovrapposizioni lineari fino all'ultimo stadio di misura in uscita dal circuito quantistico. In tale circuito però possiamo pensare che esista un opportuno operatore unitario U_f che, dati i valori di f ad esempio sui 2^L elementi della base computazionale (la tavola di verità nel caso classico), implementi la valutazione della funzione su registri a L (o più) qubit. Quindi, per linearità di U_f, potremo poi agire su combinazioni lineari arbitrarie. Ad esempio nel caso più semplice $L = 1$ avremo quattro possibili funzioni

$$f(0) = f(1) = 0$$
$$f(0) = f(1) = 1$$
$$f(0) = \bar{f}(1) = 0$$
$$f(0) = \bar{f}(1) = 1$$

dove con $\bar{f}$ indichiamo il NOT classico che scambia 0 con 1 e viceversa. Nei primi due casi f è costante mentre negli ultimi due è bilanciata. Come possibile scelta di U_f vediamo come va costruita la matrice 4×4 che realizza una variante del CNOT ossia $(x, y) \to (x, f(x) \oplus y)$ dove il controllo è effettuato non già da x ma da $f(x)$. Per ognuna delle quattro possibili scelte per f avremo le tavole di verità e matrici associate riportate, rispettivamente nelle tabelle 2-5. Nelle righe di U_f è presente un 1 solo dove la funzione $(x, y) \to (x, f(x) \oplus y)$ assume un valore definito nel caso classico. Comunque si può verificare che in ogni caso la matrice U_f risultante è unitaria; nel caso $f(0) = f(1) = 0$ non si opera di fatto alcun controllo e la matrice è l'identità. Nel caso $f(0) = 0$, $f(1) = 1$ invece riconosciamo il normale CNOT dell'eq. (3). Si noti anche che quando $y = 0$ U_f valuta $f(x)$ per ogni possibile valore di x.

x	y	$f(x)$	$f(x) \oplus y$
0	0	0	0
0	1	0	1
1	0	0	0
1	1	0	1

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

Tabella 2: Tavola di verità di $f(x) \oplus y$ quando $f(x)$ è la funzione ad un bit riportata in terza colonna, e matrice unitaria associata.

x	y	$f(x)$	$f(x) \oplus y$
0	0	1	1
0	1	1	0
1	0	1	1
1	1	1	0

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

Tabella 3: Come in tabella 2.

x	y	$f(x)$	$f(x) \oplus y$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

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

Tabella 4: Come in tabella 2.

x	y	$f(x)$	$f(x) \oplus y$
0	0	1	1
0	1	1	0
1	0	0	0
1	1	0	1

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

Tabella 5: Come in tabella 2.

Analogamente potremo costruire matrici $2^{L+1} \times 2^{L+1}$ per implementare la funzione $(X, y) \to (X, f(X) \oplus y)$ dove ora $X = x_1 x_2 \dots x_L$ è una stringa a L qubits. Un modo efficiente di generare tutte i 2^L possibili valori di X, ossia di esplorare tutta la base computazionale a L qubit, consiste nel prepararli tutti nello stato $|0\rangle$ per poi farli passare ciascuno per un una porta di Hadamard

$$(U_H \otimes U_H \dots \otimes U_H)\,|0\rangle|0\rangle \dots |0\rangle = \frac{(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \dots (|0\rangle + |1\rangle)}{\sqrt{2^L}} =$$

$$\frac{|0\rangle|0\rangle \dots |0\rangle + |0\rangle|1\rangle \dots |0\rangle + \dots + |1\rangle|1\rangle \dots |1\rangle}{\sqrt{2^L}}.$$

Così ora la matrice U_f (che è $2^{L+1} \times 2^{L+1}$) dopo l'applicazione di queste L porte di Hadamard in parallelo ed il bit ausiliario y posto a 0 restituisce

$$U_f \left(U_H \otimes U_H \ldots \otimes U_H\right) |0\rangle|0\rangle \ldots |0\rangle|y=0\rangle = \frac{1}{\sqrt{2^L}} \sum_X |X\rangle|f(X)\rangle,$$

essendo $f(X)$ la funzione f a L bit valutata nell'argomento $X = x_1 x_2 \ldots x_L$. Si noti che nella combinazione lineare abbiamo appunto simultaneamente la funzione valutata su tutti i possibili argomenti. Si tratta ora di confrontarli in modo pure simultaneo. Anziché usare $y = 0$ come bit ausiliario usiamo il qubit posto nello stato $(|0\rangle - |1\rangle)/\sqrt{2}$ che a sua volta si può ottenere dalla porta di Hadamard mettendo $|1\rangle$ come ingresso. Ritornando per un momento al caso $L = 1$ ricordiamo che con $y = 1$ l'azione di U_f è quella di restituire $(x, \bar{f}(x))$. Allora per linearità avremo

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \rightarrow \frac{|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle}{2} - \frac{|0\rangle|\bar{f}(0)\rangle + |1\rangle|\bar{f}(1)\rangle}{2}$$

e vediamo che se $f(0) = f(1) = f$ allora si riproduce lo stato $(|0\rangle + |1\rangle)(|f\rangle - |\bar{f}\rangle)/2 = \pm(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)/2$ dove il segno superiore va preso quando $f = 0$ e quello inferiore quando $f = 1$ (in forma compatta $(-1)^f$). Invece se $f(0) = \bar{f}(1) = f$ troviamo $(|0\rangle - |1\rangle)(|f\rangle - |\bar{f}\rangle)/2 = \pm(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)/2$. La differenza sta nel segno relativo nello stato del primo qubit; applicando su questo un'ulteriore porta di Hadamard ritorniamo agli stati della base computazionale $|0\rangle$ o $|1\rangle$ rispettivamente. In forma compatta possiamo scrivere lo stato finale come $|f(0) \oplus f(1)\rangle(|0\rangle - |1\rangle)/\sqrt{2}$. Per capire cosa succede nel caso a L qubit osserviamo innanzi tutto che nel caso costante quando tutti i valori di $f(X)$ coincidono si ritrova lo stato $(-1)^f|X\rangle(|0\rangle - |1\rangle)$ per ogni termine della somma sui valori di X. In caso contrario ogni termine $|f(X)\rangle - |\bar{f}(X)\rangle$ andrà preso con il suo segno nella somma cioè come $(-1)^{f(X)}(|0\rangle - |1\rangle)$. In formule scriviamo gli stati ai passi I e II in fig. 3

$$|\Psi\rangle_I = \frac{1}{\sqrt{2^L}} \sum_X |X\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$|\Psi\rangle_{II} = \frac{1}{\sqrt{2^L}} \sum_X (-1)^{f(X)} |X\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

da cui si vede che l'azione di f è quella di **sfasare** con segni diversi i vari termini nella somma. Infine, per fare in modo che questi diversi "cammini" interferiscano, facciamo passare lo stato degli L qubit attraverso un'ultima porta di Hadamard multipla. Per il singolo qubit osserviamo che possiamo scrivere in forma concisa $U_H|x\rangle \rightarrow \sum_{z=0,1}(-1)^{zx}|z\rangle/\sqrt{2}$; i due possibili valori $z = 0, 1$ vengono combinati con segno diverso solo quando $x = 1$. L'espressione si generalizza direttamente al caso $L > 1$

$$U_H \otimes U_H \ldots \otimes U_H |X\rangle = \frac{1}{\sqrt{2^L}} \sum_{z_1, z_2 \ldots z_L = 0,1} (-1)^{x_1 z_1 + x_2 z_2 + \ldots x_L z_L} |z_1 z_2 \ldots z_L\rangle = \frac{1}{\sqrt{2^L}} \sum_Z (-1)^{X \cdot Z} |Z\rangle$$

dove $X \cdot Z$ indica il prodotto scalare dei vettori $(x_1, x_2, \ldots, x_L)$ e $(z_1, z_2, \ldots, z_L)$. Pertanto lo stato al passaggio III si scrive come

$$|\Psi\rangle_{III} = \frac{1}{2^L} \sum_{X,Z} (-1)^{X \cdot Z + f(X)} |Z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Ora, fra tutti i possibili stati di uscita, esaminiamo qual'è la probabilità di ottenere quello con $|Z = 00\ldots0\rangle$. Essendo tutti stati ortonormali avremo

$$p_0 = \text{prob}(Z = 0) = \left| \frac{1}{2^L} \sum_{X} (-1)^{f(X)} \right|^2.$$

E quindi se f è costante nella somma abbiamo 2^L termini uguali a $(-1)^f$ perciò $p_0 = 1$. Se invece f è bilanciata avremo esattamente la metà dei termini con un segno e l'altra metà col segno opposto da cui $p_0 = 0$. In sostanza per rispondere alla domanda del problema di Deutsch-Josza si applica **una** sola volta la funzione f all'interno della porta U_f, anziché almeno $2^{L-1}+1$ volte come nel caso classico, e si misura l'osservabile proiettiva $|Z = 0\rangle\langle Z = 0| \otimes \mathbb{I}_y$ con valore di aspettazione

$${}_{III}\langle\Psi|Z = 0\rangle\langle Z = 0|\Psi\rangle_{III} = p_0.$$

A parità di stato iniziale, e nel caso ideale di un circuito quantistico che non introduce errori di alcun tipo, il risultato sarà sempre $p_0 = 0$ oppure $p_0 = 1$ in ogni ripetizione della misura. Quindi, se si osserva $p_0 = 0$ significa che la funzione è bilanciata ed i vari casi hanno interferito distruttivamente nella costruzione dello stato con $Z = 00\ldots0$ mentre se $p_0 = 1$ si ha la funzione costante con la massima interferenza costruttiva. Dal punto di vista del numero di valutazioni della f necessarie per la risposta al problema posto, si passa da un andamento esponenziale nel numero di qubit ad un valore costante (uno in questo esempio); si dice che si è realizzato un guadagno (*speedup*) esponenziale.

Un altro algoritmo piuttosto noto è quello di Shor e permette, con un computer quantistico, di ridurre il costo computazionale per la fattorizzazione in numeri primi di un numero a N cifre da $O\left(2^{L^{1/3}}\right)$, usando il miglior algoritmo classico, a $O(L^3)$ dove $L \sim \log N$ il numero minimo di bit necessari per rappresentare il numero in questione. Si passa da una funzione esponenziale ad una polinomiale (o algebrica) ed il guadagno è ancora esponenziale.

2 Introduzione all'entanglement

Consideriamo un sistema fisico C composto da due sottosistemi A e B (come in fig. 4, ignorando per il momento il sistema universo U) descritto, a livello quantistico, da uno stato $|\Psi\rangle_C$. Diciamo che, rispetto alla partizione in A e B, **lo stato $|\psi\rangle_C$ è separabile se lo si può scrivere come prodotto di uno stato riferito solo ad A ed uno stato riferito solo a B: $|\Psi\rangle_C = |\psi\rangle_A \otimes |\psi\rangle_B$. In caso contrario, sarà detto non separabile o entangled**.

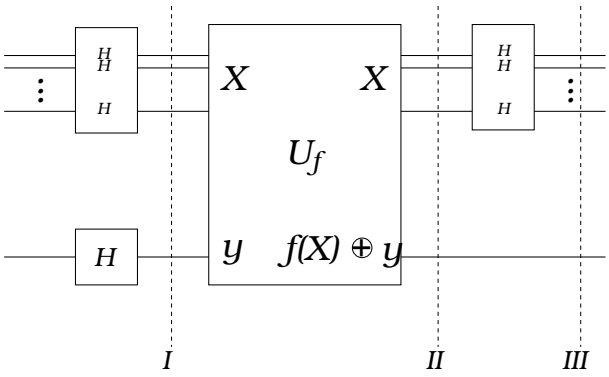

Figura 3: Schema di circuito quantistico per la realizzazione dell'algoritmo di Deutsch-Jozsa a partire dallo stato iniziale $|0\rangle|0\rangle \ldots |0\rangle|1\rangle$. Il blocco H indica la porta di Hadamard.

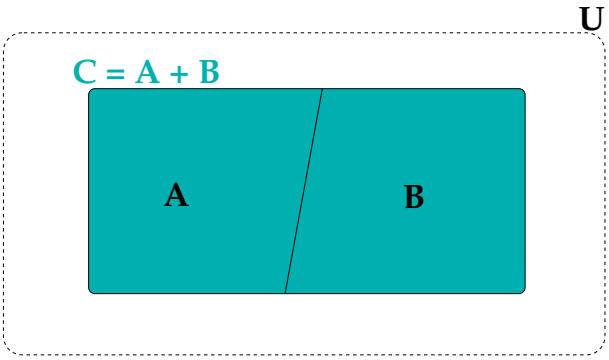

Figura 4: Partizione di un sistema isolato C nelle due parti A e B. Quando invece C non è isolato in generale dovremo considerare la presenza di un sistema (isolato) universo U che lo contiene.

Va ribadito che **l'entanglement riferito ad un dato stato e ad una data partizione**. Uno stesso sistema fisico può in certe condizioni essere descritto da uno stato separabile e, in altre condizioni, essere descritto invece da uno stato entangled. E a sua volta uno stato può risultare separabile rispetto ad una certa partizione ed invece risultare entangled rispetto ad una partizione diversa. Ad esempio, se pensiamo a B come ad un sistema di due qubit B' e B" con $|\Psi\rangle_C = |\psi\rangle_A \otimes |\psi\rangle_B$ e

$$|\psi\rangle_B = \frac{|0\rangle_{B'} \otimes |1\rangle_{B''} - |1\rangle_{B'} \otimes |0\rangle_{B''}}{\sqrt{2}} \tag{4}$$

allora $|\psi\rangle_C$ risulterà separabile alla separazione A/B'B" ma non separabile rispetto alla partizione AB'/B". In effetti vedremo che, quale che sia $|\psi\rangle_A$, non esiste nessuna scelta di stati $|\tilde{\psi}\rangle_{B'}$ e $|\tilde{\psi}\rangle_{B''}$ (rispettivamente in B' e B") tale che la combinazione lineare in eq. (4) si possa riscrivere come $|\tilde{\psi}\rangle_{B'} \otimes |\tilde{\psi}\rangle_{B''}$.

2.1 Paradosso di Einstein-Podolsky-Rosen (EPR)

L'esperimento concettuale suggerito nell'articolo di Einstein, Podolsky e Rosen nel 1935 [15] mira a concludere che la meccanica quantistica, almeno nella sua formulazione più diffusa, non è una teoria fisica completa. Al fine di mantenere la questione su un piano operativo e non già meramente filosofico, in quel contesto si definiva **completa** una teoria che potesse comprendere almeno tutti gli elementi di realtà fisica. E' piuttosto intuitivo dare come condizione sufficiente per essere un **elemento di realtà** il fatto che una certa quantità fisica possa essere predetta con certezza prima dell'atto di misura. Quindi una teoria fisica completa deve tener conto almeno di quelle quantità che possono essere predette con certezza prima della misura (in condizioni ideali di assenza di qualsiasi fonte di "rumore").

Nella loro formulazione originaria, EPR considerarono un sistema di due particelle con variabili coniugate di posizione e impulso relativi, e posizione e impulso del centro di massa definiti. Tuttavia l'esperimento ideale proposto da EPR non era particolarmente adatto ad una verifica sperimentale. Perciò considereremo una situazione totalmente equivalente proposta da Bohm in cui due particelle A e B di spin $1/2$ sono inizialmente preparate nello stato di singoletto con spin totale $S = 0$. Il punto che, secondo EPR, risulta incompleto nella meccanica quantistica sono essenzialmente le relazioni di indeterminazione di Heisenberg. Per illustrare l'argomento EPR abbiamo sostanzialmente bisogno di due fattori:

- **Osservabili non compatibili**, ossia descritte da operatori hermitiani non commutanti. Nel nostro caso sia lo spin della particella A e della particella B soddisfano le regole di commutazione

  $$[S^\alpha, S^\beta] = i\hbar\epsilon^{\alpha\beta\gamma} S^\gamma$$

  o, in termini di matrici di Pauli $\sigma^\alpha = 2/\hbar S^\alpha$ con $\alpha = x, y, z$

  $$[\sigma^\alpha, \sigma^\beta] = 2i\epsilon^{\alpha\beta\gamma}\sigma^\gamma$$

dove $\hbar$ è la costante di Planck ridotta $h/2\pi$ e $\epsilon^{\alpha\beta\gamma}$ è il simbolo totalmente antisimmetrico di Levi-Civita (non nullo solo quando α, β e γ sono tutti diversi; $+1$ se sono una permutazione ciclica di x, y, z e -1 altrimenti).

- **Simmetrie** che vincolino lo stato relativo in cui si trovano le due particelle. Ad esempio in questo caso possiamo pensare ad un decadimento di una particella di spin zero in due particelle di spin $1/2$. In assenza di forze esterne dalla conservazione della quantità di moto totale abbiamo che nel sistema del centro di massa le particelle si allontanano con impulso $\vec{p}_A = -\vec{p}_B$, mentre dalla conservazione del mometo angolare totale sappiamo (indipendentemente dalla teoria che stiamo adottando) che lo spin di A è sempre antiparallelo a quello di B.

Le due particelle vengono poi lasciate volare a grande distanza, ben oltre qualunque raggio di interazione. A questo punto l'osservatrice in A (Alice) decide di misurare σ_A^z, la componente z dello spin della sua particella, ottenendo $+1$ o -1. Siccome lo stato globale è un singoletto, siamo in grado di predire con certezza che la componente z dello spin che della particella B , σ_B^z , deve avere il valore opposto. E qui interviene l'ipotesi di **località**, cioè che lo stato della particella B non può essere modificato dalla misura di A se i due eventi associati ad A e B sono fuori dal cono luce (definito da $d_{A-B} > ct$ dove d_{A-B} è la distanza spaziale e t il tempo di volo) e per cui non sussiste relazione di causa-effetto. Quindi, secondo EPR l'autovalore di σ_B^z rappresenta un elemento di **realismo**. Ma avremmo potuto fare lo stesso esperimento eseguendo le misure lungo l'asse x, giungendo alla conclusione che anche σ_B^x rappresenta un elemento di realismo. Però questo è in contrasto con la visione quantomeccanica, dal momento che σ_B^z e σ_B^x non commutano e per questo non hanno valori entrambi definiti. Con ciò EPR vollero mettere in discussione la completezza della meccanica quantistica.

Si noti che, solo sulla base della conservazione dello spin totale $\vec{S}_{tot} = \vec{S}_A + \vec{S}_B$, possiamo affermare che, dato un qualunque asse di quantizzazione $\hat{n}$ lo stato complessivo delle particelle A e B in un qualunque istante del volo prima della misura si esprime come un **singoletto** di spin con autovalori $S_{tot} = 0$ e $S^n = \hat{n} \cdot \vec{S}_{tot} = 0$ ossia nella forma (4) –riferita qui alla partizione A/B– dove si associa ad esempio lo stato $|0\rangle_A$ con l'autovalore $-\hbar/2$ di S_A^n e lo stato $|1\rangle_A$ con l'autovalore $+\hbar/2$. Questo è vero per qualunque scelta dell'asse $\hat{n}$ e l'argomento di EPR poggia in maniera decisiva sul fatto che lo stato entangled di singoletto mantiene una correlazione antiferromagnetica (spin antiparalleli) tra A e B a qualunque distanza.

2.2 Disuguaglianza di Bell

Il risultato dell'esperimento concettuale di EPR viene definito talvolta un paradosso poichè, almeno in una versione puramente realista e locale, lo stato dello spin sotto osservazione di B risulta instantaneamente determinato una volta che A ha fatto la sua misura. A questo livello possiamo dire che il paradosso non sussiste se siamo disposti ad ammettere che la meccanica quantistica contempla l'esistenza di **correlazioni non locali** come l'entanglement. Ad ogni

modo, affinchè A e B possano utilizzare operativamente queste correlazioni e questo passaggio di informazione virtualmente istantaneo debbono comunque comunicarsi le loro procedure ed i relativi risultati. Questa comunicazione deve avvenire, secondo il principio di relatività, a velocità non superiori a quella della luce e quindi complessivamente l'operazione condotta da A e B non viola alcuna relazione di causa-effetto. Storicamente, nello stesso anno, nella stessa rivista e con un articolo dallo stesso titolo di quello di EPR [6], Bohr afferma il principio di complementarità come elemento di consistenza per la formulazione della teoria quantistica nella visione "di Copenhagen", ampiamente adottata poi nel XX secolo.

Con l'intento di spostare il problema della completezza e del realismo da un piano epistemologico ad un livello più direttamente fisico, Bell riuscì a riformulare la questione EPR in termini di quantità misurabili. L'idea è quella di confrontare i risultati predetti dalla meccanica quantistica con quelli predetti invece da un'ipotetica teoria alternativa in cui l'indeterminazione sia il frutto sostanzialmente di una conoscenza solo parziale del sistema. In aggiunta ai gradi di libertà che abbiamo sotto controllo, possiamo in generale ammettere che vi siano degli ulteriori gradi di libertà – le cosiddette **variabili nascoste** – che determinerebbero completamente lo stato in senso classico. Il fatto di non accedervi (o di non potervi accedere) fa sì che lo stato e le osservabili associate ad esso si comportino in modo non deterministico nell'atto di misura. Ad esempio, consideriamo ancora uno spin $1/2$ quantizzato lungo una direzione $\hat{n}$ definita dagli angoli polari θ e φ: $\hat{n} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$. Vediamo come sono scritti gli autovettori nella base di quantizzazione lungo z

$$S^n \equiv \hat{n}\cdot\vec{S} = \frac{\hbar}{2}(\sin\theta\cos\varphi\sigma^x + \sin\theta\sin\varphi\sigma^y + \cos\theta\sigma^z) \to \frac{\hbar}{2}\begin{pmatrix} \cos\theta & \sin\theta e^{-i\varphi} \\ \sin\theta e^{+i\varphi} & -\cos\theta \end{pmatrix}$$

$$|\uparrow_n\rangle = \cos\frac{\theta}{2}|\uparrow_z\rangle + e^{i\varphi}\sin\frac{\theta}{2}|\downarrow_z\rangle\ ,\quad |\downarrow_n\rangle = \sin\frac{\theta}{2}|\uparrow_z\rangle - e^{i\varphi}\cos\frac{\theta}{2}|\downarrow_z\rangle$$

avendo usato la forma delle matrici di Pauli in (2). Gli stati $|\uparrow_n\rangle$ e $|\downarrow_n\rangle$, con autovalori di S^n rispettivamente $\hbar/2$ e $-\hbar/2$, sono definiti ciascuno a meno di una fase globale. In particolare invertendo abbiamo $|\uparrow_z\rangle = \cos\frac{\theta}{2}|\uparrow_n\rangle + \sin\frac{\theta}{2}|\downarrow_n\rangle$ così che, secondo la meccanica quantistica, preparando uno spin $1/2$ con autovalore $\hbar/2$ lungo z abbiamo una probabilità $p_+ = \cos^2\frac{\theta}{2}$ di trovarlo diretto parallelamente a $\hat{n}$ e una probabilità $1 - p_+$ di trovarlo antiparallelo. In un'ottica di variabili nascoste, possiamo interpretare in modo equivalente questo stato dicendo che, dato l'angolo θ, al momento di preparare lo stato in modo classico c'è una variabile aleatoria λ che non è sotto controllo (per semplicità distribuita uniformemente tra 0 e 1) e tale che il nostro stato risulta preparato come $|\uparrow_n\rangle$ se $0 \le \lambda < p_+$ e invece come $|\downarrow_n\rangle$ se $p_+ \le \lambda \le 1$.

Ora, nello spirito dell'esperimento di EPR, ammettiamo che per Alice esistano (almeno) due quantità Q e R che possono assumere ciascuna i valori discreti $q = \pm 1$ e $r = \pm 1$. In una teoria quantistica Q e R possono essere ad esempio lo spin misurato lungo due direzioni distinte, riscalato di un fattore $2/\hbar$. Affinchè le relazioni di indeterminazione non pregiudichino il confronto con una eventuale

teoria a variabili nascoste, ammettiamo che l'osservatore in A decida di volta in volta di misurare Q oppure R nell'ipotesi però che le proprietà fisiche associate a Q ed R siano in qualche modo oggettive, cioè i valori q ed r sono dati una volta che lo stato delle due particelle in volo è stato preparato. Analogamente l'osservatore in B (Bob) può decidere di misurare sul suo sottosistema uno di due quantità, S o T. Sia $p(q,r,s,t)$ la distribuzione di probabilità congiunta che, nella preparazione dello stato a due particelle A e B, per effetto di variabili nascoste fuori controllo, la quantità Q sia pari a q, R sia pari a r, S pari a s e T pari a t. Si noti che in un tale schema a variabili nascoste, tutte e quattro le quantità hanno un valore definito in ogni prova dell'esperimento. Si ripetono poi molte prove ed in ciascuna di queste Alice e Bob registrano la proprietà che hanno misurato (Q o R da un lato e S o T dall'altro) e poi calcolano la seguente quantità

$$\mathcal{B} = \mathsf{E}(QS)+\mathsf{E}(RS)+\mathsf{E}(RT)-\mathsf{E}(QT) = \mathsf{E}(QS+RS+RT-QT) = \sum_{q,r,s,t=\pm 1} p(q,r,s,t)(qs+rs+rt-qt)$$

dove E indica il valore di aspettazione in senso statistico usando la distribuzione di probabilità $p(q,r,s,t)$. Ma in ogni caso $|q+r|$ vale 0 oppure 2, e di conseguenza $|q-r| = 2$ oppure 0. Quindi $qs+rs+rt-qt = (q+r)s-(q-r)t \leq 2$ dato che $|s| = |t| = 1$ e pertanto abbiamo la **disuguaglianza di Bell**

$$\mathcal{B} \leq 2.$$

Valutiamo adesso $\mathcal{B}$ nel contesto della meccanica quantistica scegliendo ad esempio $Q = \sigma_A^z$, $R = \sigma_A^x$, $S = -\frac{1}{\sqrt{2}}(\sigma_B^x + \sigma_B^z)$ e $T = \frac{1}{\sqrt{2}}(\sigma_B^z - \sigma_B^x)$. Si noti il fattore $1/\sqrt{2}$ nelle quantità misurate da B, in modo tale che gli autovalori siano ± 1 come richiesto sopra. Inoltre, ammettiamo che in ognuna delle molte prove dell'esperimento lo stato su cui valutare le medie sia sempre quello di singoletto come nell'eq. (4) per due spin 1/2 in A e B. Sfruttando la regola in appendice per rappresentare i prodotti tensori in forma matriciale sulla base computazionale abbiamo

$$QS \to \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}, \quad RS \to \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 0 & -1 & -1 \\ 0 & 0 & -1 & 1 \\ -1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \end{pmatrix}$$

$$QT \to \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad RT \to \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & -1 \\ 1 & -1 & 0 & 0 \\ -1 & -1 & 0 & 0 \end{pmatrix} \quad (5)$$

Lo stato di singoletto ha coefficienti $\pm 1/\sqrt{2}$ solo sul secondo e terzo elemento della base computazionale. Da cui

$$\langle QS \rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(\langle 01|QS|01\rangle + \langle 10|QS|10\rangle) = \frac{1}{\sqrt{2}}$$

$$\langle RS\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(-\langle 01|RS|10\rangle - \langle 10|RS|01\rangle) = \frac{1}{\sqrt{2}}$$
$$\langle QT\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(\langle 01|QT|01\rangle + \langle 10|QT|10\rangle) = -\frac{1}{\sqrt{2}}$$
$$\langle RT\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(-\langle 01|RT|10\rangle - \langle 10|RT|01\rangle) = \frac{1}{\sqrt{2}}$$

Ma allora $\mathcal{B} = 4/\sqrt{2} = 2\sqrt{2}$ e, **secondo la previsione della meccanica quantistica, la disuguaglianza di Bell è violata**.

A questo punto possiamo vedere in un esperimento finalizzato a misurare $\mathcal{B}$ se i risultati sono consistenti con la derivazione della disuguaglianza che non fa uso della meccanica quantistica ($\mathcal{B} < 2$) o meno. Negli ultimi decenni vari esperimenti effettuati tipicamente con implementazioni ottiche di qubit hanno sistematicamente mostrato che la disuguaglianza di Bell è violata (fino a trenta deviazioni standard! Vedi [3] e referenze ivi citate per un aggiornamento recente.) Da un punto di vista filosofico e a livello di fondamenti della teoria quantistica rimangono aperte alcune controversie, ma la visione più comunemente accettata è che la violazione della disuguaglianza di Bell implica che la nostra visione della Natura non soddisfa uno dei due criteri con cui si deriva la disuguaglianza: o non vale il realismo (le quantità fisiche non hanno valori definiti indipendentemente dall'osservazione) oppure la teoria non è locale. Come detto sopra, la seconda ipotesi è quella che si preferisce (specialmente nell'informazione quantistica per via dell'entanglement), fatto salvo il nesso di causa-effetto che è rispettato dalla necessità di concludere in definitiva ogni osservazione con uno o più comunicazioni su canali classici.

Ritorniamo per un momento sulla scelta fatta per le quantità Q, R, S e T per osservare che, costruita una certa osservabile di Bell $\mathcal{B}$ a partire da tali quantità, la violazione della disuguaglianza è anche legata alla forma dello stato relativo delle due particelle. Introduciamo ad esempio, anche per convenienza futura, la cosiddetta **base di Bell a due qubit**

$$|\Psi^-\rangle = \frac{|0\rangle|1\rangle - |1\rangle|0\rangle}{\sqrt{2}}\ , \quad |\Psi^+\rangle = \frac{|0\rangle|1\rangle + |1\rangle|0\rangle}{\sqrt{2}}$$
$$|\Phi^-\rangle = \frac{|0\rangle|0\rangle - |1\rangle|1\rangle}{\sqrt{2}}\ , \quad |\Phi^+\rangle = \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} \tag{6}$$

dove lo stato $|\Psi^-\rangle$ è il singoletto già introdotto nella eq. (4) mentre lo stato $|\Psi^+\rangle$ invece non è altro che la combinazione simmetrica a $S = 1$, $S^z_{tot} = 0$ nella somma di due spin 1/2. Gli stati $|\Phi^\pm\rangle$ invece sono combinazioni simmetrica ed antisimmetrica dei due stati a $S = 1$, $S^z_{tot} = \pm 1$ ma ciascuno di essi non ha autovalore definito di S^z_{tot}. Sono stati scelti in questo modo perché, come vedremo quantitativamente più avanti, sono tutti e quattro stati massimamente entangled. Ciononostante non è detto che violino tutti la disuguaglianza di Bell costruita con le quantità in eq. (5). Ad esempio, prendendo i valori medi su $|\Phi^-\rangle$ anziché $|\Psi^-\rangle$ troviamo

$$\langle QS\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(\langle 00|QS|00\rangle + \langle 11|QS|11\rangle) = -\frac{1}{\sqrt{2}}$$

$$\langle RS\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(-\langle 00|RS|11\rangle - \langle 11|RS|00\rangle) = \frac{1}{\sqrt{2}}$$
$$\langle QT\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(\langle 00|QT|00\rangle + \langle 11|QT|11\rangle) = \frac{1}{\sqrt{2}}$$
$$\langle RT\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(-\langle 00|RT|11\rangle - \langle 11|QS|00\rangle) = \frac{1}{\sqrt{2}}$$

e quindi $\mathcal{B} = 0$. Quindi quella particolare disuguaglianza di Bell non risulta violata. Vedremo dopo che, dato un qualunque stato entangled a due qubit, esiste sempre almeno una scelta di Q, R, S e T tale che costruendo $\mathcal{B}$ si arriva ad una violazione della disuguaglianza di Bell per quel particolare stato. L'entità della violazione dipenderà da quanto è entangled lo stato. Ci chiediamo ora quale è la violazione massima che ci possiamo aspettare, scrivendo le quattro osservabili ad un qubit nella forma generale

$$Q = \hat{a}\cdot\vec{\sigma}_A\ ,\quad R = \hat{a}'\cdot\vec{\sigma}_A\ ,\quad S = \hat{b}\cdot\vec{\sigma}_B\ ,\quad T = \hat{b}'\cdot\vec{\sigma}_B \tag{7}$$

dove $\hat{a}$, $\hat{a}'$, $\hat{b}$ e $\hat{b}'$ sono quattro versori. Usando le proprietà (29) si ha $Q^2 = R^2 = S^2 = T^2 = \mathbb{I}$ e ciascuna delle quattro matrici ha autovalori ± 1. Inoltre due si riferiscono ad A e due a B pertanto

$$[Q,S] = [Q,T] = [R,S] = [R,T] = 0$$

e sviluppando i prodotti

$$(QS + RS + RT - QT)^2 = 4\mathbb{I} + [Q,R][S,T].$$

Sia ora $\hat{\mathcal{B}} = QS+RS+RT-QT$ tale che $\mathcal{B} = \langle\hat{\mathcal{B}}\rangle$. Usiamo la norma operatoriale data dall'estremo superiore

$$\|M\| \equiv \sup_{|\Psi\rangle}\frac{\|M|\Psi\rangle\|}{\||\Psi\rangle\|}$$

che soddisfa la disuguaglianza triangolare $\|M+N\| \le \|M\| + \|N\|$ ed anche $\|MN\| \le \|M\|\|N\|$. Abbiamo

$$\|\hat{\mathcal{B}}^2\| \le 4 + \|[Q,R]\|\|[S,T]\| \le 8$$

poichè $\|\mathbb{I}\| = 1$ e $\|[M,N]\| \le 2\|M\|\|N\|$ e le quantità dell'eq. (7) sono tali che $\|Q\| = \|R\| = \|S\| = \|T\| = 1$. Infatti quantizzando lo spin lungo il corrispondente versore si hanno autovalori ± 1 e, ad esempio, $\|Q|\Psi\rangle\|^2 = \langle\Psi|\Psi\rangle\ \forall|\Psi\rangle$. Osserviamo poi che per un operatore hermitiano $M^\dagger = M$ si ha $\langle(M-\langle M\rangle)^2\rangle = \langle M^2\rangle - \langle M\rangle^2 \ge 0$ da cui

$$\langle M\rangle \le \sqrt{\langle M^2\rangle} = \sqrt{\langle M\Psi|M\Psi\rangle} = \|M|\Psi\rangle\| \le \|M\|$$

per stati normalizzati. Ma allora ponendo $M = \hat{\mathcal{B}}^2$ troviamo il cosiddetto **limite superiore di Cirel'son**

$$\langle\hat{\mathcal{B}}\rangle \le \sqrt{\langle\hat{\mathcal{B}}^2\rangle} \le \sqrt{\|\hat{\mathcal{B}}^2\|} = 2\sqrt{2}.$$

e scopriamo che il limite $2\sqrt{2}$ ottenuto nell'esempio precedente costituisce in generale la massima violazione possibile della disuguaglianza di Bell per due qubit.

2.3 Matrici densità ridotte

Il concetto di matrice densità è di grande utilità nello studio di sistemi quantistici aperti in contatto con un ambiente esterno. Facendo ancora riferimento alla fig. 4 supponiamo di avere per il momento un sistema chiuso C che si trova complessivamente nello stato $|\Psi\rangle_C$ e di essere però interessati solo a quanto accade nel sottosistema A. In altri termini ci interessano le osservabili della forma $O_A \otimes \mathbb{I}_B$. Introduciamo innanzi tutto una base dello spazio di Hilbert del sistema C, costituita ad esempio da tutti i possibili prodotti $|i\rangle_A|j\rangle_B$ dove $|i\rangle_A$ e $|j\rangle_B$ indicano , rispettivamente, gli elementi di una base per A e per B. Scrivendo $|\Psi\rangle_C = \sum_{ij} c_{ij}|i\rangle_A|j\rangle_B$ abbiamo

$$\langle O_A\rangle \equiv {}_C\langle\Psi|O_A\otimes\mathbb{I}_B|\Psi\rangle_C = \sum_{i,i'}\left(\sum_j c^*_{i'j}c_{ij}\right){}_A\langle i'|O_A|i\rangle_A.$$

Ora se interpretiamo l'espressione dentro parentesi tonda come l'elemento di una matrice ρ_A

$${}_A\langle i|\rho_A|i'\rangle_A \equiv \sum_j c^*_{i'j}c_{ij} \tag{8}$$

possiamo riscrivere

$$\langle O_A\rangle = \sum_i {}_A\langle i|\rho_A\left(\sum_{i'}|i'\rangle_{AA}\langle i'|\right)O_A|i\rangle_A = \mathrm{tr}_A\rho_A O_A. \tag{9}$$

Quindi, per calcolare il valore di aspettazione di un qualunque operatore O_A relativo al solo sottosistema A, non abbiamo bisogno di conoscere tutti i coefficienti c_{ij}, ossia tutto lo stato, ma ci basta conoscere la matrice (o l'operatore) ρ_A, che viene detta **matrice densità ridotta al sottosistema A**. Una volta nota ρ_A i valori di aspettazione si ottengono mettendo sotto traccia gli operatori moltiplicati per l'operatore densità stesso. Questa formulazione è così generale che il concetto di matrice densità estende di fatto la nozione di stato di un sistema quantistico: quando non possiamo ritenere che il sistema A sia completamente isolato da un ambiente circostante in generale dovremo ammettere che il suo stato è descritto da una matrice densità.

Per chiarire meglio questa estensione, vediamo le tre principali proprietà di una matrice densità:

- $\rho_A = \rho_A^\dagger$. Infatti dall'espressione degli elementi di matrice su una base generica (8) ${}_A\langle i'|\rho_A|i\rangle^*_A = \sum_j c_{ij}c^*_{i'j} = {}_A\langle i|\rho_A|i'\rangle_A$.
- $\mathrm{tr}_A\rho_A = 1$. Infatti $\sum_i {}_A\langle i|\rho_A|i\rangle_A = \sum_{ij}|c_{ij}|^2 = 1$ se lo stato $|\Psi\rangle_C$ è normalizzato.

- ρ_A è semidefinita positiva, ossia per ogni vettore $|\psi\rangle_A \in \mathcal{H}_A$ si deve avere ${}_A\langle\psi|\rho_A|\psi\rangle_A \geq 0$. Usando ancora l'espressione per componenti

$${}_A\langle\psi|\rho_A|\psi\rangle_A = \sum_{ii'} \psi_i^* \psi_{i'\,A}\langle i|\rho_A|i'\rangle_A = \sum_j \left(\sum_i \psi_i^* c_{ij}\right)\left(\sum_{i'} \psi_{i'} c_{i'j}^*\right) = \sum_j |z_j|^2 \geq 0$$

avendo posto $z_j = \sum_i \psi_i c_{ij}^*$ (si noti infatti che l'indice di somma i è muto).

Dalla prima proprietà vediamo che ρ_A è diagonalizzabile con autovalori p_i reali

$$\rho_A = \sum_i p_i |i\rangle_{AA}\langle i|.$$

Dalla terza proprietà vediamo che $p_i \geq 0\ \forall i$ e dalla seconda proprietà abbiamo infine $\sum_i p_i = 1$. La collezione di numeri p_i si può interpretare a tutti gli effetti come una distribuzione di probabilità classica normalizzata. Quale è il suo significato operativo? Ricordando che

$$\langle O_A\rangle = \mathrm{tr}\rho_A O_A = \sum_i p_{i\ A}\langle i|O_A|i\rangle_A$$

è come se avessimo diversi stati quantistici $|i\rangle_A$ per il sistema A ciascuno dei quali pesato da un fattore p_i. In questo senso la matrice densità contiene informazioni su come vengono visti i vari stati stati del sistema A dall'ambiente. Ad esempio si può interpretare la relazione di sopra pensando al valore di aspettazione come risultato della media su molti esperimenti ripetuti nei quali, però, lo stato del sistema inizialmente non è preparato sempre in modo identico ma, in una frazione p_1 dei casi è inizializzato a $|1\rangle_A$, in una frazione p_2 a $|2\rangle_A$ ecc. Si dice che il sistema A si trova in questo caso in uno **stato misto** (o mistura) ρ_A. Per contro, quando uno solo dei pesi è diverso da zero (e quindi pari a 1), ritroviamo la situazione usuale di uno **stato puro** $\rho_A = |\psi\rangle_{AA}\langle\psi|$ in cui lo stato del sistema è descritto a tutti gli effetti da un vettore $|\psi\rangle_A$ nello spazio di Hilbert (corrispondente a $|i\rangle_A = |1\rangle_A$ con $p_1 = 1$). La formulazione della meccanica quantistica in termini di operatori densità può essere fatta in modo più rigoroso ed assiomatico rispetto a quanto brevemente esposto qua (per maggiori dettagli si veda ad esempio 4.1.2 in [22]). Prima di proseguire con l'uso della nozione di matrice densità nel contesto della teoria dell'informazione quantistica osserviamo però che tale nozione in qualche modo viene già invocata quando si tratta la termodinamica di un sistema quantistico: se sappiamo che fisicamente il sistema si trova in equilibrio termico con un bagno esterno a temperatura T, possiamo affermare che il suo stato è descritto da una funzione d'onda nello spazio di Hilbert? La risposta è negativa. In effetti la meccanica statistica prevede che in senso termodinamico, e cioè come visto da un osservatore esterno che ha accesso solo a quantità macroscopiche quali ad esempio numero di particelle N e volume V,[2] lo stato del sistema sia descritto da una matrice densità termica $\rho_{\text{canonica}} = Z^{-1}\exp(-H/K_B T)$ dove H è l'operatore hamiltoniano del sistema

[2] Fissando T , N e V stiamo considerando il cosiddetto *ensemble* canonico.

in esame, K_B è la costante di Boltzmann e $Z = \mathrm{tr}\exp(-H/K_BT)$ è un fattore di normalizzazione (la funzione di partizione) tale che $\mathrm{tr}\rho_{\mathrm{canonica}} = 1$. Ne risulta che la probabilità che il sistema si trovi ad energia E è data dal peso di Boltzmann $p_E = Z^{-1} g_E \exp(-E/K_BT)$ dove g_E è di fatto la degenerazione del livello di energia E nello spettro di H e dipenderà, tra le altre cose, dalla natura fermionica o bosonica delle particelle che compongono il sistema.

2.4 Decomposizione di Schmidt

Uno stato puro $|\Psi\rangle_C$ può essere scritto in una forma standard che presenta una certa utilità: la decomposizione di Schmidt. Un vettore arbitrario in $\mathcal{H}_A \otimes \mathcal{H}_B$ si può sviluppare nella base prodotto degli stati ortonormali $\{|i\rangle_A\}$ e $\{|j\rangle_B\}$:

$$|\Psi\rangle_C = \sum_{i,j} c_{ij} |i\rangle_A |j\rangle_B \equiv \sum_i |i\rangle_A \left|\tilde{i}\right\rangle_B$$

dove abbiamo definito gli stati $\left|\tilde{i}\right\rangle_B \equiv \sum_j c_{ij} |j\rangle_B$, i quali non sono necessariamente ortonormali.

Ora, supponiamo che la base $\{|i\rangle_A\}$ sia proprio quella che diagonalizza la matrice densità ridotta su A,

$$\rho_A = \sum_i p_i |i\rangle_A \langle i|_A . \tag{10}$$

La matrice ρ_A si calcola esplicitamente eseguendo la traccia parziale su B

$$\begin{aligned} \rho_A &= \mathrm{tr}_B \left(|\Psi\rangle_C \langle\Psi|_C\right) = \mathrm{tr}_B \left(\sum_{i,j} |i\rangle_A \langle j|_A \otimes \left|\tilde{i}\right\rangle_B \left\langle\tilde{j}\right|_B \right) \\ &= \sum_{i,j} |i\rangle_A \langle j|_A \,\mathrm{tr}_B \left(\left|\tilde{i}\right\rangle_B \left\langle\tilde{j}\right|_B\right) = \sum_{i,j} |i\rangle_A \langle j|_A \sum_k \left(\langle k|\tilde{i}\rangle \left\langle\tilde{j}|k\right\rangle\right)_B \\ &= \sum_{i,j} |i\rangle_A \langle j|_A \sum_k \left(\left\langle\tilde{j}|k\right\rangle \langle k|\tilde{i}\rangle\right)_B = \sum_{i,j} |i\rangle_A \langle j|_A \left\langle\tilde{j}|\tilde{i}\right\rangle_B . \end{aligned} \tag{11}$$

Confrontando le eq.(10) e (11) si ottiene

$$\left\langle\tilde{j}|\tilde{i}\right\rangle_B = p_i \delta_{ij}$$

che ci dice che la base $\left\{\left|\tilde{i}\right\rangle_B\right\}$ è ortogonale. Possiamo ortonormalizzare attraverso il riscalamento $|i'\rangle_B = p_i^{-1/2} \left|\tilde{i}\right\rangle_B$, eseguito solo per gli elementi diagonali i per i quali $p_i \neq 0$. In tal modo, si ottiene la **decomposizione di Schimdt** di $|\Psi\rangle_C$

$$|\Psi\rangle_C = \sum_i \sqrt{p_i} |i\rangle_A |i'\rangle_B . \tag{12}$$

Ogni stato puro si può esprimere in questa forma, ma la base utilizzata dipende dallo stato in questione.

E' interessante notare che la matrice densità ridotta del sistema B,

$$\rho_B = \mathrm{tr}_A \left(|\Psi\rangle_C \langle\Psi|_C \right) = \sum_i p_i \, |i'\rangle_B \langle i'|_B$$

possiede gli stessi autovalori non nulli, anche se le dimensioni di $\mathcal{H}_A$ e $\mathcal{H}_B$ sono diverse; in tal caso, sarà diverso il numero di autovalori nulli.

Ad ogni stato puro si associa un **numero di Schmidt**, che è il **numero di autovalori non nulli di** ρ_A, ovvero il numero di termini dello stato bipartito $|\Psi\rangle_C$ nella decomposizione di Schmidt. Se il numero di Schmidt è 1, allora lo stato è separabile in quanto $|\Psi\rangle_C$ si decompone in un solo termine. Se invece è maggiore di uno, allora si dice che lo stato è entangled proprio perché non è possibile nessuna ulteriore riduzione in forma di somma di prodotti. Nel caso di $|\Psi\rangle_C$ separabile, ρ_A e ρ_B descrivono stati puri, ossia caratterizzati da ordinari vettori nello spazio di Hilbert, $|\psi\rangle_A$ e $|\psi'\rangle_B$ rispettivamente (dove abbiamo indicato con ψ e ψ' i due stati corrispondenti a i e i' con $p_i = 1$). Nel caso di $|\Psi\rangle_C$ entangled, ρ_A e ρ_B sono stati misti.

Se gli autovalori non nulli sono tutti diversi fra loro, l'informazione fornita da ρ_A e ρ_B è sufficiente a fissare la decomposizione di Schmidt. Diversamente, in caso di degenerazione, vi è ambiguità nella scelta della base (gli autovalori sono comunque fissati univocamente). Un esempio tipico è dato dallo stato di singoletto di due spin 1/2; tale stato si trova già nella forma di Schmidt con coefficienti $1/\sqrt{2}$ e $-1/\sqrt{2}$. Tuttavia il singoletto assume la stessa forma in qualsiasi base ruotata $|0_n\rangle$, $|1_n\rangle$, con asse di quantizzazione $\hat{n}$, a patto di ruotare simultaneamente su A e su B. Corrispondentemente alle infinite scelte di $\hat{n}$ avremo infinite decomposizioni di Schmidt possibili.

2.4.1 Violazione della disuguaglianza di Bell versus entanglement

La decomposizione di Schmidt (12) per un generico stato di due qubit entangled secondo la partizione A/B prende la forma

$$|\Psi\rangle_C = \sqrt{p}|0\rangle_A|0'\rangle_B + \sqrt{1-p}|1\rangle_A|1'\rangle_B$$

dato che al massimo esistono due autovalori p e $(1-p)$ non nulli della matrice densità (che è appunto 2×2). Nell'espressione di sopra abbiamo indicato con $|0\rangle_A, |1\rangle_A$ e $|0'\rangle_B, |1'\rangle_B$ le due basi ortonormali di Schmidt $|i\rangle_A$ e $|i'\rangle_B$. Questa forma ci è utile per capire se e quanto è violata una disuguaglianza di Bell su stati che non sono necessariamente massimamente entangled come il singoletto. Per il momento ci basta osservare che il contenuto di entanglement è misurato in qualche modo dal determinante della matrice densità ridotta $\Delta = p(1-p)$. Per stati separabili $p = 0$ o 1 e $\Delta = 0$ mentre il massimo $\Delta = 1/4$ si ha per $p = 1 - p = 1/2$ come nel caso degli stati di Bell. Riprendiamo la espressione generica (7) per le osservabili Q, R, S e T dove le matrici di Pauli sono ora da intendersi scritte rispetto alle basi $|0\rangle_A, |1\rangle_A$ e $|0'\rangle_B, |1'\rangle_B$. Abbiamo così

$${}_C\langle\Psi|\hat{\mathcal{B}}|\Psi\rangle_C = p\,{}_A\langle 0|Q|0\rangle_A\,{}_B\langle 0'|S|0'\rangle_B + (1-p)\,{}_A\langle 1|Q|1\rangle_A\,{}_B\langle 1'|S|1'\rangle_B + \sqrt{\Delta}({}_A\langle 0|Q|1\rangle_A\,{}_B\langle 0'|S|1'\rangle_B +$$

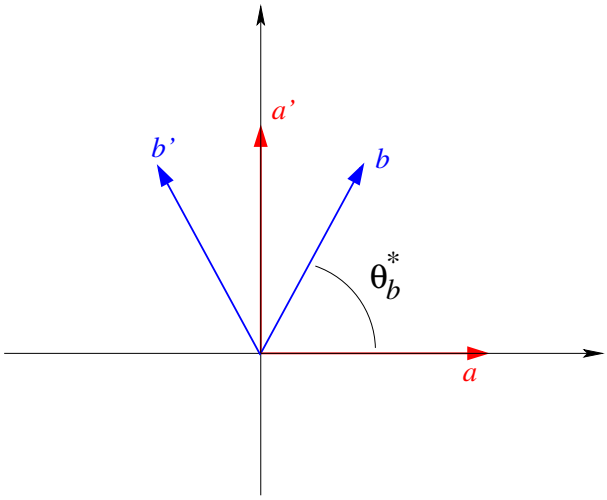

Figura 5: Scelta dei versori $\hat{a}$, $\hat{a}'$, $\hat{b}$ e $\hat{b}'$ che definiscono le osservabili Q, R, S e T nella costruzione della disuguaglianza di Bell, secondo la eq. (7). I quattro versori giaciono sullo stesso piano e θ_b^* viene fissato in modo ottimale secondo $\tan\theta_b^* = 2\sqrt{\Delta}$ a seconda di quanto è entangled lo stato che condividono A e B. Se $\Delta = 0$ non c'è violazione della disuguaglianza. *Choice of unit vectors $\hat{a}$, $\hat{a}'$, $\hat{b}$ and $\hat{b}'$ that define the observables Q, R, S and T in the construction of Bell inequality, according to eq. (7). The four unit vectors lie on the same plane and θ_b^* is fixed at the optimal value such that $\tan\theta_b^* = 2\sqrt{\Delta}$, depending on Δ, that is, on how much is entangled the state shared by A and B. If $\Delta = 0$ no violation of the inequality occurs.*

$$\langle 1|Q|0\rangle_{AB}\langle 1'|S|0'\rangle_B) + (Q \to R) + (Q \to R, S \to T) - (S \to T)$$

dove gli ultimi tre termini sono ottenuti da quelli per gli elementi di matrice di Q e S operando le sostituzioni indicate. Se (θ_a, φ_a) sono gli angoli che definiscono $\hat{a}$ e così $(\theta_{a'}, \varphi_{a'})$ per $\hat{a}'$, (θ_b, φ_b) per $\hat{b}$ e $(\theta_{b'}, \varphi_{b'})$ per $\hat{b}'$ troviamo

$$\mathcal{B} = \cos\theta_a\cos\theta_b + 2\sqrt{\Delta}\sin\theta_a\sin\theta_b\cos(\varphi_a+\varphi_b) + (a \to a') + (a \to a', b \to b') - (b \to b').$$

Per l'argomento che stiamo sviluppando qua non è restrittivo prendere $\varphi_{a,a',b,b'} = 0$, ossia i quattro versori sullo stesso piano, ed anche $\theta_a = 0$ e $\theta_{a'} = \pi/2$. Infine poniamo $\theta_{b'} = \pi - \theta_b$ come in fig. 5. In tal modo

$$\mathcal{B} = \cos\theta_b + 2\sqrt{\Delta}\sin\theta_b + 2\sqrt{\Delta}\sin(\pi-\theta_b) - \cos(\pi-\theta_b) = 2(\cos\theta_b + 2\sqrt{\Delta}\sin\theta_b).$$

Finora abbiamo scelto l'orientazione di tre versori e rimane la facoltà di regolare θ_b. Cerchiamo il massimo di questa espressione derivando rispetto a θ_b

$$\frac{\partial\mathcal{B}}{\partial\theta_b} = 2(-\sin\theta_b + 2\sqrt{\Delta}\cos\theta_b) = 0 \Rightarrow \tan\theta_b^* = 2\sqrt{\Delta}$$

e, restringendosi a $0 \leq \theta_b \leq \pi/2$, abbiamo $\cos\theta_b^* = 1/\sqrt{1+\tan^2\theta_b} = 1/\sqrt{1+4\Delta}$ e $\sin\theta_b^* = \tan\theta_b/\sqrt{1+\tan^2\theta_b} = 2\sqrt{\Delta}/\sqrt{1+4\Delta}$, da cui

$$\mathcal{B}(\theta_b^*) = 2\left(\frac{1}{\sqrt{1+4\Delta}} + 2\sqrt{\Delta}\frac{2\sqrt{\Delta}}{\sqrt{1+4\Delta}}\right) = 2\sqrt{1+4\Delta} \geq 2$$

$$\frac{\partial^2\mathcal{B}}{\partial\theta_b^2}|_{\theta_b^*} = -\mathcal{B}(\theta_b^*) \leq 0.$$

Quindi, dato un qualunque stato entangled con $\Delta > 0$ possiamo sempre trovare una scelta opportuna delle quantità Q, R, S e T che formano l'osservabile di Bell tale che $\mathcal{B}_{max} > 2$ e quindi quella particolare disuguaglianza di Bell è violata. L'entità della violazione è $2(\sqrt{1+4\Delta}-1)$ e, come abbiamo già visto, è massima per $\Delta = 1/4$ per cui $\mathcal{B}_{max} = 2\sqrt{2}$; il limite superiore di Cirel'son è saturato dagli stati massimamente entangled.

Bell inquality violation versus entanglement

Schmidt decomposition (12) for a generic two-qubits entangled state according to the A/B partition takes the form

$$|\Psi\rangle_C = \sqrt{p}|0\rangle_A|0'\rangle_B + \sqrt{1-p}|1\rangle_A|1'\rangle_B$$

because there are at most two nonvanishing eigenvalues of the (2×2) density matrix, p and $(1-p)$. In the expression above we have indicated with $|0\rangle_A, |1\rangle_A$ and $|0'\rangle_B, |1'\rangle_B$ the two orthonormal Schmidt bases $|i\rangle_A$ e $|i'\rangle_B$. This form is useful to understand if and how much is violated a Bell inequality using states that are not necessarily maximally entangled as the singlet one. For the moment it will suffice to notice that the entanglement content is measured in some way by the determinant of the reduced density matrix $\Delta = p(1-p)$. For separable states $p = 0$ or 1 and $\Delta = 0$ while the maximum $\Delta = 1/4$ is obtained when $p = 1-p = 1/2$ like in the case of Bell states. Now, let us recall the generic expression (7) for observables Q, R, S e T where now Pauli matrices are expressed in the bases $|0\rangle_A, |1\rangle_A$ and $|0'\rangle_B, |1'\rangle_B$. Hence we have

$${}_C\langle\Psi|\hat{\mathcal{B}}|\Psi\rangle_C = p\,{}_A\langle 0|Q|0\rangle_A\,{}_B\langle 0'|S|0'\rangle_B + (1-p)\,{}_A\langle 1|Q|1\rangle_A\,{}_B\langle 1'|S|1'\rangle_B + \sqrt{\Delta}({}_A\langle 0|Q|1\rangle_A\,{}_B\langle 0'|S|1'\rangle_B +$$

$$\langle 1|Q|0\rangle_A\,{}_B\langle 1'|S|0'\rangle_B) + (Q\to R) + (Q\to R, S\to T) - (S\to T)$$

where the last three terms are obtained from those of matrix elements of Q and S by operating the substitutions indicated by the arrows. Now, if (θ_a, φ_a) are the angles that define $\hat{a}$ and similarly for $(\theta_{a'}, \varphi_{a'})$ for $\hat{a}'$, (θ_b, φ_b) for $\hat{b}$ and $(\theta_{b'}, \varphi_{b'})$ for $\hat{b}'$ we find

$$\mathcal{B} = \cos\theta_a\cos\theta_b + 2\sqrt{\Delta}\sin\theta_a\sin\theta_b\cos(\varphi_a+\varphi_b) + (a\to a') + (a\to a', b\to b') - (b\to b').$$

In the treatment proposed here it is not restrictive to choose $\varphi_{a,a',b,b'} = 0$, that is four unit vectors on the same plane, and also $\theta_a = 0$ and $\theta_{a'} = \pi/2$. Finally we fix $\theta_{b'} = \pi - \theta_b$ as in fig. 5. In such a way

$$\mathcal{B} = \cos\theta_b + 2\sqrt{\Delta}\sin\theta_b + 2\sqrt{\Delta}\sin(\pi-\theta_b) - \cos(\pi-\theta_b) = 2(\cos\theta_b + 2\sqrt{\Delta}\sin\theta_b).$$

Up to now we have fixed the orientation of three unit vectors and there remain the freedom of tuning θ_b. Let us find the maximum of the expression above by differentiating with respect to θ_b

$$\frac{\partial\mathcal{B}}{\partial\theta_b} = 2(-\sin\theta_b + 2\sqrt{\Delta}\cos\theta_b) = 0 \Rightarrow \tan\theta_b^* = 2\sqrt{\Delta}$$

and, by restricting to $0 \leq \theta_b \leq \pi/2$, we have $\cos\theta_b^* = 1/\sqrt{1+\tan^2\theta_b} = 1/\sqrt{1+4\Delta}$ and $\sin\theta_b^* = \tan\theta_b/\sqrt{1+\tan^2\theta_b} = 2\sqrt{\Delta}/\sqrt{1+4\Delta}$, yielding

$$\mathcal{B}(\theta_b^*) = 2\left(\frac{1}{\sqrt{1+4\Delta}} + 2\sqrt{\Delta}\frac{2\sqrt{\Delta}}{\sqrt{1+4\Delta}}\right) = 2\sqrt{1+4\Delta} \geq 2$$

$$\frac{\partial^2\mathcal{B}}{\partial\theta_b^2}|_{\theta_b^*} = -\mathcal{B}(\theta_b^*) \leq 0.$$

Hence, given any entangled state with $\Delta > 0$ one can always find a suitable choice of the quantities Q, R, S and T that form Bell's observable such that $\mathcal{B}_{max} > 2$ and that particular Bell inequality is violated. The amount of violation is $2(\sqrt{1+4\Delta}-1)$ and, as already seen, is maximal when $\Delta = 1/4$ giving $\mathcal{B}_{max} = 2\sqrt{2}$; Cirel'son upper bound is saturated by maximally entangled states.

2.5 Sfera di Bloch per un qubit

Dato uno stato misto di un qubit ρ possiamo, in quanto matrice hermitiana 2×2 espanderla su una base di matrici costituita da $\mathbb{I}$, σ^x, σ^y, σ^z. Dalle eq. (29) si può vedere infatti che costituiscono una base ortonormale rispetto al prodotto scalare tra matrici indotto dalla traccia. Poniamo quindi $\rho = c_0\mathbb{I} + \vec{c}\cdot\vec{\sigma}$. Dalla proprietà $\mathrm{tr}\rho = 1$ abbiamo $2c_0 = 1$ e

$$\rho = \begin{pmatrix} 1/2 + c^z & c^x - ic^y \\ c^x + ic^y & 1/2 - c^z \end{pmatrix}.$$

Affinché $\rho = \rho^\dagger$ si deve avere $\vec{c}$ a componenti reali. Se λ e $1-\lambda$ sono gli autovalori reali di ρ si vede che $\Delta \equiv \det\rho = \lambda(1-\lambda)$ come funzione di $0 \leq \lambda \leq 1$ è tale che $0 \leq \Delta \leq 1/4$; in particolare $\Delta = 0$ per $\lambda = 0$ o 1 nel qual caso ρ è uno stato puro ed invece $\Delta = 1/4$ quando $\lambda = 1/2$ e $\rho = 1/2\mathbb{I}$ è massimamente entangled. Quindi dalla relazione $\Delta = 1/4 - \|\vec{c}\|^2 \geq 0$ scopriamo che $\|\vec{c}\| \leq 1/2$. Scrivendo $\vec{c} = 1/2\vec{n}$ abbiamo infine

$$\rho = \frac{\mathbb{I} + \vec{n}\cdot\vec{\sigma}}{2} \tag{13}$$

dove $\vec{n}$ è un vettore che appartiene alla palla tridimensionale di raggio unitario, detta **sfera di Bloch**. Quando il vettore si trova sulla superficie sferica $\|\vec{n}\| = 1$ allora $\Delta = 0$ e lo stato è puro e corrisponde all'autovettore di $\vec{n}\cdot\vec{\sigma}$ con autovalore $+1$

$$\rho = |\psi\rangle_A \, {}_A\langle\psi| \ , \quad |\psi\rangle_A = \cos\frac{\theta}{2}|0\rangle - e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{14}$$

dove θ e φ sono gli angoli che definiscono il versore $\vec{n} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$. Se invece $\vec{n}$ è interno alla sfera ($\|\vec{n}\| < 1$) allora lo stato ρ è misto.

2.5.1 Convessità dello spazio delle matrici densità per qudit generici: analogie e differenze con la sfera di Bloch

Essendo un operatorie hermitiano, semidefinito positivo e a traccia unitaria le matrici densità si possono sempre scrivere come[3]

$$\rho = \sum_j p_j |j\rangle\langle j|$$

dove p_j indicano gli autovalori tali che $\sum_j p_j = 1$ (includendo le possibili degenerazioni d_j) e $|j\rangle$ gli autostati associati. Da un punto di vista matematico gli operatori $\sum_{a=1,\ldots,d_j} |j_a\rangle\langle j_a|$ sono proiettori ortogonali sui sottospazi d_j-dimensionali relativi agli autovalori p_j e la combinazione lineare con coefficienti reali non negativi e a somma 1 si dice **convessa**. Lo stesso spazio delle matrici densità presenta una struttura convessa nel senso che, date due matrici densità ρ_1 e ρ_2 una loro combinazione lineare convessa $\rho_\lambda = \lambda\rho_1 + (1-\lambda)\rho_2$ con $0 \leq \lambda \leq 1$ ha ancora le proprietà di una matrice densità. Infatti $\rho_\lambda^\dagger = \lambda^*\rho_1^\dagger + (1-\lambda^*)\rho_2^\dagger = \rho_\lambda$, $\mathrm{tr}\rho_\lambda = \lambda\mathrm{tr}\rho_1 + (1-\lambda)\mathrm{tr}\rho_2 = 1$ e la semi-positività si vede prendendo il valore di aspettazione su un stato generico $|\psi\rangle$

$$\langle\psi|\rho_\lambda|\psi\rangle = \lambda\langle\psi|\rho_1|\psi\rangle + (1-\lambda)\langle\psi|\rho_2|\psi\rangle \geq 0$$

in quanto $\langle\psi|\rho_{1,2}|\psi\rangle \geq 0$. Dati due "punti" dell'insieme ρ_1 e ρ_2, l'insieme è convesso se contiene tutti i punti del "segmento" ρ_λ.

Questa costruzione presenta però un'ambiguità, nel senso che una data matrice densità può essere espressa come combinazione lineare convessa di stati puri $|\psi\rangle\langle\psi|$ in modi diversi. La **decomposizione convessa in generale non è unica**. Basterà un esempio, ancora con qubit: dati gli stati normalizzati $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ e $|\psi_2\rangle = \alpha|0\rangle - \beta|1\rangle$ costruiamo la matrice $\rho = \frac{1}{2}|\psi\rangle_{11}\langle\psi| + \frac{1}{2}|\psi\rangle_{22}\langle\psi|$. Espandendo i prodotti troviamo $\rho = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|$ che è un'altra legittima combinazione lineare convessa.

Fanno però eccezione gli stati puri. Infatti supponiamo per assurdo che $\rho = |\psi\rangle\langle\psi|$ possa essere scritto in forma alternativa come $\lambda\rho_1 + (1-\lambda)\rho_2$ con

[3] Implicitamente ci stiamo riferendo per semplicità a casi finito-dimensionali; per una trattazione più esaustiva e rigorosa sono necessarie alcune ipotesi aggiuntive (si veda ad es. 4.1.2 in [22]).

Implicitly we are referring for simplicity to finite-dimensional cases; for an exhaustive and rigorous treatment some additional hypotesis are necessary (see for ex. 4.1.2 in [22]).

$\lambda \neq 0, 1$. Allora il valore d'aspettazione su uno stato $|\psi_\perp\rangle$ ortogonale a $|\psi\rangle$ dà

$$\langle\psi_\perp|\rho|\psi_\perp\rangle = |\langle\psi_\perp|\psi\rangle|^2 = 0 = \lambda\langle\psi_\perp|\rho_1|\psi_\perp\rangle + (1-\lambda)\langle\psi_\perp|\rho_2|\psi_\perp\rangle$$

essendo $\lambda \geq 0$ e $1-\lambda \geq 0$ arriviamo alla condizione $\langle\psi_\perp|\rho_1|\psi_\perp\rangle = \langle\psi_\perp|\rho_2|\psi_\perp\rangle = 0$ per ogni $|\psi_\perp\rangle$ ortogonale a $|\psi\rangle$, che implica poi $\rho_1 = \rho_2 = \rho$.[4]

Quindi per un sistema quantistico con $d = \dim\mathcal{H}$ scopriamo che un generico stato è rappresentato da una matrice densità hermitiana parametrizzata da $d^2 - 1$ parametri reali (un vincolo sui d^2 parametri viene dalla condizione di traccia unitaria). La frontiera di questa varietà è definito dalla condizione di avere tutti gli autovalori non negativi. Su questa frontiera uno o più autovalori si annullano. In particolare appartengono alla frontiera gli stati puri con $d-1$ autovalori nulli, i quali si scrivono in modo unico come combinazioni convesse estremali. Il caso del qubit $d = 2$ è speciale, nel senso che l'annullarsi di almeno un autovalore caratterizza già lo stato come puro. Ma nel caso $d > 2$ alla frontiera possono appartenere anche stati entangled. Gli stati massimamente entangled a d generica sono semplicemente proporzionali all'identità con autovalori tutti uguali: $\rho = \mathbb{I}/d$.

---

[4] Possiamo costruire una base $|i\rangle$ di stati alla Gram-Schmidt iniziando proprio con $|\psi\rangle$ e completando con un insieme di stati ortogonali ad esso. In questa base gli elementi sulle diagonali $\langle i|\rho_1|i\rangle = 0$ per $|i\rangle \neq |\psi\rangle$. Se restringiamo l'operatore ρ_1 al sottospazio $\mathcal{M}_\perp$, complemento ortogonale a quello generato da $|\psi\rangle$, abbiamo un operatore hermitiano $\rho_{1\perp}$ che nella forma diagonale ha tutti autovalori nulli, ossia $\rho_{1\perp} = 0$. Quindi la matrice che rappresenta ρ_1 ha un elemento 1 in corrispondenza di $|\psi\rangle\langle\psi|$ ed una riga ed una colonna eventualmente non nulle in corrispondenza di $|\psi\rangle\langle i|$ e $|i\rangle\langle\psi|$ con $|i\rangle \neq |\psi\rangle$, $i = 2, \ldots d-1$ dove $d = \dim\mathcal{H}$: $u_i \equiv \langle i|\rho_1|\psi\rangle$. Scriviamo ora l'equazione agli autovalori λ_1 per $|v\rangle = v_1|\psi\rangle + \sum_i v_i|i\rangle$ che fornisce

$$(1-\lambda_1)v_1 + v_2u_2^* + \ldots v_du_d^* = 0\,, \quad u_iv_1 = \lambda_1 v_i.$$

Cerchiamo soluzioni non nulle per $\lambda_1 \neq 0$ che danno luogo all'equazione $\lambda_1(1-\lambda_1)+\sum_i |u_i|^2 = 0$. Ma se almeno un $u_j \neq 0$ si ha un autovalore $\lambda_1 < 0$ che contraddice l'ipotesi che ρ_1 sia una matrice densità. Le uniche possibilità che rimangono sono o $\lambda_1 = 0$, che corrisponde però a $\rho_1 = 0$, oppure $u_j = 0\ \forall j$ da cui $\rho_1 = |\psi\rangle\langle\psi|$. Stesso ragionamento per ρ_2.

We can build a basis of states $|i\rangle$ according to Gram-Schmidt procedure by starting just with $|\psi\rangle$ and completing with states orthogonal to it. In this basis the matrix elements $\langle i|\rho_1|i\rangle = 0$ for $|i\rangle \neq |\psi\rangle$. If we restrict the operator ρ_1 to the subspace $\mathcal{M}_\perp$, orthogonal complement to the space spanned by $|\psi\rangle$, we have a hermitean operator $\rho_{1\perp}$ that in diagonal form has only vanishing eigenvalues, that is $\rho_{1\perp} = 0$. Hence the matrix that represents ρ_1 has one element 1 in relation to $|\psi\rangle\langle\psi|$ and at most one nonvanishing row and column corresponding to $|\psi\rangle\langle i|$ and $|i\rangle\langle\psi|$ with $|i\rangle \neq |\psi\rangle$, $i = 2, \ldots d-1$ where $d = \dim\mathcal{H}$: $u_i \equiv \langle i|\rho_1|\psi\rangle$. Let us write the eigenvalue equation for λ_1 by inserting $|v\rangle = v_1|\psi\rangle + \sum_i v_i|i\rangle$ that yields

$$(1-\lambda_1)v_1 + v_2u_2^* + \ldots v_du_d^* = 0\,, \quad u_iv_1 = \lambda_1 v_i.$$

We look for nonvanishing solutions with $\lambda_1 \neq 0$ that result in the equation $\lambda_1(1-\lambda_1) + \sum_i |u_i|^2 = 0$. But if at least one $u_j \neq 0$ we have a negative eigenvalue $\lambda_1 < 0$ agains the hypotesis that ρ_1 is a density matrix. The only possibilities are either $\lambda_1 = 0$, corresponding to $\rho_1 = 0$, or $u_j = 0\ \forall j$ from which $\rho_1 = |\psi\rangle\langle\psi|$. Same reasoning for ρ_2.

Convexity in density matrices space for generic qudits: analogies and differences with Bloch sphere

Being a hermitean operator, positive semidefinite and with unit trace, density matrices can always be cast in the form

$$\rho = \sum_j p_j |j\rangle\langle j|$$

where p_j indicates the j-th eigenvalue, satisfying $\sum_j p_j = 1$ (including possible degeneracies d_j) and $|j\rangle$ indicate associated eigenstates. From a mathematical point of view the operators $\sum_{a=1,\ldots,d_j} |j_a\rangle\langle j_a|$ are orthogonal projectors over d_j-dimensional subspaces associated with eigenvalue p_j and the linear combination with non-negative real coefficients that sum to 1 is termed ***convex****. The density matrices space itself has a convex structure in the sense that, given two density matrices ρ_1 and ρ_2 a convex linear combination $\rho_\lambda = \lambda\rho_1 + (1-\lambda)\rho_2$ with $0 \leq \lambda \leq 1$ still has all the properties of a density matrix. In fact $\rho_\lambda^\dagger = \lambda^*\rho_1^\dagger + (1-\lambda^*)\rho_2^\dagger = \rho_\lambda$, $\mathrm{tr}\rho_\lambda = \lambda\mathrm{tr}\rho_1 + (1-\lambda)\mathrm{tr}\rho_2 = 1$ and semi-positivity is checked by taking the expectation value on a generic state $|\psi\rangle$*

$$\langle\psi|\rho_\lambda|\psi\rangle = \lambda\langle\psi|\rho_1|\psi\rangle + (1-\lambda)\langle\psi|\rho_2|\psi\rangle \geq 0$$

because $\langle\psi|\rho_{1,2}|\psi\rangle \geq 0$. Given two "points" ρ_1 and ρ_2, the set is said to be convex if it contains all the points of the "segment" ρ_λ.

This construction however contains a degree of ambiguity, in the sense that a given density matrix may be expressed as convex linear combination over pure states $|\psi\rangle\langle\psi|$ in different ways. ***Convex decomposition in general is not unique****. An example will suffice, again with qubits: given the normalised states $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\psi_2\rangle = \alpha|0\rangle - \beta|1\rangle$ let us build the matrix $\rho = \frac{1}{2}|\psi\rangle_{11}\langle\psi| + \frac{1}{2}|\psi\rangle_{22}\langle\psi|$. By expanding the products we find $\rho = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|$ that is another legitimate convex linear combination.*

Nonetheless pure states are an exception. In fact, suppose by absurd that $\rho = |\psi\rangle\langle\psi|$ can be written in alternative form as $\lambda\rho_1 + (1-\lambda)\rho_2$ with $\lambda \neq 0, 1$. Then the expectation value on a state $|\psi_\perp\rangle$ orthogonal to $|\psi\rangle$ gives

$$\langle\psi_\perp|\rho|\psi_\perp\rangle = |\langle\psi_\perp|\psi\rangle|^2 = 0 = \lambda\langle\psi_\perp|\rho_1|\psi_\perp\rangle + (1-\lambda)\langle\psi_\perp|\rho_2|\psi_\perp\rangle$$

and being $\lambda \geq 0$ and $1-\lambda \geq 0$ we arrive at the condition $\langle\psi_\perp|\rho_1|\psi_\perp\rangle = \langle\psi_\perp|\rho_2|\psi_\perp\rangle = 0$ for every $|\psi_\perp\rangle$ orthogonal to $|\psi\rangle$, that implies $\rho_1 = \rho_2 = \rho$.

Hence for a quantum system with $d = \dim\mathcal{H}$ we arrive at the conclusion that a generic state is represented by a hermitean density matrix parametrisable with $d^2 - 1$ real parameters (a constraint on the d^2 parameters comes from the condition of unit trace). The boundary of this manifold is defined by the condition of having non-negative eigenvalues. On this boundary one or more eigenvalues pass through zero. In particular we find on the boundary pure states with $d-1$ zero eigenvalues, and these are uniquely expressed as extremal convex combinations. The qubit case $d = 2$ is special, in that the vanishing of one eigenvalue

already characterises the state as pure. But in the case $d > 2$ on the boundary we can find also entangled states. Maximally entangled states with generic d are simply proportional to the identity matrix with all equal eigenvalues: $\rho = \mathbb{I}/d$.

2.6 Fedeltà di uno stato rispetto ad un altro

Come per due versori in uno spazio euclideo il prodotto scalare quantifica la sovrapposizione e la distanza

$$\mathrm{dist}(\hat{a}, \hat{b}) = \|\hat{a} - \hat{b}\| = \sqrt{2 - 2\hat{a} \cdot \hat{b}}$$

così, almeno intuitivamente, possiamo quantificare quanto due stati quantistici sono sovrapposti attraverso il modulo del prodotto scalare $F = |\langle\phi|\psi\rangle|^2$; se $|\phi\rangle = |\psi\rangle$ a meno di una fase allora $F = 1$ e se invece sono ortogonali $F = 0$. Nel contesto della teoria dell'informazione quantistica F viene detta **fedeltà** (di $|\psi\rangle$ rispetto $|\phi\rangle$, e viceversa). Va però notato che la distanza indotta dalla norma in uno spazio di Hilbert complesso $\|\psi - \phi\| = \sqrt{2 - 2\Re\langle\psi|\phi\rangle}$ non è invariante rispetto alla moltiplicazione di ψ e/o ϕ per un fattore di fase, che normalmente si considera arbitrario nella normalizzazione di uno stato.

Per stati misti poi un possibile prodotto interno scalare viene indotto dalla traccia $(A, B) = \mathrm{tr}A^\dagger B$ e così potremmo pensare di quantificare quanto ρ_1 è "fedele" rispetto a ρ_2 calcolando $F = \mathrm{tr}\rho_1\rho_2$. In letteratura tuttavia, per ragioni che esulano dallo scopo di questa introduzione, si usa la defininizione più complicata $F = \left(\mathrm{tr}\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_2}}\right)^2$ (9.2.2 in [23] per maggiori dettagli). Osserviamo comunque che nel caso in ρ_1 si riduca ad uno stato puro $|\psi\rangle\langle\psi|$ abbiamo $\sqrt{\rho_1} = |\psi\rangle\langle\psi| = \rho_1$ da cui, ponendo $\bar{\rho}_2 \equiv \langle\psi|\rho_2|\psi\rangle$,

$$F = \left(\mathrm{tr}\sqrt{\bar{\rho}_2|\psi\rangle\langle\psi|}\right)^2 = \bar{\rho}_2\mathrm{tr}(\sqrt{|\psi\rangle\langle\psi|})^2 = \bar{\rho}_2\mathrm{tr}(|\psi\rangle\langle\psi|)^2 = \langle\psi|\rho_2|\psi\rangle. \qquad (15)$$

Se poi a sua volta ρ_2 è puro abbiamo $F = \langle\psi|\phi\rangle\langle\phi|\psi\rangle = |\langle\psi|\phi\rangle|^2$, come sopra.

Vediamo subito un esempio. Supponiamo di avere un qubit e sapere solamente che si trova in uno stato puro come in eq. (14) e di volerne creare in qualche modo una copia $|\phi\rangle$, compatibilmente con il teorema di non clonabilità. La strategia più rozza sembra essere quella di scegliere a caso una direzione $\hat{m}$ e scrivere lo stato (comunque puro) nella forma $\rho_2 = (\mathbb{I} + \hat{m} \cdot \vec{\sigma})/2$; la misura di fedeltà dei due stati è allora

$$F = \frac{\mathrm{tr}(\mathbb{I} + \hat{n} \cdot \vec{\sigma})(\mathbb{I} + \hat{m} \cdot \vec{\sigma})}{4} = \frac{(2 + 2\hat{n} \cdot \hat{m})}{4} = \frac{1 + \cos\vartheta}{2}$$

dove ϑ indica l'angolo fra $\hat{n}$ e $\hat{m}$. La prima uguaglianza si deve al fatto che per stati entrambi puri possiamo esprimere la fedeltà anche come $F = \mathrm{tr}|\psi\rangle\langle\psi|\phi\rangle\langle\phi| = \langle\psi|\phi\rangle\mathrm{tr}|\psi\rangle\langle\phi| = |\langle\psi|\phi\rangle|^2$ (si esprimano $|\psi\rangle$ e $|\phi\rangle$ su una base per vedere che $\mathrm{tr}|\psi\rangle\langle\phi| = \langle\phi|\psi\rangle$), mentre la seconda uguaglianza è stata ottenuta sfruttando le proprietà delle matrici di Pauli (29). Ripetendo molte scelte casuali si ottiene (mediando su ϑ) $\bar{F} = 1/2$.

Intuitivamente ci aspettiamo di avere una fedeltà maggiore se sfruttiamo qualche conoscenza sullo stato misurando ad esempio σ^z

$$\langle\psi|\sigma^z|\psi\rangle = \mathrm{tr}\sigma^z \frac{(\mathbb{I} + \hat{n}\cdot\vec{\sigma})}{2} = n^z = \cos\theta.$$

Per uno stato nella forma $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ con $|\alpha|^2 + |\beta^2| = 1$ ci aspettiamo $\langle\sigma^z\rangle = -|\alpha|^2 + |\beta|^2 = 2|\beta|^2 - 1$ da cui $|\alpha|^2 = (1-\cos\theta)/2$, $|\beta|^2 = (1+\cos\theta)/2$ con cui possiamo costruire in senso statistico lo stato misto che fornisce lo stesso valore dell'osservabile

$$\rho_2 = \mathrm{prob}(\sigma^z \to +1)|1\rangle\langle 1| + \mathrm{prob}(\sigma^z \to -1)|0\rangle\langle 0| \to \begin{pmatrix} |\beta|^2 & 0 \\ 0 & |\alpha|^2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+\cos\theta & 0 \\ 0 & 1-\cos\theta \end{pmatrix}$$

da cui

$$F = \langle\psi|\rho_2|\psi\rangle = \frac{1}{4}[(1+\cos\theta)^2 + (1-\cos\theta)^2] = \frac{1+\cos^2\theta}{2}$$

che, mediata su θ con la misura polare sferica $(\sin\theta)/2d\theta$, dà $\bar{F} = 2/3$.

2.7 Sfruttare l'entanglement in un protocollo quantistico: Il teletrasporto

Supponiamo che Alice debba inviare a Bob un qubit $|\psi\rangle_I$ in suo possesso (ma che ella non conosce) attraverso una comunicazione su un canale classico. Un modo potrebbe essere per lei quello di misurare σ^z sullo stato e poi comunicare a Bob il risultato. A questo punto Bob può preparare il suo stato $|\phi\rangle_B$ uguale a $|1\rangle$ o $|0\rangle$ a seconda che il risultato di Alice sia stato $+1$ o -1. Come abbiamo visto nel sottosezione 2.6, questo procedimento ci consente di avere una fedeltà media $\bar{F} = 2/3$, che è sempre meglio della scelta a caso che dà $\bar{F} = 1/2$. Classicamente, non si può fare di meglio perché ormai abbiamo compromesso lo stato iniziale con la misura.

Tuttavia, le proprietà non locali degli stati entangled permettono di spingersi oltre, come illustrato nel protocollo di teletrasporto quantistico elaborato da Bennett e collaboratori nel 1993 [5]. Il protocollo prevede che Alice e Bob condividano una coppia entangled, ad esempio $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B))$, avendo ciascuno una delle due particelle. A questo punto, Alice esegue una misura congiunta **nella base di Bell** sul sistema "I+A" formato dallo stato $|\psi\rangle_I$ e dalla particella A appartenente a $|\Phi^+\rangle_{AB}$. Con questa terminologia intendiamo una misura in linea di principio concepibile in meccanica quantistica il cui esito come valori osservati sia una serie di numeri che rispondono alla domanda "*In quale stato di una base è finito il sistema dopo la misura?*". Nella appendice viene fornito qualche argomento per comprendere meglio come questo tipo di misure siano concepibili usando una serie di proiettori ortogonali associati ad una base. Rimane certamente aperta la questione di quali siano le osservabili finali di laboratorio che corrispondono a misurare questi oggetti. Nel caso specifico di esperimenti con fotoni si tratta in ultima analisi di una serie di elementi

ottici (ad es. polarizzatori o lamine) e rivelatori; esaminando i conteggi di una sequenza opportuna di questi ultimi si può rispondere in modo non ambiguo alla domanda di cui sopra. Si noti che questo tipo di misure in generale sono molto distruttive e la risposta finale di quale stato si sia ottenuto riguarda appunto la *fine* della sequenza di misura e non lo stato *prima* dell'inizio della misura che rimane sostanzialmente incognito.

Ora, nel caso specifico dei due qubit i possibili risultati della misura nella base di Bell sono quattro, pertanto Alice comunica 2 bit classici $b_1 b_2$ di informazione a Bob, il quale applica una tra quattro trasformazioni unitarie alla sua particella B di $|\Phi^+\rangle_{AB}$. Il risultato è che dopo la trasformazione unitaria Bob si ritrova con una copia esatta $|\phi\rangle = |\psi\rangle$ (cioè $F = 1$).

Vediamo in dettaglio come ciò avviene. Scriviamo lo stato da trasferire come $|\psi\rangle_I = \alpha\,|0\rangle_I + \beta\,|1\rangle_I$ con $|\alpha|^2 + |\beta|^2 = 1$, pertanto globalmente abbiamo

$$\begin{aligned}
|\psi\rangle_I\,|\Phi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}\,(\alpha\,|0\rangle_I + \beta\,|1\rangle_I)\,(|0\rangle_A\,|0\rangle_B + |1\rangle_A\,|1\rangle_B) \\
&= \frac{1}{\sqrt{2}}\,(\alpha\,|000\rangle_{IAB} + \alpha\,|011\rangle_{IAB} + \beta\,|100\rangle_{IAB} + \beta\,|111\rangle_{IAB}) \\
&= \frac{|\Phi^+\rangle_{IA} + |\Phi^-\rangle_{IA}}{2}\alpha\,|0\rangle_B + \frac{|\Psi^+\rangle_{IA} + |\Psi^-\rangle_{IA}}{2}\alpha\,|1\rangle_B \\
&+ \frac{|\Psi^+\rangle_{IA} - |\Psi^-\rangle_{IA}}{2}\beta\,|0\rangle_B + \frac{|\Phi^+\rangle_{IA} - |\Phi^-\rangle_{IA}}{2} + \beta\,|1\rangle_B \\
&= \frac{1}{2}|\Phi^+\rangle_{IA}\mathbb{I}_B\,|\psi\rangle_B + \frac{1}{2}|\Psi^+\rangle_{IA}\sigma_B^x\,|\psi\rangle_B \\
&+ \frac{1}{2}|\Psi^-\rangle_{IA}\,(i\sigma_B^y)\,|\psi\rangle_B - \frac{1}{2}|\Phi^-\rangle_{IA}\sigma_B^z\,|\psi\rangle_B
\end{aligned}$$

dove abbiamo usato la trasformazione inversa alla (6) e, nell'ultima equazione, abbiamo riscritto le combinazioni lineari di $|0\rangle_B$ e $|1\rangle_B$ che moltiplicano i quattro stati della base di Bell su I+A come matrici di Pauli agenti sullo stato $\alpha|0\rangle_B + \beta|1\rangle_B$

$$\begin{aligned}
\alpha|1\rangle_B + \beta|0\rangle_B &= \sigma_B^x(\alpha|0\rangle_B + \beta|1\rangle_B) \\
\alpha|1\rangle_B - \beta|0\rangle_B &= i\sigma_B^y(\alpha|0\rangle_B + \beta|1\rangle_B) \\
\alpha|0\rangle_B - \beta|1\rangle_B &= -\sigma_B^z(\alpha|0\rangle_B + \beta|1\rangle_B)
\end{aligned}$$

Ora, la misura congiunta sulla base di Bell che Alice effettua su I+A, fa collassare lo stato in una delle quattro equiprobabili possibilità. Allora, dopo aver comunicato il ricevuto i bit $b_1 b_2$ che codificano le quattro possibilità, Bob esegue una operazione unitaria secondo la tabella e ritrova nella sua particella B esattamente lo stato quantistico che era in A, pur senza conoscerlo o averlo misurato.

Risultato di Alice	Operazione di Bob
$\|\Phi^+\rangle$	I (non fa nulla)
$\|\Psi^+\rangle$	σ^x
$\|\Psi^-\rangle$	σ^y
$\|\Phi^-\rangle$	σ^z

Va sottolineato che comunque il teorema di non clonabilità rimane valido. Infatti, al momento della misura di Alice lo stato $|\psi\rangle_I$ cessa di esistere e la particella I si trova in uno stato entangled con la particella A. In tal senso è avvenuto un "trasferimento" dello stato. Per di più l'informazione trasferita alla fine del processo è maggiore di due bit, poichè lo stato quantistico ingloba due numeri complessi. Tuttavia Bob non può estrarre tutta l'informazione dello stato. Egli sa solamente che lo stato è stato trasferito per intero. Infine, osserviamo anche che la procedura di teletrasporto si compie definitivamente, solo quando Bob è in possesso dei due bit classici che necessariamente vengono trasferiti ad una velocità non superiore a quella della luce e pertanto non si viola il principio di relatività.

Nel 1997 è stata data la prima dimostrazione sperimentale di questo protocollo con fotoni [9]; l'anno seguente una collaborazione che ha coinvolto anche ricercatori italiani [7] ha riverificato l'effetto considerando stati di fotoni con entanglement fra i lori gradi di libertà orbitali (direzione di propagazione) e di polarizzazione. Nel 2004 poi il gruppo di Vienna ha dato una dimostrazione spettacolare teletrasportando lo stato di un fotone da un lato all'altro del Danubio usando come canale quantistico una fibra ottica di 800 m di lunghezza [29]. Per uniformità con alcuni testi va osservato che, magari proprio per la particolare implementazione fisica dei qubit e delle porte, può essere più conveniente da un punto di vista operativo effettuare le quattro misure nella base computazionale a due qubit anziché in quella di Bell. Pertanto a volte il protocollo prevede un'ulteriore passaggio dei qubit in I attraverso una porta di Hadamard e poi dei due qubit I e A attraverso un CNOT

$$U_{IA} = \mathrm{CNOT}_{IA}(U_{H,I}\otimes\mathbb{I}_A) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$

ed i quattro stati nella base di Bell prima della misura di Alice vengono quindi trasformati secondo $U_{IA}|\Phi^+\rangle_{IA} = |00\rangle_{IA}$, $U_{IA}|\Psi^+\rangle_{IA} = |01\rangle_{IA}$, $U_{IA}|\Phi^-\rangle_{IA} = |10\rangle_{IA}$ e $U_{IA}|\Psi^-\rangle_{IA} = |11\rangle_{IA}$ e i quattro possibili stati di Bob vengono ad essere in corrispondenza proprio con gli stati della base computazionale a due qubit.

Su una procedura molto simile a quella qui descritta per il teletrasporto si basa anche un altro algoritmo quantistico, detto **codifica densa**, che permette ad Alice di spedire a Bob il contenuto di informazione di due bit classici inviando di fatto un solo qubit (per maggiori dettagli si veda, ad esempio, 4.2.1 in [1]).

3 Entropia ed indicatori di entanglement

3.1 Compressione dei dati classica

Supponiamo di avere a che fare con un messaggio formato da una lunga stringa di n caratteri, scritta in un alfabeto di k lettere

$$\{a_1, a_2, \ldots, a_k\}$$

Come in ogni linguaggio, alcune lettere compaiono più frequentemente di altre. Assumendo l'assenza di correlazioni, in una data posizione ciascuna lettera a_i avrà una certa probabilità $p(a_i)$ di comparire, con la condizione $\sum_{i=1}^{k} p(a_i) = 1$. Il caso più semplice si ha nel caso di un alfabeto binario dove l'uno appare con probabilità p e lo zero con probabilità$1-p$.

Ora ci chiediamo: dato un messaggio di n caratteri, fino a che punto possiamo comprimerlo pur mantenendo la stessa informazione?

Per grandi n, un messaggio tipico nel caso binario conterrà $n(1-p)$ caratteri "0" e np "1". Il numero di possibili messaggi di questa forma sarà $\binom{n}{np}$ ed usando la formula di Stirling $\log n! = n\log n - n$ otteniamo

$$\log\binom{n}{np} = n\log n - n - np\log np + np - n(1-p)\log n(1-p) + n(1-p) = nH(p)$$

dove

$$H(p) = -\left(p\log p + (1-p)\log(1-p)\right)$$

è la funzione **entropia** e il logaritmo è in base 2 (in tal modo $H(p) = 1$ nel punto di massimo $p = 1/2$). Il numero di stringhe tipiche è dell'ordine di $2^{nH(p)}$, dove $nH(p)$ gioca il ruolo del numero di bit effettivi del messaggio compresso.

Il concetto si generalizza facilmente al caso di k lettere scrivendo

$$H(X) = -\sum_{x=1}^{k} p(x)\log p(x) \tag{16}$$

ovvero l'**entropia di Shannon** associata alla distribuzione $X = \{x, p(x)\}$.

In definitiva, data una stringa di n caratteri, H ci dice quale è la predicibilità del carattere $n+1$-esimo. Se $H = 0$, nel messaggio c'è solo una lettera, per cui ogni carattere del messaggio è predeterminato. La situazione opposta si ha quando tutte le lettere sono equiprobabili e il messaggio è incomprimibile. Possiamo anche dire che H è l'informazione media contenuta in ciascun carattere e asintoticamente il codice ottimale comprime ogni lettera ad H bit.

3.2 Estensione al caso quantistico: Entropia di von Neumann

L'obiettivo di questa sottosezione è quello di fornire l'analogo del risultato di Shannon nel caso quantistico. Assumiamo di avere una sorgente di stati $|\psi_i\rangle$, $i = 1, \ldots, k$, descritta dalla matrice densità

$$\rho = \sum_{i=1}^{k} p_i |\psi_i\rangle\langle\psi_i| \tag{17}$$

Un messaggio di caratteri non correlati sarà dato dalla matrice densità totale

$$\rho^n = \underbrace{\rho \otimes \rho \otimes \ldots \otimes}_{n \text{ volte}}.$$

Analogamente al caso classico in cui si sono considerati i messaggi tipici, ora considereremo invece i sottospazi tipici, ovvero quelli maggiormente probabili. Per vederlo, diagonalizziamo la nostra matrice densità ρ

$$\rho = \sum_{i=1}^{k} \lambda_i |\phi_i\rangle\langle\phi_i|$$

dove stavolta abbiamo $\langle\phi_i|\phi_j\rangle = \delta_{ij}$. Una volta fatto ciò, dal momento che i $|\phi_j\rangle$ sono ortogonali, possiamo utilizzare il risultato di Shannon. E' come avere un alfabeto di k "lettere classiche", ognuna con probabilità λ_i di apparire. Il teorema di Shannon dice che possiamo comprimere un messaggio di n caratteri in un messaggio di nH bit (o qubit), con H data dall'eq.(16). Definiamo quindi l'**entropia di Von Neumann** come

$$S(\rho) = -\mathrm{tr}(\rho \log \rho) \tag{18}$$

che si calcola diagonalizzando la ρ, ottenendo quindi

$$S = -\sum_{i=1}^{k} \lambda_i \log \lambda_i.$$

Pertanto, possiamo affermare che la dimensione dello spazio di Hilbert più probabile è

$$\dim \mathcal{H}_{prob} = 2^{nS(\rho)}.$$

Di conseguenza, Alice può comprimere il suo messaggio di n stati in nS qubit. In definitiva, l'entropia di Von Neumann quantifica il contenuto di informazione incomprimibile di una sorgente quantistica così come l'entropia di Shannon quantifica il contenuto di informazione incomprimibile di una sorgente classica. Si veda anche cap. 11 di [23].

Infine, prima di ritornare all'entanglement, effettuiamo il calcolo dell'entropia di von Neumann nel caso di una matrice densità termica canonica $\rho_{\mathrm{canonica}} = Z^{-1}\exp(-H/K_BT)$ con $Z = \mathrm{tr}\exp(-H/K_BT)$ come discusso alla fine della sottosezione 2.3. Dalla termodinamica statistica [22] si sa che l'energia libera di Helmholtz F è legata alla funzione di partizione Z secondo $F = -K_BT\ln Z$. Allora l'entropia di von Neumann (usando la base naturale dei logaritmi) diventa

$$S = -\mathrm{tr}\frac{\exp(-H/K_BT)}{Z}\ln\frac{\exp(-H/K_BT)}{Z} = \frac{1}{K_BT}\mathrm{tr}\rho_{\mathrm{canonica}}H + \ln Z\,\mathrm{tr}\rho_{\mathrm{canonica}} = \frac{\langle H\rangle - F}{K_BT}.$$

Il valore di aspettazione della hamiltoniana $\langle H\rangle$ rappresenta il contenuto di energia interna e quindi, a parte il fattore moltiplicativo dimensionale K_B, l'entropia di von Neumann in questo caso è proprio la funzione di stato entropia in senso termodinamico.

3.3 Entropia come misura di entanglement per stati puri

L'entropia di Von Neumann rappresenta anche la prima vera **misura di entanglement bipartito all'interno di uno stato puro** che incontriamo in questa introduzione. Qualitativamente pensiamo all'entanglement come ad una forte interazione o correlazione (vedremo dopo quanto in un caso particolare) fra due sottosistemi A e B. Ci aspettiamo allora che trasformazioni (unitarie) **globali** sul sistema complessivo non modifichino la quantità di entanglement. A livello locale invece possiamo pensare a trasformazioni unitarie su A o B, ma essendo l'entanglement una sorta di correlazione che si instaura tra le parti ci aspettiamo l'entanglement tra di esse non possa crescere se operiamo solo localmente. Inoltre stiamo pensando all'entanglement come ad una proprietà genuinamente quantistica, non riconducibile a correlazioni di tipo classico. Quindi, se A e B effettuano operazioni congiunte che però poggiano su un canale classico, richiediamo che nemmeno in questa situazione il grado di entanglement possa crescere. La definizione quantitativa dell'ammontare di entanglement in uno stato puro $|\Psi\rangle_C$ può essere formulata appunto sulla base di queste operazioni locali (OL) o comunicazioni classiche (CC): Date n copie di uno stato $|\Psi\rangle_C$, possiamo operare su $|\Psi\rangle_{C1} \otimes \ldots \otimes |\Psi\rangle_{Cn}$ con OLCC e creare da queste $n' \leq n$ copie di uno stato massimamente entangled $|\chi\rangle_{C1} \otimes \ldots \otimes |\chi\rangle_{Cn'} \otimes \ldots$. Questa procedura si chiama tecnicamente **distillazione** dell'entanglement. Il rapporto $E = n'/n$ (per $n \to \infty$) viene definita entanglement di distillazione di $|\Psi\rangle_C$. Se scriviamo la sua decomposizione di Schmidt

$$|\Psi\rangle_C = \sum_i \sqrt{p_i} |i\rangle_A |i'\rangle_B$$

la misura di entanglement è proprio l'entropia (risultato che qui non dimostriamo)

$$E(|\Psi\rangle_C) = -\sum_i p_i \log p_i.$$

Da ciò segue che dato uno stato puro $|\Psi\rangle_C$ il valore di E è dato dall'entropia di Von Neumann delle tracce parziali

$$E = S(\rho_A) = S(\rho_B)$$

con $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ e $\rho_B = \mathrm{Tr}_A(\rho_{AB})$.

Vediamo che $E = 0$ per uno stato separabile con $p_1 = 1$, $p_{i>1} = 0$, mentre $E = 1$ (massimo) per uno stato della forma $\rho = \mathbb{I}/d$ (se il logaritmo è preso in base d). Si noti anche che in una definizione a priori dell'entanglement di distallazione è necessario aver definito cosa si intende per stato massimamente entangled $|\chi\rangle_C$, e fondamentalmente in analogia con gli stati di Bell per qubit ($d = 2$), si può procedere identificando questi stati come quelli che sotto traccia parziale restituiscono appunto una $\rho_A = \mathbb{I}_A/d_A$. Senza perdita di generalità, abbiamo considerato il caso in cui A è la parte con lo spazio di Hilbert eventualmente a dimensione minore (così la matrice densità ridotta a B ha lo stesso numero d_A di autovalori non nulli ed identici a $1/d_A$). Nell'identificazione con

l'entropia di von Neumann come misura quantitativa e rigorosa di entanglement è sufficiente che qualche stato nello spazio degli operatori densità mostri la proprietà di avere entropia massima, e a posteriori questi stati risultano appunto quelli con autovalori massimamente equipartiti. Purtroppo non avendo un equivalente delle disuguaglianze di Bell per stati a $d > 2$ nel caso generale, non possiamo chiudere logicamente e fisicamente il ragionamento per mostrare che questi stati che chiamiamo massimamente entangled hanno anche la proprità di violare al massimo alcune disuguaglianze di Bell generalizzate, come invece possiamo fare compiutamente per due qubit con $d = 2$.

Elenchiamo ora alcune proprietà importanti dell'entropia di Von Neumann:

- **Purezza.** Uno stato puro ha entropia nulla.
- **Invarianza.** L'entropia è invariante per trasformazioni unitarie.

$$S(U\rho U^{-1}) = S(\rho).$$

- **Massimo.** Se ρ ha dimensione $d \times d$, allora $S(\rho) \leq \log d$. L'uguaglianza vale nel caso di equipartizione.
- **Concavitâ.** Per $\lambda_1, \lambda_2 \geq 0$ e $\lambda_1 + \lambda_2 = 1$, si ha

$$S(\lambda_1\rho_1 + \lambda_2\rho_2) \geq \lambda_1 S(\rho_1) + \lambda_2 S(\rho_2)$$

- **Subadditività.** Dato un sistema bipartito AB nello stato ρ_{AB}, allora vale

$$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$$

dove $\rho_A = \mathrm{Tr}_B(|\Psi\rangle_{CC}\langle\Psi|)$ e $\rho_B = \mathrm{Tr}_A(|\Psi\rangle_{CC}\langle\Psi|)$. L'entropia del tutto è minore dell'entropia delle parti. L'uguaglianza vale nel caso di stati prodotto indipendenti. Questo ci dice anche che la somma delle entropie cresce accendendo un interazione tra A e B.

Riprendendo ora il discorso della sezione precedente sulla entropia di von Neumann per uno stato termico, il fatto che $S > 0$ per $T > 0$ indica che un ipotetico stato puro del sistema più l'ambiente che costituisce il bagno termico è generalmente entangled rispetto alla separazione sistema/ambiente. Ma questo non ci dice altro che in qualche modo sono necessarie delle interazioni microscopiche tra le due parti per mantenere l'equilibrio termico. Fisicamente può essere più sottile la risposta a quest'altra domanda: Dato che il sistema C in esame si trova in uno stato misto ρ_C, come possiamo stabilire se è entangled rispetto ad una partizione in due sottosistemi A e B? Abbiamo appena interpretato l'entropia di von Neumann associata alla matrice densità ridotta ρ_A come una misura di entanglement. Questa interpretazione però è corretta solamente nel caso in cui C si trovi in uno stato puro. Ma, più in generale, si può pensare che a sua volta il sistema C sia parte di un universo U (si faccia riferimento alla fig. 4) il quale si trova in uno stato puro $|U\rangle$. Possiamo considerare una sequenza di matrici densità ridotte prima al sistema C tracciando idealmente

su tutti i gradi di libertà di U tranne C, $\rho_C = \mathrm{tr}_{U\setminus C}|U\rangle\langle U|$ e successivamente definire ancora la matrice densità ridotta ad A come $\rho_A = \mathrm{tr}_B \rho_C$. Vogliamo però caratterizzare l'entanglement nella separazione A/B senza ritornare a fare riferimento all'universo ma partendo direttamente da ρ_C. Il punto è che non abbiamo sviluppato ancora una nozione di separabilità e quindi di entanglement per stati misti. Iniziamo allora a definire come **separabile uno stato misto che si può scrivere nella forma**

$$\rho_C^{\text{separabile}} = \sum_j c_j \rho_{Aj} \otimes \rho_{Bj} \tag{19}$$

dove ρ_{Aj} e ρ_{Bj} sono stati (in generale misti) di A e B, rispettivamente, ed il pedice j indicizza i vari termini della combinazione lineare convessa. Analogamente al caso di stati puri, diremo che ρ_C è entangled rispetto alla partizione A/B se non si può scrivere in questa forma. Ma come possiamo stabilire questo fatto ed eventualmente misurare il contenuto di entanglement?

3.4 Assiomi per una misura di entanglement soddisfacente

Assioma E1 (Normalizzazione). $E(\rho) = 0$ per stati separabili.

Assioma E2 (non crescente sotto OLCC). $E(\Theta(\rho)) \leq E(\rho)$ per mappe (superoperatori) Θ che realizzano OLCC. In particolare ciò implica che deve essere invariante per OL. Infatti se operiamo localmente su A con U_A e su B con U_B avremo $E\left(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger\right) \leq E(\rho)$ (si noti la forma con cui evolve lo stato ρ). Ma a partire dal nuovo stato $\rho' = \Theta_{OL}(\rho) = U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger$ possiamo operare la trasformazione inversa $U_{A,B}^\dagger = U_{A,B}^{-1}$ che è ancora unitaria locale e quindi $E\left(U_A^\dagger \otimes U_B^\dagger \rho' U_A \otimes U_B\right) = E(\rho) \leq E(\rho')$, da cui appunto $E(\rho) = E(\rho')$.

Inoltre l'entanglement non dovrebbe essere generato facendo la miscela di due (o più) matrici densità. Questo perché, pensando alla miscela come a diverse preparazioni dello stato con diversi pesi p_i la statistica che introduciamo è sostanzialmente di tipo classico e non genuinamente quantistico come ci aspettiamo che sia invece l'entanglement. Da cui

Assioma E3 (Convessità). E è una funzione convessa: $E(\lambda\rho_1 + (1-\lambda)\rho_2) \leq \lambda E(\rho_1) + (1-\lambda) E(\rho_2)$. Si noti la differenza con la concavità dell'entropia. Questa è essenzialmente la ragione per cui possiamo adottare a tutti gli effetti l'entropia di von Neumann come misura di entanglement solo per stati complessivamente puri che ammettono una sola rappresentazione come combinazione lineare convessa estremale ($\lambda = 0$ o 1).

Dovrebbe poi essere sempre vero che l'entanglement non può crescere semplicemente mettendo insieme due stati:

Assioma E4a (Subadditività). Per ogni coppia di stati bipartiti ρ, σ vale $E(\rho \otimes \sigma) \leq E(\rho) + E(\sigma)$.

Un'altra versione simile ma non identica è la seguente:

Assioma E4b (Addittività debole). Per ogni stato ρ vale $E\left(\rho^{\otimes N}\right) = NE\left(\rho\right)$.

3.4.1 Entanglement di formazione e concorrenza per qubit

Una possibile definizione dell'entanglement per stati misti che soddisa gli assiomi appena elencati è il cosiddetto **entanglement di formazione**

$$E_F(\rho_C) = \min_{p_i} \sum_i p_i S(|i\rangle_{CC}\langle i|) \tag{20}$$

dove è stato sfruttato il fatto che un qualunque stato misto si può decomporre come combinazione convessa di stati puri di C, $\rho_C = \sum_i p_i |i\rangle_{CC}\langle i|$ (non si faccia confusione con la definizione di separabilità (19)). Tale combinazione però non è unica e nella definizione si sceglie il minimo (in accordo con l'Assioma E3) fra tutte le possibili combinazioni tali che $\sum_i p_i = 1$.

Sfortunatamente non è noto in generale come effettuare la procedura di minimizzazione nella eq. (20). Per uno **stato misto di due qubit** tuttavia Wootters nel 1998 [33] è riuscito a trovare un'espressione involuta ma calcolabile dell'entanglement di formazione attraverso la cosiddetta **concorrenza (concurrence)**. Per uno stato generico misto a due qubit

$$E_F(\rho_C) = -\lambda \log \lambda - (1-\lambda)\log(1-\lambda)$$

con $\lambda = (1+\sqrt{1-\mathcal{C}^2})/2$ e la concorrenza $\mathcal{C}$ a sua volta calcolata esplicitamente come

$$\mathcal{C} = \max(0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4) \tag{21}$$

e $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4$ sono le radici degli autovalori della matrice 4×4: $M_W = \rho_C \Sigma_{AB} \rho_C^* \Sigma_{AB}$, con $\Sigma_{AB} = \sigma_A^y \otimes \sigma_B^y$ e ρ_C^* è la matrice densità complessa coniugata espressa nella base computazionale. E' come se avessimo l'entropia di von Neumann per uno stato puro a due qubit in cui il determinante Δ della matrice densità viene rimpiazzato da $\mathcal{C}^2/4$ nella espressione degli "autovalori" λ e $(1-\lambda)$.

3.4.2 Concorrenza versus correlazioni

A parte la formula di Wootters, che significato fisico possiamo attribuire alla concorrenza? Vediamo alcuni casi particolari.

- Stati puri $|\Psi\rangle_C$: Definendo la funzione di **correlazione connessa** a due spin

  $$Q_{\hat{a}\hat{b}} \equiv_C \langle\Psi|(\vec{\sigma}_A \cdot \hat{a})(\vec{\sigma}_B \cdot \hat{b})|\Psi\rangle_C - {}_C\langle\Psi|\vec{\sigma}_A \cdot \hat{a})|\Psi\rangle_{CC}\langle\Psi|\vec{\sigma}_B \cdot \hat{b}|\Psi\rangle_C$$

  (dove $\hat{a}$ e $\hat{b}$ definiscono due direzioni per misurare lo spin di A e B rispettivamente) si può dimostrare che la concorrenza è la massima correlazione possibile nel senso che

  $$\mathcal{C}(|\Psi\rangle_C) = \max_{\hat{a},\hat{b}} Q_{\hat{a}\hat{b}}.$$

- Stati misti invarianti per rotazioni spaziali tridimensionali. Si può dimostrare che

$$\mathcal{C}(\rho_C) = \frac{1}{2}\max(0, -1 - \langle \vec{\sigma}_A \cdot \vec{\sigma}_B \rangle) \tag{22}$$

dove $\langle \vec{\sigma}_A \cdot \vec{\sigma}_B \rangle = \mathrm{tr}\rho_C \vec{\sigma}_A \cdot \vec{\sigma}_B$. Si noti che questo valore di aspettazione è anch'esso una correlazione a due spin ma diverso da $Q_{\hat{a}\hat{b}}$ ed in particolare la simmetria di rotazione è tale che $\langle \vec{\sigma}_{A,B} \rangle = 0$. Osserviamo poi che dalla somma dei momenti angolari $\hbar/2\vec{\sigma}_A$ e $\hbar/2\vec{\sigma}_B$ troviamo

$$(\vec{\sigma}_A + \vec{\sigma}_B)^2 = \frac{4}{\hbar^2} S^2_{tot} = \vec{\sigma_A} \cdot \vec{\sigma}_A + \vec{\sigma_B} \cdot \vec{\sigma}_B + 2\vec{\sigma_A} \cdot \vec{\sigma}_B = 2(3\mathbb{I} + \vec{\sigma_A} \cdot \vec{\sigma}_B)$$

da cui $\langle \vec{\sigma}_A \cdot \vec{\sigma}_B \rangle = \frac{2}{\hbar^2}\mathrm{tr}\rho_C S^2_{tot} - 3$. Ma se ρ_C è invariante per rotazione avremo un blocco 1×1 con autovalore p per il settore di singoletto a spin totale 0 ed un blocco 3×3 con autovalore $(1-p)/3$ per il tripletto a spin totale 1 e $\langle S^2_{tot} \rangle = \hbar^2 2$. Così $\langle \vec{\sigma}_A \cdot \vec{\sigma}_B \rangle = 4(1-p) - 3 = 1 - 4p$ ed essendo $0 \leq p \leq 1$

$$-3 \leq \langle \vec{\sigma}_A \cdot \vec{\sigma}_B \rangle \leq 1.$$

All'estremo inferiore abbiamo un singoletto puro ($p = 1$) ed all'estremo superiore invece uno stato di tripletto misto invariante per rotazione ($p = 0$). Dalla eq. (22) vediamo che la **soglia** per avere $\mathcal{C} > 0$ è data dalla condizione $\langle \vec{\sigma}_A \cdot \vec{\sigma}_B \rangle < -1$. In effetti il max nella formula (21) si riflette nel fatto che per avere entanglement (e quindi concorrenza) non nullo **è necessario che vi siano non solo correlazioni fra A e B, ma anche che queste eccedano in valore assoluto una certa soglia**. In questo senso ora possiamo dire che l'entanglement non è solo una generica forma di correlazione, ma l'intensità di tale correlazione deve essere sufficientemente alta; solo in questo caso si possono manifestare effetti puramente quantistici come ad esempio la violazione della disuguaglianza di Bell che si ha appunto per $\Delta = \mathcal{C}^2/4 > 0$ (vedi sottosez. 2.4.1). Inoltre, la quantità $\varepsilon = -\langle \vec{\sigma}_A \cdot \vec{\sigma}_B \rangle/3$ gioca un ruolo importante anche nello studio dei canali quantistici di comunicazione che preservano la simmetria di rotazione. Si può dimostrare [10] che, ad esempio, a partire da uno stato in ingresso $|I\rangle$ l'utilizzo di un tale canale per la procedura di teletrasporto descritta nella sezione 2.7 porta Bob ad avere uno stato misto in cui solo una frazione riproduce lo stato iniziale di Alice. Si dice che il teletrasporto è avvenuto su un **canale depolarizzante**

$$|I\rangle \to \mathcal{T}(|I\rangle) = \varepsilon |I\rangle\langle I| + \frac{1-\varepsilon}{2}\mathbb{I}. \tag{23}$$

Si noti che $\mathrm{tr}\mathcal{T} = 1$ come deve essere. Calcoliamo quanto è fedele $\mathcal{T}$ a $|I\rangle\langle I|$ usando la formula (15): $F = \langle I|\mathcal{T}|I\rangle = \varepsilon + (1-\varepsilon)/2 = (1+\varepsilon)/2$, che risulta maggiore di quella media classica ($\bar{F} = 2/3$) quando $\varepsilon > 1/3$ ossia $\langle \vec{\sigma}_A \cdot \vec{\sigma}_B \rangle < -1$ che è proprio la soglia per avere entanglement tra A e B.

3.4.3 Disuguaglianze di monogamia

Un'altra caratteristica che differenzia la nozione di entanglement da quella generica di correlazioni è che queste, in sistemi a molti corpi con interazioni locali, tipicamente decadono con la distanza ed una particella si trova molto correlata con quella immediatamente vicina, un po' meno con quella a secondi vicini ecc. Non esiste però un limite massimo alle correlazioni complessive che la particella può instaurare con le altre del sistema. Nel 2006 invece è stata dimostrata da Osborne e Verstraete [24] la cosiddetta **congettura di Coffman-Kundu-Wootters che stabilisce una sorta di "monogamia" dell'entanglement**. Dato un sistema composto da varie parti (qubit) che indichiamo con A, B_1, B_2,... ecc. la disuguaglianza di monogamia dice che

$$\mathcal{C}^2(A|B_1) + \mathcal{C}^2(A|B_2) + \ldots \leq 4\Delta_A \leq 1 \tag{24}$$

dove $\mathcal{C}^2(A|B_k)$ indica la concorrenza del (sotto)sistema bipartito di qubit $A|B_k$ associata alla matrice densità ridotta ρ_{AB_k} a partire dal sistema globale e Δ_A è invece il determinante della matrice ridotta ad un qubit ρ_A. Si vede quindi che non è possibile per A essere molto entangled con vari sottosistemi B; se ad esempio è molto entangled con B_1 allora necessariamente lo dovrà essere poco o per niente con i restanti. Il limite superiore è comunque $4\Delta_A$ che quantifica complessivamente l'entanglement fra A e tutto il resto del sistema. Il concetto espresso dalla disuguaglianza (24) è illustrato nella figura 6. L'eventuale discrepanza tra il membro di sinistra ed il membro centrale (detto anche one-tangle) quando la disuguaglianza non è stretta, ossia

$$4\Delta_A - \sum_j \mathcal{C}^2(A|B_j)$$

esprime una forma di entanglement genuinamente *multipartito*, che non è riconducibile a coppie.

Esercizio: Si consideri uno stato della forma

$$|\Psi\rangle_C = \alpha|0_A 0_{B_1} 0_{B_2} \ldots 0_{B_N}\rangle + \beta|1_A 1_{B_1} 1_{B_2} \ldots 1_{B_N}\rangle$$

dove i pedici A e B_j denotano $N+1$ qubit, e $|\alpha|^2 + |\beta|^2 = 1$ per normalizzare all'unità lo stato visto che i due ket nella sovrapposizione sono due elementi (ad es. il primo e l'ultimo in un certo ordine) della base computazionale ortonormale per gli $N+1$ qubit. Ora, per vedere nel dettaglio le disuguaglianze nella congettura di Coffmann-Kundu-Wootters osserviamo innanzi tutto che lo stato è completamente simmetrico per lo scambio di due qubit qualsiasi, per cui ci basterà calcolare la concorrenza tra A e, ad esempio, B_1. Lo si fa attraverso la matrice densità ridotta

$$\rho_{AB_1} = \mathrm{Tr}_{B_2 \ldots B_N} \rho_C = \mathrm{Tr}_{B_2 \ldots B_N} |\Psi\rangle_{CC}\langle\Psi|$$

Sviluppando i quattro termini con coefficienti $|\alpha|^2$, $|\beta|^2$, $\alpha^*\beta$ e $\alpha\beta^*$ dall'espressione dello stato $|\Psi\rangle_{CC}\langle\Psi|$ nella traccia di sopra si vede che solo due danno

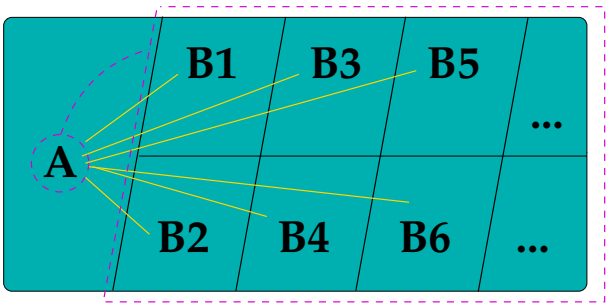

Figura 6: In un sistema a molti qubit A, B_1, B_2, ... l'entanglement che un dato qubit A stabilisce con tutto il resto (linee magenta tratteggiate) è misurato da $4\Delta_A$ nella eq. (24) e maggiora la somma degli entanglement di coppia misurati da $\mathcal{C}^2(A|B_1)$, $\mathcal{C}^2(A|B_2)$, ... (linee gialle continue); ogni coppia di qubit $A|B_k$ si trova in generale in uno stato misto per effetto di tutte le altre parti. *In a many-qubits system A, B_1, B_2, ... the entanglement that a given qubit A supports with all the rest (magenta dashed lines) is measured by $4\Delta_A$ in eq. (24) and bounds from above the sum of pairwise entanglements measured by $\mathcal{C}^2(A|B_1)$, $\mathcal{C}^2(A|B_2)$, ... (continuous yellow lines); each qubits pair $A|B_k$ in general is in a mixed state due to the effect of all other parts.*

contributo non nullo, perché l'operazione di traccia consiste nella somma degli elementi di matrice diagonali presi su una base di $N-1$ qubit $B_2 \ldots B_N$ e, di nuovo, questa base può essere scelta come quella computazionale. Avremo allora come contributi non nulli solo quelli che vengono dagli stati (ortogonali tra loro) $|00\rangle_{AB_1} \otimes |0\ldots0\rangle_{B_1\ldots B_N}$ e $|11\rangle_{AB_1} \otimes |1\ldots1\rangle_{B_1\ldots B_N}$; nella notazione abbiamo usato esplicitamente il prodotto tensore per evidenziare come gli elementi della base a $N+1$ qubit siano composti da quelli della base a $N-1$ qubit. Dalla traccia parziale su $B_2 \ldots B_N$ rimane allora

$$\rho_{AB_1} = |\alpha|^2 |00\rangle_{AB_1 AB_1}\langle 00| + |\beta|^2 |11\rangle_{AB_1 AB_1}\langle 11|$$

che nella base computazionale di AB_1 prende la forma matriciale

$$\rho_{AB_1} = \begin{pmatrix} |\alpha|^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & |\beta|^2 \end{pmatrix}.$$

E' bene osservare che questa matrice rappresenta lo stato misto di AB_1 che a loro volta sono parti del sistema C, che si trova in uno stato complessivamente puro. Con la stessa filosofia calcoliamo subito anche la traccia parziale su B, in modo da avere la matrice densità per il qubit A

$$\rho_A = \mathrm{Tr}_{B_1\ldots B_N} |\Psi\rangle_{CC}\langle\Psi| = \mathrm{Tr}_{B_1} \rho_{AB_1} = |\alpha|^2 |0\rangle_{AA}\langle 0| + |\beta|^2 |1\rangle_{AA}\langle 1|.$$

L'entanglement di A *con tutto il resto* (cioè i qubit $B_1B_2\ldots B_N$) si parametrizza con il determinante

$$\Delta_A = |\alpha|^2|\beta|^2 = |\alpha|^2(1-|\alpha|^2)$$

mentre per valutare l'entanglement che esiste tra A e B_1 nello stato misto ρ_{AB_1} usiamo appunto la concorrenza di Wootters. Non avendo simmetrie particolari per rotazione dobbiamo usare la formula (21), costruendo prima la matrice ausiliaria $\Sigma_{AB_1} = \sigma_A^y \otimes \sigma_{B_1}^y$. Nella base computazionale usiamo la formula della appendice A

$$\Sigma_{AB_1} = \begin{pmatrix} 0 & -\mathrm{i}\sigma^y \\ \mathrm{i}\sigma^y & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

Dato che ρ_{AB_1} in questo esempio è reale nella base computazionale abbiamo la semplificazione $M_W = (\rho_{AB_1}\Sigma_{AB_1})^2$, da cui

$$M_W = \begin{pmatrix} 0 & 0 & 0 & -|\alpha|^2 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -|\beta|^2 & 0 & 0 & 0 \end{pmatrix}^2 = |\alpha|^2|\beta|^2 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Si noti che M_W non è una matrice densità e che, quali che siano α e β, ha sempre autovalori $\lambda_1 = \lambda_2 = |\alpha|^2|\beta|^2$ e $\lambda_3 = \lambda_4 = 0$ così che dalla eq. (21) $\mathcal{C} = 0$. La disuguaglianza di monogamia (24) allora si legge $0+\ldots+0 \leq 4|\alpha|^2(1-|\alpha|^2) \leq 1$, che significa che non appena $|\alpha| \neq 0, 1$ si "accende" un entanglement tra A e il gruppo dei qubit $B_1B_2\ldots B_N$ ma l'entanglement tra A e ciascuno dei B_j è sempre nullo. Parliamo quindi di entanglemente *multipartito* non riconducibile ad entanglement bipartito. Se poi $|\alpha| = |\beta| = 1/\sqrt{2}$ abbiamo entanglement massimo tra A ed il resto e lo stato corrispondente $|\Psi\rangle_C$ va sotto il nome di stato di Greenberger-Horne-Zeilinger (GHZ), uno stato che risulta usato come risorsa quantica computazionale in diversi protocolli.

Axioms for a satisfactory measure of entanglement

Axiom E1 *(Normalisation). $E(\rho) = 0$ for separable states, that is states of the form (19) where ρ_{Aj} and ρ_{Bj} are states (mixed in the most general case) of A and B, respectively, and the subscript j labels the terms of the convex linear combination.*

Axiom E2 *(not increasing under LOCC). $E(\Theta(\rho)) \leq E(\rho)$ for maps (superoperators) Θ that represent LOCC. In particular this implies that is has to be invariant under LO. In fact, if we locally operate on A with U_A and on B with U_B we will have $E\left(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger\right) \leq E(\rho)$ (note the evolved form of the state ρ). But, starting from a the new state $\rho' = \Theta_{OL}(\rho) =$*

$U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger$ we can operate with the inverse transformatiom $U_{A,B}^\dagger = U_{A,B}^{-1}$ that is still local and unitary so $E\left(U_A^\dagger \otimes U_B^\dagger \rho' U_A \otimes U_B\right) = E(\rho) \leq E(\rho')$, from which we conclude $E(\rho) = E(\rho')$.

Moreover entanglement should not be generated by mixing two (or more) density matrices. The reason is that, by interpreting the mixture as different state preparations with different weigths, the statistics we introduce in such a way is essentially classical and not genuinely quantum as we expect to be the notion of entanglement. Hence we ask

Axiom E3 *(Convexity). E is a convex function: $E(\lambda\rho_1 + (1-\lambda)\rho_2) \leq \lambda E(\rho_1) + (1-\lambda) E(\rho_2)$. Now note the difference with entropy concavity. This is essentially the reason why we can adopt in all respects von Neumann entropy as entanglement measure only for globally pure states that admit only one representation as extremal convex linear combination ($\lambda = 0$ or 1).*

Furthermore, it should always be true that entanglement cannot increase by juxtaposing two states:

Axiom E4a *(Subadditivity). For every possible pair of bipartite states ρ, σ it holds $E(\rho \otimes \sigma) \leq E(\rho) + E(\sigma)$.*

Another similar although not identical version is the following:

Axiom E4b *(Weak additivity). For every state ρ it holds $E\left(\rho^{\otimes N}\right) = NE(\rho)$.*

Entanglemt of formation and concurrence for qubits

A possible definition of entanglement that satisfies the axioms above is the so-called ***entanglement of formation*** *[see eq. (20)] where we exploit the fact that any mixed state can be decomposed as convex combination of pure states of C, $\rho_C = \sum_i p_i |i\rangle_{CC}\langle i|$ (not to be confused with the notion of separability (19)). Such a combination however is not unique so in the definition we need to choose the minimum (according to Axiom E3) over all possible combinations such that $\sum_i p_i = 1$.*

Unfortunately to date is not known how to carry on, in general, the minimisation procedure in eq. (20). Nonetheless, for a ***mixed state of two qubits*** *in 1998 Wootters [33] was able to find an intricate, though computable, expression for the entanglement of formation passing through the so-called* ***concurrence****. For a generic two-qubits mixed state*

$$E_F(\rho_C) = -\lambda \log \lambda - (1-\lambda)\log(1-\lambda)$$

with $\lambda = (1 + \sqrt{1 - \mathcal{C}^2})/2$ and the concurrence $\mathcal{C}$ in turn is computed explicitly as in eq. (21) where $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4$ are the square roots of the eigenvalues of the 4×4 matrix: $M_W = \rho_C \Sigma_{AB} \rho_C^* \Sigma_{AB}$, with $\Sigma_{AB} = \sigma_A^y \otimes \sigma_B^y$ and ρ_C^* is the conjugated density matrix expressed in the computational basis. It's like as if we would have the von Neumann entropy for a pure two-qubits state in which the density matrix determinant Δ is replaced by $\mathcal{C}^2/4$ in the formal expression of the "eigenvalues" λ and $(1-\lambda)$.

Concurrence versus correlations

Apart from Wootters' formula what is the physical meaning that we can give to the concurrence? For this sake let us see some special cases:

- *Pure states $|\Psi\rangle_C$: By defining the two-spins* ***connected correlation function***

$$Q_{\hat{a}\hat{b}} \equiv_C \langle\Psi|(\vec{\sigma}_A\cdot\hat{a})(\vec{\sigma}_B\cdot\hat{b})|\Psi\rangle_C - {}_C\langle\Psi|\vec{\sigma}_A\cdot\hat{a})|\Psi\rangle_C{}_C\langle\Psi|\vec{\sigma}_B\cdot\hat{b}|\Psi\rangle_C$$

  (where $\hat{a}$ and $\hat{b}$ define two directions to measure A and B spin, respectively) it can be shown that the concurrence is the maximum possible correlation in the sense that

$$\mathcal{C}(|\Psi\rangle_C) = \max_{\hat{a},\hat{b}} Q_{\hat{a}\hat{b}}.$$

- *Mixed states invariant under 3D spatial rotations. It can be shown that $\mathcal{C}(\rho_c)$ in this case reads as in eq. (22) where $\langle\vec{\sigma}_A\cdot\vec{\sigma}_B\rangle = \mathrm{tr}\rho_C\vec{\sigma}_A\cdot\vec{\sigma}_B$. Note that this expectation value is itself a two-spins correlation but different from $Q_{\hat{a}\hat{b}}$ and in particular rotational symmetry is such that $\langle\vec{\sigma}_{A,B}\rangle = 0$. Let us observe further that from the quantum sum of angular momenta $\hbar/2\vec{\sigma}_A$ and $\hbar/2\vec{\sigma}_B$ we find*

$$(\vec{\sigma}_A+\vec{\sigma}_B)^2 = \frac{4}{\hbar^2}S^2_{tot} = \vec{\sigma_A}\cdot\vec{\sigma}_A + \vec{\sigma_B}\cdot\vec{\sigma}_B + 2\vec{\sigma_A}\cdot\vec{\sigma}_B = 2(3\mathbb{I} + \vec{\sigma_A}\cdot\vec{\sigma}_B)$$

  and so $\langle\vec{\sigma}_A\cdot\vec{\sigma}_B\rangle = \frac{2}{\hbar^2}\mathrm{tr}\rho_C S^2_{tot} - 3$. But if ρ_C is rotationally invariant we would have a 1×1 block with eigenvalue p for the singlet sector (0 total spin) and a 3×3 block with eigenvalues $(1-p)/3$ for the triplet (total spin 1) and $\langle S^2_{tot}\rangle = \hbar^2 2$. So $\langle\vec{\sigma}_A\cdot\vec{\sigma}_B\rangle = 4(1-p) - 3 = 1 - 4p$ and being $0\leq p\leq 1$ we find

$$-3 \leq \langle\vec{\sigma}_A\cdot\vec{\sigma}_B\rangle \leq 1.$$

  In the lower bound we have a pure singlet ($p=1$) while in the upper bound we find a triplet mixed state with rotational invariance ($p=0$). From eq. (22) we see that the ***threshold*** *to have $\mathcal{C} > 0$ is given by the condition $\langle\vec{\sigma}_A\cdot\vec{\sigma}_B\rangle < -1$. In fact, the* max *in formula (21) corresponds to the situation where in order to have nonvanishing entanglement (and hence concurrence)* ***it is necessary that there are not only correlations between A and B, but also that these exceed in magntiude a certain threshold****. In this sense we can now affirm that entaglement is not only a generic form of correlation, but the intensity of such a correlation should be sufficiently strong; only in this case purely quantum effects can manifest like for example in the case of Bell inequalities that are violated for $\Delta = \mathcal{C}^2/4 > 0$ (see subsec. 2.4.1). Moreover, the quantity $\varepsilon = -\langle\vec{\sigma}_A\cdot\vec{\sigma}_B\rangle/3$ plays an important role also in the study of so-called quantum communication channels, for instance those that preserve rotational invariance. It can bw shown [10] that starting from an input pure state $|I\rangle$ the employment of such a*

channel in the teleportation procedure described befor in section 2.7 leads Bob to have a mixed state in which only a fraction reproduces Alice's initial state. It is then said that teleportation took place on a ***depolarising channel (see also Appendix 5)***

$$|I\rangle \to \mathcal{T}(|I\rangle) = \varepsilon |I\rangle\langle I| + \frac{1-\varepsilon}{2}\mathbb{I}.$$

Note that $\mathrm{tr}\mathcal{T} = 1$ *as it should be. Let us compute how much close is* $\mathcal{T}$ *to* $|I\rangle\langle I|$ *using the fidelity measure (15):* $F = \langle I|\mathcal{T}|I\rangle = \varepsilon + (1-\varepsilon)/2 = (1+\varepsilon)/2$*, that turns out to be greater than the classical average* ($\bar{F} = 2/3$) *when* $\varepsilon > 1/3$ *that is* $\langle \vec{\sigma}_A \cdot \vec{\sigma}_B \rangle < -1$*, just the threshold to cross in order to have entanglement between* A *and* B*.*

Monogamy inequality

Another feature that marks the difference between the notion of entanglement and the generic one of correlations is that the latter, in many-body systems with local interactions, typically decay with the distance and one particle is very correlated with the closely neighbouring ones, less correlated with next-to-neighbouring ones and so on. However, no maximum limit is present in principle on the total correlations that the particle can have with other ones of the system. In 2006, instead, the so-called ***Coffmann-Kundu-Wootters conjecture*** *was proven by Osborne and Verstraete [24], and it establishes a sort of "monogamy" in entanglement correlations. Given a system composed by various parts (qubits) that we will denote by* A*,* B_1*,* B_2*,... etc. the monogamy inequality eq. (24) dictates that the sum of all squared concurrences* $\mathcal{C}^2(A|B_k)$ *of the bipartite qubit subsystems* $A|B_k$ *(computed through the reduced density matrices* ρ_{AB_k}*) is bounded by the determinant* Δ_A *of the single-qubit density matrix* ρ_A*. Hence it can be appreciated that it is not possible for* A *to be very entangled with various subsystems* B*; if, for example, it is very entangled with* B_1 *then necessarily it should have essentially no entanglement with the remaining ones. The upper bound is in any case* $4\Delta_A$ *that quantifies the global entanglement between* A *and all the rest of the system. The concept expressed in inequality (24) is also depicted in figure 6. The possible difference between the left-hand side and the central term* $4\Delta_A$ *(that could be called one-tangle in this context), when the inequality is not saturated, that is*

$$4\Delta_A - \sum_j \mathcal{C}^2(A|B_j)$$

expresses a form of genuine ***multipartite*** *entanglement, that is not possible to ascribe to pairwise quantum correlations.*

Exercise: *Consider a state of the form*

$$|\Psi\rangle_C = \alpha|0_A 0_{B_1} 0_{B_2} \ldots 0_{B_N}\rangle + \beta|1_A 1_{B_1} 1_{B_2} \ldots 1_{B_N}\rangle$$

where subscripts A *and* B_j *denote* $N+1$ *qubits and* $|\alpha|^2 + |\beta|^2 = 1$ *in order to normalise to unit since the two kets in the superposition are two elements (for*

example the first and last one in a given order) of the computational orthonormal basis for $N+1$ qubits. Now, in order to inspect in detail the inequalities in Coffmann-Kundu-Wootters conjecture let us observe first that the state is completely symmetric under the exchange of any two qubits, so it will suffice to compute the concurrence between A and, for instance, B_1. It can be done via the reduced density matrix

$$\rho_{AB_1} = Tr_{B_2 \ldots B_N} \rho_C = Tr_{B_2 \ldots B_N} |\Psi\rangle_{CC}\langle\Psi|$$

By expanding the four terms with coefficients $|\alpha|^2$, $|\beta|^2$, $\alpha^*\beta$ e $\alpha\beta^*$ from the expression of the state $|\Psi\rangle_{CC}\langle\Psi|$ within the Trace above it is seen that only two give nonvanishing contribution, because the trace operation is the sum of diagonal matrix elements taken on a basis for $N-1$ qubits $B_2 \ldots B_N$ and, again, this basis can be chosen as the computational one. Then we will have as nonvanishing contributions only those comping from the states $|00\rangle_{AB_1} \otimes |0 \ldots 0\rangle_{B_1 \ldots B_N}$ and $|11\rangle_{AB_1} \otimes |1 \ldots 1\rangle_{B_1 \ldots B_N}$ (that are mutually orthogonal); in the notation we have put in explicit the tensor product to outline how the elements in the N+1-qubits basis are built from that of $N-1$ qubits. From the partial trace on $B_2 \ldots B_N$ there remain

$$\rho_{AB_1} = |\alpha|^2 |00\rangle_{AB_1 AB_1}\langle 00| + |\beta|^2 |11\rangle_{AB_1 AB_1}\langle 11|$$

that in AB_1 computational basis has the form

$$\rho_{AB_1} = \begin{pmatrix} |\alpha|^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & |\beta|^2 \end{pmatrix}.$$

It is worth observing that this matrix represents the mixed state of AB_1 that in turn are part of the system C, described by a global pure state. With the same philosophy we readily compute also the partial trace on B, so to have the density matrix for qubit A

$$\rho_A = Tr_{B_1 \ldots B_N} |\Psi\rangle_{CC}\langle\Psi| = Tr_{B_1} \rho_{AB_1} = |\alpha|^2 |0\rangle_{AA}\langle 0| + |\beta|^2 |1\rangle_{AA}\langle 1|.$$

The ***entanglement of A with all the rest*** *(that is qubits $B_1 B_2 \ldots B_N$) is parametrised through the determinant*

$$\Delta_A = |\alpha|^2 |\beta|^2 = |\alpha|^2 (1 - |\alpha|^2)$$

while the entanglement that exists between A and B_1 in the mixed state ρ_{AB_1} we use just Wootters concurrence. Having no particular symmetries under rotation we need to use formula (21), building first the auxiliary matrix $\Sigma_{AB_1} = \sigma_A^y \otimes \sigma_{B_1}^y$. In computational basis let us employ the formula in appendix A

$$\Sigma_{AB_1} = \begin{pmatrix} 0 & -i\sigma^y \\ i\sigma^y & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

Since ρ_{AB_1} in this example turns out to be real in computational basis we have a simplification $M_W = (\rho_{AB_1}\Sigma_{AB_1})^2$, yielding

$$M_W = \begin{pmatrix} 0 & 0 & 0 & -|\alpha|^2 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -|\beta|^2 & 0 & 0 & 0 \end{pmatrix}^2 = |\alpha|^2|\beta|^2 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Notice that M_W is not a reduced density matrix and, for every α and β, the eigenvalues are always $\lambda_1 = \lambda_2 = |\alpha|^2|\beta|^2$ and $\lambda_3 = \lambda_4 = 0$, so that in eq. (21) $\mathcal{C} = 0$. Monogamy inequality (24) then reads $0 + \ldots + 0 \leq 4|\alpha|^2(1 - |\alpha|^2) \leq 1$, that means that whenever $|\alpha| \neq 0, 1$ an entanglement between A and the qubit group $B_1B_2\ldots B_N$ is "switched on" but the entanglement between A and any of the B_j is always zero. We will speak in this case of multipartite entanglement that cannot be ascribed to bipartite entanglement. If $|\alpha| = |\beta| = 1/\sqrt{2}$ we have maximum entanglement between A and the rest and the corresponding state $|\Psi\rangle_C$ is termed Greenberger-Horne-Zeilinger (GHZ), a state that is particularly employed as computational quantum resource in various protocols.

3.5 Testimoni (witness) di entanglement

La difficoltà di trovare misure quantitative per stati misti e quella di misurare poi realmente le quantità microscopiche che ci permettono di risalire al contenuto di entanglement in sistemi estesi ha portato ad un concetto forse più operativo denominato **testimone di entanglement**. Per capire l'idea enunciamo subito il **teorema degli Horodecki** [20]:

> Per ogni stato misto bipartito ed entangled ρ_C, cioè tale che **non** lo si può scrivere nella forma (19) esiste sempre un operatore W tale che $\langle W\rangle = \mathrm{tr}\rho_C W < 0$ e che $\tilde{W} = \mathrm{tr}\tilde{\rho}_C W > 0$ per ogni $\tilde{\rho}_C$ separabile.

Vediamo ora un esempio interessante di testimone di entanglement nel contesto dei sistemi magnetici quantistici a bassa temperatura [21]. Consideriamo N particelle a spin s in un campo magnetico esterno $\vec{B}$. Si chiama **suscettività magnetica** la variazione della magnetizzazione totale $\vec{M} = \sum_i \langle \vec{s}_i\rangle$ rispetto al campo applicato. Per le tre componenti spaziali $a = x, y, z$

$$\chi^a = \frac{\partial M^a}{\partial B^a}.$$

In meccanica statistica [22], per un ensemble canonico con Hamiltoniana H_0, la magnetizzazione si ottiene a sua volta per derivazione rispetto al campo esterno

$$M^a = \mathrm{tr}\rho_{\mathrm{canonica}} \sum_i s_i^a = \mathrm{tr}\frac{e^{-\beta(H_0 - B^a \sum_j s_j^a)}}{Z} \sum_i s_i^a = K_B T \frac{\partial \ln Z}{\partial B^a},$$

dove abbiamo usato la funzione di partizione canonica $Z = \mathrm{tr}\exp(-\beta H)$ associata ad una Hamiltoniana totale $H = H_0 - B^a \sum_i s_i^a$ e abbiamo assunto $[H, \sum_i s_i^a] = 0$. Quindi, applicando la derivata seconda, troviamo per la suscettività

$$\chi^a = \frac{\langle (M^a)^2 \rangle - \langle M^a \rangle^2}{K_B T} = \frac{1}{K_B T} \left(\sum_{i,j=1}^{N} \langle s_i^a s_j^a \rangle - \left\langle \sum_i s_i^a \right\rangle^2 \right) = \frac{\mathrm{Var}(S_{tot}^a)}{K_B T}$$

ossia χ^a risulta proporzionale alla varianza (fluttuazione) quanto-statistica dello spin totale $S_{tot}^a = \sum_i s_i^a$. Una relazione di questo tipo prende il nome di **teorema di fluttuazione-dissipazione** perché, appunto, si lega una risposta del sistema alle fluttuazioni di una opportuna quantità osservabile (nello specifico suscettività e magnetizzazione, rispettivamente).

Consideriamo ora stati misti, a causa del bagno termico (pedice τ), ma separabili negli N spin

$$\rho = \sum_\tau w_\tau \rho_\tau^1 \otimes \rho_\tau^2 \otimes \ldots \otimes \rho_\tau^N .$$

Per ciascuno degli stati $\rho_\tau = \rho_\tau^1 \otimes \rho_\tau^2 \otimes \ldots \otimes \rho_\tau^N$ nella somma abbiamo $\langle s_i^a s_j^a \rangle_\tau = \mathrm{tr}\rho_\tau s_i^a s_j^a = \langle s_i^a \rangle_\tau \langle s_i^a \rangle_\tau$ per $i \neq j$ e così isolando il termine $i = j$ troviamo

$$\chi_\tau^a = \frac{1}{K_B T} \sum_i \left[\langle (s_i^a)^2 \rangle_\tau - \langle s_i^a \rangle_\tau^2 \right].$$

A questo punto, possiamo immaginare di misurare le suscettività lungo le tre componenti spaziali ortogonali e lasciare tendere il campo magnetico a zero, in modo che la relazione di fluttuazione-dissipazione valga simultaneamente per $a = x, y, z$. Ma dalla trattazione quantistica del momento angolare sappiamo che $\langle \vec{s}_i^2 \rangle = \hbar^2 s(s+1)$ ed invece il modulo quadro del vettore valore di aspettazione $\vec{m}_i = \langle \vec{s}_i \rangle$ soddisfa $\vec{m}_i^2 \leq \hbar^2 s^2$ (si veda in appendice) così che

$$\chi_\tau^x + \chi_\tau^y + \chi_\tau^z \geq \frac{\hbar^2}{K_B T} \sum_i [s(s+1) - s^2] = \frac{\hbar^2 N s}{K_B T}.$$

Infine, osservando che

$$\chi^a = \beta \mathrm{Var}(S_{tot}^a) = \beta \mathrm{tr}\rho (S_{tot}^a - \langle S_{tot}^a \rangle)^2 = \beta \sum_\tau w_\tau \mathrm{tr}\rho_\tau (S_{tot}^a - \langle S_{tot}^a \rangle)^2$$

possiamo scrivere la disuguaglianza

$$\chi^x + \chi^y + \chi^z - \frac{\hbar^2 N s}{K_B T} \geq 0 \tag{25}$$

per ogni stato ρ tale che $\sum_\tau w_\tau = 1$. L'uguaglianza vale nel caso in cui per ogni spin lo stato abbia varianza minima, il che accade quando $\langle s_i^x \rangle^2 + \langle s_i^y \rangle^2 + \langle s_i^z \rangle^2 =$

s^2, ossia lo stato è puro e con autovalore massimo s di s_i^z lungo una certa direzione. Qualsiasi violazione della disuguaglianza (25) è invece da attribuire ad una qualche forma di entanglement nello stato a N spin ρ.

Misurando la suscettività lungo i tre assi coordinati abbiamo quindi un testimone di entanglement; qualitativamente, tanto più bassa è T tanto maggiore è il peso del termine con coefficiente negativo e quindi per una temperatura sufficientemente bassa ci aspettiamo di entrare in una regione in cui gli spin del sistema sono entangled. Aumentando la temperatura invece si aumenta pure l'energia media e gli spin tenderanno a disordinarsi distruggendo correlazioni ed entanglement. In realtà anche la suscettività non è costante ma dipende da T e quindi per determinare con precisione a quale temperatura questo "entanglement termico" si manifesta bisogna conoscere tale dipendenza risolvendo il modello in esame o effettuando una serie di misure di magnetizzazione al variare della temperatura.

Entanglement witnesses

The difficulty in finding quantitative measures for mixed states and in measuring practically the microscopic quantities that are related to th entanglement content in extended systems led to a concept that is maybe more useful on practical grounds, ***entanglement witnesses****. In order to understand the idea let us state first* ***Horodeckis' theorem*** *[20]:*

> *For every mixed bipartite entangled state ρ_C, that hence* ***cannot*** *be expressed in the form (19), there exists always an operator W such that $\langle W\rangle = \mathrm{tr}\rho_C W < 0$ and that $\tilde{W} = \mathrm{tr}\tilde{\rho}_C W > 0$ on every separable $\tilde{\rho}_C$.*

Let us now see an interesting example of entanglement witness in the context of quantum magnetic systems at low temperature [21]. Let us consider N particles with spin s in an external magnetic field $\vec{B}$. ***Magnetic subsceptibility*** *is the variation of the total magnetisation $\vec{M} = \sum_i \langle \vec{s}_i\rangle$ with respect to the applied field. For the three spatial components $a = x, y, z$*

$$\chi^a = \frac{\partial M^a}{\partial B^a}.$$

In statistical mechanics [22], for a canonical ensamble with Hamiltonian H_0, the magnetisation is obtained in turn by differentiating with respect to the external field

$$M^a = \mathrm{tr}\rho_{\mathrm{canonica}} \sum_i s_i^a = \mathrm{tr}\frac{e^{-\beta(H_0 - B^a \sum_j s_j^a)}}{Z} \sum_i s_i^a = K_B T \frac{\partial \ln Z}{\partial B^a},$$

where we have used the canonical partition function $Z = \mathrm{tr}\exp(-\beta H)$ associated to the total Hamiltonian $H = H_0 - B^a \sum_i s_i^a$ and have assumed $[H, \sum_i s_i^a] = 0$.

Hence, by applying second derivative, we obtain for the subsceptibility

$$\chi^a = \frac{\langle (M^a)^2 \rangle - \langle M^a \rangle^2}{K_B T} = \frac{1}{K_B T} \left(\sum_{i,j=1}^{N} \langle s_i^a s_j^a \rangle - \left\langle \sum_i s_i^a \right\rangle^2 \right) = \frac{\mathrm{Var}(S_{tot}^a)}{K_B T}$$

that is, χ^a becomes proportional to the quantum-statistical variance (fluctuation) of the total spin $S_{tot}^a = \sum_i s_i^a$. A relation of this kind is usually termed fluctuation-dissipation theorem because it relates a response of the system to the fluctuations of a certain observable (subsceptibility and magnetisation, respectively, in the specific case).

Now let us consider mixed states, due to the thermal bath (subscript τ) but separable from the point of view of the N spins

$$\rho = \sum_\tau w_\tau \rho_\tau^1 \otimes \rho_\tau^2 \otimes \ldots \otimes \rho_\tau^N.$$

For every single state $\rho_\tau = \rho_\tau^1 \otimes \rho_\tau^2 \otimes \ldots \otimes \rho_\tau^N$ in the sum we find $\langle s_i^a s_j^a \rangle_\tau = \mathrm{tr} \rho_\tau s_i^a s_j^a = \langle s_i^a \rangle_\tau \langle s_i^a \rangle_\tau$ for $i \neq j$ and by isolating the term $i = j$ we get

$$\chi_\tau^a = \frac{1}{K_B T} \sum_i \left[\langle (s_i^a)^2 \rangle_\tau - \langle s_i^a \rangle_\tau^2 \right].$$

At this stage we can imagine to measure the subsceptibility along the three spatial components and to let the magnetic field go to zero, so that the fluctuation-dissipation relation holds simultaneously for $a = x, y, z$. But from the theory of quantum angular momentum we know that $\langle \vec{s}_i^2 \rangle = \hbar^2 s(s+1)$ and the modulus square of the expectation value vector $\vec{m}_i = \langle \vec{s_i} \rangle$ satisfies $\vec{m}_i^2 \leq \hbar^2 s^2$ (see appendix) so that

$$\chi_\tau^x + \chi_\tau^y + \chi_\tau^z \geq \frac{\hbar^2}{K_B T} \sum_i [s(s+1) - s^2] = \frac{\hbar^2 N s}{K_B T}.$$

Finally, by observing that

$$\chi^a = \beta \mathrm{Var}(S_{tot}^a) = \beta \mathrm{tr} \rho (S_{tot}^a - \langle S_{tot}^a \rangle)^2 = \beta \sum_\tau w_\tau \mathrm{tr} \rho_\tau (S_{tot}^a - \langle S_{tot}^a \rangle)^2$$

we can write down the inequality in eq. (25) for every state ρ such that $\sum_\tau w_\tau = 1$. The equality holds in the case of minimum variance of for every spin state, that happens when $\langle s_i^x \rangle^2 + \langle s_i^y \rangle^2 + \langle s_i^z \rangle^2 = s^2$, that is the state is pure and with maximal eigenvalue s of s_i^z along a certain direction. Any violation of the inequality, instead, is to be ascribed to some form of entanglement in the N-spins state ρ.

By measuring the subsceptibility along the three orthognal axes we then find an entanglement witness; qualitatively, the lower is T the higher is the weight of the term wit h negative coefficient and for a sufficiently low temperature we expect to enter a region in which the spins of the system are entangled. By

raising the temperature instead also the average energy increases and spins will tend to disorder, destroying correlations and entanglement. To be precise also the subsceptibility is not a constant but rather depends on T and hence to pinpoint with accuracy the temperature for which this "thermal entanglement" appears we need to know the actual dependence by solving the model or through magnetisation measurements at varying temperature.

4 Alcuni risultati sull'entanglement in sistemi a molti corpi

Nelle sezioni precedenti abbiamo visto che risultati di carattere abbastanza generale sulla presenza e quantità di entanglement bipartito si hanno o nel caso di un sistema complessivamente puro diviso in due parti A e B, oppure per due qubit in uno stato complessivamente misto tipicamente a causa del fatto che si trovano in un ambiente e/o in sistema piu' ampio. Se con l'utilizzo di testimoni di entanglement rinunciamo in qualche modo ad avere una misura quantitativa ed una condizione necessaria e sufficiente per la presenza di entanglement, un'altra via possibile, discussa in questa sezione, è quella di prendere in considerazione alcuni modelli specifici e non banali per i quali esistono formulazioni analitiche dello stato fondamentale e degli stati eccitati, così da poter valutare esplicitamente le espressioni viste in precedenza per entropia e concorrenza.

Prima di procedere in tal senso però soffermiamoci a constatare che, sulla base di un'equazione tipo la (18) per la entropia di von Neumann o delle considerazioni della sezione 3.4.2, ci possiamo già aspettare che una misura opportuna di entanglement sia in ultima analisi espressa in termini delle varie funzioni di correlazione che coinvolgono i gradi di libertà della parte di sistema, diciamo A, che stiamo considerando per valutare l'entanglement con il resto (nel caso dell'entropia) o al suo interno (ad esempio nel caso di concorrenza di qubit).

Per fissare le idee consideriamo sempre sistemi con un numero finito di gradi di libertà, tipicamente sistemi su un reticolo spaziale C costituito da N siti in cui si trovano qudit il cui spazio di Hilbert locale ha dimensione d_i. Se A è il sottoreticolo di C con n siti, il suo spazio di Hilbert avrà la forma $\mathcal{H}_A = \otimes_{i=1}^{n} \mathcal{H}_i$ e la matrice densità ridotta $\rho_A = \mathrm{tr}_B \rho_C$ è un operatore che rimane espresso come matrice $d_A \times d_A$ (con $d_A = \Pi_{i=1}^{n} d_i$) una volta che è definita una specifica base di stati su $\mathcal{H}_A$. In quanto tale ci sarà però anche una **base di operatori** η_K su cui esprimere linearmenteρ_A

$$\rho_A = \sum_K r_K \eta_K.$$

Se nello spazio degli operatori su $\mathcal{H}_A$ è assegnato un prodotto scalare (O_A, O'_A) allora i coefficienti r_K risultano dall'espressione $r_K = (\eta_K, \rho_A)$ purchè gli operatori di base siano ortonormali

$$(\eta_K, \eta_J) = \delta_{KJ}.$$

Stiamo usando indici maiuscoli K, J, ... per indicare che il loro numero in generale è pari alla dimensione ossia al numero di parametri complessi della matrice d_A^2. Tuttavia, essendo la ρ_A hermitiana, il numero effettivo di parametri indipendenti risulta da d_A numeri reali sulla diagonale e $(d_A^2 - d_A)/2$ numeri complessi fuori diagonale; inoltre si ha un vincolo $\mathrm{Tr_A}\rho_\mathrm{A} = 1$ che riduce il numero di parametri reali indipendenti che risulta quindi $d_A^2 - 1$. L'esempio che già si è visto è quello della sfera di Bloch per un qubit (d_A=2) caratterizzata dal vettore $\vec{n}$ e per la quale gli operatori di base normalizzati sono $\mathbb{I}_A/\sqrt{2}$ e $\sigma_A^{x,y,z}/\sqrt{2}$. In generale possiamo usare come prodotto scalare quello definito dalla traccia

$$(O_A, O'_A) = \mathrm{Tr}_A O_A^\dagger O'_A$$

e i coefficienti che definiscono la matrice densità risultano dall'espressione

$$r_K = \mathrm{Tr}_A \rho_A \eta_K = \langle \eta_K \rangle_A \tag{26}$$

avendo usato la ciclicità della traccia, la hermiticità di ρ_A e la relazione (9) che esprime i valori di aspettazione quanto-meccanici (esiti di misura) su stati definiti da matrici densità. L'ultima equazione si può quindi interpretare dicendo che **i parametri che definiscono la matrice densità sono in ultima analisi valori di aspettazione di operatori - ossia determinate osservabili - definite fisicamente su A. Quando A si estende su piu' siti allora i valori di aspettazione $\langle \eta_K \rangle_A$ sono di fatto le diverse funzioni di correlazione che coinvolgono i siti di A.**

Questa costruzione concettuale però è di scarsa utilità pratica specialmente se il numero di siti che supportano la matrice densità ρ_A è elevato. La connesione tra matrice densità/entanglement e correlazioni si può rendere più trasparente per una serie di modelli cosiddetti liberi, nei quali l'operatore densità ha una forma che può essere congetturata sulla base della forma della Hamiltoniana del sistema globale H_C. Nel formalismo della seconda quantizzazione per fermioni una Hamiltoniana del tipo

$$H_C = -\frac{1}{2} \sum_{\langle m,r \rangle} t_{mr} c_m^\dagger c_r \tag{27}$$

dove la matrice di accoppiamento tra i siti primi vicini m ed r (la condizione di primi vicini è indicata da $\langle m, r \rangle$) è hermitiana $t_{mr} = t_{rm}^*$ (affinchè lo sia la Hamiltoniana) e gli operatori c_r definiscono particelle fermioniche senza spin sul sito r-esimo, è detta appunto libera visto che è in un'ultima analisi quadratica negli operatori fondamentali. Questi operatori debbono soddisfare le regole di anticommutazione:

$$\{c_r^\dagger, c_m\} = \delta_{mn} \ , \ \{c_r, c_m\} = 0$$

e se l'indice r si riferisce unicamente al sito r il significato sarà che viene creata una particella dal vuoto con l'azione $c_r^\dagger |\emptyset\rangle$ avendo definito il vuoto $|\emptyset\rangle$ come lo stato distrutto da *tutti* gli operatori c_m sul reticolo. Anche se la eq. (27) non è

già scritta in forma esplicita come operatori numero $N_r = c_r^\dagger c_r$, che hanno autovalori 0 o 1 per ogni r, la si può diagonalizzare invocando la diagonalizzabilità di t_{mr}

$$t_{mr} = \sum_{ij} (P^\dagger)_{mi} (\Lambda)_{ij} (P)_{jr}$$

dove Λ è la matrice diagonale degli autovalori ω_i di t e P è il cambio di base (trasformazione canonica sugli operatori)

$$\gamma_j = \sum_r P_{jr} c_r$$

che porta a

$$H_C = -\frac{1}{2} \sum_{ij} \gamma_i^\dagger (\Lambda)_{ij} \gamma_j = -\frac{1}{2} \sum_i \omega_i \gamma_i^\dagger \gamma_i$$

per cui gli stati a molti corpi sono costruiti semplicemente dagli stati a un corpo definiti dagli autovalori dei nuovi operatori numero $\gamma_i^\dagger \gamma_i$. In verità fino a qua abbiamo supposto, secondo la (27), che i fermioni fossero senza spin e si muovessero su reticolo per effetto del termine di *hopping* t_{mr} che parametrizza il processo per cui viene distrutta una particella in un sito e ricreata nel sito primo vicino, ma la struttura che porta alla diagonalizzazione in termini dei nuovi operatori γ è generale fin tanto che la Hamiltoniana è quadratica tipo $c^\dagger c$ e i pedici degli stati si possono riferire a qualunque insieme completo di stati di particella singola. Pertanto non è realmente necessario richiedere che gli indici siano spaziali e ristretti solo ai primi vicini. Ritorneremo su questo punto nella sottosezione 4.2 per discutere l'estensione spaziale dell'entanglement e delle correlazioni.

La diagonalizzabilità in termini dei nuovi fermioni γ però non è l'unico pregio dei sistemi tipo (27); per quanto ci interessa qua la cosa notevole, discussa nella referenza di Peschel e Eisler [25], è che la struttura libera della Hamiltoniana consente di scrivere una forma compatta ed esplicita per la matrice densità ridotta

$$\rho_A = \mathcal{K} \exp(-\sum_{m,r}^{n} h_{mr} c_m^\dagger c_r)$$

dove $\mathcal{K}$ è una costante opportuna di normalizzazione in modo che $\mathrm{Tr}_A \rho_A = 1$ e la somma si estende agli n siti del sottosistema A considerato. La cosa notevole è che la matrice densità risulta un esponenziale di un operatore bilineare nei c_r. Questo fatto è legato ad un risultato noto nella teoria dei sistemi a molti corpi, il teorema di Wick per sistemi quadratici, che stabilisce che qualunque funzione di correlazione a p corpi della forma $\langle c_{m_1}^\dagger \dots c_{m_p}^\dagger c_{r_1 \dots} c_{r_p} \rangle$ (con un ugual numero di operatori di creazione e distruzione, altrimenti non si avrebbe la conservazione del numero di fermioni) si riconduce ad opportune combinazioni di p correlazioni di coppia $\langle c_m^\dagger c_r \rangle$ per tutte le possibili coppie m ed r (prese con opportuni segni). Abbiamo prima stabilito che ρ_A è esprimibile su una base di operatori η_K, qua il fatto notevole è che seppur gli operatori η_K abbiano supporto su n siti, il tutto si riesce a ricompattare come espressioni di tutte le possibili correlazioni di coppie

di siti in A. Un punto non banale è come determinare la matrice h_{mr}. Sappiamo però da una formula tipo la (26) che le funzioni di correlazione stesse su siti di A sono ottenibili come valori di aspettazione e di conseguenza coinvolgono ρ_A stessa. Per autoconsistenza richiediamo che h_{mr} sia fatta proprio in modo tale da riprodurre con la matrice ρ_A che genera i corretti valori di aspettazione a due punti. In forma matriciale si trova la relazione [25]

$$\mathbb{H} = \ln[(\mathbb{I} - \mathbb{C})/\mathbb{C}]$$

da intendersi appunto come legame tra le matrici $\mathbb{H}$ di elementi h_{mr} e $\mathbb{C}$ di elementi $c_{mr} \equiv \langle c_m^\dagger c_r \rangle$.

4.1 Entropie di Rényi e spettro di entanglement

Nella sottosezione 3.3 abbiamo discusso come l'entropia di von Neumann rappresenti una misura rigorosa di entanglement tra due parti di un sistema complessivamente puro. Nella letteratura riguardante il concetto e l'uso dell'entropia sono state introdotte, prima classicamente poi per estensione anche quantisticamente, delle **entropie generalizzate dette di Rényi**. Una volta noti gli autovalori λ_i di ρ_A possiamo definire una sorta di momento α-esimo

$$S_\alpha = \frac{1}{1-\alpha} \ln \sum_i \lambda_i^\alpha$$

detto appunto entropia di Rényi di ordine α della distribuzione $\{\lambda\}$. Per sistemi finiti l'espressione non ha problemi di convergenza e rimane definita per ogni α, almeno positivo. La versione quantomeccanica operatoriale dell'entopia generalizzata α-esima è $S_\alpha = \frac{1}{1-\alpha} \ln \mathrm{tr} \rho^\alpha$. Il caso $\alpha = 1$ che sembra singolare si può trattare nel limite. Usando la regola di de l'Hôpital in α troviamo

$$S_1 = \lim_{\alpha \to 1} S_\alpha = -\sum_i \lambda_i \ln \lambda_i$$

cioè proprio la entropia di Shannon/von Neumann. Un altro caso scrivibile facilmente ed utilizzato nella letteratura tecnica sull'informazione quantistica è la entropia (o entanglement) di singola copia. Tornando alla distillazione ci possiamo anche chiedere cosa accade prendendo non molte copie ma una sola dello stato $|\Psi\rangle_C$. Se con operazioni OLCC su una sola copia si ottiene uno stato massimamente entangled di "lunghezza" massima M ossia (non normalizzato) lo stato bipartito a pesi uguali $|0,0\rangle_{A,B} + \ldots |M-1, M-1\rangle_{A,B}$ allora diciamo che nello stato di partenza c'era un entanglement di singola copia $\log M$. Ora, prendiamo proprio l'autovalore più grande di ρ_A, diciamo $\lambda_{\max}$, con degenerazione $g_{\max}$. Vediamo cosa accade nella equazione per S_α quando $\alpha \gg 1$: Raccogliendo il termine dominante

$$\sum_i \lambda_i^\alpha = \lambda_{\max}^\alpha \sum_i \left(\frac{\lambda_i}{\lambda_{\max}} \right)^\alpha \approx g_{\max} \lambda_{\max}^\alpha$$

da cui $\ln \sum_i \lambda_i \approx \alpha \ln \lambda_{\max} + \ln g_{\max}$ e nel limite $\alpha \to \infty$

$$S_\infty = \lim_{\alpha \to \infty} S_\alpha = -\ln \lambda_{\max} = \ln(1/\lambda_{\max}).$$

Quindi formalmente l'autovalore massimo di ρ_A esprime l'entanglement di singola copia che si può distillare dallo stato bipartito come entropia di Rényi di ordine infinito. E' un concetto utile sul piano pratico perché in diversi problemi di meccanica statistica è accessibile magari solo l'autovalore massimo e non tutto lo spettro di ρ_A.

Nella letteratura dell'informazione quantistica per questi motivi lo spettro $\{\lambda\}$ viene detto **spettro di entanglement**. La formula delle entropie di Rényi suggerisce che il passaggio dallo spettro di entanglement a $S_\alpha \forall \alpha$ in qualche modo è una trasformata e l'informazione contenuta complessivamente negli λ_i viene trasferita nell'entropia di Rényi intesa come funzione di α. Nella referenza di Peschel e Eisler [25] ci sono diversi esempi di spettro di entanglement derivati per sistemi integrabili e/o con approcci numerici. Qua ci vogliamo focalizzare su quello dei **sistemi fermionici critici**.

4.2 Sistemi fermionici critici e legge dell'area

Ritorniamo all'ipotesi che i coefficienti di *hopping* nella Hamiltoniana (27) siano a primi vicini $\langle m, r \rangle$. Come detto questo non è necessario per la diagonalizzabilità dell'intero spettro ma fisicamente il fatto di avere "interazioni" a corto raggio (o locali) ha delle implicazioni importanti per l'entanglement. Intanto ricordiamo che nella meccanica statistica classica e quantistica si possono avere modelli e sistemi con un raggio di interazioni finito e in determinate condizioni, dette critiche, la lunghezza di correlazione ξ (ossia la scala caratteristica con cui decadono le funzioni correlazione) può comunque divergere. Questo segnala l'insorgere di un fenomeno collettivo spesso caratterizzato da invarianza di scala (il sistema appare simile a sè stesso osservandolo a diverse scale, superiori a quelle atomiche). Ora, una relazione tipo la (22) ci ricorda che l'entanglement è sì una forma di correlazione ma poiché misura la parte genuinamente quantistica ci aspettiamo che decada spazialmente non più lentamente delle correlazioni stesse. Quindi, in un sistema C in cui ξ è limitata, ci aspettiamo anche che dividendolo in due parti A e B **l'entaglement tra di esse sia limitato da quanto è grande la regione di spazio in cui si instaurano le correlazioni significative tra A e B**. Fisicamente queste sono indotte dalle interazioni a corto raggio e con una formula nota come **legge dell'area** si congettura [16] che l'entropia di von Neumann scali secondo la legge

$$S_A \propto |\partial_A| \propto N^{(D-1)/D} \tag{28}$$

dove $|\partial_A|$ è la misura della frontiera tra A e B (stiamo considerando qua solo il caso di partizioni spaziamente regolari, cioè non frattali, ecc.) e la seconda proporzionalità nasce dal fatto che in un (sotto)sistema con N siti in D dimensioni la estensione lineare va come $N^{1/D}$ e la frontiera come la potenza $(D-1)$-esima. Si noti che per l'entropia termodinamica di un sistema all'equilibrio termico ci

aspetteremmo che questa fosse estensiva, ossia scalasse come N. Quale è l'origine di tale discrepanza? Intanto si noti che siamo legittimati a pensare S_A sia come entropia di entanglement che come quantità termodinamica solo se appunto B è quel sistema che realizza per A l'equilibrio termico. Inoltre il concetto di entropia di entanglement richiede che C sia complessivamente puro, ossia la matrice densità ρ_A deriva da una traccia parziale di $|\Psi\rangle_{CC}\langle\Psi|$, ma non è detto in generale che ρ_A con questa costruzione abbia una forma termica alla Boltzmann (nel caso canonico, ad esempio). Infine, la legge dell'area (28) è un comportamento che tipicamente ci si aspetta nei casi in cui $|\Psi\rangle_C$ è uno stato speciale del sistema a molti corpi, frequentemente lo **stato fondamentale di** H_C. Richiamiamo qua il teorema 10 di referenza [16] che permette di mettere in relazione il decadimento delle funzioni di correlazione con un limite superiore all'entanglement bipartito:

> Se le funzioni di correlazione sullo stato fondamentale nondegenere di una Hamiltoniana fermionica libera soddisfano
>
> $$\langle c_m^\dagger c_r\rangle \leq \frac{K_0}{\|R_m - R_r\|^\eta}$$
>
> per una certa costante K_0 ed un esponente η superiore a $D+1$ (dove nel denominatore si ha la distanza sul reticolo dei siti m ed r supposti distinti), allora
>
> $$S \leq K_0 C_D \zeta(1+\epsilon)|\partial_A|$$
>
> dove la costante C_D dipende solo dalla dimensionalità e ζ è la funzione di Riemann nel cui argomento compare $\epsilon = (\eta - D - 1)/2$.

In sostanza, finché lo stato fondamentale è unico con correlazioni che decadono in modo sufficientemente rapido l'entropia di von Neumann segue strettamente una legge dell'area.

Per via della sua importanza nel contesto della fisica dei buchi neri, ed anche nello sviluppo storico della legge dell'area, va ricordato che un andamento simile, cioè sub-estensivo con l'area e non con il volume, si ha nella **entropia termodinamica di Bekenstein-Hawking**

$$S_{BH} = \frac{K_B c^3 \mathcal{A}_h}{4G\hbar}$$

dove c, $\hbar$, G e K sono tutte costanti fondamentali e $\mathcal{A}_h$ è l'area associata all'orizzonte degli eventi del buco nero. Poiché in questo contesto stiamo trattando di informazione, solo a titolo informativo possiamo anche richiamare la congettura detta **principio olografico**, che (anche a seguito dei risultati esatti nel caso conforme di sotto) si enuncia dicendo che per un sistema fisico contenuto in un dato volume la informazione al suo interno si può rappresentare equivalentemente attraverso una opportuna teoria di campo definita invece sulla frontiera del volume stesso.

Il caso $D = 1$ è in qualche modo peculiare perché la equazione (28) significa che in un sistema bipartito unidimensionale con interazioni a corto raggio la entropia **non cresce** con la taglia (ossia il numero di siti) del sistema N. In effetti in una catena di siti in cui si realizza una bipartizione il numero di siti di frontiera che collega le due parti è comunque un numero finito di punti anche quando $N \to \infty$ (a meno che non si faccia una bipartizione tipo "pettine" in cui A e B sono due sottoreticoli che si compenetrano). **Anche se il numero di gradi di libertà del sistema cresce sempre più la quantità di entanglement che il sistema può supportare nella bipartizione è comunque finita.** C'è però una eccezione, o meglio una correzione, alla eq. (28) che va apportata nel caso di sistemi critici in cui le interazioni sono a corto raggio ma (per effetto cooperativo delle correlazioni termiche e/o quantistiche) si ha una lunghezza di correlazione $\xi \to \infty$ che segnala appunto la criticità del sistema. Grazie a risultati esatti e all'approccio conforme (vedi sotto), supportati da numerose simulazioni, si può stabilire che nel caso critico la legge dell'area in un sistema quantistico unidimensionale può avere una correzione logaritmica del tipo $S \propto \ln N$. In tal caso è conveniente scrivere $S \propto \ln \xi$, per comprendere il fatto che fin tanto che ξ è finita anche S lo è, ma nel caso critico l'entanglement misurato da S tende a divergere. La questione è perché la divergenza sia logaritmica. Rigorosamente in meccanica statistica classica un sistema può divenire critico solo nel limite $N \to \infty$ (cfr. teorema di Lee-Yang), ma un sistema a taglia finita che si "appresta" ad essere critico ha una lunghezza di correlazione che solitamente cresce come N. Quindi, con l'espressione $S \propto \ln \xi$, unita alla relazione di scala $\xi \propto N$ per un sistema quasi-critico a taglia finita, si esprime la legge dell'area in 1D sia nel caso critico che in quello non critico a ξ finita.

Ad esempio in un modello unidimensionale di fermioni con *hopping* a primi vicini $t_{mr} = \delta_{m,r\pm1}$ è possibile vedere calcolare direttamente il correlatore e stabilire che il modello è critico nel senso appena detto poiché la matrice delle correlazioni decade come

$$\langle c_m^\dagger c_r \rangle = \frac{\sin[k_F(m-r)]}{\pi(m-r)}$$

dove k_F è il momento di Fermi legato alla densità di fermioni sul reticolo N_F/N; indipendentemente dal valore specifico di k_F si vede un andamento algebrico a potenza, ossia senza nessuna scala caratteristica, il che si traduce in $\xi \to \infty$. (Inoltre l'esponente di decadimento è $\eta = 1$ e non siamo nelle condizioni del teorema di sopra.) **Attraverso la costruzione vista all'inizio della sessione si può determinare prima la matrice $\mathbb{C}$ poi la matrice $\mathbb{H}$ e di conseguenza il suo spettro che esponenziato restituisce lo spetto di entanglement $\{\lambda\}$.** Ne risulta che per grandi i gli autovalori decadono come $\lambda_i \approx \exp[-a(\ln i)^2]$ e nei casi non critici a risulta un numero finito ma nei casi critici si ha $a \propto 1/\ln N$ che in ultima analisi implica un decadimento sempre più lento degli autovalori λ_i in funzione dell'indice i e di conseguenza un aumento dell'entropia (perché gli autovalori sensibilmente diversi da 0 sono sempre meno) [25]. In sintesi si dimostra appunto che in questo caso che l'entropia di entanglement scala come il logaritmo di N e la costante di proporzionalità è 1/3 (se il modello ha condizioni

al contorno periodiche, vedi sotto)

$$S_{\mathrm{fsf1D}} = \frac{1}{3} \ln N + \mathcal{O}(1)$$

(il pedice "fsf1D" si riferisce il modello *free spinless fermions in 1D*).

E' interessante a questo punto notare che la costante di proporzionalità si riesce a calcolare esattamente anche nel contesto delle cosiddette **teorie di campo conformi, che in molti casi descrivono i sistemi critici quantistici in $D = 1$ nel regime di basse eccitazioni energetiche**. Un risultato fondamentale è stato derivato da Calabrese e Cardy [11] e fissa la costante di proporzionalità nella formula logaritmica di S vs $\ln N$ alla quantità adimensionale $\nu c/6$ dove ν è appunto il numero di punti di frontiera che dividono il sottosistema A dal suo complemento (ad esempio $\nu = 1$ in un segmento con estremi aperti diviso a metà o $\nu = 2$ in un cerchio con condizioni periodiche diviso in due) e c **è un parametro universale che caratterizza la teoria conforme detto carica centrale** dell'algebra di Virasoro sottostante. Il pregio dell'approccio a teorie conformi di Calabrese e Cardy è che, pur perdendo informazioni dettagliate sul limite reticolare in cui la teoria di campo differisce dal modello su reticolo, nel cosiddetto limite del continuo per cui la lunghezza d'onda in gioco è maggiore del passo reticolare emerge una formula appunto universale valida per una grande serie di modelli critici quantistici unidimensionali, e non solo fermioni liberi. Per l'entropia di entanglement di un segmento di lunghezza N immerso in un dominio di lunghezza L si ha

$$S = \frac{c}{3} \ln \left[\frac{L}{\pi} \sin \left(\frac{\pi N}{L} \right) \right] + c_1'$$

dove abbiamo riportato la formula esatta a taglia finita per il caso di dominio con condizioni periodiche ai bordi (un risultato del tutto simile si ha nel caso di dominio aperto), che coinvolge appunto le due lunghezze N e L (nel limite del continuo abbiamo identificato numero di siti e lunghezza), la carica centrale c e infine la costante non universale c_1' (questa sì dipendente dal modello specifico). Si noti che per $N = L/2$ oppure per $N \ll L$ abbiamo appunto l'andamento in N anticipato sopra. Inoltre, mediante la costruzione nota come trucco delle repliche [11], si riescono a trattare nell'approccio conforme direttamente le potenze dell'operatore densità ρ^α e abbiamo un risultato analitico per la parte universale (e dominante per grandi N) di tutte le entropie di Rényi

$$S_\alpha = \frac{c}{6} \left(1 + \frac{1}{\alpha} \right) \ln N + \mathcal{O}(1)$$

che si riconduce alla formula dell'entropia di von Neumann S per $\alpha \to 1$ e che ci dà, per l'entanglement di singola copia $S_\infty = c/6 \ln N$, ovvero la sua metà.

Concludiamo questa sezione ritornando al caso di dimensionalità spaziale generica richiamando un secondo teorema, specifico per reticoli quadrati ma fisicamente illustrativo, ancora una volta ripreso dalla rassegna di Eisert, Cramer & Plenio [16] che ci serve per capire come può essere violata una legge dell'area pura da correzioni logaritmiche in $D > 1$:

Per una Hamiltoniana fermionica libera definita su reticolo quadrato D-dimensionale (critica) esistono due costanti positive c_0 e c_1 tali che l'entropia di entanglement tra A e B soddisfa

$$c_0|\partial_A| \ln N \leq S \leq c_1|\partial_A|(\ln N)^2$$

dove N è il numero di siti della regione A e $|\partial_A|$ è la misura della frontiera con il complemento B.

5 Altre applicazioni[5]

- Immagini fantasma [2, 28]
- *Quantum Information Meets Quantum Matter -- From Quantum Entanglement to Topological Phase in Many-Body Systems [34]*

Appendice A: Alcune relazioni utili (*Useful relations*)

- Per **matrici di Pauli**:

$$\det \sigma^\alpha = -1 \,, \quad \mathrm{tr}\sigma^\alpha = 0 \tag{29}$$

$$(\sigma^\alpha)^2 = \mathbb{I} \,, \quad \{\sigma^\alpha, \sigma^\beta\} = 2\delta^{\alpha\beta}\mathbb{I} \,, \quad \sigma^\alpha\sigma^\beta = i\epsilon^{\alpha\beta\gamma}\sigma^\gamma + \delta^{\alpha\beta}\mathbb{I}$$

- **Modulo del vettore medio $\vec{m} = \langle\vec{s}\rangle$ per una particella a spin** s. Le componenti (operatori) s^a del vettore di spin si trasformano come un vettore tridimensionale e così pure le componenti m^a del vettore valor medio. Senza perdita di generalità possiamo scegliere la direzione di quantizzazione in modo tale che $m^x = m^y = 0$. Per la componente z avremo allora gli autovalori ed autostati usuali

$$s^z|m\rangle = \vec{s}\cdot\frac{\vec{m}}{\|\vec{m}\|}|m\rangle = \hbar m|m\rangle \,, \quad m = -s, -s+1, \ldots, s-1, s$$

e, per un generico stato misto di spin ρ_s,

$$m^z = \langle s^z\rangle = \mathrm{tr}\rho_s s^z = \sum_{m'}\langle m'|\rho_s s^z|m'\rangle = \hbar\sum_{m'} m'\rho_{s,m'm'} \leq \hbar s\sum_{m'}\rho_{s,m'm'} = \hbar s$$

dato che per le proprietà generali delle matrici densità $\rho_{s,m'm'} = \langle m'|\rho_s|m'\rangle \geq 0$ e $\mathrm{tr}\rho_s = 1$. In conclusione, il modulo del vettore $\vec{m}$ soddisfa alla disuguaglianza $\langle s^x\rangle^2 + \langle s^y\rangle^2 + \langle s^z\rangle^2 \leq \hbar^2 s^2$.

[5] Parte non svolta e non richiesta.

- ***Modulus of the average vector*** $\vec{m} = \langle \vec{s} \rangle$ ***for a spin*** s ***particle***. *The components (operators)* s^a *of the spin vector transform as a three-dimensional spatial vector and so the components* m^a *of the average vector. Without loss of generality we can choose the quantisation direction in such a way that* $m^x = m^y = 0$. *For the* z *component we will then have usual eigenvectors and eigenvalues*

$$s^z|m\rangle = \vec{s} \cdot \frac{\vec{m}}{\|\vec{m}\|}|m\rangle = \hbar m|m\rangle \ , \quad m = -s, -s+1, \ldots, s-1, s$$

and, with a generic mixed spin state ρ_s,

$$m^z = \langle s^z \rangle = \mathrm{tr}\rho_s s^z = \sum_{m'} \langle m'|\rho_s s^z|m'\rangle = \hbar \sum_{m'} m' \rho_{s,m'm'} \leq \hbar s \sum_{m'} \rho_{s,m'm'} = \hbar s$$

since from general properties of density matrices $\rho_{s,m'm'} = \langle m'|\rho_s|m'\rangle \geq 0$ *and* $\mathrm{tr}\rho_s = 1$. *In conclusion, the modulus of vector* $\vec{m}$ *obeys the inequalilty* $\langle s^x \rangle^2 + \langle s^y \rangle^2 + \langle s^z \rangle^2 \leq \hbar^2 s^2$.

- **Prodotti tensori sulla base computazionale**. Per operatori a un qubit scritti nella base $|0\rangle$ e $|1\rangle$ (o anche $|\downarrow\rangle$ $|\uparrow\rangle$)

$$M_A \to \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} e \ , \quad M_B \to \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix}$$

cerchiamo gli elementi della matrice che rappresenta il prodotto tensore $M = M_A \otimes M_B$. Se i valori possibili del primo qubit sono indicati da α e quelli del secondo da β abbiamo sedici possibili elementi di matrice $\langle \alpha\beta|M|\alpha'\beta'\rangle = \langle \alpha|M_A|\alpha'\rangle\langle \beta|M_B|\beta'\rangle$ in corrispondenza dei quattro elementi della base computazionale a due qubit $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Seguendo questo ordinamento risulta

$$M \to \begin{pmatrix} a_{00}M_B & a_{01}M_B \\ a_{10}M_B & a_{11}M_B \end{pmatrix}$$

ossia una "matrice" 2×2 composta a sua volta di matrici 2×2 ottenute ripetendo M_B moltiplicata per dei coefficienti secondo la struttura della matrice M_A.

- ***Tensor products on computational basis***. *For one-qubit operators in the computational basis* $|0\rangle$ *and* $|1\rangle$ *(or also* $|\downarrow\rangle$ $|\uparrow\rangle$*)*

$$M_A \to \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \ , \quad M_B \to \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix}$$

let us write down the matrix elements of their tensor product $M = M_A \otimes M_B$. *If the possible values of the first qubit are labeled by* α *and those for the second one by* β *we have sixteen possible matrix elements* $\langle \alpha\beta|M|\alpha'\beta'\rangle =$

$\langle\alpha|M_A|\alpha'\rangle\langle\beta|M_B|\beta'\rangle$ corresponding to the four elements of the two-qubits computational basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Following this ordering

$$M \to \begin{pmatrix} a_{00}M_B & a_{01}M_B \\ a_{10}M_B & a_{11}M_B \end{pmatrix}$$

that is a 2×2 "matrix" composed, in turn, by 2×2 matrices given by repeating M_B multiplied by coefficients that follow the structure of M_A.

Appendice B: Misure con proiettori

Se consideriamo in generale uno stato $|\psi\rangle \in \mathcal{H}$ tra le varie possibilità di misure di osservabili compatibili possiamo scegliere in linea di principio quella in cui si misura la sequenza di osservabili

$$P_1 = |\phi_1\rangle\langle\phi_1|,\ P_2 = |\phi_2\rangle\langle\phi_2|, \dots P_d = |\phi_d\rangle\langle\phi_d|$$

dove $d = \dim\mathcal{H}$ e $\{P_k = |\phi_k\rangle\langle\phi_k|\}$ è una serie di proiettori ortogonali associati ad ogni elemento di una base ortonormale$\{|\phi_k\rangle\}$ di $\mathcal{H}$. In particolare se gli stati di base sono ortogonali allora i proiettori corrispondenti sono compatibili poiché commutano sempre a due a due ,$[P_k, P_n] = \delta_{k,n}P_k$. Abbiamo quindi a che fare con una collezione di osservabili le quali - al di là del problema operativo di come siano accessibili in laboratorio per la misura - forniscono in linea di principio una serie di esiti di misura compatibili (autovalori simultanei). Per chiarire meglio ricordiamo quali sono gli autovalori (esiti possibili) di ciascuno di queste osservabili proiettive. Dato un proiettore P_k, relativo alla varietà unidimensionale generata dal vettore di base $|\phi_k\rangle$ gli autovalori possibili sono $p_k^{(k)} = 1$ e $p_k^{(j)} = 0$ per $j \neq k$ e quindi $d-1$ volte degenere (l'apice indica l'indice dell'autovalore e il pedice lo specifico proiettore considerato). Ogni elemento della base $|\phi_k^{(j)}\rangle$ è caratterizzato da una sequenza ben precisa di questi autovalori, ovvero $P_k|\phi_k^{(j)}\rangle = \delta_{j,k}|\phi_k^{(j)}\rangle$.

Per un momento immaginiamo il caso più semplice, ossia un qubit. La procedura potrebbe quindi partire selezionando lo stato di base $|0\rangle$ ed il suo proiettore $|0\rangle\langle 0|$. Lo si misura e l'esito può essere o $p_0^{(0)} = 1$ nel qual caso si capisce che dopo la misura lo stato è già collassato in $|0\rangle\langle 0|$ e quindi diciamo che abbiamo misurato lo stato $|0\rangle$, oppure si ha $p_0^{(0)} = 0$ che è l'altro autovalore possibile, quindi dobbiamo accedere al sottospazio ortogonale a quello generato da $|0\rangle$ che in questo caso è generato da $|1\rangle$. In questo caso specifico necessariamente troveremo $p_1^{(1)} = 1$, che conclude la misura. Questa procedura dura al massimo due passaggi e fornisce come risultato una sequenza di autovalori 0 e 1 che permettono di stabilire in quale elemento della base di stati è finito lo stato iniziale per effetto delle successive contrazioni della funzione d'onda.

Per un caso a dimensione $d > 2$, occorre stabilire una sequenza per esclusione, che è sempre possibile costruire almeno per $d < \infty$. Si seleziona un primo stato e se ne misura l'autovalore. Se si ottiene 1 la procedura si arresta, altrimenti si

passa al sottospazio ortogonale e così via, fino a che una misura non restituisce come autovalore misurato 1; questo esito deve necessariamente presentarsi nella sequenza non fosse altro che per il caso più "sfortunato" in cui bisogna portare la sequenza di misure fino a considerare per esclusione un sottospazio ortogonale a dimensione 1. I valori registrati di $p_k^{(j)}$ saranno delle sequenze di 0 che terminano con un 1 e permettono di indicizzare in quale stato della base il sistema è finito dopo la sequenza di misure. Il primo elemento della sequenza potrà sempre essere indicato da 1 (e implicitamente una sequenza di 0 perché si arresta subito la procedura di misura), mentre l'ultimo elemento risulterà da $00\ldots0$ (in $d-1$ casi) e infine 1; si tratta in fondo di una indicizzazione inversa degli stati di base in numerazione binaria. Si comprende anche come in generale questa sequenza ripetuta di misure compatibili sia piuttosto distruttiva perché dà luogo a vari collassi del vettore di stato.

Appendix C: Entanglement swapping in a teleportation setting

Using the notation of subsec. 2.7 here we admit that the unknown qubit is in a mixed state $\rho_I = \mathrm{tr}_J |\Psi\rangle_{JIJI}\langle\Psi|$ *due to the presence of another ancilla qubit J and also that the entangled "resource"* χ_{AB} *shared by A and B is generic and not necessarily maximally entangled as it would be for the original recipe where* $\chi_{AB} = |\Phi^+\rangle_{ABAB}\langle\Phi^+|$. *In fact, this is the setting considered in ref. [10], where the Bell measurement is still performed on qubits I+A but now the starting overall four qubits state is* $\rho_{JIAB} = |\Psi\rangle_{JIJI}\langle\Psi| \otimes \chi_{AB}$ *(for the time being we have put in explicit the tensor product but it could be removed in multiple qubits calculations for the sake of compactness). We need to express the measurement on Bell basis in the formalism of density matrices; this is accomplished using four orthogonal operators* E^γ, $\gamma = 0, 1, 2, 3$ *as in [10] according to the general formalism of von Neumann projective measurements [1, 23]. First, it can be seen by direct inspection that the Bell observable* $\mathcal{B}$ *of subsec. 2.2 in the computational basis has the form*

$$\mathcal{B} = \sqrt{2} \begin{pmatrix} -1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ -1 & 0 & 0 & -1 \end{pmatrix}$$

and that its eigenvectors are precisely the four Bell states (and the eigenvalues $-2\sqrt{2}, 0, 0, 2\sqrt{2}$*). Note that in ref. [10] the standard state for teleportation is taken to be* $|\Psi^+\rangle$ *while in these notes we have used* $|\Phi^+\rangle$*; nonetheless if we wish that the four operators* E^γ *are related to the four projectors onto Bell states we can start from a reference one, say* $|\Psi^+\rangle$ *to stick to notations of [10], and then act on one of the two composing qubits "n+m", say the second one "m", with Pauli operators*

$$E^0_{nm} = |\Psi^+\rangle_{nmnm}\langle\Psi^+|$$
$$E^1_{nm} = |\Phi^+\rangle_{nmnm}\langle\Phi^+| = \sigma^x_m E^0_{nm} \sigma^x_m$$

Columns $\|\delta\rangle_{IA}$	$\|\Psi^+\rangle_{IA}$	$\|\Phi^+\rangle_{IA}$	$\|\Phi^-\rangle_{IA}$	$\|\Psi^-\rangle_{IA}$
$\beta = 0\ \Psi^+$	$\|\Psi^+\rangle_{JB} = \mathbb{I}_J\|\Psi^+\rangle_{JB}$	$\|\Phi^+\rangle_{JB} = \sigma_J^x\|\Psi^+\rangle_{JB}$	$-\|\Phi^-\rangle_{JB} = -i\sigma_J^y\|\Psi^+\rangle_{JB}$	$-\|\Psi^-\rangle_{JB} = -\sigma_J^z\|\Psi^+\rangle_{JB}$
$\beta = 1\ \Phi^+$	$\|\Phi^+\rangle_{JB} = \mathbb{I}_J\|\Phi^+\rangle_{JB}$	$\|\Psi^+\rangle_{JB} = \sigma_J^x\|\Phi^+\rangle_{JB}$	$-\|\Psi^-\rangle_{JB} = -i\sigma_J^y\|\Phi^+\rangle_{JB}$	$-\|\Phi^-\rangle_{JB} = -\sigma_J^z\|\Phi^+\rangle_{JB}$
$\beta = 2\ \Phi^-$	$\|\Phi^-\rangle_{JB} = \mathbb{I}_J\|\Phi^-\rangle_{JB}$	$-\|\Psi^-\rangle_{JB} = \sigma_J^x\|\Phi^-\rangle_{JB}$	$\|\Psi^+\rangle_{JB} = -i\sigma_J^y\|\Phi^-\rangle_{JB}$	$-\|\Phi^+\rangle_{JB} = -\sigma_J^z\|\Phi^-\rangle_{JB}$
$\beta = 3\ \Psi^-$	$\|\Psi^-\rangle_{JB} = \mathbb{I}_J\|\Psi^-\rangle_{JB}$	$-\|\Phi^-\rangle_{JB} = \sigma_J^x\|\Psi^-\rangle_{JB}$	$\|\Phi^+\rangle_{JB} - i\sigma_J^y\|\Psi^-\rangle_{JB}$	$-\|\Psi^+\rangle_{JB} = -\sigma_J^z\|\Psi^-\rangle_{JB}$

Tabella 6: States $|S_\delta^\beta\rangle$*in the expansion of* $|\Psi^+\rangle_{JI}|\beta\rangle_{AB}$ *for each* β *(rows) as a sum of contributions* $|\delta\rangle_{IA}|S_\delta^\beta\rangle_{JB}/2$.

$$E^2_{nm} = |\Phi^-\rangle_{nmnm}\langle\Phi^-| = \sigma^y_m E^0_{nm}\sigma^y_{nm}$$
$$E^3_{nm} = |\Psi^-\rangle_{nmnm}\langle\Psi^-| = \sigma^z_m E^0_{nm}\sigma^z_{nm}$$

Now the strategy is to express χ_{AB} *using the 16 basis operators* $|\beta\rangle_{ABAB}\langle\beta'|$ *where* β *labels the four possible Bell states of A+B*

$$\chi_{AB} = \sum_{\beta,\beta'} |\beta\rangle_{ABAB}\langle\beta'|\chi(\beta,\beta')$$

What is the effect of a Bell measurement on the pair I+A in this setting? Let us consider the special case when $|\Psi\rangle_{JI} = |\Psi^+\rangle_{JI}$ *as done in ref. [10] and references therein (Bose, Vedral & Knight, 1998) to highlight the so-called entanglement swapping between a perfectly entangled states of J+I and a new generic entangled state of J+B after a Bell measurement performed on the pair I+A; the goal is to show that the resulting state of J+B has the same form, meaning the same matrix elements* $\langle\beta|\chi|\beta'\rangle \equiv \chi(\beta,\beta')$*, of the original resource "living" originally on A+B and living on J+B after the measurement of* E^γ_{IA}*. The measurement modifies the initial state according to*

$$\rho_{JIAB} \mapsto \sum_\gamma (\mathbb{I}_J \otimes E^\gamma_{IA} \otimes \mathbb{I}_B)\rho_{JIAB}(\mathbb{I}_J \otimes E^\gamma_{IA} \otimes \mathbb{I}_B) =$$

$$= \sum_{\gamma,\beta,\beta'} \chi(\beta,\beta')\mathbb{I}_J|\gamma\rangle_{IAIA}\langle\gamma|\mathbb{I}_B|\Psi^+\rangle_{JI}|\beta\rangle_{ABAB}\langle\beta'|_{JI}\langle\Psi^+|\mathbb{I}_J|\gamma\rangle_{IAIA}\langle\gamma|\mathbb{I}_B$$

(in the last line we have dropped the tensor products for the sake of compactness and because every state has a subscript indicating its qubits)

We now need to re-write each of the states $|\Psi^+\rangle_{JI}|\beta\rangle_{AB}$ *in terms of Bell states of I+A; a direct calculation (based on the inversion from Bell to computational bases as in subsec. 2.7) shows that the general expression has the form* $\frac{1}{2}\sum_\delta |\delta\rangle_{IA}|S_\delta^\beta\rangle_{JB}$ *where now* $\{|\delta\rangle_{IA}\}$ *label Bell's basis on I+A and* $|S_\delta^\beta\rangle$ *are associated states of J+B according to Table 6.*

So we have this kind of expression

$$\frac{1}{4}\sum_\gamma |\gamma\rangle_{IAIA}\langle\gamma|\sum_{\beta,\beta'}\chi(\beta,\beta')|S^\beta_\gamma\rangle_{JBJB}\langle S^{\beta'}_\gamma|$$

but from the equalities in the table we can exploit that each ket or bra can be thought as $|S^{\beta}_{\gamma}\rangle_{JB} = \mathsf{R}_J(\gamma)|\beta\rangle_{JB}$, *i.e. a unitary for each* γ *applied to states labeled by* δ *only. The unitaries (collecting signs and imaginary factors) can be written again as* $\sigma^{\gamma}_J \mathbb{I}_B$. *So the density matrix before the last unitary performed by B can be expressed as*

$$\frac{1}{4}\sum_{\gamma}|\gamma\rangle_{IAIA}\langle\gamma|\otimes U_J(\gamma)\left(\sum_{\delta,\delta'}\chi(\delta,\delta')|\delta\rangle_{JBJB}\langle\delta'|\right)U_J^{\dagger}(\gamma) = \frac{1}{4}\sum_{\gamma}|\gamma\rangle_{IAIA}\langle\gamma|\otimes U_J(\gamma)\chi_{JB}U_J^{\dagger}(\gamma)$$

where we have "reconstructed" the original resource χ *but on J+B apart from the unitary and the outcomes of the measurement on I+A* $|\gamma\rangle_{IAIA}\langle\gamma|$ *with probabilities* $\frac{1}{4}$.

This mechanism of entanglement swapping is also at the heart of the generalised depolarising channel considered in ref. [10] that one obtains by "blindly" applying the standard teleportation protocol of Bennett and co-workers [5] to the four qubit setting I+J+A+B if the resource on A+B is not necessarily maximally entangled; in the case of rotational invariance in the Hilbert space of A+B the part of the outcoming state that does not reproduce the initial one is then simply proportional to the identity, i.e. without useful information, as in eq. (23).

Riferimenti bibliografici

[1] http://www.theory.caltech.edu/people/preskill/ph229 (dispense/libro di John Preskill nella sezione Lecture Notes).

[2] http://technology.newscientist.com/article/dn13825-quantum-camera-snaps-objects-it-cannot-see.html.

[3] Alain Aspect. To be or not to be local. *Nature*, 446:866, 2007.

[4] Simon C. Benjamin, Brendon W. Lovett, and Jason M. Smith. Prospects for measurement-based quantum computing with solid state spins. *Laser and Photonics Reviews*, 3:556, 2009.

[5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895, 1993.

[6] Niels Bohr. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 48:696, 1935.

[7] D. Boschi, S. Branca, F. De Martini, Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 80:1121, 1998.

[8] Dirk Bouwmeester, Artur Ekert, and Anton Zeilinger, editors. *The physics of quantum information*. Springer, 2000.

[9] Dirk Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Herald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390:575, 1997.

[10] G. Bowen and S. Bose. Teleportation as a depolarizing quantum channel, relative entropy, and classical capacity. *Physical Review Letters*, 87:267901, 2001.

[11] Pasquale Calabrese and John Cardy. Entanglement entropy and quantum field theory, 2004. http://arxiv.org/abs/hep-th/0405152.

[12] W. A. Coish and Daniel Loss. Quantum computing with spins in solids, 2006. http://arxiv.org/cond-mat/0606550, contribution to the Handbook of Magnetism and Advanced Magnetic Materials, vol. 5 (Wiley).

[13] David DiVincenzo. The physical implementation of quantum computation, 2000. http://arxiv.org/abs/quant-ph/0002077.

[14] David DiVincenzo, Guido Burkard, Daniel Loss, and E. V. Sukhorukov. Quantum computation and spin electronics, 1999. http://arxiv.org/abs/cond-mat/9911245.

[15] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777, 1935.

[16] J. Eisert, M. Cramer, and M. B. Plenio. Area laws for the entanglement entropy - a review. *Reviews of Modern Physics*, 82:277, 2010.

[17] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467, 1982.

[18] Vitaly N. Golovach and Daniel Loss. Electron spins in artificial atoms and molecules for quantum computing. *Semicond. Sci. Technol.*, 17:355, 2002.

[19] H. Häffner, C. F. Roos, and R. Blatt. Quantum computing with trapped ions. *Physics Reports*, 469:155, 2008.

[20] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223:1, 1996.

[21] M. Wieśniak, V. Vedral, and Č. Brukner. Magnetic susceptibility as a macroscopic entanglement witness. *New Journal of Physics*, 7:258, 2005.

[22] Giuseppe Morandi, Franco Napoli, and Elisa Ercolessi. *Statistical mechanics. An intermediate course*. World scientific, 2001.

[23] Michael Nielsen and Isaac Chuang. *Quantum computation and quantum information*. Cambridge, 2000.

[24] T. J. Osborne and F. Verstraete. General monogamy inequality for bipartite qubit entanglement. *Physical Review Letters*, 96:220503, 2006.

[25] I. Peschel and V. Eisler. Reduced density matrices and entanglement entropy n free lattice models. *Journal of Physics A: Mathematical and Theoretical*, 42:504003, 2009.

[26] Chandrasekhar Ramanathan, Nicolas Boulant, Zhiying Chen, David G. Cory, Isaac Chuang, and Matthias Steffen. Nmr quantum information processing. *Quantum Information Processing*, 3:15, 2004.

[27] P. Recher, Daniel Loss, and J. Levy. Spintronics and quantum computing with quantum dots, 2000. http://arxiv.org/abs/cond-mat/0009270.

[28] Yanhua Shih. The physics of ghost imaging, 2008. http://arxiv.org/abs/0805.1166.

[29] Rupert Ursin, Thomas Jennewein, Markus Aspelmeyer, Rainer Kaltenbaek, Michael Lindenthal abd Philip Walther, and Anton Zeilinger. Quantum teleportation across the Danube. *Nature*, 430:849, 2004.

[30] S. J. van Enk, H. J. Kimble, and H. Mabuchi. Quantum information processing in cavity-QED. *Quantum Information Processing*, 3:75, 2004.

[31] Marek Šašura and Vladimir Bužek. Cold trapped ions as quantum information processors. *Journal of Modern Optics*, 49:1593, 2002.

[32] Göran Wendin. Scalable solid-state qubits: challenging decoherence and read-out. *Philosophical Transactions of the Royal Society of London A*, 361:1363, 2003.

[33] William K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Physical Review Letters*, 80:2245, 1998.

[34] Bei Zeng, Xie Chen, Duan-Lu Zhou, and Xiao-Gang Wen. Quantum information meets quantum matter – from quantum entanglement to topological phase in many-body systems, 2015. http://arxiv.org/abs/1508.02595.