UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Fisica e Astronomia "Galileo Galilei"

Corso di Laurea in Fisica

Tesi di Laurea

No-cloning e categorie

Relatore

Prof. Pieralberto Marchetti

Laureando

Anna Bison

Anno Accademico 2021/2022

Introduzione

Dopo la pubblicazione delle disuguaglianze di Bell (1964), che avevano dimostrato l'incompatibilità della meccanica quantistica con una qualsiasi teoria locale non completa che soddisfi il principio di realtà di Einstein, non escludendo quindi l'esistenza di "spaventose azioni a distanza" realizzabili attraverso l'*entanglement*, era iniziata la ricerca di un esperimento che ne verificasse gli effetti.
Il risultato decisivo arriva solo nel 1982, anno in cui viene illustrato l'esperimento FLASH, la cui struttura teorizza un tipo di processo che, pochi mesi più tardi, verrà dimostrato essere impossibile da realizzare poiché in contrasto con gli assiomi della meccanica quantistica. La formalizzazione matematica di tale impossibilità è il teorema No-cloning, che asserisce l'impossibilità di copiare un generico stato puro, un risultato che si è rivelato fondamentale per lo sviluppo della teoria quantistica dell'informazione, in particolare per quanto concerne la crittografia quantistica.
L'importanza evidenziata da tale fenomeno ha portato successivamente allo studio del problema del cloning in meccanica classica. Benché la generazione di copie sia notoriamente realizzabile nell'ambito della teoria dell'informazione classica (copiare un generico bit è possibile) tale processo non è estendibile con naturalezza e a livello generale alla meccanica classica, in cui i sistemi sono composti tramite prodotto cartesiano di varietà di Poisson, strutture che non ammettono cloning universale. Il problema classico tuttavia ha suscitato meno interesse del suo analogo quantistico. La tesi quindi si concentrerà principalmente sulle strutture classiche che ammettono cloning, e soprattutto *separabili* per confrontarle con gli analoghi quantistici.
La teoria delle categorie, una recente branca dell'algebra astratta che ha tra i suoi obiettivi una nuova formulazione della meccanica quantistica, ha reso evidente la limitazione espressa dal no-cloning come conseguenza della differenza tra le strutture categoriali che descrivono l'informazione classica e l'informazione quantistica. L'obiettivo di questa tesi è illustrare come il teorema No-cloning sia conseguenza diretta della particolare struttura categoriale *di tipo quantistico* degli spazi di Hilbert finito dimensionali, e tra le principali proprietà che differenziano tale struttura da quella delle categorie *di tipo classico*. Dopo una introduzione generale sul teorema No-cloning, sarà deifnito il formalismo degli string diagrams, la cui potenza espressiva sarà necessaria per dare una dimostrazione semplice del teorema Cloning-Collapse, un teorema analogo al No-cloning le cui ipotesi sono però differenti. La completezza della categoria degli spazi di Hilbert finito dimensionali rispetto agli string diagrams consentirà poi di applicare tale risultato alla teoria quantistica a spazi finiti.

Indice

Capitolo 1

Teorema No-cloning

La pubblicazione del paradosso EPR (1935) e delle conseguenti disuguaglianze di Bell (1964) ha dato inizio ad indagini sia teoriche che sperimentali sui possibili effetti non locali della meccanica quantistica.
Tali effetti sono generati dal fenomeno dell'*entanglement*, che consiste nel non poter scrivere ogni stato di un sistema quantistico composto come prodotto degli stati dei singoli sottosistemi; in altre parole la meccanica quantistica presenta una struttura intrinseca in generale *non separabile*.
Nel 1982 viene pubblicato un articolo che teorizza un metodo di comunicazione superluminale sulla base di misure di sistemi fisici entangled. Tale ipotetico esperimento, chiamato FLASH, avrebbe coinvolto un particolare strumento capace di clonare i sistemi fisici. Pochi mesi dopo Dieks, Wootters e Zurek pubblicano quasi contemporaneamente due articoli che dimostrano l'impossibilità di realizzare un tale apparato, dimostrando che se impiegato in una situazione di tipo EPR avrebbe condotto ad un assurdo.
[1]Si considerino due sperimentatori Alice (A) e Bob (B), che dispongano di un sistema fisico bipartito in uno stato entangled, per esempio generato dal decadimento $\pi^0 \longrightarrow e^- + e^+$ con il pione a riposo.
Essendo $s_{\pi^0} = 0$, per conservazione del momento angolare il sistema e^-e^+ deve trovarsi nello stato di singoletto $|e^+e^-\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$. Si supponga che A possa eseguire misure sul positrone e B sull'elettrone, e che B disponga di uno strumento di clonazione (come definito in FLASH) posto lungo la traiettoria di e^-, che assorbe in input la particella e ne emette N copie identiche.
Prima che e^- raggiunga il dispositivo, A effettua una misura dello spin di e^+ potendo decidere se misurarlo lungo l'asse z o x. Lo stato di e^- collasserà di conseguenza, e il dispositivo duplicatore emetterà un fascio di N elettroni nel medesimo stato. Solo a tal punto, B eseguirà su tutte le N particelle una misura di S_z, dal cui esito potrà dedurre la decisione presa da A.
Nel primo caso, in cui A sceglie di misurare S_z, lo stato di e^- collassa in un autostato di S_z e quindi B ottiene N misure dello stesso valore. Viceversa, se A misura S_x, il sistema collassa in un autostato di tale operatore, costituito da una combinazione lineare di autostati di S_z. A questo punto per ciascuno degli N elettroni prodotti B può ottenere con una misura di S_z lo stato $|\downarrow\rangle$ oppure $|\uparrow\rangle$, ed essendo i due equiprobabili, il risultato finale è un fascio con circa $\frac{N}{2}|\downarrow\rangle$ e circa $\frac{N}{2}|\uparrow\rangle$. Ecco che B è in grado di dedurre la decisione presa da A senza aver comunicato direttamente, e poiché non sono state fatte ipotesi sulla distanza tra i due sperimentatori, possiamo supporla di tipo spazio rispetto alla durata dell'esperimento, il che rende di fatto la comunicazione superluminale.
Il problema di fondo che rende però tale situazione impossibile da realizzare risiede nella definizione del dispositivo di clonazione, che secondo le ipotesi dovrebbe essere in grado di copiare gli autostati di S_z, effettuando una trasformazione U tale che (nel caso semplice in cui sia generata solo una copia dello stato iniziale):

$$|\uparrow\rangle \otimes |0\rangle \xrightarrow{U} |\uparrow\rangle \otimes |\uparrow\rangle \equiv |\uparrow\uparrow\rangle \tag{1.1}$$

$$|\downarrow\rangle \otimes |0\rangle \xrightarrow{U} |\downarrow\rangle \otimes |\downarrow\rangle \equiv |\downarrow\downarrow\rangle \tag{1.2}$$

In cui $|0\rangle$ costituisce l'analogo quantistico del *foglio bianco* in una fotocopiatrice classica.
Nel caso in cui però e^- si trovi in un autostato di S_x l'operatore U per linearità dovrà produrre il seguente

[1]Di seguito è proposta una versione modificata dell'esperimento, ispirata alla variante di David Bohm (EPRB).

output:

$$\frac{1}{\sqrt{2}}(|\uparrow\rangle \pm |\downarrow\rangle) \otimes |0\rangle \xrightarrow{U} \frac{1}{\sqrt{2}} |\uparrow\uparrow\rangle \pm \frac{1}{\sqrt{2}} |\downarrow\downarrow\rangle \tag{1.3}$$

che permette di ottenere da una misura una coppia di particelle entrambe $|\uparrow\rangle$ oppure entrambe $|\downarrow\rangle$, risultato ben diverso da quello desiderato:

$$(\frac{1}{\sqrt{2}} |\uparrow\rangle \pm \frac{1}{\sqrt{2}} |\downarrow\rangle) \otimes (\frac{1}{\sqrt{2}} |\uparrow\rangle \pm \frac{1}{\sqrt{2}} |\downarrow\rangle) = \frac{1}{2} |\uparrow\uparrow\rangle + \frac{1}{2} |\downarrow\downarrow\rangle \pm \frac{1}{2}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) \tag{1.4}$$

che avrebbe ammesso invece anche la possibilità di trovare le particelle in due autostati diversi.
Ecco che dunque, se il dispositivo deve poter clonare autostati di S_z, per linearità non può clonare autostati di S_x, essendo tali operatori non compatibili. Per questo motivo la trasformazione descritta nell'esperimento non è realizzabile, e quello che accadrebbe realmente è che Bob misurerebbe lo stesso valore di S_z per tutti gli N elettroni del fascio anche se Alice decidesse di misurare S_x, rendendo tale caso indistinguibile dal primo sulla base delle misure.

Le limitazioni evidenziate dal precedente esperimento costituiscono la versione concreta del teorema No-cloning, di cui esiste anche una dimostrazione molto semplice:

Teorema 1 (No-cloning quantistico)**.** Siano $|\psi\rangle$ e $|\phi\rangle$ due stati e sia U una trasformazione unitaria tale che:

$$|\psi\rangle \otimes |0\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle \tag{1.5}$$

$$|\phi\rangle \otimes |0\rangle \xrightarrow{U} |\phi\rangle \otimes |\phi\rangle \tag{1.6}$$

Allora $\langle\psi|\phi\rangle$ vale 0 oppure 1.

Dimostrazione.

$$\langle\psi|\phi\rangle = (\langle\psi| \otimes \langle 0|)(|\phi\rangle \otimes |0\rangle) = (\langle\psi| \otimes \langle\psi|)(|\phi\rangle \otimes |\phi\rangle) = \langle\psi|\phi\rangle^2 \iff \langle\psi|\phi\rangle = 0 \vee 1 \tag{1.7}$$

Essendo U un operatore unitario che come tale preserva il prodotto scalare. □

Esiste anche una dimostrazione che si serve esclusivamente del postulato della misura in meccanica quantistica. Supponendo infatti di misurare la direzione di polarizzazione di un fotone polarizzato in una direzione inclinata di un angolo β rispetto all'orizzontale, rappresentata dalla seguente funzione d'onda ($|0\rangle$ e $|1\rangle$ sono rispettivamente lo stato di polarizzazione orizzontale e verticale):

$$|\psi\rangle = \cos\beta\,|0\rangle + \sin\beta\,|1\rangle \tag{1.8}$$

dal postulato della misura è noto che si otterrebbe $|0\rangle$ con una probabilità $p_{|0\rangle} = \cos^2\beta$ e $|1\rangle$ con $p_{|1\rangle} = \sin^2\beta$. Tale condizione impone che la misura di polarizzazione di un singolo fotone porti un bit di informazione, costituito dall'esito della misura (0 oppure 1). Se per assurdo esistesse una macchina in grado di clonare il fotone generando un numero N arbitrariamente grande di copie di $|\psi\rangle$ si potrebbe dedurre, dalla quantità di $|0\rangle$ e $|1\rangle$ ottenuti, una stima di β con arbitraria precisione, estraendo dalla misura un numero di bit grande a piacere (tutti quelli necessari a scrivere β con la precisione desiderata). Tale possibilità sarebbe dunque in contrasto con il postulato della misura. Ecco che si è giunti alla tesi senza coinvolgere la linearità, ottenendo una versione più forte della dimostrazione.

È fondamentale tenere presente che il teorema No-cloning riguarda l'impossibilità di clonare un *generico* stato. Se infatti fosse noto a priori che il *qubit* si trovasse in uno dei due stati ortogonali $|0\rangle$ oppure $|1\rangle$, allora una misura sarebbe sufficiente a conoscere precisamente tale stato e sarebbe possibile produrne un qualsiasi numero di copie. In tal caso infatti il qubit si comporterebbe come un bit classico, e ammetterebbe cloning.
La possibilità di clonare bit classici nell'ambito della crittografia classica rende impossibile sapere con certezza se un messaggio sia stato intercettato o meno, dal momento che l'atto di clonare non lascia tracce

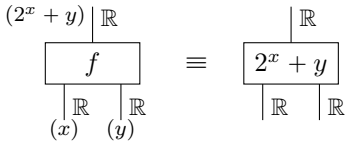
sull'originale.
Il fatto che nei sistemi quantistici il processo di misura modifichi in modo irreversibile e casuale (dunque incontrollabile) lo stato del sistema consente invece di rilevare le intrusioni, e il teorema No-cloning impone una limitazione decisiva affinché ciò accada, rendendo non realizzabile ad esempio un attacco di tipo *man in the middle*.
Se infatti Alice volesse trasmettere a Bob una chiave costituita da una stringa di bit classici codificati dalle polarizzazioni di un fascio di fotoni (selezionate accuratamente) e un *eavesdropper* Eve (E) cercasse di intercettare il fascio, il no-cloning gli impedirebbe di clonarlo e di spedire l'originale a Bob senza lasciare traccia. Sarebbe sufficiente quindi che A e B confrontassero tra loro i rispettivi risultati delle misure per rilevare un'eventuale intrusione e di conseguenza eliminare la chiave.

Capitolo 2

Teorie processuali

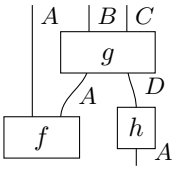
Si introduce di seguito un formalismo diagrammatico che si dimostra efficace e consistente nel descrivere la meccanica quantistica a spazi finiti. Esso consente di scrivere equazioni grafiche applicando regole semplici e intuitive, che si concentrano sull'interazione tra i sistemi più che sulla natura dei singoli, facilitando la visione d'insieme. I risultati ottenibili da equazioni diagrammatiche minimali possono essere dimostrate anche algebricamente, ma spesso richiedono innumerevoli passaggi che complicano la visione dell'idea di fondo.

Si chiama *processo* un ente con zero o più input e zero o più output. Si può rappresentare un processo tramite un *box*, a cui vengono connessi *fili* alla base, che rappresentano gli input, e dal cui lato opposto fuoriescono altri *fili*, che rappresentano gli output.
Un esempio di processo è la funzione $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} :: (x, y) \mapsto 2^x + y$, rappresentata come:

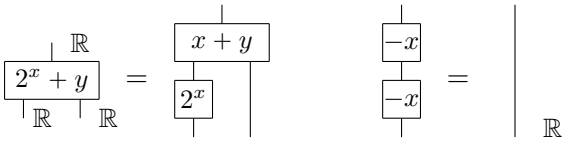


(2.1)

Su ogni filo è specificato il *tipo di sistema*, abbreviato in *tipo*. Nel caso delle funzioni, i tipi sono gli insiemi. Si possono connettere tra loro processi semplici per definirne di più complessi, rappresentati da *diagrammi*:



Un diagramma può essere creato connettendo gli output di un certo processo agli input di un altro processo, se questi sono dello stesso tipo, in modo che si verifichi la coerenza a cui ci si riferisce comunemente con *matching types*. Tale restrizione è cruciale nel linguaggio dei diagrammi, perché consente di capire quando l'applicazione di un processo ad un certo sistema è sensata.



(2.2)

Per descrivere in modo completo un diagramma è necessario definire il contenuto di ciascun box e il modo preciso in cui i box sono connessi tra loro. In altre parole, il diagramma consiste nella rappresentazione grafica indipendentemente dall'interpretazione teorica sottesa. Questo implica che se due diagrammi possono essere deformati uno nell'altro senza variarne le connessioni, allora sono uguali.

Definizione 1. Una *teoria processuale* è costituita da:

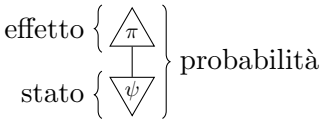
- una collezione T di *tipi di sistema* rappresentati dai fili
- una collezione P di *processi* rappresentata dai box, tale che per ogni processo in P i tipi di input e i tipi di output appartengano a T
- un'operazione di composizione di processi tale che un diagramma composto da più processi in P costituisca a sua volta un processo in P.

La terza proprietà garantisce che le teorie processuali siano chiuse rispetto alla composizione di processi. Una teoria processuale comprende equazioni, che consentono di trarre conclusioni sui processi che vi compaiono, e ci si aspetta che in qualità di teoria consenta di fare previsioni costituite da numeri che le rendano verificabili sperimentalmente. A questo proposito si definiscono due speciali tipi di processo:

- processi senza input, chiamati *stati*: 

- processi senza output, chiamati *effetti*: 

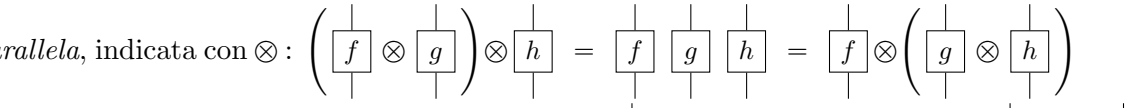
Consistentemente la composizione di uno stato e di un effetto restituisce un terzo genere di processo che non ha né input né output, chiamato *numero*. Un numero può essere interpretato come la probabilità che dato un sistema in un preciso stato ψ, si verifichi un certo effetto π:



Tale espressione prende il nome di *regola di Born generalizzata*. Tale terminologia è mutuata dalla teoria generale della misura in Meccanica quantistica in cui le probabilità degli esiti della misura si ottengono applicando stati (in generale matrici densità) ad effetti (operatori positivi con media tra 0 e 1).

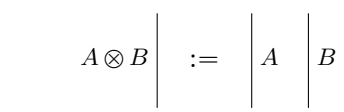
2.1 String Diagrams

I processi possono essere composti tramite due operazioni di composizione associative:

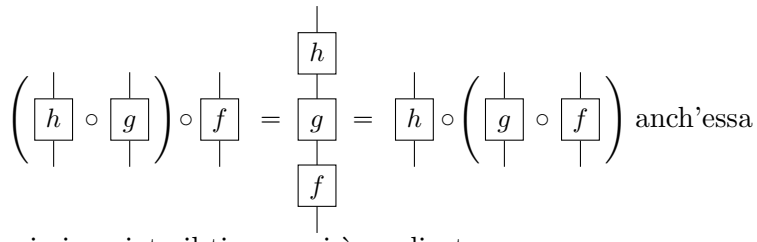
- *composizione parallela*, indicata con $\otimes$: 

munita di processo unitario rappresentato dal diagramma vuoto: 

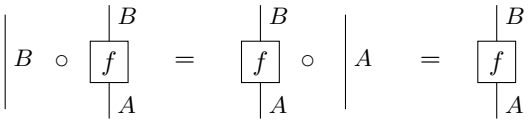
estendibile ai tipi per rappresentare un sistema composto, per esempio bipartito:



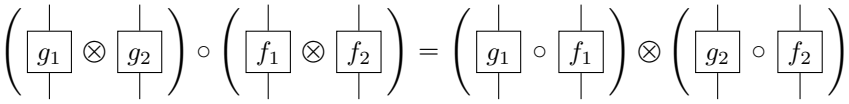
Per tale operazione tra tipi è definito un analogo di unità dato dal tipo vuoto, denotato con I, rispetto al quale il diagramma vuoto rappresenta l'identità;

- *composizione sequenziale*, indicata con $\circ$:  anch'essa

  munita di identità indicata con 1_A, che lascia invariato il tipo a cui è applicata:



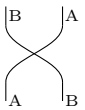
Tali operazioni obbediscono ad una legge di interscambio da cui segue:



Esempio 1. Un analogo del processo di identità nel caso degli spazi di Hilbert finito dimensionali nel formalismo di Dirac è dato dalla *completezza*, che in $\mathbb{C}^2$ risulta:

$$\mathbb{I}_{\mathbb{C}^2} = |0\rangle\langle 0| + |1\rangle\langle 1|$$

Si può invertire l'ordine di due tipi tramite il *swap*:



Esempio 2. Un processo analogo al swap è dato dalla permutazione degli stati di un sistema quantistico bipartito, che in $\mathbb{C}^2 \otimes \mathbb{C}^2$ è eseguito dal seguente operatore:

$$swap = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$$

Definizione 2. Si chiama *circuito* un diagramma che può essere costruito componendo i box, includendo identità e swap, tramite $\otimes$ e $\circ$.

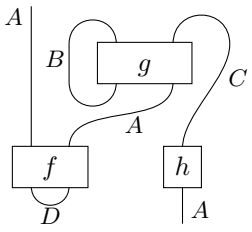
Definizione 3. Si definiscono *string diagrams* i diagrammi che soddisfano le seguenti proprietà:

- sono *circuiti* muniti di un particolare stato e di un particolare effetto:

  gli string diagrams chiamati rispettivamente *cup* e *cap*, per i quali siano valide le seguenti uguaglianze, che prendono il nome di *yanking equations*:

(2.3)

- sono composti da box e fili in cui gli input di un dato processo si possono connettere agli output dello stesso, come si verifica nel seguente esempio:



  proprietà realizzata grazie all'implemento dei cup e dei cap.

Le uguaglianze sopra disegnate possono essere visualizzate immaginando che il LHS sia un filo di ferro, e di doverlo deformare afferrandone un'estremità con ciascuna delle proprie mani, fino ad ottenere il pattern del RHS.

Esempio 3. I cup e i cap costituiscono una rappresentazione particolarmente efficace degli stati bipartiti negli spazi di Hilbert composti, in particolare degli stati entangled, essendo il filo continuo assimilabile alla non-separabilità che li caratterizza. Nel caso di $\mathbb{C}^2 \otimes \mathbb{C}^2$ si ha che cup e cap sono analoghi rispettivamente ai seguenti stati:

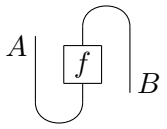
$$\cup = |00\rangle + |11\rangle \qquad\qquad \cap = \langle 00| + \langle 11|$$

Componendo il cap con il swap, si ottiene un risultato che verifica la prima yanking equation:

$$\cap \circ \mathit{swap} = (\langle 00| + \langle 11|)(|00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|) = \langle 00| + \langle 11| = \cap$$

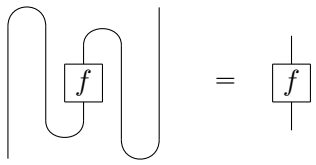
e analogamente per il cup. Ciò conferma la consistenza dell'interpretazione.

Definizione 4. Il *trasposto* di un processo f si indica con f^T ed è definito dal seguente diagramma:

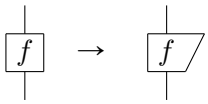


$$= (1_A \otimes \cap_B) \circ (1_A \otimes f \otimes 1_B) \circ (\cup_A \otimes 1_B)$$

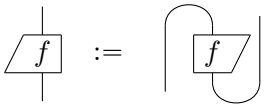
La trasposizione di un processo è involutiva, ovvero $(f^T)^T = f$: usando le yanking equations otteniamo



Per inglobare tale definizione nel formalismo si modifica la forma del box di f:



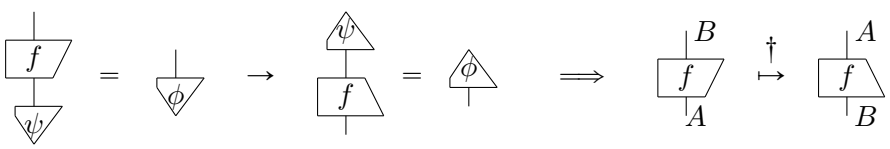
potendo così esprimere graficamente la trasposta di f come la rotazione di π del box di f:



In accordo con l'idea di "deformare i fili" per ottenere identità si affina la notazione relativa agli stati, aumentandone il potere espressivo:

L'effetto che verifica lo stato di un sistema (cioè per il quale la relativa probabilità è 1) è rappresentato dallo stato da verificare girato sottosopra:

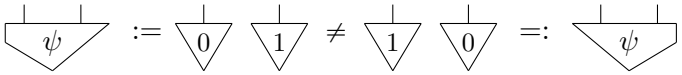
L'effetto così ottenuto è l'*aggiunto* dello stato ψ, da cui è definibile come diretta conseguenza l'aggiunto di un processo f: esso è il processo che trasforma l'aggiunto di ψ nell'aggiunto dello stato in cui f mappa ψ:



In cui la seconda equazione è ottenuta girando sottosopra la prima. Come nel caso della trasposizione, anche l'operazione di aggiunto è involutiva, dato che girando sottosopra due volte di seguito un oggetto si riottiene la configurazione di partenza.

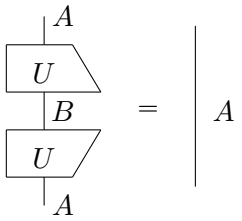
Sostanzialmente, il modo in cui si calcola l'aggiunto di un processo dipende dalla teoria. Ogni teoria fornisce una interpretazione particolare dei diagrammi sin qui illustrati. Nel caso delle mappe lineari l'aggiunto di un processo f è $f^\dagger$ tale che $\forall\ \psi, \phi$ si abbia $\langle\psi|f(\phi)\rangle = \langle f^\dagger(\psi)|\phi\rangle$, la cui matrice è ottenuta facendo la trasposta e complessa coniugata della matrice di f.
L'operazione di *coniugazione* per un processo è definibile in termini generali attraverso i diagrammi, componendo il processo trasposto con l'aggiunto, operazione anch'essa involutiva. Dal punto di vista grafico ciò è equivalente a riflettere orizzontalmente i box di un diagramma. Per stati ed effetti che siano uguali ai propri coniugati si può utilizzare la notazione a triangoli:

Mentre i coniugati di stati composti formati da sottostati singolarmente auto-coniugati non sono in generale auto-coniugati:



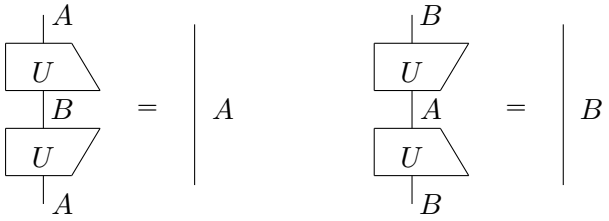
In cui gli stati sono indicati con 0 e 1 per evidenziarne la differenza.

Definizione 5. Un processo U è un'*isometria* se è valida la seguente equazione:



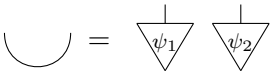
Dalla definizione di aggiunto segue che in un'isometria l'aggiunto coincide con l'inverso da un lato di U, e nel caso in cui coincida con l'inverso da entrambi i lati, dà luogo ad un processo unitario:

Definizione 6. Un processo U è *unitario* se vale:

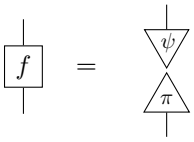


Esempi di processi unitari sono l'identità, il swap e la composizione parallela di processi unitari.
La ragione per cui è necessario introdurre gli string diagrams[1] è la necessità che esistano stati ed effetti non separabili, caratteristica propria anche della meccanica quantistica. I cup e i cap si rivelano fondamentali nella rappresentazione di sistemi non separabili, dal momento che non è consentito *tagliare il filo.*

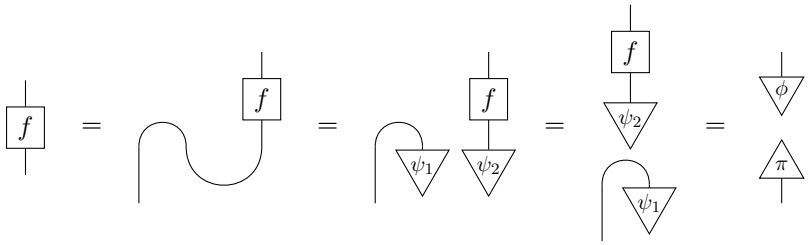
Proposizione 1. Se una teoria è descritta dagli string diagrams, e tutti gli stati bipartiti ψ sono $\otimes$-separabili, cioè se esistono due stati ψ_1 e ψ_2 tali che



[1] I circuiti, che sono diagrammi più restrittivi degli string diagrams, rappresentano le categorie monoidali simmetriche, mentre gli string diagrams rappresentano le categorie chiuse compatte dagger. Si ha quindi che più sofisticato è il tipo di diagramma e più è semplice il genere di SMC che rappresenta.

allora per ogni processo f esistono uno stato ψ e un effetto π tali che f è $\circ$-*separabile*: 

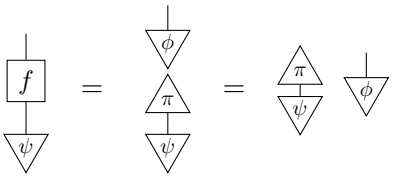
Dimostrazione. Componendo l'input di f con l'identità, riscrivendo quest'ultima considerando le yanking equations ed essendo $\cup$ $\otimes$-separabile per ipotesi:



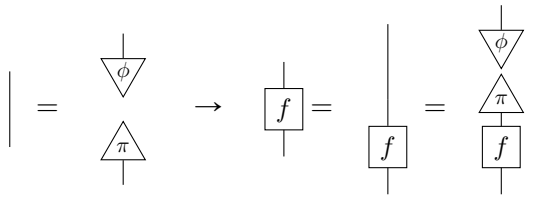
□

Le teorie in cui tutti i processi siano $\circ$-separabili sono banali. Se infatti si applica un processo separabile f ad uno stato ψ arbitrario ciò che si ottiene è lo stato ϕ (nella notazione della Proposizione 1) a meno di una costante (data da 

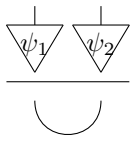
):



Poiché tutti i processi sono $\circ$-separabili, deve esserlo anche l'identità, e di converso deve accadere che se l'identità è separabile allora tutti i processi lo sono a loro volta, dal momento che ogni f è scrivibile come composizione di sé stesso con l'identità:

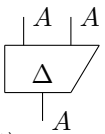


Una teoria chiusa rispetto agli string diagrams che possieda processi non banali nel senso appena specificato, non può dunque possedere stati bipartiti che siano tutti $\otimes$-separabili. Nel caso della meccanica quantistica l'entanglement non è quindi un accidente, ma una proprietà fondamentale. La più importante caratteristica della teoria quantistica è direttamente implementata nella struttura dei diagrammi che la descrivono.

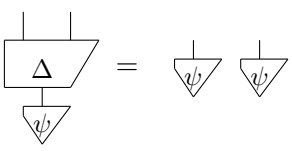


$$= \frac{\text{separabile}}{\text{non-separabile}} = \frac{\text{classico}}{\text{quantistico}}$$

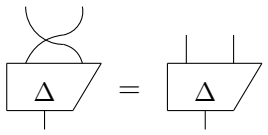
La classe di risultati a cui appartiene il precedente è nota come *teoremi no-go*, ed esprimono l'impossibilità che qualcosa di notoriamente possibile nell'esperienza comune accada.

Si definisce *processo di cloning* di un sistema di tipo A il seguente processo Δ: 

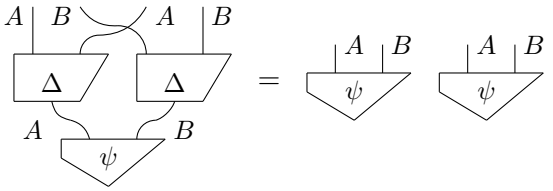
che dato uno stato ψ in input ne produce una copia, in modo che l'output sia costituito da due $|\psi\rangle$:

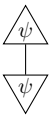


Ci si aspetta che un tale processo debba rispettare alcune condizioni precise. Per prima cosa, essendo i due stati in output identici, deve essere indifferente quale dei due si considera per primo, il che è reso imponendo che "*swap* $\circ$ Δ" sia ancora uguale a Δ:

(1) 

Nel caso di uno stato bipartito ψ di tipo $A \otimes B$ si vuole che il processo di cloning dello stato sia ottenuto clonando separatamente ciascuno dei due tipi:

(2) 

La terza ipotesi è che la teoria processuale considerata possieda almeno uno stato normalizzato: 

=

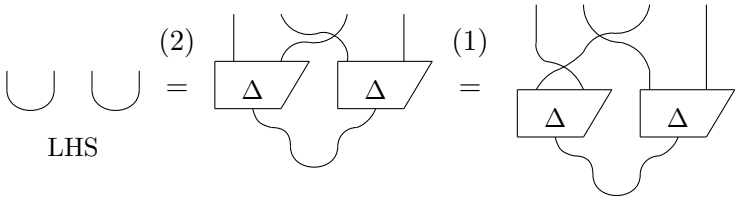

:= 1

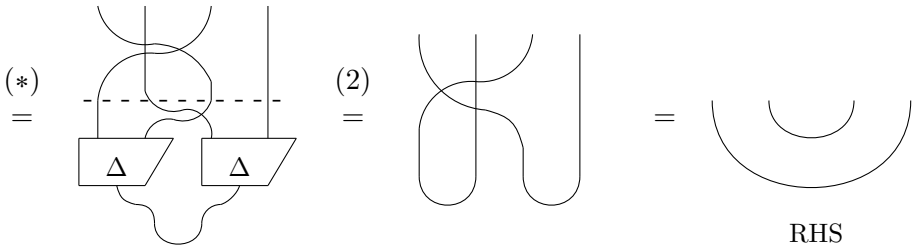
Senza quest'ultima condizione non ci sarebbe nulla da clonare.

Teorema 2 (**Cloning-Collapse**)**.** Si consideri una teoria processuale che ammetta string diagrams. Se esiste un processo di cloning per il sistema di tipo A che soddisfa le tre condizioni precedenti, allora ogni processo che abbia A come tipo di input deve essere $\circ$-separabile.

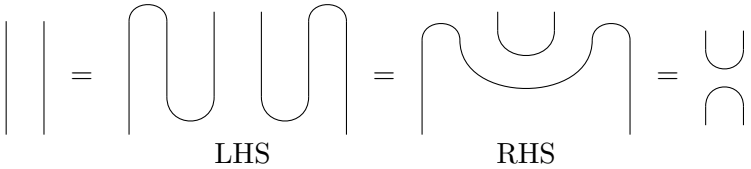
Dimostrazione. Considerando il seguente stato nei successivi passaggi: 

:= 

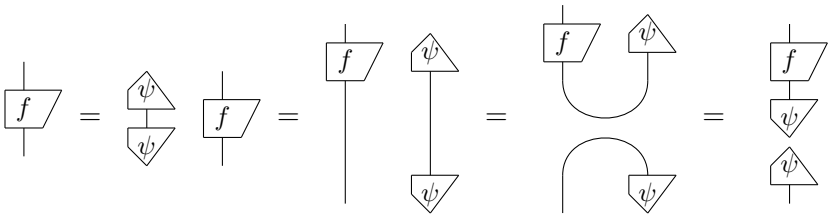




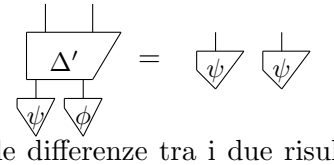
In cui tutti i fili sono di tipo A, $(*)$ è solo una deformazione del diagramma e i tratteggi distinguono la parte inferiore che viene sostituita da due cup al passaggio successivo in accordo con la (2), dalla parte superiore che resta invariata. L'ultimo passaggio equivale infine ad uno *yank* delle due estremità di filo centrali.
Convertendo dunque gli output esterni di LHS e RHS in input si ottiene:



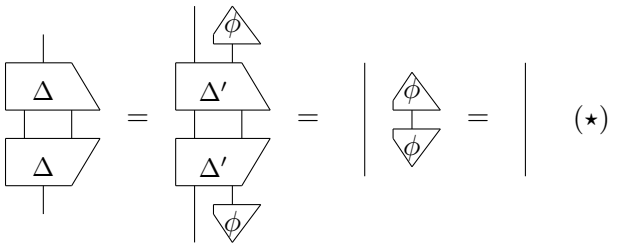
da cui si deduce che l'identità in una coppia di sistemi separabili è separabile. Utilizzando tale risultato:



□

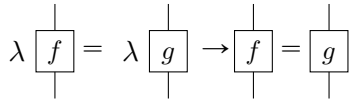
Il Teorema 2 permette di concludere che se esiste un processo di cloning per un sistema di tipo A allora la teoria processuale è banale rispetto ad A, e se ogni tipo di sistema possiede un processo di cloning, allora la teoria è banale del tutto. L'ipotesi più restrittiva è la (2), che sarebbe soddisfatta solo se fosse possibile agire separatamente su ciascun sottosistema per generare la copia, richiesta impossibile da soddisfare se si pensa che la non-separabilità impedisce anche solo di descrivere uno stato bipartito trattando i due sottostati come indipendenti.
Questo teorema non è però equivalente al Teorema 1. Una prima differenza evidente ma non decisiva risiede nel mancato utilizzo di uno stato ausiliario, il *foglio bianco* $|\phi\rangle$ che viene sovrascritto dalla copia di $|\psi\rangle$. Apportando la seguente sostituzione, è però possibile dimostrare equivalentemente per Δ' il precedente risultato: 

senza dunque intaccare la struttura della dimostrazione. Per rendere evidenti le differenze tra i due risultati si illustra di seguito la dimostrazione del Teorema 1 espressa nel formalismo a diagrammi.
Sia ϕ normalizzato, Δ e Δ' definiti come sopra. Chiedendo che Δ' sia unitario si ottiene che Δ deve essere un'isometria.

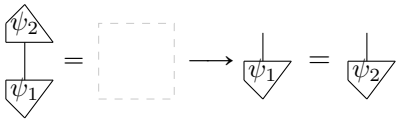


Si assuma che esista una tale isometria Δ e che sia un *processo di cloning* come definito in precedenza. L'assunzione implicita prevista dal Teorema 1 è che si stia considerando la teoria dei processi quantistici, che però non è necessaria. Le ipotesi necessarie sono solo due e coinvolgono i numeri di una teoria qualsiasi:

(a) $\forall \lambda \neq 0$:

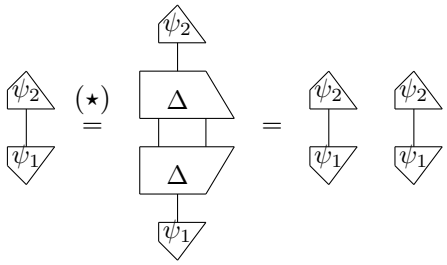


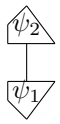
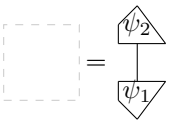
(b) Per ψ_1, ψ_2 normalizzati si ha:

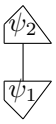


Teorema 3. In una teoria che ammetta string diagrams e che soddisfi le condizioni (a) e (b) descritte sopra, se esiste una isometria Δ in grado di clonare entrambi gli stati normalizzati ψ_1 che ψ_2 allora essi devono essere coincidenti oppure ortogonali.

Dimostrazione.



Se accade che  $\neq 0$, per (a) si ha: 

e per l'assunzione (b) si ha che ψ_1 e ψ_2 sono uguali. Nel caso in cui invece sia  $= 0$, si ha che ψ_1 e ψ_2 sono ortogonali. □

Corollario 1 (**Secondo No-cloning**)**.** Assumendo le ipotesi del Teorema 3, se una teoria processuale possiede almeno due stati di tipo A né uguali né ortogonali, allora non può esistere un processo di cloning per il tipo A.

Adesso che entrambi i teoremi sono stati resi nello stesso formalismo se ne denota la differenza: il teorema No-cloning assume che Δ' sia unitario come conseguenza del fatto che deve essere un processo quantistico, rendendo superflue le ipotesi (1) e (2) che invece costituiscono il Cloning-Collapse. Ciò riduce le teorie a cui poter applicare il No-Cloning, che imponendo l'unitarietà e la normalizzazione richiede quantomeno che queste siano definite in una teoria, per poter essere preso in considerazione.
Per esempio, nel caso della teoria delle relazioni, il Cloning-Collapse risulta applicabile, tuttavia non potendo soddisfare la condizione (b)[2] richiesta dal No-cloning, quest'ultimo non risulta applicabile, sebbene dimostri la stessa proprietà. Il Cloning-Collapse inoltre non si basa sugli aggiunti, e in questo senso è più generale del No-cloning. Tuttavia quest'ultimo rende superflue ulteriori condizioni sul dispositivo di cloning, si può quindi concludere che il Cloning-Collapse non implica il No-Cloning.
Sebbene dunque il No-cloning risulti per certi aspetti meno generale del Cloning-Collapse, resta comunque un risultato utile perché dimostra che è possibile clonare congiuntamente stati tramite un unico processo purché siano *ortogonali*. Nel caso della meccanica quantistica questa proprietà è connessa al fatto che i dati classici possono essere codificati in stati ortogonali tra loro, e che l'informazione che può essere estratta deve comportarsi in modo classico.

[2]Nella categoria **Rel** delle relazioni il fatto che la contrazione tra uno stato e un effetto (costituiti da insiemi) dia come risultato 1 non implica che i due siano uguali, ma solo che hanno intersezione non vuota.

Capitolo 3

Teoria delle Categorie

Si dimostra che gli string diagrams sono completi rispetto alla teoria matematica delle categorie monoidali chiuse compatte dagger. Ciò significa che ciascuno dei risultati ottenuti nel capitolo precedente è vero *se e solo se* è dimostrabile equivalentemente nel formalismo categoriale. La meccanica quantistica a spazi finiti è descrivibile a sua volta tramite tale formalismo, dal momento che possiede una struttura che ne soddisfa gli assiomi.

La prima definizione di categoria è dovuta a Samuel Eilenberg e Saunders Mac Lane e risale al 1945, nel tentativo di sviluppare un ambiente in grado di descrivere in modo unico un'ampia varietà di strutture matematiche. L'esempio più frequente di struttura matematica è quello di un insieme munito di specifiche operazioni e proprietà, per esempio un *gruppo*:

- un *gruppo* è un insieme G con un'operazione binaria associativa $- \bullet - : G \times G \to G$ e un elemento neutro[1] bilaterale $1 \in G$ rispetto al quale ciascun elemento possiede un inverso: $\forall g \in G \; \exists \; g^{-1} \in G$ tale che $g \circ g^{-1} = 1$.

Esistono poi particolari mappe che preservano le strutture. Un esempio nel caso dei gruppi sono gli *omomorfismi*: dati due gruppi $(G, \bullet), (P, *)$, si ha che $\phi : G \to P$ è un omomorfismo se $\forall x, y \in G, \phi(x \bullet y) = \phi(x) * \phi(y) \in P$, in cui $\bullet$ e $*$ rappresentano l'operazione binaria nei gruppi G e P rispettivamente, da cui segue la preservazione dell'elemento neutro e degli inversi. Questa è la base per definire la categoria **Grp** (dei gruppi).

La teoria della categorie consente di alzare lo sguardo dalla struttura interna di un oggetto, consentendo allo stesso tempo di analizzarne agevolmente l'interazione con altri oggetti.

Definizione 7. Una *categoria* $\mathbf{C}$ è costituita da:

- Una classe di oggetti denotata con $|\mathbf{C}|$;
- $\forall A, B \in |\mathbf{C}|$ un insieme di *morfismi* da A a B denotato con $\mathbf{C}(A, B)$;
- $\forall A, B, C \in |\mathbf{C}|$, $\forall f \in \mathbf{C}(A, B)$, $\forall g \in \mathbf{C}(B, C)$, esiste un *morfismo composto* $g \circ f \in \mathbf{C}(A, C)$, ossia $\forall A, B, C \in |\mathbf{C}|$ esiste una *operazione di composizione*

  $$- \circ - : \mathbf{C}(A, B) \times \mathbf{C}(B, C) \longrightarrow \mathbf{C}(A, C) :: (f, g) \mapsto g \circ f,$$

  con la proprietà di essere *associativa* e munita di elemento neutro, rispettivamente:

  i. $\forall f \in \mathbf{C}(A, B), g \in \mathbf{C}(B, C)$ e $h \in \mathbf{C}(C, D)$ si ha

  $$h \circ (g \circ f) = (h \circ g) \circ f$$

  ii. $\forall A \in |\mathbf{C}|$ esiste un morfismo $1_A \in \mathbf{C}(A, A)$ detto *identità*, tale che $\forall f \in |\mathbf{C}|$ sia

  $$f = f \circ 1_A = 1_B \circ f$$

[1] anche chiamato *elemento unità* o *unità*

Un esempio di categoria è **Set**, che presenta:

1. gli insiemi come oggetti,
2. le funzioni tra insiemi come morfismi: dati due insiemi X, Y se $f : X \to Y$ allora $f \in \mathbf{Set}(X, Y)$,
3. la composizione sequenziale tra morfismi è costituita dall'usuale composizione di funzioni: $\forall f : X \to Y$ e $g : Y \to Z$ si ha $(g \circ f)(x) := g(f(x))$ e $g \circ f : X \to Z$,
4. la funzione identità $1_X(x) := x$.

La composizione di funzioni è infatti associativa e $\forall\ f : X \to Y$ vale $(1_Y \circ f)(x) = f(x) = (f \circ 1_X)(x)$.

Analogamente, l'insieme degli spazi di Hilbert finito-dimensionali con le mappe lineari come morfismi costituisce la categoria **FdHilb**.
Si è descritta sopra una struttura matematica come un insieme con una certa struttura interna. Una categoria si definisce però riferendosi solo ad una classe di oggetti, e per ogni coppia di questi un insieme di morfismi, senza alcun cenno dunque alla struttura interna di ciascun oggetto. A prima vista non sembra dunque esserci alcuna referenza alla natura (di insieme, spazio, gruppo, ecc.) che potrebbero avere gli oggetti, come se si stesse perdendo l'informazione sulla natura distintiva di ciascuno di essi, nel passaggio da struttura matematica a categoria. Tuttavia il problema non sussiste, perché il fatto di considerare come morfismi mappe che preservano la struttura consente di risalire alla struttura matematica di partenza: gli elementi di ciascun oggetto sono dunque a bordo, codificati opportunamente in specifici costituenti della categoria.
Si consideri per esempio un insieme $X \in |\mathbf{Set}|$, e un certo elemento $x \in X$. La funzione

$$e_x : \{*\} \to X :: * \mapsto x$$

in cui $\{*\}$ rappresenta il singoletto[2], mappa l'unico elemento di $\{*\}$ nell'elemento x. Se X ha cardinalità n, per ciascuno dei suoi elementi esiste una funzione definita come sopra, la struttura interna di X è quindi codificata nell'insieme dei morfismi da $\{*\}$ a X, indicato con $\mathbf{Set}(*, X)$.

Analogamente è possibile estrarre i vettori negli spazi di Hilbert: dato $\mathcal{H} \subset |\mathbf{FdHilb}|$ e fissato un vettore $v \in \mathcal{H}$ la mappa lineare

$$e_v : \mathbb{C} \mapsto \mathcal{H} :: 1 \to v$$

mappa $\mathbb{C}$ nel sottospazio vettoriale generato dal vettore v, essendo infatti $1 \in \mathbb{C}$ una base per lo spazio $\mathbb{C}$.

Dalla necessità di considerare due o più oggetti in parallelo senza che questo ne alteri la struttura (e quindi ottenendo un nuovo oggetto composto che ancora appartenga alla medesima categoria), si arriva alla definizione di monoide, e dalla necessità che tale operazione sia estendibile ai morfismi, alla definizione di categoria monoidale. Il monoide è una struttura un po' più semplice di un gruppo, differisce da quest'ultimo solo perché non richiede che sia definito un elemento inverso[3].

Definizione 8. Un *monoide* $(M, \bullet, 1)$ è un insieme munito di un'operazione binaria chiusa, associativa e di un elemento neutro rispetto ad essa

$$- \bullet - : M \times M \longrightarrow M$$

Definizione 9. Una *categoria monoidale stretta* C è una struttura costituita da:

1. una classe di oggetti avente struttura monoidale $(|\mathbf{C}|, \otimes, I)$ tale che $\forall A, B, C \in |\mathbf{C}|$ si abbia

$$A \otimes (B \otimes C) = (A \otimes B) \otimes C \quad I \otimes A = A = A \otimes I,$$

[2] un insieme costituito da un unico elemento.
[3] se infatti ci si limita a comporre parallelamente oggetti in modo chiuso non è necessario definire un oggetto inverso.

2. $\forall\ A, B, C, D \in |\mathbf{C}|$ esiste un'operazione[4] associativa munita di identità 1_I:

$$- \otimes - : \mathbf{C}(A, B) \times \mathbf{C}(C, D) \longrightarrow \mathbf{C}(A \otimes C, B \otimes D) :: (f, g) \to f \otimes g$$

$$f \otimes (g \otimes h) = (f \otimes g) \otimes h \quad 1_I \otimes f = f = f \otimes 1_I,$$

3. $\forall f, g, h, k$ morfismi con tipi coerenti si ha

$$(g \circ f) \otimes (k \circ h) = (g \otimes k) \circ (f \otimes h)$$

4. $\forall A, B \in |\mathbf{C}|$

$$1_A \otimes 1_B = 1_{A \otimes B}$$

Il termine *stretta* si riferisce all'associatività e neutralità di $\otimes$, in una categoria monoidale non stretta è infatti sufficiente che tali proprietà siano valide a meno di isomorfismi. Nel caso non stretto le uguaglianze della 1. sono sostituite da:

$$(A \otimes B) \otimes C \cong A \otimes (B \otimes C) \qquad A \otimes I \cong A \otimes I \otimes A$$

Tramite una dimostrazione costituita da una procedura chiamata *restrizione* è possibile dimostrare il seguente teorema di coerenza:

Teorema 4. Ogni categoria monoidale **C** è equivalente ad una categoria monoidale stretta **C'**.

Questo risultato sarà utilizzato in modo implicito ogni volta che si tratteranno come uguali oggetti differenti a meno di parentesi associative.

La categoria **Set** è una *categoria monoidale* rispetto al prodotto cartesiano, avente come oggetto neutro il *singoletto*. Se si considera poi una generica funzione f tra due set, si ha che se esiste l'inversa f^{-1}, vale $f \circ f^{-1} = 1$. Le funzioni biiettive soddisfano ora tutte le caratteristiche proprie di un gruppo, e pertanto una tale restrizione della categoria dei **Set**, che prende il nome di **Bijec** costituisce un *gruppoide*[5], cioè una categoria monoidale in cui ogni morfismo sia invertibile.

In **FdHilb** si ottiene la struttura monoidale considerando il prodotto tensore tra spazi di Hilbert. Se poi si considerano come morfismi gli operatori unitari tra essi si ottiene la categoria **FdUnit** che è a sua volta un gruppoide.

Set è una sottocategoria delle *relazioni*.

Definizione 10. Una *relazione* da un insieme A ad un insieme B è un sottoinsieme $R \subseteq A \times B$. Un elemento a è detto in relazione con un elemento b se $(a, b) \in R$. Altre notazioni equivalenti sono $R :: a \mapsto b$, equivalentemente $R(a) := \{b \mid R : a \mapsto b\}$ oppure più semplicemente aRb.

Dal punto di vista processuale una relazione può essere vista come una funzione *non deterministica*, in cui cioè un singolo input può essere mandato in zero, uno o più output. Un sistema che può trovarsi in uno stato costituito da un insieme di elementi prende infatti il nome di sistema non deterministico.

Esempio 4. La categoria monoidale **Rel** è costituita da:

- gli insiemi come classe di oggetti;
- le relazioni $R : X \to Y$ come morfismi;

[4] talvolta chiamata "tensore", diminutivo di "prodotto monoidale", che a priori non ha niente a che vedere con il prodotto tensore.

[5] da non confondersi con il *magma*, una struttura molto generale costituita da un insieme la cui operazione binaria soddisfa solo l'assioma di chiusura, e di cui il medesimo termine è sinonimo.

- date $R_1 : X \to Y$ e $R_2 : Y \to Z$ la composizione associativa $R_2 \circ R_1 \subseteq X \times Z$ è così definita:

$$R_2 \circ R_1 := \{(x, z) | \exists\, y \in Y \mid xR_1y, yR_2z\}$$

  Inoltre $\forall\, X \in |\mathbf{Rel}|$ si ha

$$1_X := \{(x, x) \mid x \in X\}$$

- il prodotto monoidale di due set è dato dal prodotto cartesiano, rispetto al quale l'elemento neutro è costituito dal singoletto, e il prodotto cartesiano si estende a prodotto monoidale per le relazioni: date $R_1 : X_1 \to Y_1$ e $R_2 : X_2 \to Y_2$ si definisce $R_1 \times R_2 \subseteq X_1 \times X_2 \to Y_1 \times Y_2$ come

$$R_1 \times R_2 := \{((x, x'), (y, y')) \mid xR_1y,\ x'R_2y'\} \subseteq (X_1 \times X_2) \times (Y_1 \times Y_2)$$

Definizione 11. Una categoria monoidale stretta *simmetrica* è una categoria monoidale stretta con un morfismo *swap*:

$$\sigma_{A,B} : A \otimes B \to B \otimes A$$

definito per tutti gli oggetti, tale che $\forall\, f : A \to A' e g : B \to B'$:

$$\sigma_{B,A} \circ \sigma_{A,B} = 1_{A\otimes B} \qquad \sigma_{A,I} = 1_A$$

$$(f \otimes g) \circ \sigma_{A,B} = \sigma_{B',A'} \circ (g \otimes f)$$

$$(1_B \otimes \sigma_{A,C}) \circ (\sigma_{A,B} \otimes 1_C) = \sigma_{A,B\otimes C}$$

In **FdHilb** il prodotto tensore $\otimes$ e la somma diretta $\oplus$ sono strutture monoidali molto diverse, come dimostra il ruolo che ciascuna di esse ricopre nella teoria quantistica. Nello specifico, come espresso da Schrödinger, la descrizione dei sistemi fisici composti tramite il prodotto tensore dei loro spazi è l'origine di ciò che differenzia la fisica quantistica dalla fisica classica. Per questo motivo, ci si può riferire alle strutture monoidali che si comportano come $\otimes$ in **FdHilb** chiamandole *"quantistiche"* e a quelle che si comportano come $\oplus$ in **FdHilb** chiamandole *"classiche"*. Come visto, i tensori (intesi come operazioni monoidali) *"quantistici"* comportano correlazioni tra sottosistemi, con la conseguenza che uno stato composto in generale non può essere decomposto (*separato*) in stati dei sottospazi singoli.

Al contrario, i tensori *"classici"* possono descrivere solo sistemi fisici *separati*, in cui cioè ciascuno stato possa essere descritto dagli stati dei sottospazi singoli.
Sebbene il prodotto cartesiano $\times$ si comporti come un tensore *"classico"* in **Set**, si può dimostrare che è un tensore *"quantistico"* in **Rel**, sebbene **Rel** contenga **Set** come sottocategoria e come tale ne erediti la struttura monoidale degli oggetti. La natura *"classica"* o *"quantistica"* è qualcosa che quindi coinvolge non solo gli oggetti, ma anche la struttura del tensore monoidale e dei morfismi.

In ogni categoria monoidale $\mathbf{C}$ l'insieme di morfismi $\mathbb{S} := (I, I)$ è sempre un monoide con la composizione categoriale come operazione monoidale. Perciò $\mathbb{S}_{\mathbf{C}}$ prende il nome di *monoide scalare* della categoria monoidale $\mathbf{C}$.

Teorema 5 (**Kelly-Laplaza**)**.** In qualsiasi categoria monoidale non necessariamente simmetrica il monoide scalare è sempre commutativo.

Tale risultato comporta conseguenze fisiche. In precedenza si è osservato come le categorie monoidali strette modellizzino i sistemi fisici e i processi tra essi. Adesso si è osservato che qualsiasi categoria monoidale stretta $\mathbf{C}$ possiede sempre un monoide commutativo di endomorfismi $\mathbb{S}_{\mathbf{C}}$. Quindi se si prova a modificare una teoria quantistica cambiando il campo $\mathbb{K}$ che ne definisce lo spazio vettoriale, nell'ambito delle categorie è sempre necessario restringersi a campi commutativi.

Esempio 5. Gli elementi di $\mathbb{S}_{\mathbf{FdHilb}}$ sono in corrispondenza biunivoca con gli elementi di $\mathbb{C}$:

$$\mathbb{S}_{(\mathbf{FdHilb},\otimes,\mathbf{C})} \cong \mathbb{C}$$

In **Set**, essendo l'identità l'unica funzione di tipo $\{*\} \to \{*\}$, si ha che $\mathbb{S}_{(\mathbf{Set},\times,\{*\})}$ è a sua volta un singoletto:

$$\mathbb{S}_{(\mathbf{Set},\times,\{*\})} \cong \{*\}$$

Dunque, la struttura scalare di $(\mathbf{Set}, \times, \{*\})$ è triviale. D'altra parte, nel caso di **Rel** ci sono due relazioni di tipo $\{*\} \to \{*\}$: l'identità e la relazione vuota. Quindi

$$\mathbb{S}_{(\mathbf{Rel},\times,\{*\})} \cong \mathbb{B}$$

i cui $\mathbb{B}$ rappresenta i booleani. Dunque la struttura di $(\mathbf{Rel}, \times, \{*\})$ è non triviale. Dal punto di vista pratico, si possono interpretare tali due scalari come rispettivamente possibile e impossibile.
Se invece si considera in **FdHilb** $\oplus$ al posto di $\otimes$ si ottiene di nuovo una struttura scalare triviale, dal momento che esiste un'unica mappa lineare dallo spazio di Hilbert zero-dimensionale in sé stesso:

$$\mathbb{S}_{(\mathbf{FdHilb},\oplus,\{*\})} \cong \{*\}$$

Emerge come dunque gli scalari e i loro multipli siano maggiormente legati alla struttura del tensore moltiplicativo rispetto che a quella di tensore additivo.
Confrontando poi tra loro le categorie *"classiche"* con quelle *"quantistiche"* si nota come in generale siano le strutture monoidali quantistiche a possedere una struttura scalare non triviale.

Le mappe tra categorie che ne preservano la struttura sono dette *funtori*.

Definizione 12. Date due categorie **C** e **D** un **funtore**

$$F : \mathbf{C} \to \mathbf{D}$$

consiste di:

1. Una mappa
$$F : |\mathbf{C}| \to |\mathbf{D}| :: A \mapsto F(A);$$

2. $\forall\ A, B \in |\mathbf{C}|$ una mappa
$$F : \mathbf{C}(A, B) \to \mathbf{D}(F(A), F(B)) :: f \mapsto F(f)$$
che preservi le identità e la composizione, rispettivamente:
i. $\forall f \in \mathbf{C}(A, B)$ e $g \in \mathbf{C}(B, C)$ sia
$$F(g \circ f) = F(g) \circ F(f),$$
ii. $\forall A \in |\mathbf{C}|$ sia
$$F(1_A) = 1_{F(A)}$$

Si introduce adesso il concetto di *dualità*, che in pratica equivale ad invertire il verso dei morfismi di una categoria.

Definizione 13. Un *funtore controvariante* $F : \mathbf{C} \to \mathbf{D}$ è un funtore che preserva le identità ma inverte le composizioni:

$$F(g \circ f) = Ff \circ Fg$$

I tensori ordinari sono dunque detti *covarianti*.

Definizione 14. Data una categoria **C** se ne definisce l'opposta e la si indica con $\mathbf{C}^{op}$ come segue:

- gli stessi oggetti di **C**,
- i morfismi rovesciati:
$$f \in \mathbf{C}(A, B) \iff f \in \mathbf{C}^{op}(B, A) := f^{op}$$

- morfismi identità in comune con $\mathbf{C}$ e

$$f^{op} \circ g^{op} = (g \circ f)^{op}$$

Dalla precedente defizione consegue che è possibile definire i funtori controvarianti di tipo $\mathbf{C} \to \mathbf{D}$ come funtori di tipo $\mathbf{C}^{op} \to \mathbf{D}$.
Invertire due volte il verso di un processo porta a riottenere il processo di partenza: l'operazione di inversione di una categoria è dunque involutiva.

Esempio 6. Il gruppoide **FdUnit** è una sottocategoria di **FdHilb**, che può essere estratta da quest'ultima tramite un funtore controvariante che estrae gli aggiunti:

$$\dagger : \mathbf{FdHilb}^{op} \to \mathbf{FdHilb}$$

tale che

- coincida con l'identità rispetto agli oggetti:

$$\dagger : |\mathbf{FdHilb}^{op}| \to |\mathbf{FdHilb}| :: \mathcal{H} \to \mathcal{H}$$

- assegni ad un morfismo il suo aggiunto

$$\dagger : \mathbf{FdHilb}^{op}(\mathcal{H}, \mathcal{K}) \to \mathbf{FdHilb}(\mathcal{K}, \mathcal{H}) :: f \to f^\dagger$$

Tale funtore è controvariante dal momento che presi $f \in \mathbf{FdHilb}(\mathcal{H}, \mathcal{K})$, $g \in \mathbf{FdHilb}(\mathcal{K}, \mathcal{L})$ si ha

$$1^\dagger_{\mathcal{H}} = 1_{\mathcal{H}} \qquad (g \circ f)^\dagger = f^\dagger \circ g^\dagger$$

Essendo poi $\forall\ f, f^{\dagger\dagger} = f$, il funtore è involutivo.

Sebbene i morfismi di **FdHilb** non tengano traccia della struttura di prodotto interno, quest'ultimo è necessario per definire l'aggiunto, grazie al quale è possibile quindi ridefinire il prodotto scalare in termini puramente categoriali.

Si può infatti definire una notazione di Dirac estesa partendo dalla seguente definizione:

Definizione 15. Una *categoria monoidale stretta dagger* $\mathbf{C}$ è una categoria monoidale stretta equipaggiata con un funtore controvariante involutivo e neutro sugli oggetti:

$$\dagger : \mathbf{C}^{op} \to \mathbf{C}$$

tale che $\forall\ A \in |\mathbf{C}|$ sia $A^\dagger = A$ e per ogni morfismo f si abbia $f^{\dagger\dagger} = f$, che inoltre preservi il tensore:

$$(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$$

Dato un processo $A \xrightarrow{f} B$ si definisce il suo *aggiunto* come $B \xrightarrow{f^\dagger} A$.

Ecco che è possibile definire in una qualsiasi categoria monoidale $\mathbf{C}$

- gli *elementi* di un oggetto $A \in |\mathbf{C}|$ come morfismi di tipo $I \to A$;
- i *co-elementi*, morfismi di tipo $A \to I$
- gli *scalari*, come morfismi di tipo $I \to I$

Siano ora $\psi, \phi : I \to A$ elementi in $\mathbf{C}$. Il loro *prodotto interno* è lo scalare

$$\langle \phi | \psi \rangle := \phi^\dagger \circ \psi : I \to I$$

Definizione 16. Una *categoria chiusa compatta* è una categoria monoidale simmetrica $\mathbf{C}$ tale che per ogni oggetto $A \in |\mathbf{C}|$ esista un altro oggetto $A^* \in |\mathbf{C}|$ e i seguenti morfismi:

$$\eta_A : I \to A^* \otimes A \qquad \epsilon_A : A \otimes A^* \to I$$

detti rispettivamente *unità* e *counità*, tali che:

$$(\epsilon_A \otimes 1_A) \circ (1_A \otimes \eta_A) = 1_A \qquad (1_{A^*} \otimes \epsilon_A) \circ (\eta_A \otimes 1_{A^*}) = 1_{A^*}$$

Nel caso la categoria sia anche simmetricamente autoduale (tale cioè che $A = A^*$), tali morfismi soddisfano inoltre

$$\epsilon_A \circ \sigma_{A,A} = \epsilon_A \qquad \sigma_{A,A} \circ \eta_A = \eta_A \qquad (\star)$$

La proprietà di *chiusura* di una categoria assicura che per ogni coppia di oggetti A e B gli elementi di $\mathbf{C}(A, B)$ siano rappresentabili a loro volta come un oggetto, denotato con $A \Rightarrow B$. La compattezza si verifica quando questi particolari oggetti hanno la seguente forma:

$$A \Rightarrow B := A^* \otimes B$$

che nel caso autoduale diventa

$$A \Rightarrow B := A \otimes B$$

proprietà che esprimono la dualità processo-stato.

Definizione 17. Una *categoria chiusa compatta dagger* è una categoria chiusa compatta il cui funtore dagger sia tale che

$$\epsilon_A^\dagger = \eta_{A^*}$$

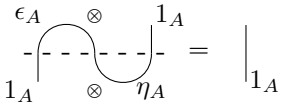
La categoria **FdHilb** è chiusa compatta dagger. Un funtore dagger è infatti definibile tramite gli aggiunti, come descritto nell'Esempio 6.

Unità e counità possono essere descritti in modo efficace dai diagrammi di cup e cap rispettivamente:

$$\cup : \eta_A : I \to A^* \otimes A \qquad \cap : \epsilon_A : A \otimes A^* \to I$$

e la proprietà che devono soddisfare equivale ad una yanking equation:

$$(\epsilon_A \otimes 1_A) \circ (1_A \otimes \eta_A) = 1_A \qquad \equiv$$



$$(\diamond)$$

Nel caso in cui sia anche $A = A^*$, le uguaglianze $(\star)$ sono l'equivalente delle rimanenti due yanking equations.

Esempio 7. Preso uno spazio di Hilbert $\mathcal{H}$ autoduale, fissata una base $\{e_i\} \in \mathcal{H}$ siano

$$\eta_{\mathcal{H}} : \mathbb{C} \to \mathcal{H} \otimes \mathcal{H} \qquad \epsilon_{\mathcal{H}} : \mathcal{H} \otimes \mathcal{H} \to \mathbb{C}$$

mappe lineari, rispettivamente unità e counità, definite come segue:

$$\eta_{\mathcal{H}}(1) = \sum_i e_i \otimes e_i \qquad \epsilon_{\mathcal{H}}(e_i \otimes e_j) = \delta_i^j$$

in notazione di Dirac:

$$\eta_{\mathcal{H}} = \sum_i |i\rangle \otimes |i\rangle \qquad \epsilon_{\mathcal{H}} = \sum_i \langle i| \otimes \langle i|$$

Verificare nel formalismo di Dirac che $\epsilon_{\mathcal{H}}$ e $\eta_{\mathcal{H}}$ soddisfano $(\diamond)$ necessita di applicare l'operatore $(\epsilon_{\mathcal{H}} \otimes 1_{\mathcal{H}}) \circ (1_{\mathcal{H}} \otimes \eta_{\mathcal{H}})$ ad un generico stato $|\psi\rangle \in \mathcal{H}$, e di eseguire una serie di passaggi ben più lunga:

$$\Big(\sum_i \langle ii| \ \otimes \ 1_{\mathcal{H}}\Big)\Big(1_{\mathcal{H}} \otimes \sum_j |jj\rangle\Big)\,|\psi\rangle$$

$$= \Big(\sum_i \langle ii| \otimes 1_{\mathcal{H}}\Big) \sum_j |\psi jj\rangle = \sum_{ij} \langle ii|\psi j\rangle\, |j\rangle = \sum_{ij} \langle i|\psi\rangle\, \delta_{ij}\, |j\rangle = \sum_i \langle i|\psi\rangle\, |i\rangle = \mathbb{I}_{\mathcal{H}}\, |\psi\rangle$$

che ancora una volta è consistente con quanto espresso sopra. Si nota dunque quanto sia vantaggioso l'utilizzo del formalismo diagrammatico nelle uguaglianze tra operatori.

La definizione di $\eta_{\mathcal{H}}$ e $\epsilon_{\mathcal{H}}$ data all'esempio precedente nel caso di **FdHilb** dipende dalla scelta della base. Per questo motivo è utile la definizione generale che distingue lo spazio duale di $\mathcal{H}$, cioè $\mathcal{H}^*$, definendo $\epsilon_{\mathcal{H}}$ e $\eta_{\mathcal{H}}$ come segue:

$$\epsilon_{\mathcal{H}} :\ \xi \otimes a \mapsto \xi(a) \qquad\qquad \eta_{\mathcal{H}} : 1 \mapsto \sum_i \langle i| \otimes |i\rangle$$

tale definizione fissa univocamente $\epsilon_{\mathcal{H}}$ e di conseguenza $\eta_{\mathcal{H}}$ indipendentemente dalla scelta della base.

3.0.1 Cloning

Definizione 18. Dati due funtori $F, G : \mathbf{C} \to \mathbf{D}$ una *trasformazione naturale* $\xi : F \Rightarrow G$ è una famiglia $\{\xi_A : FA \to GA\}_A$ di morfismi in $\mathbf{D}$ tale che per ogni morfismo $f : A \to B$ in $\mathbf{C}$ il seguente diagramma commuti:

$$\begin{array}{ccc} FA & \xrightarrow{Ff} & FB \\ \downarrow{\scriptstyle \xi_A} & & \downarrow{\scriptstyle \xi_B} \\ GA & \xrightarrow{Gf} & GB \end{array}$$

Si definisce una operazione uniforme e naturale di cloning in una categoria $|\mathbf{C}|$, detta *diagonale*:

$$\Delta = \{A \xrightarrow{\Delta_A} A \otimes A \mid A \in |\mathbf{C}|\}$$

tale che il seguente diagramma commuti:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle \Delta_A} & & \downarrow{\scriptstyle \Delta_B} \\ A \otimes A & \xrightarrow{f \otimes f} & B \otimes B \end{array}$$

Il precedente diagramma commuta quando applicare un processo f ad un sistema A e in seguito copiarlo è equivalente a copiare prima il sistema A e in seguito applicare f su ciascuna delle due copie.
Il termine chiave è l'*uniformità* dell'operazione di cloning, che è espressa formalmente dalla *naturalità monoidale* della diagonale.

Nel caso della categoria **Set** il seguente processo:

$$\{\Delta_X : X \to X \times X :: x \mapsto (x, x) \mid X \in |\mathbf{Set}|\}$$

costituisce una operazione uniforme di copia, dal momento che il corrispondente diagramma commuta:

$$\begin{array}{ccc} X & \xrightarrow{x \mapsto f(x)} & Y \\ \downarrow{\scriptstyle x \mapsto (x,x)} & & \downarrow{\scriptstyle f(x) \mapsto (f(x), f(x))} \\ X \times X & \xrightarrow{(x,x) \mapsto (f(x), f(x))} & Y \times Y \end{array}$$

Dato che le funzioni sono particolari relazioni, si può provare a considerare la medesima Δ_X definita sopra, che costituisce una diagonale per **Set**, e capire se costituisce una diagonale anche per **Rel**.
Tuttavia, il diagramma di copia nel caso delle relazioni non commuta, è immediato un controesempio che coinvolge un morfismo tra $I_{\mathbf{Rel}} = \{*\}$ e i booleani $\mathbb{B}$:

$$\begin{array}{ccc} \{*\} & \xrightarrow{\{(*,0),(*,1)\}} & \{0,1\} \\ \downarrow{\scriptstyle \{(*,(*,*)\}} & & \downarrow{\scriptstyle \{(0,(0,0)),(1,(1,1))\}} \\ \{(*,*)\} = \{*\} \times \{*\} & \xrightarrow{\{(*,0),(*,1)\} \times \{(*,0),(*,1)\}} & \{0,1\} \times \{0,1\} \end{array}$$

Infatti lungo il primo percorso si ottiene lo stato

$$\{(*,(0,0)),(*,(1,1))\} = \{*\} \times \{(0,0),(1,1)\}$$

mentre il secondo percorso porta a

$$\{(*,(0,0)),(*,(0,1)),(*,(1,0)),(*,(1,1))\} = \{*\} \times (\{0,1\} \times \{0,1\})$$

Analogamente a quanto osservato nel caso delle relazioni, si ha che per **FdHilb** non esiste una operazione uniforme di copia. Si è visto infatti che se si tenta di definire una diagonale

$$\Delta_{\mathcal{H}} : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H} :: \psi \mapsto \psi \otimes \psi$$

si giunge immediatamente ad un assurdo dal momento che essa non è nemmeno lineare. Se però si fissa una base ortonormale $\{|i\rangle\}_i$, si può considerare

$$\{\Delta_{\mathcal{H}} : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H} :: |i\rangle \mapsto |i\rangle \otimes |i\rangle \mid \mathcal{H} \in |\mathbf{FdHilb}|\}$$

Tuttavia il diagramma di seguito non commuta:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{1 \mapsto |0\rangle + |1\rangle} & \mathbb{C} \oplus \mathbb{C} \\ \downarrow{\scriptstyle 1 \mapsto 1 \otimes 1} & & \downarrow{\scriptstyle \begin{array}{l} |0\rangle \mapsto |0\rangle \otimes |0\rangle \\ |1\rangle \mapsto |1\rangle \otimes |1\rangle \end{array}} \\ \mathbb{C} \cong \mathbb{C} \otimes \mathbb{C} & \xrightarrow{1 \otimes 1 \mapsto (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)} & (\mathbb{C} \oplus \mathbb{C}) \otimes (\mathbb{C} \oplus \mathbb{C}) \end{array}$$

dal momento che lungo il primo percorso di ottiene lo stato entangled

$$1 \mapsto |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$$

mentre lungo il secondo si ottiene lo stato separabile

$$1 \mapsto (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)$$

L'impossibilità di definire una operazione uniforme di copia è un'ulteriore espressione dell'impossibilità di clonare un generico stato puro quantistico, stavolta però resa nel formalismo dei diagrammi commutativi.
Nel formalismo delle categorie si formalizza l'idea di separabilità definendo un *prodotto*:

Definizione 19. Un *prodotto* di $A_1,\ A_2 \in |\mathbf{C}|$ è una tripla $(A_1 \times A_2, \pi_1, \pi_2)$:

$$A_1 \times A_2 \in |\mathbf{C}| \qquad \pi_1 : A_1 \times A_2 \to A_1 \qquad \pi_2 : A_1 \times A_2 \to A_2$$

tale che $\forall\ C \in |\mathbf{C}|$ la seguente mappa:

$$(\pi_1 \circ -, \pi_2 \circ -) : \mathbf{C}(C, A_1 \times A_2) \to \mathbf{C}(C, A_1) \times \mathbf{C}(C, A_2)$$

ammetta un'inversa $\langle -, - \rangle_{C,A_1,A_2}$.

La precedente proprietà richiede che tutti i morfismi di una categoria siano decomponibili in modo biunivoco nel prodotto di isomorfismi agenti su singoli oggetti.
Il prodotto tensore di **FdHilb** non costituisce pertanto un prodotto nel senso categoriale del termine, dal momento che la dualità stato-processo esclude di poter separare nel modo sopra descritto tutti i processi equivalenti a stati entangled.

Definizione 20. Una categoria $\mathbf{C}$ è detta *cartesiana* se ogni coppia di oggetti $A, B \in |\mathbf{C}|$ ammette un non necessariamente unico *prodotto*.

La categoria **Set** è cartesiana. Vale infatti il seguente risultato:

Proposizione 2. Ogni categoria cartesiana ammette una operazione di copia uniforme.

Considerando infatti

$$\Delta_A := \langle 1_A, 1_A \rangle$$

e una qualsiasi $A \xrightarrow{f} B$ si ha;

$$\langle 1_B, 1_B \rangle \circ f = \langle 1_B \circ f, 1_B \circ f \rangle = \langle f \circ 1_A, f \circ 1_A \rangle = (f \times f) \circ \langle 1_A, 1_A \rangle,$$

ciò verifica dunque che Δ è una trasformazione naturale, e dunque una operazione di copia uniforme.

Capitolo 4

Conclusioni

Ricapitolando, l'impossibilità di clonare generici stati puri quantistici è stata scoperta osservando i processi tra sistemi fisici, emergendo come conseguenza della loro natura lineare. Tale limitazione è stata quindi espressa come teorema No-cloning, nel formalismo algebrico degli spazi di Hilbert.
Si è visto poi come il formalismo degli string diagrams, basandosi sulle ipotesi del tutto generali di una teoria qualsiasi, consenta di dimostrare l'esistenza della medesima limitazione attraverso un teorema differente dal primo, il Cloning-Collapse. Si presenta di seguito il risultato che consente di connettere tra loro i due percorsi:

Teorema 6. Gli string diagrams sono completi rispetto alle categorie chiuse compatte dagger. In particolare è possibile dimostrare che due morfismi f e g sono uguali tramite le equazioni di una categoria chiusa compatta dagger *se e solo se* possono essere espressi dallo stesso string diagram.

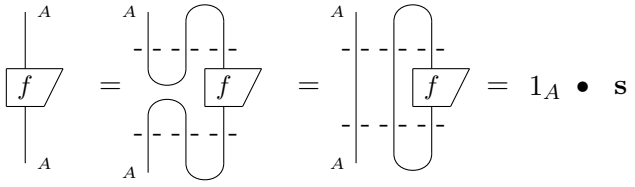
Dal momento che la categoria $\mathbf{FdHilb}(\mathcal{H}, \otimes, \mathbb{C})$, i cui processi sono mappe lineari tra spazi di Hilbert, risulta essere una categoria chiusa compatta dagger, si ha il seguente

Corollario 2 (**Selinger,** 2007)**. FdHilb** è completo rispetto agli string diagrams.

In particolare ciò significa che qualsiasi equazione tra string diagrams che coinvolga come processi $f, g, h, ...$ mappe lineari e loro aggiunte è valida in generale, si intende per tutte le possibili mappe lineari $f, g, h, ...$. Ciò permette di trarre conclusioni sulle mappe lineari anche senza doverle definire in modo preciso, trattandole come box.
Il teorema Cloning-Collapse, la cui dimostrazione è stata espressa nell'agevole formalismo degli string diagrams, può essere enunciato con riferimento specifico ad una teoria chiusa compatta dagger, e di conseguenza è possibile applicarlo ad **FdHilb**:

Teorema 7. Sia **C** una categoria compatta che ammetta cloning. Allora ogni endomorfismo è un multiplo scalare dell'identità. Più precisamente, $\forall f : A \to A$, $f = s \bullet 1_A$, con $s = \mathrm{Tr}(f)$.

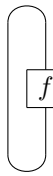
Il precedente risultato è derivabile con gli string diagrams utilizzando le uguaglianze dimostrate nel Cloning-Collapse:



Come è noto, nel caso degli spazi di Hilbert finito dimensionali esistono endomorfismi che non sono multipli dell'identità, di conseguenza non è ammesso il cloning.
Dal precedente risultato consegue che, essendo il Cloning-Collapse applicabile alla teoria quantistica dell'informazione, l'impossibilità di clonare un generico stato puro è una proprietà intrinseca della struttura matematica di **FdHilb**, una *feature* che ha origine nella *non separabilità* dei suoi stati. Espresso in termini fisici, è impossibile adattare una operazione di copia uniforme all'entanglement senza cadere nella degenerazione.

Dimensione infinita

Gli argomenti finora trattati hanno riguardato sempre e solo gli spazi di Hilbert a dimensione finita, isomorfi cioè a $\mathbb{C}^n$, $n \in \mathbb{N}$. Il motivo è che gli spazi di Hilbert a dimensione infinita e base numerabile, isomorfi a ℓ_2[1], non soddisfano gli assiomi di una categoria chiusa compatta dagger, non consentendo di definire i morfismi di unità e di counità, ed equivalentemente i cup e i cap. Si nota infatti che gli operatori definiti nell'Esempio 7 non sono estendibili naturalmente al caso infinito dimensionale, dal momento che estendendo la sommatoria ad un numero infinito di elementi non è più possibile definirne la traccia e un cup così definito non costituisce più uno stato.
In accordo con il precedente argomento si può notare come la versione categoriale del teorema Cloning-Collapse al paragrafo precedente presuma l'esistenza della traccia di un processo, costituita da uno scalare, rappresentato dal seguente diagramma:



$$= \quad \mathrm{Tr(f)} \quad \overset{\star}{=} \frac{1}{\dim_{\mathbb{C}}(\mathcal{H})} \Big(\sum_i \langle i| \otimes \langle i| \Big) \circ (1_{\mathcal{H}} \otimes f) \circ \Big(\sum_j |j\rangle \otimes |j\rangle \Big) = \sum_i \langle i| \, f \, |i\rangle$$

in cui $\star$ è l'interpretazione nel caso di uno spazio di Hilbert. Qualora non risulti definita la traccia, e quindi nel caso degli spazi infinito dimensionali, la precedente equazione perde di significato. Per spazi di Hilbert generici non risulta quindi applicabile il teorema Cloning-Collapse, resta comunque valido il teorema No-cloning, che si basa sull'unitarietà dei processi. Si verifica infatti che gli spazi di Hilbert generici muniti di operatori lineari limitati soddisfano gli assiomi di una categoria monoidale simmetrica e quindi sono ben definiti solo rispetto ai circuiti.

[1] spazio di Hilbert delle successioni $\ell_2 := \{z \equiv (z_n)_{n=1}^{\infty}, z_n \in \mathbb{C}, \text{tali che} \sum_{n=1}^{\infty} |z_n|^2 < \infty\}$

Bibliografia

[1] Abramsky, S. 2010 No-cloning in categorical quantum mechanics. *Semantic Techniques in Quantum Computation,* pages 1–28. Cambridge University Press.

[2] Abramsky, S. and Coecke, B. 2009. Categorical quantum mechanics. *Handbook of quantum logic and quantum structures*, 43, Pages 261-325. Elsevier.

[3] Coecke, Bob 2006. Introducing categories to the practicing physicist. *What is category theory? Advanced Studies in Mathematics and Logic*, 30, Pages 45-74. Polimetrica Publishing.

[4] Coecke, B. 2010. Quantum picturalism. *Contemporary Physics*, 51, Pages 59–83.

[5] Coecke, B., and Paquette, E'. O. 2011. Categories for the practicing physicist. *New Structures for Physics*, Pages 167–271. Lecture Notes in Physics. Springer.

[6] Coecke, B., and Kissinger, A. 2015. Categorical Quantum Mechanics I: Causal Quantum Processes. *Categories for the Working Philosopher*, Pages 286-328.

[7] Coecke, B., and Kissinger, A. 2017. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning.* Cambridge: Cambridge University Press.

[8] Dieks, D. G. B. J. 1982. Communication by EPR devices. *Physics Letters A*, 92(6), pages 271–272.

[9] Lectured by Reutter, D. and Vicary, J. Notes by Heunen, C., and Vicary, J. 2019. Categorical Quantum Mechanics An Introduction. Department of Computer Science, University of Oxford.

[10] Einstein, A., Podolsky, B., and Rosen, N. 1935. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10), 777.

[11] Selinger, P. 2007. Dagger compact closed categories and completely positive maps. *Electronic Notes in Theoretical Computer Science*, 170, pages 139–163.

[12] Wootters, W., and Zurek, W. 1982. A single quantum cannot be cloned. *Nature*, 299, pages 802–803.

[13] Griffiths, D. J., and Schroeter, D. F. 2018 *Introduction to Quantum Mechanics.* Third ed. Cambridge United Kingdom: Cambridge University Press.

[14] Abate, M., and Tovena, F. 2011. *Geometria differenziale.* Springer, Italia.

[15] Teh, Nicholas J. 2011 Classical Cloning and No-cloning. *Studies in the History and Philosophy of Modern Physics*, 43, pages 47-63.

[16] Benenti, G., Casati, G. and Strini, G. 2004 *Principles of Quantum Computation and Information, Volume. I: Basic Concepts.* World Scientific, Singapore City.

[17] Benenti, G., Casati, G. and Strini, G. 2007 *Principles of Quantum Computation and Information, Volume. II: Basic Tools and Special Topics.* World Scientific, Singapore City.

[18] Backens, M. 2016. *Completeness and the ZX-calculus.* PhD thesis, University of Oxford. arXiv:1602.08954