

Numero XXII  
Anno 2023



Viaggio nella Scienza

# Ithaca

Euclid e l'energia oscura

---

## **Ithaca: Viaggio nella Scienza**

---

Una pubblicazione del Dipartimento di Matematica e Fisica “*Ennio De Giorgi*” dell’Università del Salento

Registrazione presso il Tribunale di Lecce n. 6 del 30 Aprile 2013. e-ISSN: 2282-8079

Direttrice Responsabile  
**Loredana De Vitis**

Ideatore  
**Giampaolo Co’**

Comitato di redazione  
**Adriano Barra,**  
**Rocco Chirivì,**  
**Paolo Ciafaloni,**  
**Maria Luisa De Giorgi,**  
**Vincenzo Flaminio,**  
**Luigi Martina,**  
**Giuseppe Maruccio,**  
**Marco Mazzeo,**  
**Francesco Paparella,**  
**Carlo Sempi.**

Segreteria di Redazione  
**Daniela Dell’Anna**

© 2023-2033 Dipartimento di Matematica e Fisica “*Ennio De Giorgi*”  
© 2023 per i singoli articoli dei rispettivi autori. Il materiale di questa pubblicazione può essere riprodotto nei limiti stabiliti dalla licenza “Creative Commons Attribuzione - Condividi allo stesso modo 3.0 Italia” (CC BY-SA 3.0 IT).

Per il testo della licenza: <http://creativecommons.org/licenses/by-sa/3.0/it/deed.it>

**Ithaca: Viaggio nella Scienza**  
è disponibile al sito  
<http://ithaca.unisalento.it>

Scriveteci all’indirizzo  
[ithaca@unisalento.it](mailto:ithaca@unisalento.it)

# Ithaca

## Viaggio nella Scienza

---

XXII 2023

**3** In questo numero

**5** Come Euclid ci aiuterà a scoprire la storia dell'Universo

Vincenzo F. Cardone

**11** Un universo oscuro

Luigi Tedesco

**43** Euclid

Stefano Dusini, Luca Stanco

**55** La Computazione Quantistica

Luigi Martina

**91** La distribuzione quantistica di chiavi

Samuele Altilia, Michele N. Notarnicola, Stefano Olivares

**105** La seconda rivoluzione quantistica: il computer quantistico e la crittografia.

Taira Giordani, Alessia Suprano, Fabio Sciarrino

**113** Dequantizzazione Geometrica

Giuseppe Marmo, Alessandro Zampini

---

# In questo numero

---

Questo numero è nettamente suddiviso in due parti. Una prima parte raccoglie una serie di articoli legati alla missione spaziale “EUCLID” lanciata il primo Luglio 2023 dalla base di Cape Canaveral. L’articolo di Vincenzo Cardone presenta gli obiettivi scientifici della missione. Una dettagliata presentazione dei problemi cosmologici sui quali la missione “EUCLID” cercherà di far luce, energia oscura e materia oscura, è fornita da Luigi Tedesco. In questo articolo sono anche riassunti in quadro organico alcuni temi già trattati in articoli pubblicati su precedenti numeri di **Ithaca** [1, 2, 3, 4]. Una descrizione dettagliata della missione, anche nei suoi aspetti tecnici, è presentata nell’articolo di Stefano Dusini e Luca Stanco.

Dopo questi primi tre articoli legati alla missione “EUCLID” appaiono tre articoli che discutono di Computazione Quantistica. L’articolo di Luigi Martina fa un’ampia panoramica sui diversi aspetti legati alla Computazione Quantistica, parte da questioni strettamente legate alla teoria della Meccanica Quantistica come l’*entanglement* per arrivare a discutere di algoritmi e sfiora anche argomenti di tipo tecnologico ed economico. Gli articoli di Samuele Altilia, Michele N. Notarnicola, Stefano Olivares e quello di Taira Giordani, Alessia Suprano, Fabio Sciarrino sono più focalizzati su uno specifico aspetto legato alla Computazione Quantistica, quello della Crittografia. Il tema è affrontato da due differenti punti di vista che si compendiano e offrono una visione ampia del problema, accennato già da Luigi Martina.

Conclude il numero un articolo di Giuseppe Marmo e Alessandro Zampini, sempre legato alla Meccanica Quantistica. Il tema di questo articolo riguarda un problema contrario a quello che

usualmente di affronta nella presentazione didattica della Meccanica Quantistica. Normalmente ci preoccupa del passaggio dalla Meccanica Classica alla teoria della Meccanica Quantistica. In questo articolo si inverte il problema, ovvero come passare dalla Meccanica Quantistica a quella Classica.

Buona lettura,  
il Comitato di Redazione



- [1] F. De Paolis, M. Giordano, G. Ingrosso, L. Manni, A. Nucita, F. Strafella: *Macro / micro / retro "lensing" gravitazionale*, Ithaca, V (2015) 19.
- [2] Marco Cirelli: *La Materia Oscura*, Ithaca, XII (2018) 117.
- [3] Massimo Pietroni: *Energia Oscura, il motore dell’Universo*, Ithaca, XII (2018) 129.
- [4] M. Gasperini: *Teoria Gravitazionale e Applicazioni Cosmologiche: Possibili Sviluppi Futuri*, Ithaca, XXI (2023) 47.





---

# Come Euclid ci aiuterà a scoprire la storia dell'Universo

**Vincenzo F. Cardone**

*Istituto Nazionale di Astrofisica, Osservatorio Astronomico di Roma*

---

**A** metà del secolo scorso Allan Sandage, uno dei maggiori astronomi del tempo, era solito dire che la cosmologia si riduceva alla ricerca di due numeri: la costante di Hubble e il parametro di decelerazione. La prima ci dice quanto velocemente l'universo si sta espandendo, mentre il secondo permette di rispondere alla domanda se questa espansione stia accelerando o rallentando. Settanta anni dopo, quella frase ha lo stesso valore di un reperto archeologico. Ci mostra quale fosse il pensiero dominante di un'epoca e ci fa capire quanto cammino abbiamo fatto da allora. Quei due numeri oggi li conosciamo e, soprattutto, sappiamo che cosa li determina. Conosciamo, quindi, dove dobbiamo guardare per rispondere alla domanda di Sandage su quale sia il valore dell'accelerazione dell'espansione dell'universo.

Un successo? Sì, ma anche no. Perché, spesso, in cosmologia, ogni risposta si paga con nuove domande. Oggi sappiamo, infatti, che l'universo si espande in maniera accelerata e che la sua geometria è quella di uno spazio con curvatura nulla.

A dircelo sono i dati osservativi che in questi anni si sono accumulati in uno spettacolare crescendo di scoperte. Si stava per chiudere il millennio quando due *team* indipendenti pubblicavano i primi diagrammi di Hubble delle Supernovae di Tipo Ia (SNeIa) [1, 2]. Di questi oggetti stellari è possibile determinare, con una certa sicurezza, la luminosità assoluta per cui, misurando quella apparente, è possibile stimare la distanza. Il diagramma di Hubble è semplicemente un grafico della distanza in funzione del *redshift* e dipende a sua volta da come l'universo si sta espandendo (si vedano i due riquadri). Ebbene, le SNeIa in quel diagramma si trovano a distanze maggiori di dove ci si aspettava. Motivo? L'universo si sta espandendo in maniera accelerata. La cinematica dell'universo era così nota: l'espansione è un'auto che corre accelerando. Ma la pista come è fatta? Che geometria ha? Serviva tornare ancora più indietro nel tempo ed osservare di nuovo quella radiazione cosmica di fondo a microonde (CMBR secondo l'acronimo inglese) che per prima aveva fatto scoprire ai cosmologi che l'universo aveva avuto un inizio. Questo relitto dei primi minuti di vita del cosmo non è perfettamente isotropo. La temperatura della CMBR ha delle piccolissime differenze (dell'ordine di una parte su centomila), ma è proprio il modo in cui queste sono distribuite a

## Espansione dell'universo e costante di Hubble

Immaginate due punti disegnati su un palloncino sgonfio. Se gonfiate il palloncino, i due punti continueranno a restare immobili al loro posto, eppure la loro distanza aumenterà. L'universo non è un palloncino che si gonfia perché non c'è nulla intorno a lui in cui allargarsi, ma l'analogia è comunque utile a capire che cosa intendono i cosmologi come espansione dell'universo. In un certo senso, è come se voi continuaste a misurare la distanza tra due punti e questo numero aumenta perché sono le tacche sul righello ad allontanarsi. Questo righello è quello che in cosmologia è chiamato fattore di scala. Quando si inserisce la metrica di un sistema omogeneo ed isotropo nelle equazioni della relatività generale di Einstein, si ottengono le equazioni di Friedman che permettono, tra le altre cose, di stimare come varia con il tempo questo fattore di scala in base al contenuto di energia e materia e alle proprietà di queste ultime. La derivata prima del fattore di scala rispetto al tempo è diversa da zero il che vi dice che l'universo non è statico, ma in evoluzione. Quanto veloce è questa evoluzione al giorno d'oggi è quantificato dalla costante di Hubble ossia il rapporto tra la derivata prima, rispetto al tempo del fattore di scala ( $\dot{a}$ ) e il fattore di scala stesso

$$H = \frac{\dot{a}}{a} . \quad (1)$$

È questo il primo dei due numeri a cui faceva riferimento Sandage.

Il secondo è invece legato al segno della derivata seconda ( $\ddot{a}$ ), sempre rispetto al tempo. Per rendere adimensionale questo parametro lo si divide per  $H^2 a$ . Pertanto il parametro di decelerazione è dato dall'espressione

$$q = -\frac{\ddot{a}a}{\dot{a}^2} , \quad (2)$$

dove il segno negativo venne introdotto perché ai cosmologi piaceva avere a che fare con numeri positivi e la convinzione ai tempi era che l'espansione rallentasse cioè derivata seconda negativa. Con questa definizione il parametro di decelerazione sarebbe stato positivo. Ma i dati oggi ci dicono il contrario per cui i cosmologi di allora devono rassegnarsi ad avere un valore negativo.

dirci quale è la geometria dell'universo. Bisogna però misurare con precisione quello che si chiama spettro di anisotropia ossia il modo in cui queste differenze sono spazialmente correlate. Lo spettro avrà diversi picchi e sono la posizione e l'altezza relativa di questi a dirci qual è la geometria dell'universo e quanta materia c'è in esso. Un satellite americano prima (WMAP [3]) e uno europeo poi (Planck [4]) hanno dato la risposta che aspettavamo. L'universo è piatto, ossia ha una geometria sorprendentemente euclidea. Certo, qualche residua possibilità che la curvatura sia non nulla esiste ancora, ma le probabilità sono talmente basse da poter concludere che quanto detto sopra è corretto. Viviamo in un cosmo che ha una geometria piatta ed è in espansione accelerata.

Sappiamo anche il perché. Il contenuto ener-

getico dell'universo è dominato da quella che chiamiamo "energia oscura" che determina l'espansione accelerata, mentre a tenere insieme il tutto fornendo la gravità necessaria a formare le strutture che osserviamo è la "materia oscura". Due componenti accomunate nel nome dall'aggettivo "oscuro", ma nettamente diverse nelle proprietà fisiche. Soprattutto perché la prima ha una pressione negativa, mentre la seconda contribuisce ad aumentare la gravità che tiene legate le stelle all'interno delle galassie e le galassie negli ammassi. Due forze opposte che si contendono il dominio del contenuto energetico dell'universo con la prima a vincere oggi fornendo quella spinta necessaria ad accelerare l'espansione motivando così la cinematica osservata. Ah, giusto per dire, quella energia oscura è consistente con quella costante cosmologica che lo stesso Einstein

## Redshift

Gli astronomi guardano il cielo e il cielo è una splendida tela punteggiata di stelle e galassie, ma anche un problema pratico: ha solo due dimensioni. Come misurare la terza? Ossia, come quantificare le distanze relative tra gli oggetti che vediamo proiettati su quella tela? Ci viene in soccorso un fenomeno noto anche nella vita di tutti i giorni. Pensate ad un'ambulanza che si avvicina. Il suono della sirena sembrerà più acuto di quando invece si allontana. Questo perché le onde sonore in avvicinamento hanno una lunghezza d'onda minore rispetto a quelle emesse dall'ambulanza che si allontana. Lo stesso avviene per la luce emessa dalle sorgenti astrofisiche. Più sono lontane da noi, più la lunghezza d'onda della radiazione emessa è maggiore ossia è spostata verso la zona dello spettro che definiamo rossa (perché questo sarebbe il colore che vedremmo se restiamo nella banda visibile). Quindi, maggiore distanza, maggiore spostamento verso il rosso, in inglese *redshift*. Ecco la terza dimensione che gli astronomi usano per trasformare la visione bidimensionale del cielo in una mappa 3D. Ma c'è di più. Poiché la luce impiega un certo tempo finito a percorrere la strada dalla sorgente a noi, maggiore è il *redshift*, maggiore sarà il tempo impiegato a raggiungerci ossia tanto più tempo fa la luce è partita. Per questo motivo guardare sorgenti ad alto *redshift* significa guardare l'universo come era tanto tempo fa. Insomma, il *redshift* di un oggetto ci dice non solo quanto è distante da noi la sorgente luminosa (il dove), ma anche quale era l'età dell'universo al momento in cui la luce è partita (il quando). Un solo numero per passare dalla tela del cielo al dove e quando del cosmo.

aveva introdotto nella sua teoria per poi pentirsi e ritrattare troppo presto. E che ci debba essere nel conto non è più il frutto di una intuizione geniale dettata da un motivo puramente opportunistico. C'è quella costante cosmologica perché il vuoto stesso ha una sua energia e non perché, come ad Einstein sarebbe piaciuto, l'universo possa restare uguale a sé stesso in eterno senza mai espandersi. Costante cosmologica e materia oscura sono i due pilastri che reggono il modello  $\Lambda$ CDM. *Nomen omen*,  $\Lambda$ CDM =  $\Lambda$  + CDM a ricordare i due protagonisti di questa storia: la costante cosmologica  $\Lambda$  e la Cold Dark Matter. Una accoppiata così vincente da essere in accordo talmente buono con le osservazioni a disposizione da essere definita come **Concordance Model** perché, appunto, mette d'accordo tutti.

Tutti contenti, quindi? Sì, ma anche no. E quell'anche no è racchiuso nell'aggettivo che abbiamo usato per battezzare i due costituenti principali del modello: oscuro. Più del 95% dell'universo è composto da energia e materia oscura ossia da due componenti di cui non conosciamo né la natura né le proprietà. E, quando non si sa qualcosa, l'unica via che i cosmologi possono percorrere è affidarsi a tanta buona volontà, alla

metaforica carta e penna e alla fantasia mediata dal rigore delle equazioni. Il risultato è una messe di teorie che predicono come l'universo si espande e come quelle minuscole disomogeneità che appaiono come puntini sulla mappa della temperatura della radiazione cosmica di fondo sono cresciute per diventare le spettacolari galassie che ci affascinano nelle immagini ottenute con i grandi telescopi a terra e con quei nostri occhi nello spazio che sono i satelliti come Hubble e JWST. Risposte tanto diverse che si fa fatica a credere che possano spiegare le stesse osservazioni.

Ad esempio, che cos'è l'energia oscura? La costante cosmologica, ovvio. No, invece, perché l'energia del vuoto la puoi calcolare e il risultato è in disaccordo con la misura per ben 133 ordini di grandezza. E allora forse non è costante per niente, ma la sua equazione di stato (che regola la relazione tra pressione e densità) cambia col tempo. Ma questo sposta solo il problema da "che cos'è l'energia oscura?" a "quale è la sua equazione di stato?" e scoprire questo arcano è impresa più ardua di quella precedente. Perché di formule per quella quantità e di motivi per cui debba avere questa o quella forma ne sono state proposte a iosa e tutte fanno il loro dovere: sono

in accordo con i dati osservativi.

Contenti? Ancora no, ovviamente. Perché avere tante teorie che spiegano i dati è lo stesso che non averne nessuna. Avere mille risposte ugualmente valide alla stessa domanda significa ritrovarsi al via dopo essersi sforzati di partire a tutta velocità. Ma se le risposte sono così tante è perché la domanda era troppo vaga. Detto in termini più pratici, i dati che abbiamo al momento non sono in grado di dirci quale teoria è quella giusta perché non sono sufficientemente precisi o non ci danno informazioni su quelle quantità che potrebbero discriminare tra teorie diverse. Diverse in cosa? Nelle previsioni che fanno sul modo in cui l'universo si espande? Di nuovo: sì, ma anche no. Perché teorie pure radicalmente differenti possono prevedere la stessa espansione accelerata. Ma non la stessa crescita delle strutture. Ci serve, quindi, qualche osservabile che ci dia informazioni su entrambi gli aspetti: evoluzione e crescita.

La natura sarà anche maligna come ha imparato a sue spese l'immaginario viaggiatore islandese di Leopardi, ma non lo è tanto da non offrirci gli strumenti adatti per imparare a conoscere il cosmo. Per capirlo, dobbiamo fare un passo indietro nel tempo. Tornare a quel 1915 in cui Einstein (sempre lui) formulò la sua teoria della relatività generale che ci insegna che la gravità deforma lo spazio-tempo. Conseguenza ne è che la traiettoria più breve tra due punti sarà diversa a seconda che nel mezzo ci sia o no una distribuzione di materia. Se i due punti sono una sorgente luminosa distante, che sia una stella o una galassia, e un osservatore dall'altro lato di un telescopio, quello che accadrà è che l'immagine dell'oggetto apparirà diversa da quella che realmente è. Questo effetto è ciò che chiamiamo **lensing gravitazionale** dall'analogia con il ben noto fenomeno delle lenti in ottica geometrica. Se le distanze coinvolte sono su scala cosmologica, il raggio di luce nel suo percorso incontrerà la distribuzione della materia dell'universo stesso e viaggerà mentre l'espansione sta avendo luogo. La distorsione dell'immagine è, quindi, una misura indiretta dell'espansione e della crescita. È, cioè, quello che stavamo cercando. Solo che tra il dire e il fare c'è di mezzo... la natura maligna che ci complica le misure. Dal momento che l'universo è in media omogeneo e isotropo,

la distorsione dovuta al lensing gravitazionale è talmente piccola che non si può misurare direttamente. Fine dei giochi? No, perché c'è un altro effetto che possiamo sfruttare. Nell'ipotesi ragionevole che le galassie siano orientate in maniera casuale, la media su un numero molto grande di galassie darebbe una ellitticità media nulla<sup>1</sup>. Se non ci fosse, appunto, il *lensing* gravitazionale! La media non farà zero, ma sarà uguale proprio a quella distorsione minuscola che pensavamo di non poter misurare. Di più. Se riuscissimo a fare questa misura in diversi punti del cielo, potremmo studiare come queste distorsioni sono correlate ossia, semplificando grossolanamente, quale è la probabilità che, avendo osservato una certa distorsione qui ed ora, si trovi lo stesso valore lì e allora, dove lì e allora sono misurati dalla distanza angolare sul cielo e dal *redshift*. E questa misura sappiamo come prevederla per cui il gioco è ora trovare nel pagliaio di teorie l'ago che ci pungerà proprio nel modo giusto. Ossia, fuor di metafora, il valore dei parametri della teoria che prevedono una correlazione a due punti dello *shear* in accordo con quella misurata.

Detto, fatto? Eh, magari. Già il primo passo di questa avventura rischia di incastrarsi in una buca o di schiacciare una mina. Perché le distorsioni di cui sopra sono comunque piccole per cui bisogna essere sicuri di aver misurato correttamente la forma delle galassie rimuovendo tutti quegli effetti che possono mimare quello del *lensing* gravitazionale. Per esempio, bisogna rimuovere l'effetto dell'atmosfera terrestre, il che si può fare nel modo migliore andando nello spazio. Poi sottrarre le distorsioni dovute agli strumenti il che richiede di caratterizzare accuratissimamente i parametri che caratterizzano le ottiche del telescopio e della camera ed essere sicuri che i loro valori siano stabili nel tempo. Bisogna che l'immagine sia nitida e non sommersa nel rumore il che richiede lunghi tempi di esposizione o un filtro ampio o un telescopio con

<sup>1</sup>L'ellitticità di una galassia è un vettore che permette di quantificare la sua forma. Se approssimiamo la galassia come un'ellisse con asse maggiore  $a$  e asse minore  $b$ , la sua ellitticità è un vettore le cui due componenti sono  $(e_1, e_2) = (e \cos \alpha, e \sin \alpha)$  dove il modulo è  $e = \sqrt{(a^2 - b^2)/(a^2 + b^2)}$ , e l'orientazione è data da  $\alpha = \arctan(b/a)$ . Poiché, in assenza di *lensing* gravitazionale, l'orientazione è casuale, la media di  $(e_1, e_2)$  è nulla.

grande specchio primario. Ed ancora non basta. Perché se vogliamo studiare le correlazioni nello spazio e nel tempo dobbiamo mappare un'area molto grande ed arrivare a *redshift* alti. Insomma, l'ideale è una *survey* fotometrica a grande area e profonda eseguita da un telescopio con ottiche stabili e una camera a grande campo e grande risoluzione in orbita nello spazio. C'è? Sì, Euclid!

Euclid eseguirà quella che viene definita una *survey* di *lensing* gravitazionale di quarta generazione. Unirà precisione, profondità, area, risoluzione e stabilità per permettere una misura tomografica (ossia a diversi *redshift*) dello spettro di potenza (che altro non è che un modo diverso di quantificare le correlazioni di cui dicevamo prima) dello *shear* cosmico ossia l'effetto di *lensing* gravitazionale della struttura su larga scala. Ma Euclid potrà fare ancora di più. Perché, infatti, limitarsi ad una correlazione a due punti se hai galassie in abbondanza per misurare correlazioni a più punti? E perché accontentarsi di queste correlazioni se puoi costruire una mappa sul cielo della distribuzione di materia proiettata e dalle proprietà topologiche di questa ricavare informazioni ulteriori? Parlando in un linguaggio più tecnico, la quantità e qualità delle misure di *shear* fornite da Euclid permetterà di studiare il campo di distorsione usando statistiche di ordine superiore con una accuratezza finora impensabile. Tutte queste misure permetteranno di testare sia come l'universo si è espanso negli ultimi dieci miliardi di anni, sia come le perturbazioni di densità sono cresciute. Espansione e crescita: il binomio di cui avevamo bisogno per rendere più fitte le maglie del setaccio attraverso cui far passare la messe di teorie di cui parlavamo.

Un grande passo in avanti, ma perché accontentarsi e non provare a fare proprio un grande balzo? Si fa molta più strada saltando. Per capire come mettere le molle sotto le nostre suole, dobbiamo notare che il *lensing* gravitazionale è sensibile al prodotto di evoluzione e crescita, ma non i due singoli aspetti separatamente. È un po' come sapere che il risultato di una moltiplicazione di due numeri interi  $A$  e  $B$  è 36. Potete escludere tanti numeri, ma potete ottenere 36 se  $(A, B) = (2, 18)$  o  $(3, 12)$  o  $(4, 9)$  o  $(6, 6)$ . Quale sarà la combinazione giusta? Per scoprirlo ser-

ve qualcosa che misuri  $A$  o  $B$  individualmente. Ossia, venendo al caso nostro, qualcosa che misuri o la sola espansione o la sola crescita delle strutture.

Ancora una volta questo qualcosa c'è ed è il *galaxy clustering*. Torniamo a guardare il cielo, ma immaginiamo di poter misurare di ogni galassia non solo la sua posizione sulla volta celeste, ma anche la sua distanza. Potremmo costruire in questo modo una mappa tridimensionale dell'universo osservabile e andare anche a determinare se le strutture sono più o meno addensate tra di loro. Potremmo, cioè, determinare quale è la probabilità di trovare una galassia in una certa posizione di questa mappa 3D se so di averne già trovata una in una data posizione. L'oggetto matematico che quantifica questa proprietà è la funzione di correlazione che, nello spazio di Fourier (una sorta di artificio ideale che i cosmologi usano per semplificare alcuni conti) diventa lo spettro di potenza. Ed è qui che arriva il bello. A determinare quanto fitta è la rete che le galassie disegnano nello spazio-tempo è la gravità e come essa guida il processo di crescita delle strutture. Ossia, il *galaxy clustering* misura la crescita delle strutture. Proprio quello che cercavamo: una misura di  $A$  o di  $B$  e non di  $A \times B$ .

Ma come si fa una mappa 3D? Serve un telescopio che misuri non solo la posizione in cielo, ma anche il *redshift* con una accuratezza dell'ordine di una parte su mille. E lo deve fare, di nuovo, su un'area grande e in un intervallo di *redshift* ampio e ricco di informazioni. Servirebbe quella che viene definita una *survey* spettroscopica di quarta generazione. Ce l'abbiamo? Copia e incolla la risposta di prima: sì, è Euclid! La missione ESA misurerà la posizione e il *redshift* di oltre dieci milioni di galassie costruendo una mappa 3D dell'universo nel range di *redshift* compreso tra 0.9 e 1.8, ossia proprio quello che non era stato possibile testare con gli strumenti da terra nelle *survey* precedenti.

Manco a dirlo, c'è un problema anche qui. Anzi, più di uno, almeno tre. I nostri modelli teorici sono in grado di prevedere le proprietà di *clustering* degli aloni di materia oscura, ma quello che misuriamo è il *clustering* delle galassie. C'è una corrispondenza 1 a 1 tra le due cose? Purtroppo, no perché ogni alone può ospitare più di una galassia. Si dice, quindi, che lo spettro di potenza

delle galassie è una versione distorta di quello degli aloni e proprio questo *bias* è una ulteriore incognita che si aggiunge a quelle del modello cosmologico. Un problema che è anche un'opportunità. Misurare il *bias* ci permette, infatti, di discriminare tra diversi modelli di formazione delle galassie aggiungendo un tassello ulteriore alla nostra comprensione di come la luce delle galassie si accenda all'interno dell'oscurità degli aloni. Problema numero due: noi misuriamo il *redshift*, ma il *redshift* non è la distanza. Ci direbbe quale è la distanza della galassia se conoscessimo il modello cosmologico che è proprio quello che stiamo cercando di scoprire. Dobbiamo, quindi, introdurre una correzione che tenga conto dell'eventuale differenza tra il modello che abbiamo ipotizzato a priori essere quello giusto e quello che invece i dati ci dicono essere il più adatto a spiegarli. Infine, il moto relativo delle galassie l'una rispetto all'altra dipende da come evolve il potenziale gravitazionale della struttura su larga scala ossia da come le strutture cosmiche si assemblano. Ed anche la differenza tra le nostre ipotesi e i dati è una funzione di quei parametri cosmologici che vogliamo misurare.

Tre problemi che quindi, ci danno informazioni in più una volta che abbiamo capito come quantificarli e una volta che la nostra *survey* abbia sufficiente risoluzione in *redshift* e ampiezza in area di cielo per garantirne una misura. E, arrivati a questo punto l'avrete capito: Euclid ha entrambe le caratteristiche richieste.

*Lensing* gravitazionale più *galaxy clustering* su un'area di 15000 gradi quadrati (circa un terzo del cielo) e su un *range* che copre gli ultimi dieci miliardi di anni di storia dell'universo. Uno sguardo unico su come il cosmo si è espanso e su come le strutture sono cresciute. Il tutto in un'unica missione capace di fare ciò che le *survey* di galassie finora non sono riuscite a fare nonostante l'impiego delle migliori risorse osservative. Questo è Euclid: la luce che viene nelle tenebre per illuminare l'oscuro. Non vediamo l'ora di farci abbagliare!



[1] A. G. Riess et al.: *Observational Evidence from Supernovae for an Accelerating Universe and a Cosmological Constant*, *Astronomical Journal*, 116 (1998) 1009.

- [2] S. Perlmutter et al.: *Measurements of  $\Omega$  and  $\Lambda$  from 42 High-Redshift Supernovae*, *Astrophysical Journal*, 517 (1999) 565.
- [3] D. N. Spergel et al.: *First-Year Wilkinson Microwave Anisotropy Probe (WMAP) Observations: Determination of Cosmological Parameters*, *Astrophysical Journal Supplement Serie*, 148 (2003) 175.
- [4] P. A. R. Ade et al.: *Planck early results. XVIII. The power spectrum of cosmic infrared background anisotropies*, *Astronomy and Astrophysics*, 536 (2011) 1.

---

**Vincenzo F. Cardone:** è ricercatore presso l'Osservatorio Astronomico di Roma. Si occupa di *lensing* gravitazionale e modelli cosmologici ed è membro della collaborazione Euclid da più di dieci anni. In Euclid è *leader* del gruppo responsabile dell'estrazione dei parametri cosmologici dalle misure di *weak lensing* e *galaxy clustering*.

---

# Un universo oscuro

*Fare ricerca vuol dire guardare ciò che altri hanno visto e vedere ciò che gli altri non hanno guardato.*

---

**Luigi Tedesco**

Dipartimento interateneo di Fisica Università di Bari  
Istituto Nazionale di Fisica Nucleare, Sez. di Bari

---

**I**l Cosmo è molto più di quello che vediamo. Noi stessi, il nostro mondo, lo spazio nell'universo, è permeato da qualcosa che non conosciamo. Da un lato abbiamo una componente che sembra essere materia e formata da particelle che non conosciamo e che però costituiscono il cuore delle strutture nell'universo, la chiamiamo "materia oscura". Dall'altro lato una forma di energia, anch'essa di natura ignota e distribuita in modo uniforme ovunque, ma inosservata e con la particolarità di generare una potente forza antigravitazionale che costringe lo spazio nell'universo ad espandersi sempre più rapidamente, la chiamiamo "energia oscura". L'aggettivo oscura è la traduzione dall'inglese di *dark* che contiene più informazione di quanto non sia la sua traduzione italiana. Il significato di *dark* è legato non solo al fatto che queste due entità non si vedono, ma significa anche "non spiegate, misteriose", appunto, oscure. L'universo è composto per circa il 70% da energia oscura, il restante 30% da materia di cui circa il 25% è materia oscura e il 5% è materia ordinaria. Possiamo quantificare il tutto affermando che meno di 1/20 della densità totale del cosmo è il mondo che conosciamo, tutto il resto è un mistero fitto.



**Figura 1:** Percentuale in energia e materia di cui è composto l'universo

## Introduzione

L'uomo ha sempre cercato di capire di cosa siamo fatti. Nei secoli si sono scoperti elementi chimici che compongono la struttura della materia e in seguito si sono scoperte particelle quantistiche che hanno consolidato le nostre conoscenze su ciò di cui siamo fatti. Oggi tutto questo castello di conoscenze non fornisce più una visione onnicomprensiva della materia, ma neppure della energia, che si trova nell'universo. Entrambe assumono caratteristiche e proprietà completamente ignote. La cosa che accomuna la materia oscura e l'energia oscura è l'enorme portata concettuale, oltre al fatto che vengono coinvolte le nostre conoscenze su tutte le scale della fi-

sica dall'infinitamente piccolo all'infinitamente grande.

Le conoscenze attuali ci dicono che materia oscura ed energia oscura sono molto abbondanti nel cosmo, la somma delle due componenti è circa il 95% del contenuto dell'universo e queste proporzioni già di per sè rappresentano un vero enigma.

La materia ordinaria, che compone tutto ciò che conosciamo è circa il 5% del totale. La percentuale di massa in una galassia è composta da circa 10% materia ordinaria e 90% materia oscura. Questo rapporto non è costante, nel senso che vi son galassie piccole per cui il 99% è materia oscura.

Se della materia oscura non conosciamo praticamente nulla, sappiamo che è una forma di materia non ordinaria, per quanto riguarda l'energia oscura ne sappiamo ancora meno, perchè come vedremo, non capiamo il vero motivo per cui lo spazio vuoto nell'universo sembra avere una energia i cui effetti sono simili ad una forza anti-gravitazionale! Il termine "energia oscura" fu introdotto da M. Turner e da D. Huterer. Si tenne a Princeton nel 1996 un convegno dal titolo "Critical dialogues in cosmology" dove parteciparono studiosi di prima grandezza, come Jim Peebles, Martin Rees, Richard Gott, David Spergel e tanti altri. L'ultimo relatore fu Michael Turner dell'Università di Chicago che ipotizzò per la prima volta che l'universo potesse essere permeato da una energia costante che chiamò "energia oscura", e questo ben due anni prima della scoperta delle supernovae IA. I partecipanti rimasero molto freddi. La consacrazione del termine "energia oscura" avvenne successivamente con l'articolo di Ref. [1].

Nelle nostre dinamiche mentali, quando parliamo di materia oscura e di energia oscura facciamo riferimento a qualcosa che sta fuori da noi, nello spazio cosmico. Invece non è così, le due componenti oscure sono qui, nel nostro mondo, accanto al lettore di queste pagine, nella stanza in cui ci troviamo, invisibili e dappertutto. In questo momento miliardi di particelle della materia oscura ci stanno attraversando, senza che noi ce ne accorgiamo.

Diciamo subito che le due componenti oscure si differenziano perchè mentre la materia oscura, come vedremo, non è distribuita in modo omo-

geneo, ma è spesso solidale con la galassia, distribuendosi intorno e rappresenta circa 6/7 volte la materia ordinaria, l'energia oscura è 15 volte più abbondante della materia ordinaria ed è perciò la componente più presente nell'universo.

Da un punto di vista teorico, spiegare l'energia oscura è una avventura ancora più affascinante ed intrigante del mistero della materia oscura perchè essa è qualcosa di omogeneo, che permea tutto l'universo, senza buchi nonostante abbia una densità molto piccola. In un volume come la terra si può calcolare che vi sono circa 7 mg di essa.

La letteratura scientifica sulla materia oscura e sulla energia oscura è sterminata (si vedano i suggerimenti bibliografici alla fine di questo articolo) ed in questo articolo discuterò solo alcune linee generali per una semplice e non esaustiva panoramica. Non sarà una lezione, non ne ha le caratteristiche, ma solo una affascinante ed incompleta avventura intellettuale su uno dei più spinosi e incomprensibili misteri della natura.

## La materia oscura: un enigma che continua

### Zwicky (1898-1974)

Chi ha pronunciato per la prima volta la frase "materia oscura"? La prima notizia in questo senso risale al 1877 quando il gesuita e astronomo Angelo Secchi parla di "masse oscure" [2]; nel 1906 Henry Poincarè affermava che le stelle a noi vicine avendo un moto lento escludono la presenza di materia oscura<sup>1</sup>. Nei primi anni del secolo scorso, l'astronomo olandese Jacobus Cornelius Kapteyn e il britannico astronomo, matematico e fisico James Hopwood Jeans discutevano della presenza di materia oscura vicino al Sole in base alla velocità delle stelle. In [5] Kapteyn dice testualmente:

"It is incidentally suggested when the theory is perfected it may be possible to

<sup>1</sup>H. Poincarè, in Ref [3], usava un termine francese "matière obscure" in relazione ad un commento ad un calcolo di Lord Kelvin del 1884. Infatti Kelvin calcolò il numero di stelle attorno al Sole in base alla velocità di rotazione delle stesse stelle, stabilendo che forse molte di esse non erano luminose ma "corpi oscuri" [4].

determine 'the amount of dark matter' from its gravitational effect."

Nel 1930 Knut Lundmark comprese, per primo, che l'universo dovesse contenere più materia di quanto se ne osservava [6].

Kapteyn e il suo studente famoso Jan Hendrik Oort furono attaccati dal fisico svizzero Fritz Zwicky che, nel 1933, sosteneva che la materia oscura vicino al Sole fosse quantitativamente molto più presente (si veda Ref. [7]).

Nel 1932, Oort pensò alla esistenza di materia oscura vicino al Sole a causa di uno strano moto ortogonale al piano della Via Lattea di alcune stelle [8]. Nel 1933 Zwicky propose in modo sistematico il concetto di materia oscura. Egli studiò l'ammasso della Chioma di Berenice<sup>2</sup> che aveva ha 1000 galassie ed in particolare analizzò la velocità della galassie nell'ammasso [9]. Trovò che le velocità di rotazione erano eccessive e questo voleva dire che la somma delle masse delle singole galassie visibili era di gran lunga inferiore alla massa necessaria a far girare le galassie nell'ammasso, in modo da controbilanciare l'attrazione gravitazionale e quindi fuggire dall'ammasso stesso (dopo vedremo più in dettaglio questa questione).

Zwicky stimò che l'ammasso della Chioma dovesse avere 400 volte la somma di tutte le masse delle sue galassie e chiamò questo surplus di massa "materia oscura". In verità la stima era eccessiva perchè Zwicky trascurò la materia ordinaria sotto forma di gas intergalattico. Ma Zwicky fece un altro errore, perchè stimava in modo errato l'espansione dell'universo, parametro fondamentale se si vuole determinare la posizione delle galassie.

Un ricalcolo diceva che la quantità di massa necessaria era ~ 150 volte quella visibile affinché l'ammasso stesso non collassasse o non evaporasse, cioè raggiungesse l'equilibrio.

C'è da dire che gli astronomi dell'epoca per la maggior parte, forse tutti, erano convinti che migliorando le osservazioni la materia oscura sarebbe scomparsa per cui non diedero molto

<sup>2</sup>Questo ammasso non ha alcuna stella luminosa. Il nome fu dato nel 246 a.c. dal matematico Conone, maestro di Archimede, in onore della moglie di Tolomeo III, Berenice II. La chioma è visibile ad occhio nudo a forma di V vicino alla coda dell'Orsa Maggiore.



**Figura 2:** Ammasso della Chioma o Abell 1656. Si trova a circa 350 milioni di anni luce da noi. La maggior parte dei corpi nella foto è data da galassie. I corpi che presentano nella foto una croce invece sono stelle della nostra Via Lattea. *Image Credit: Russ Carroll, Robert Gendler, e Bob Franke; Dan Zowada Memorial Observatory.*



**Figura 3:** Fritz Zwicky nel suo studio

peso a questa novità che stava emergendo dalle analisi di Zwicky.

Certamente, come mise in evidenza l'astronomo olandese Sidney van der Bergh nel 1960 [10], con tale velocità di rotazione delle galassie attorno all'ammasso, si sarebbe avuta una evaporazione dell'ammasso stesso. Oggi sappiamo che negli ammassi di galassie, mediamente il 10% è materia ordinaria di cui il 9% è gas e l'1% galassie, il rimanente 90% è materia oscura.

Il lavoro di Zwicky fu dimenticato per quasi 40

anni (anche se questa cosa non è del tutto vera<sup>3</sup>). Il principale motivo è legato al fatto che Zwicky aveva un pessimo carattere. Non fu preso sul serio anche perchè rimase mitica la sua frase celebre secondo cui "tutti gli astronomi sono bastardi sferici" [11] perchè la sfera non aveva angoli per cui da qualunque parte li si osservava rimanevano tali. Ma esiste anche un motivo scientifico per cui non fu preso sul serio, infatti Zwicky usava il teorema del viriale (che vedremo dopo) per analizzare l'ammasso della Chioma. Ma il teorema del viriale è applicabile solo se il sistema è in equilibrio, cosa che nessuno poteva garantire per quell'ammasso. Vi era anche un motivo legato al fatto che i "collegi sferici" dell'epoca ritenevano, come detto in precedenza, che in fondo migliorando le tecniche sperimentali quell'eccesso di massa necessario per far tornare i conti, sarebbe sparito. Inoltre, Zwicky fu assecondato anche perchè difendeva idee che si erano rivelate non corrette, come ad esempio quella che contestava il modello di universo in espansione e che spiegava lo spostamento verso il rosso della luce delle galassie con la "teoria della luce stanca" in cui la frequenza dei fotoni emessi variava in modo strano.

Inoltre, lo stesso Zwicky era in disaccordo con se stesso, attribuendo ai gas e alle polveri la velocità eccessiva delle stelle nella galassia.

### Vera Rubin (1928-2016)

Vera Rubin è stata una astronoma americana. Nel 1948 ottenne la Bachelor, una sorta di laurea di primo livello all'università di Vassar, nello stato di New York. Dopo tentò l'iscrizione a Princeton che la rifiutò in quanto donna (questo vergognoso rifiuto delle donne sopravvisse fino al 1975). Rubin andò in un'altra università, la Cornell ed ebbe come professori R. Feynman e H. Bethe. Alla Cornell University e conseguì un master nel 1951. Nel 1954 conseguì il dottorato di ricerca all'università di Georgetown sotto la direzione di George Gamow. Qui Vera Rubin sperimentò

<sup>3</sup>Nel 1939 l'astronomo Horace Babcock misurò la velocità di rotazione delle stelle più esterne della galassia di Andromeda [12]. Nel 1940 analoghe misurazioni furono fatte da Ian Oort [13] che ottenne stessi risultati: la velocità di rotazione delle stelle presupponeva una enorme quantità di materia invisibile.

ancora una volta la discriminazione di genere perchè Gamow la invitò ad incontrarlo nella biblioteca del Dipartimento di Magnetismo Terrestre del Carnegie Institute vicino Washington, praticamente nell'atrio della università, perchè le donne non potevano entrare. Nove anni dopo ottenne un posto a tempo indeterminato a Washington, al Carnegie Institute.



**Figura 4:** In alto: Vera Rubin alle prime armi negli anni '50. In basso: nel 2009 - la seconda da sinistra in occasione della conferenza sulle donne in astronomia (fonte Jay Freidlander NASA).

Nel dicembre del 1950, 6 mesi prima di acquisire il master presentò al congresso dell'American Astronomical society ad Havenford (Pennsylvania) i risultati di un suo lavoro in cui misurava il red-shift di 108 galassie, sottraendo i moti recessionali, quelli dovuti al fatto che l'universo si espande. Ciò che rimaneva erano naturalmente i moti peculiari, in altri termini le galassie erano gravitazionalmente legate e quindi non risentivano della espansione dell'universo, come ad esempio il pianeta intorno al Sole. Lo studio fu accolto con estremo scetticismo. I motivi di tale freddezza erano diversi: era una donna, i risultati furono presentati malissimo, i dati erano deboli e poi, cosa non trascurabile, non si accordavano con la legge di Hubble. Vera Rubin pensò che fosse normale tra gli astronomi un tale atteggiamento che rasentava lo snobismo, dato che era la prima volta che faceva una presentazione.

Il Washington Post il giorno dopo ne fece un articolo dal titolo, da sottolineare come fu appellata, non come studiosa o ricercatrice ma: "Giovane madre individua il centro della creazione con i moti delle stelle". Vera Rubin era talmente

principiante che neppure lei stessa si rese conto della portata delle sue analisi. In ogni caso Vera Rubin non aveva mai fatto osservazioni con un telescopio per cui non si considerava una astronoma. Furono pochissimi che presero seriamente questi risultati fra cui l'astronomo francese che lavorava in Australia, Gerard de Vancoulers, che in quel periodo stava ipotizzando l'esistenza di ammassi di galassie.

Vera Rubin prese i dati esistenti ipotizzando le galassie in 3D, in funzione della posizione nel cielo ed il 15 luglio 1954 pubblicò il suo studio di tesi nei proceedings della National Academy of Science, in cui diceva essenzialmente che le galassie a causa della gravità si raggruppavano tra loro. La reazione fu: silenzio assoluto! Vera Rubin rimase senza lavoro e qualche anno dopo, nel 1964 chiese di lavorare al suo amico radioastronomo Bernard Burke. Burke rimase stupito della richiesta e nella mensa dell'istituto presentò W. Kent Ford, esperto strumentista, col quale in seguito divise la stanza al Carnegie Institution di Washington.

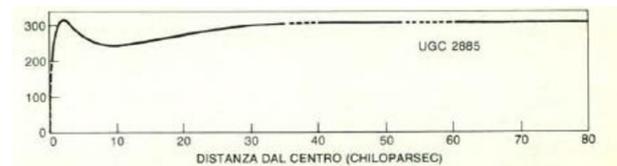
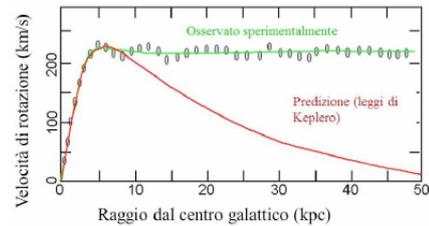
Lo spettrografo costruito da Ford, molto usato in seguito da entrambi, era un tubo che convertiva i deboli fotoni catturati da un corpo celeste e li convertiva in corrente elettrica che incideva su uno schermo fosforescente la cui regione colpita si illuminava. In pratica questa tecnica rivoluzionaria riduceva del 90% il tempo di esposizione della luce ricevuta da un corpo celeste.

Loro due si misero a studiare le velocità delle stelle nelle galassie a spirale e venne fuori una delle più chiare prove della esistenza della materia oscura<sup>4</sup>.

Analizzarono circa 60 galassie e ciò che si aspettavano era che maggiore era la distanza della stella dal centro della galassia più lentamente doveva orbitare, altrimenti la forza centrifuga avrebbe strappato le stelle dalla galassia ospitante. Niente di tutto ciò fu trovato, anzi utilizzando l'effetto Doppler delle nubi di idrogeno esterno delle galassie, usate quindi come traccianti, trovarono i grafici in Figura 5.

Nel 1970 Vera Rubin e Kent Ford pubblicarono un lavoro su *Astrophysical Journal* intitolato "Rotazione della nebulosa di Andromeda a

<sup>4</sup>Per correttezza bisogna dire che nello stesso periodo l'astronomo australiano Ken Freeman osservò una strana rotazione anomala in diverse galassie a spirale.



**Figura 5:** In alto - Curva di rotazione di una galassia. La curva rossa è quella attesa secondo le leggi di Keplero, quella verde è dovuta ai dati sperimentali (fonte Marco Casolino - Scienza per tutti INFN). In basso - Curva di rotazione della galassia UGC 2885 ricavata da Vera Rubin.

partire da una indagine spettroscopica delle regioni di emissione" [14]. In pratica, puntarono il loro telescopio verso Andromeda, dove vi era una enorme concentrazione di stelle al centro e si aspettavano che le miriadi di stelle che ruotavano attorno al centro galattico lo facessero seguendo la legge di Newton, come fanno i pianeti attorno al Sole, più sono lontani dal centro più lentamente si muovono. Ad esempio il pianeta Mercurio gira intorno al Sole in 88 giorni, mentre Nettuno per compiere un giro completo attorno al Sole impiega 165 anni. Ci vollero più di due anni per calcolare le velocità di 90 stelle di Andromeda. La cosa sorprendente fu che tutte le stelle si muovevano alla stessa velocità indipendentemente dalla distanza dal centro: 250 km/s. E questa cosa fu trovata in tutte le galassie.

Stabilire la velocità di rotazione di una stella che si trova ad una certa distanza  $r$  dal centro della galassia non è una cosa complessa. Schematizzando il problema, dalla fisica classica, come conseguenza della legge di Newton, la velocità del corpo in orbita,  $v$  è data da

$$v = \sqrt{\frac{Gm}{r}} \quad (1)$$

con  $m$  la massa che attrae il corpo. In altri termini, se conosciamo la velocità di rotazione delle stelle, siamo in grado di risalire a quanta massa  $c'$  è all'interno dell'orbita tra il centro e la distanza  $r$  dove si trova la stella, proprio attraverso l'

Equazione (1). D'altra parte la cosa è intuitiva, se non fosse così, cioè se la massa all'interno non fosse sufficiente a trattenere il corpo celeste, questo fuggirebbe via dando luogo alla cosiddetta "evaporazione delle galassie".

La cosa sorprendente fu che la massa ottenuta in questo modo era di gran lunga maggiore della massa luminosa che componeva il sistema in esame. In altri termini è come se, nella Equazione (1), all'aumento di  $r$  al denominatore ci sia una compensazione data dall'aumento simultaneo della massa, in modo tale che il rapporto rimanga costante.

### Altra evidenza astrofisica

Un'altra evidenza astrofisica dell'esistenza della materia oscura è legata alla luminosità delle galassie a spirale. Si considerano le galassie a spirale perchè sono abbastanza regolari nel senso che hanno un nucleo centrale luminoso, un disco piatto formato da braccia a spirale e un alone sferico.

Indichiamo con  $L$  la luminosità del disco ed  $R_0$  il cosiddetto **raggio ottico** cioè la distanza tra il centro della galassia e il punto in cui la luminosità non è più rilevabile, cioè si confonde col fondo.

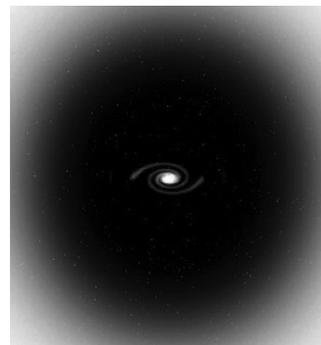
La legge empirica che collega  $L$  ad  $R$ , dove  $R$  è una distanza generica dal centro, è la seguente

$$L(R) = L_0 e^{-3.2 \frac{R}{R_0}} \quad (2)$$

con  $L_0$  più o meno costante per tutte le galassie a spirale. Ora, se  $R < R_0$  la velocità di rotazione del disco si misura con strumenti ottici, se invece  $R > R_0$ , dato che l'immagine non è più rilevabile per definizione, la velocità di rotazione si misura con mezzi radio. Dallo studio dell'Eq. (2) si rileva che la velocità di rotazione è costante come se la massa della galassia fosse proporzionale alla distanza, vedi Eq. (1).

Questa modalità di rivelazione fa sì che si possano misurare curve di rotazione fino a  $10R_0$  senza che la velocità di rotazione diminuisca e quindi si può dedurre da questi rilievi che la massa delle galassie esaminate sia almeno 10 volte maggiore di quella rilevabile otticamente.

La cosa interessante è che le galassie a spirale e quelle ellittiche, hanno proprietà completamen-



**Figura 6:** La galassia visibile è una piccola frazione di ciò di cui è composta. L'alone sferico in questa riproduzione dà il senso delle grandezze degli aloni sferici intorno alla galassia ospite. Uno dei padri "degli aloni sferici" è il premio nobel P.J.E. Peebles. Il puntino bianco al centro è la galassia. L'alone nero attorno è la materia oscura.

te differenti, ma la distribuzione della materia oscura in entrambe sembra essere la stessa e cioè una sfera.

Un altro aspetto interessante è che lo studio della materia oscura nelle galassie è diverso dallo studio della materia oscura negli ammassi di galassie. L'analisi sperimentale della materia oscura nelle galassie e tra gli ammassi di galassie è strettamente connessa al processo di formazione delle strutture su grandi scale: si sono formati prima gli ammassi e dopo le galassie o viceversa, prima le galassie che raggruppandosi per l'attrazione gravitazionale hanno dato origine agli ammassi? Nel primo caso avremmo che la materia oscura esisterebbe in grande quantità anche negli ammassi. Nel secondo caso sarebbe meno probabile trovare materia oscura nello spazio tra le galassie in quanto la gravità, nella formazione delle galassie, farebbe convogliare sulle galassie in formazione la materia oscura vagante. La risposta finale sembra essere la seconda e cioè che la materia oscura sia collegata ed associata alle galassie (si veda ad esempio [15]). Questo chiarisce un aspetto dirimente e cioè che tutta la materia oscura deve essere correlata alle galassie e quando parliamo di materia oscura degli ammassi dobbiamo intendere la somma della materia oscura delle singole galassie e non materia oscura nello spazio tra le galassie che costituiscono gli ammassi.

Come appena detto, secondo il "modello cosmologico standard" prima si formano le galassie

e poi la gravità fa il resto generando gli ammassi di galassie. È notizia recentissima (settembre 2023) di uno studio guidato da Elena Asencio dell'Università di Bonn [16] in cui si è stimata con grande precisione, utilizzando il *lensing gravitazionale*, la massa di un gigantesco ammasso di galassie detto "El Gordo" (il grasso) generato dallo scontro tra due ammassi di galassie quando l'età dell'universo era di circa 6 miliardi di anni. Ora è molto improbabile che a quell'età l'universo avesse già potuto generare questo mega-ammasso, non ne avrebbe avuto il tempo. Le cose, in questo senso si fanno sempre più intricate, anche in relazione alla materia oscura.

## Teorema del viriale

Ci sono diversi modi di stimare quantitativamente il contenuto di materia in una regione dell'universo. Uno dei primi è stato quello legato al teorema del viriale, metodo che fu applicato da Zwicky e poi da tutti gli altri studiosi per ricavare in modo semplice ma efficace, la presenza di materia oscura. Anche se verrà introdotto qui in modo molto semplificato, è semplice la logica che c'è dietro.

Consideriamo un sistema in equilibrio, fatto di  $N$  stelle, che ipotizziamo puntiformi, ognuna con massa  $m_i$  e con velocità  $v_i$ . Chiamiamo  $r_{ij}$  la distanza tra l' $i$ -esimo e il  $j$ -esimo corpo celeste. Siano  $E_c$  l'energia cinetica ed  $E_p$  l'energia potenziale del sistema globale, date rispettivamente da

$$E_c = \sum_{i=1}^N \frac{1}{2} m_i v_i^2 \quad E_p = \sum_{i<j}^N G \frac{m_i m_j}{r_{ij}}. \quad (3)$$

Si definisce **viriale** del sistema la seguente quantità

$$\text{Vir} = 2E_c - E_p. \quad (4)$$

Da considerazioni generali, come la conservazione dell'energia, si ottiene il "teorema del viriale" che asserisce che per un sistema di punti in equilibrio si ha

$$\text{Vir} = 0. \quad (5)$$

Ora, ricavando  $m_i$  dalle misure di luminosità, si ha che, ad esempio,  $\text{Vir} \neq 0$ , per cui è necessario aumentare  $m_i$  di un fattore 3, per esempio, per far sì che si riottenga eq.(5). Questo ragionamento, che sembra molto semplificato, in realtà è

molto profondo e trova che, ad esempio intorno al Sole, la massa oscura deve essere il doppio di quella che vediamo. L'applicazione del teorema del viriale consente di ritenere che la massa delle galassie sia almeno 10 volte maggiore di quella che si deduce otticamente nel visibile. Naturalmente questo è un modo di rifrasare l'Eq. (1) che è il frutto di eguaglianza tra forza centrifuga e forza newtoniana se consideriamo un'orbita circolare.

Ci siamo riferiti alla massa delle galassie, ma il teorema del viriale conferma che si sottostima la massa di un fattore 5-10 anche per gli ammassi di galassie.

## Lensing gravitazionale

Nel 1936 Einstein riteneva che osservare amplificazioni della luce di un corpo celeste, che passa nelle vicinanze di un altro corpo celeste, avrebbe avuto evidenze sperimentali talmente minimali da essere praticamente trascurabili (*lensing gravitazionale*). Nel 1937 Zwicky, nell'articolo in cui usa il teorema del viriale applicato alla Chioma Berenice [17], aggiunse un piccolo capitolo in cui riteneva, contrariamente a quanto diceva Einstein, che l'effetto sarebbe stato non trascurabile anche se le sorgenti non fossero state stelle, ma galassie.

Questa tecnica del *lensing gravitazionale* non è legata alla materia luminosa, quindi alla cinematica stellare, ma fa riferimento alla stessa luce. L'argomento è molto complesso per cui analizzarlo in questa sede non è possibile. Si accennerà solo a qualche principio che consente di inquadrare il problema [18].

In base alla Relatività Generale la gravità è la deformazione dello spazio-tempo ad opera della massa/energia. Questa deformazione, tra le tante conseguenze, ha anche quella del fenomeno del *lensing gravitazionale*: quando la luce si propaga in uno spazio-tempo curvo, essa si propaga su traiettorie curve, venendo deflessa, contrariamente a quanto accade in uno spazio-tempo piatto.

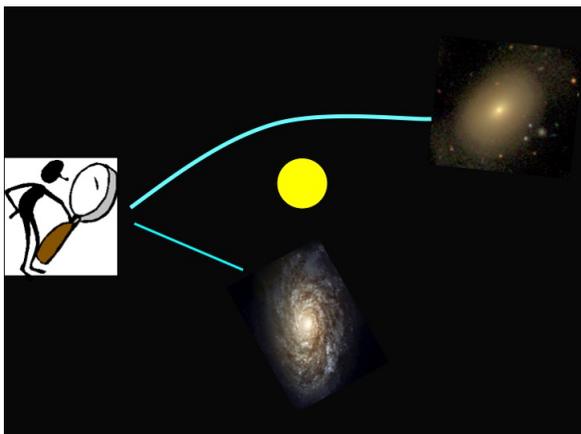
Il *lensing gravitazionale* si traduce in effetti osservabili, che coinvolgono le sorgenti da cui la luce è stata emessa:

- 1) la distorsione della forma della loro sorgente;
- 2) la presenza di immagini multiple;

3) l'amplificazione (o meno) del flusso luminoso;

4) il ritardo nella propagazione luminosa.

Collegando le proprietà modificate della sorgente alla massa che funge da lente, si è in grado di risalire al valore della massa della lente stessa. Rispetto alla analisi dinamica, che fa riferimento a traccianti luminosi, il vantaggio del *lensing* gravitazionale sta nel fatto che consente di esplorare regioni molto esterne agli aloni galattici, zone in cui la stessa analisi dinamica non sarebbe possibile. Vi sono 3 tipi di situazioni.



**Figura 7:** Lensing gravitazionale. Lo spazio-tempo curvo piega i raggi luminosi in prossimità di un corpo celeste, in giallo in figura.

## 1) Lensing forte

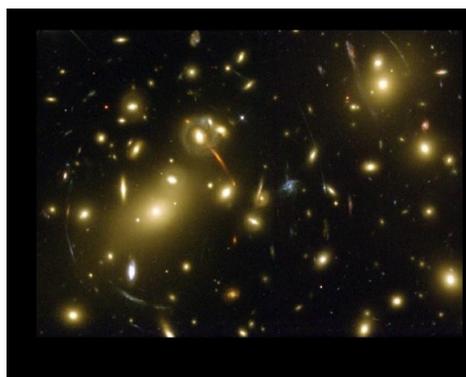


**Figura 8:** Ammasso di galassie SDSS J103842.59+484917.7. (Immagine del telescopio Hubble).

Si ha quando si vede una galassia o un ammasso di galassie insieme ad un arco molto grande.

La stima della massa-lente presente nella circonferenza che contiene l'arco gigante (detto anche anello di Einstein) non è difficile. Vi è molta differenza tra questa stima e quella che si ha sommando la materia luminosa nella stessa regione. In Figura 8 vi è un famoso ammasso di galassie che si trova nella costellazione dell'Orsa Maggiore, noto come SDSS J103842.59+484917.7 lontano da noi circa 4.6 miliardi di anni luce. I due corpi celesti al centro più luminosi sono due galassie ellittiche. Gli archi che si vedono sono galassie lontanissime e sono la dimostrazione dell'effetto lente che ha amplificato e distorto l'immagine a causa della presenza di SDSS J103842.59+484917.7, è un esempio di effetto gravitazionale forte, che genera l'anello di Einstein.

## 2) Lensing debole



**Figura 9:** Si notano gli archetti sullo sfondo in questo agglomerato di galassie.

In questo caso compaiono nella lente tanti archetti luminosi che rappresentano immagini deformate delle galassie. Una sola immagine non fornisce alcuna indicazione, lo studio statistico invece dei piccoli archi consente di avere informazione sulla massa della lente che ne deforma la traiettoria.

Il motivo è semplice, nel senso che se non ci fosse *lensing* si avrebbe una distribuzione uniforme delle galassie che stanno sullo sfondo, invece la presenza di archetti e quindi la deviazione dalla configurazione isotropa, consente di avere informazione sulla massa della lente. Questa analisi rivela la presenza considerevole di materia oscura.

### 3) Microlesing galattico

Questa tecnica fa riferimento alla materia oscura sotto forma di MACHO (Massive Astronomical Compact Halo Object) cioè corpi celesti presenti nell'alone galattico, tipo nane bianche, stelle di neutroni, buchi neri, pianeti, nane brune, nane rosse, nubi di gas freddo. Un altro modo più intuitivo è dire che i corpi celesti MACHO sono materia barionica oscura. Quello che è importante è che questi possono avere il titolo di MACHO solo se non si trovano nel piano galattico. Il problema è che questa è materia barionica, e poi che la somma in una galassia delle masse dei MACHO non dà conto della massa mancante. Ragionevolmente, la materia oscura si può anche avvalere della massa dei MACHO insieme alla materia non barionica.

#### Perchè l'idrogeno è un ottimo tracciante

Nello stato fondamentale dell'atomo dell'idrogeno, lo spin dell'elettrone e del protone sono antiparalleli. Il primo stato eccitato corrisponde alla situazione in cui i due spin sono invece paralleli. La transizione da quest'ultimo stato a quello fondamentale emette radiazione elettromagnetica con una frequenza di circa 1420 MHz o equivalentemente ad un'onda radio di 21.049 cm. Teoricamente queste linee di emissione a 21 cm furono predette dall'astronomo e matematico olandese Hendrik van Hulst nel 1945 [19], mentre da un punto di vista sperimentale queste linee furono osservate nel 1951 da H. Ewen e E. Purcell [20].

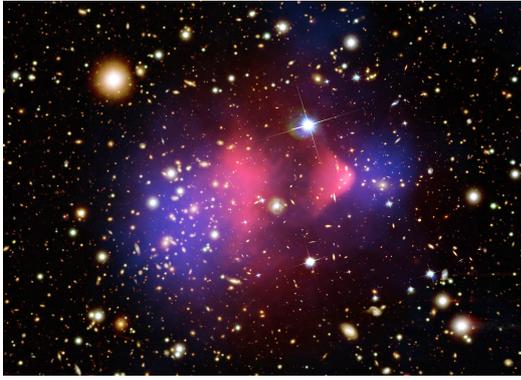
L'atomo di idrogeno è un ottimo tracciante per evidenziare, nelle regioni lontanissime dal centro galattico, la presenza di materia oscura. Vediamo perchè. L'idrogeno si trova in grandi quantità nelle parti più esterne delle galassie ed è possibile misurare con grande precisione le righe di emissione ed assorbimento in laboratorio. Quando il gas si avvicina a noi, ruotando, ha una frequenza spostata verso il blu, mentre quando si allontana da noi ha una frequenza spostata verso il rosso, a causa dell'effetto Doppler. Ma seguire in questo modo le nubi di idrogeno ha un ulteriore vantaggio perchè ad una distanza considerevole dal centro della galassia, le stelle sono molto poche e quindi è difficile effettuare misure su

di esse. Ma come si fa in pratica a capire tutto ciò? La densità media dell'idrogeno è circa 1 atomo per  $\text{cm}^3$  nello spazio interstellare? Anche se raramente, gli atomi di idrogeno si urtano, pertanto un atomo che prima dell'urto era nello stato  $J = 0$ , in cui gli spin dell'elettrone e del protone sono antiparalleli, dopo l'urto può passare nello stato eccitato  $J = 1$ , in cui i due spin sono allineati. Quasi tutti gli atomi eccitati poi ritornano nello stato fondamentale in urti successivi e una piccola frazione di questi atomi emetterà spontaneamente un fotone con una energia data da  $5.9 \times 10^{-6}$  eV. Anche se il processo è raro, mediamente una volta ogni 10 milioni di anni, data la quantità enorme di idrogeno presente, il fenomeno è osservabile e misurabile. In definitiva questo eccitamento e diseccitamento degli atomi di idrogeno nello spazio cosmico, con connesso ribaltamento delle relative direzioni degli spin, produce emissione di energia raggiante con fotoni la cui lunghezza d'onda è di 21 cm (microonde). Questo è vantaggioso anche perchè le onde radio attraversano facilmente tutto ciò che si frappone tra l'emissione e il radiotelescopio sulla terra. Usando radiotelescopi calibrati alla radiazione di 21 cm si possono determinare con precisione le zone in cui sono presenti nubi di idrogeno.

Fu proprio con questo approccio che nel 1957 Hendrick van der Hulst stimò per la galassia di Andromeda una massa circa 200 volte la massa luminosa che la componeva [21]. In seguito misure di Morton nel 1966 con onde radio, confermarono la costanza della velocità di rotazione dei corpi celesti, indipendentemente dalla distanza dal centro [22].

#### Bullet Cluster

Uno dei più interessanti ammassi di galassie che ci siano si chiama **Bullet Cluster** (o ammasso proiettile) e fu osservato nei dettagli dall'osservatorio spaziale Chandra nel 2006. Si trova a circa 3.5 miliardi di anni luce da noi ed è formato da due ammassi di galassie. La fotografia in Figura 10 è un fermo immagine di ciò che resta 150 milioni di anni dopo lo scontro tra i due ammassi. L'immagine di per se è spettacolare ed è la cristallizzazione di un ammasso che attraversa l'altro alla velocità relativa di  $10^7$  km/h. A destra



**Figura 10:** Immagine del *Bullet Cluster*. La foto è nell'ottico, ma sono state sovrapposte zone rosse indicanti gas tra i cluster, e zone blu, indicanti gas con maggiore potenziale gravitazionale. Sia le zone rosse che blu sono state individuate tramite *lensing* gravitazionale (credit: NASA - Chandra X-ray Observatory, Hubble Space Telescope, Magellan Telescope).

vi è un piccolo ammasso e a sinistra un ammasso molto più grande. L'ammasso più piccolo ha attraversato quello più grande come se fosse un proiettile alla velocità di circa 3000 km/s. I due ammassi non si sono fusi indicando che nella collisione è come se fossero stati trasparenti l'uno all'altro. E questa è la vera sorpresa di tutta la faccenda. L'ammasso di destra è caratterizzato da una specie di arco, come un'onda d'urto.

Dall'analisi dei raggi X emessi dal gas caldo (circa  $10^7\text{K}$ ), altamente ionizzato, si può avere idea della densità e della distribuzione della materia. Ebbene ciò che emerge è che senza materia oscura non è possibile che le strutture siano gravitazionalmente stabili. Inoltre gli elettroni liberi del gas caldo vengono colpiti dai fotoni con frequenza delle microonde del Big Bang e la diffondono modificandone l'energia (effetto Sunyaev-Zel'dovich)<sup>5</sup>.

L'importanza di questo Bullet Cluster è che potrebbe essere il primo caso di osservazione diretta della materia oscura perchè quando i due ammassi si sono scontrati le galassie che compongono i due ammassi non hanno quasi avvertito lo scontro conservando la loro posizione relativa. Invece il gas dell'ammasso più piccolo scontrandosi con quello più grande ha avuto la

<sup>5</sup>Gli elettroni del gas vengono colpiti dalla radiazione cosmica di fondo per cui l'interazione tra questi fotoni primordiali e gli elettroni liberi del gas dà origine ad una misurabile modifica della energia.

### Materia oscura calda e fredda

Per materia oscura calda si intende materia formata da particelle molto leggere, poco massive, dell'ordine della massa dell'elettrone o inferiore, che quindi possono viaggiare a velocità ultra-relativistiche. Per materia oscura fredda invece si intende materia composta da particelle dotate di una certa massa, dell'ordine della massa del muone o superiore, per cui non raggiungendo velocità elevate produrrebbero, appunto, materia fredda.

peggio rimanendo indietro e creando una specie di onda d'urto che ha dato origine a ciò che vediamo: materia ordinaria e gas sono state separate. La materia oscura in questo scontro non ha risentito affatto delle interazioni tra i due ammassi. Al di là delle analisi tecniche specifiche, questo cluster ci dà forte indicazione di una componente dominante non elettromagnetica non collisionale. Questa componente interagisce solo gravitazionalmente.

### Formazione di strutture nell'universo, materia barionica e non barionica

Nella formazione delle strutture (ammassi di galassie, galassie, stelle, pianeti, ecc.) la materia oscura ha un ruolo fondamentale. Alla base della formazione delle strutture vi è l'instabilità gravitazionale, nel senso che zone con maggior aggregazione di materia erano seme per un maggior accrescimento rispetto ad altre zone. Il cosmologo Jakov Zel'dovich era dell'idea che la materia oscura fosse calda dato che considerava le particelle che avrebbero composto la materia oscura, molto leggere [23]. Questa visione era in contrasto con le osservazioni anche perchè se la materia oscura fosse stata calda si sarebbero cancellate le variazioni di densità, anche per questo motivo, ma non è l'unico, siamo portati a pensare che la materia oscura debba essere considerata fredda anche ai primordi dell'universo. Infatti, quando si effettuano simulazioni, considerando materia oscura calda, queste non sono capaci di conservare le piccole strutture nel cosmo, nel senso che si parte dalla formazione di quelle più grandi e man mano si va a strutture sempre più piccole

## Ricombinazione

L'universo primordiale era una enorme fornace composta da plasma, cioè da nuclei ed elettroni dissociati e da fotoni che vagavano interagendo con entrambi. L'alta densità dell'universo impediva ai fotoni di coprire grandi distanze prima di collidere; rimanevano intrappolati, per cui l'universo era opaco (e questo è il motivo per cui non riusciamo a vedere l'universo prima di questo momento per cui non potrebbero mai raggiungerci i fotoni di questo periodo o precedente a questo periodo di tempo). Inoltre l'alta energia di questi fotoni impediva ai nuclei atomici e agli elettroni di congiungersi, nonostante fossero attirati elettricamente. Dopo circa 380 mila anni circa dal Big Bang, a causa delle continue collisioni con nuclei ed elettroni, l'energia dei fotoni era diminuita, tanto da non poter più dissociare degli atomi di idrogeno che si formavano. Questo particolare momento della storia dell'universo si chiama "ricombinazione".

che la materia oscura calda disgrega. Se invece si fanno simulazioni con materia oscura fredda, il processo di aggregazione è inverso, dal basso verso l'alto: prima si formano le strutture più piccole, che fungono da semi per processi di aggregazione e poi si formano strutture sempre più grandi. In questo caso tutto è più stabile.

La radiazione cosmica di fondo (CMB), 370 mila anni dopo il big bang, mette in evidenza i semi primordiali che poi hanno dato origine alle strutture nell'universo, infatti una forte indicazione della esistenza della materia oscura primordiale viene proprio dalla CMB. Se fosse stata presente la sola materia ordinaria nei semi primordiali della CMB, questa non avrebbe avuto la forza aggregante intorno ai semi piccoli. Occorreva un seme più grande, dato appunto dalla materia oscura, che avrebbe dovuto avere la funzione aggregante, insomma doveva essere il cemento che consentiva ai semi più piccoli di esistere ed essere efficienti nelle aggregazioni di materia. La sola materia barionica non avrebbe potuto provvedere a far questo.

La materia ordinaria e quella oscura non barionica seguono strade molto diverse durante l'evoluzione dell'universo. Vediamo un po' più in dettaglio perchè serve la materia oscura per migliorare l'efficienza nella crescita delle strutture nell'universo.

Prima della ricombinazione, i fotoni sono un ostacolo al movimento dei barioni ordinari e questo in pratica vuole dire che non si addensano grumi di materia nelle zone perturbate. L'aggregazione della materia attorno a dei semi è ostaco-

lata fino alla ricombinazione. Questo però non accade per la materia oscura non barionica, che non interagendo con la radiazione elettromagnetica comincia presto il processo di aggregazione sui semi primordiali e quindi parte prima nel formare le strutture su grandi scale. Dopo la ricombinazione la materia ordinaria trova tutto pronto dato che gran parte del lavoro di aggregazione è stato già fatto dalla materia oscura. In pratica questo vuole anche dire che la materia oscura fa sì che i semi primordiali su cui si aggrega la materia ordinaria possono essere molto più piccoli, ad esempio, di quelli considerati negli anni '70, quando si considerava solo la materia ordinaria.

In Inghilterra il cosmologo Carlos Frenk si fece promotore di una complicatissima simulazione con una enorme quantità di equazioni, per capire se partendo da una nuvola di gas primordiale si riusciva ad avere strutture come le galassie [24]. All'inizio non ci riuscì perchè la sola presenza di materia ordinaria non garantiva la gravità necessaria a non far dissipare la materia. Aggiungendovi materia oscura le simulazioni riproducevano le galassie. È come se solo la presenza di materia oscura potesse garantire la generazione e formazione di strutture su grandi scale.

Le ipotesi di partenza utilizzate per effettuare queste simulazioni sono raggruppate sotto il nome di legge di Navarro-Frenk-White (N-F-W), dal nome dei tre cosmologi che si sono occupati di questa simulazione [24]. Sembra che questo modello di formazione delle strutture con materia oscura fredda sia quello che meglio è in

grado di riprodurre le nostre osservazioni. Ma gli interrogativi sono numerosi. 1) Qual è il vero ruolo della materia ordinaria in questi processi di aggregazione e formazione delle strutture? 2) Se si calcolano il numero di galassie nane col modello di N-F-W vien fuori un numero molto, troppo alto rispetto al numero reale. 3) Le simulazioni forniscono un andamento a cuspidi nella distribuzione della materia oscura nelle parti centrali delle galassie, andamento non riscontrato nelle osservazioni che invece indicano che la luminosità della galassia presenta un massimo pronunciato al centro con una diminuzione molto rapida con la distanza radiale, mai a cuspidi, anche se questo problema sembra essere stato in parte superato, a scapito di un aumento del numero di parametri.

### **Dalla Supersimmetria alla materia oscura: WIMP**

Il Modello Standard presenta una grande quantità di simmetria che permette di indagare molte caratteristiche della natura ed in particolare della materia che conosciamo. Una specie di generalizzazione di questa simmetria è la cosiddetta supersimmetria, che in verità non è contemplata tra le simmetrie del Modello Standard. Alla parola simmetria si aggiunge il prefisso super per indicare una particolare caratteristica per cui ad ogni particella vi è un partner con le stesse proprietà della particella, sia nucleari che elettriche. Il motivo per cui queste particelle supersimmetriche non sono ancora state scoperte potrebbe essere legato al fatto che sarebbero particelle talmente massive che gli attuali acceleratori non hanno abbastanza energia per produrle. La supersimmetria vuole elevare ad un livello più elevato la semplicità e se si vuole, la regolarità nelle leggi che governano il mondo.

I modelli supersimmetrici sono in grado di fornire una soluzione al cosiddetto “problema gerarchico” dando una giustificazione alla differenza tra la scala di rottura della simmetria elettrodebole (100 GeV) e quella della grande unificazione  $10^{15}$  GeV.

Per far sì che il modello diventi supersimmetrico è necessario che si introducano altre particelle con un criterio in fondo semplice: ad ogni particella con spin intero (o frazionario) il partner su-

persimmetrico ha spin frazionario (o intero). Ad esempio al fotone che ha spin 1, il partner supersimmetrico è il fotino con spin 1/2 o all'elettrone con spin 1/2 abbiamo il partner supersimmetrico che è il seletttrone con spin 0.

I partner supersimmetrici hanno masse molto elevate e sono caratterizzati da una forte attenuazione delle interazioni elettromagnetiche.

Una spiegazione del fatto che non vediamo i partner supersimmetrici può essere dovuta al fatto che le energie ora sono molto basse, ma poco dopo il Big Bang avrebbero potuto benissimo esistere particelle e partner supersimmetrici, che avevano masse molto più elevate. Questo le ha portate a decadere più e più volte fino a scomparire. Questo decadimento multiplo e conseguente scomparsa potrebbero non essere stati un processo efficiente e ciò che è rimasto di questi residui supersimmetrici lo chiamiamo (Weak Interacting Massive Particle) WIMP .

Stime teoriche ci dicono che una particella con una massa compresa tra 10 e 1000 masse del protone e che interagisce solo con interazioni deboli e la gravità soddisfa i requisiti connessi con le caratteristiche della materia oscura non barionica. Queste particelle sono dette, genericamente WIMP e non sono presenti nel Modello Standard.

Una ipotesi sulla loro origine potrebbe essere questa. L'universo primordiale era denso e molto caldo per cui il plasma era composto da particelle con energia elevata. Questa energia si trasformava in massa, per cui questa conversione produceva particelle molto più massive delle particelle originarie. Queste sono le particelle che potrebbero comporre la materia oscura e questo spiega perchè dovrebbe avere una massa così elevata. Ora man mano che l'universo si espandeva si raffreddava, per cui non era più possibile produrre WIMP e quindi il loro numero è rimasto congelato.

Le WIMP dovrebbero essere state prodotte nell'intervallo temporale  $10^{-6}$  s -  $10^{-9}$  s dal Big Bang. Il problema è che non vi sono particelle simili nel Modello Standard perchè il neutrino, il bosone Z e il bosone di Higgs sono le particelle che interagiscono debolmente. Solo i neutrini hanno un tempo di vita lungo, ma queste particelle non possono essere considerate come candidati per la composizione della materia oscura perchè la loro massa è troppo piccola e poi dovrebbero essere

prodotti da una materia oscura calda essendo relativistici.

## Il Neutralino

La particella più leggera prevista dalle teorie supersimmetriche è il neutralino (composta da un fotino + zino, che è la parte supersimmetrica del bosone  $Z$ , + 2 higgsini) che ha tutte le caratteristiche di essere giusta per essere materia oscura, e questo perchè 1) è neutra, 2) ha la massa giusta per produrre l'abbondanza della materia oscura; stime danno una massa diverse centinaia di volte più pesante del protone; 3) è stabile; 4) è sensibile solo all'interazione debole, oltre a quella gravitazionale. La sua stabilità garantisce che durante il tempo cosmico ha fatto da collante per le strutture cosmiche.

Fino a temperature di 10 GeV i neutralini potevano essere in equilibrio con le altre particelle del plasma primordiale. Vi sono delle condizioni secondo le quali il disaccoppiamento dei neutralini dalle altre componenti lasciava un residuo di neutralini che avrebbero composto la materia oscura e questo implica un limite inferiore (detto limite di Lee-Weinberg [25]) alla massa dei neutralini dell'ordine del GeV. I neutralini non sono mai stati identificati.

## L'assione

Questo argomento è molto tecnico e va oltre gli scopi di questo articolo. In modo sommario diciamo che l'interazione forte rispetta la simmetria di  $CP$  (prodotto di due simmetrie discrete  $C$  = coniugazione di carica e  $P$  = parità), mentre la cromodinamica quantistica, la teoria che descrive l'interazione forte, ne prevede la violazione, mai osservata. Se la simmetria di  $CP$  fosse violata si avrebbe un grosso momento di dipolo elettrico del neutrone, cosa non ancora vista.

Roberto Peccei e Helen Quinn nel 1977 [26] risolsero il problema della non osservata violazione della simmetria  $CP$  nell'interazione forte, proponendo un meccanismo, o meglio una nuova simmetria, detta simmetria di Peccei-Quinn. Successivamente Weinberg [27] e Wilczek [28] trovarono che la nuova simmetria implicava l'esistenza di una nuova particella a cui diedero il nome di assione.

L'assione non è elettricamente carico, dovrebbe avere una massa tra  $10^{-2} - 10^{-5}$  eV, dovrebbe interagire molto debolmente con la materia ordinaria. Data la sua piccola massa l'assione dovrebbe essere troppo leggero per essere un candidato opportuno per la materia oscura. Però gli assioni primordiali verrebbero prodotti subito dopo il Big Bang in abbondanza con un meccanismo non termico e questo significa che essi verrebbero generati in modo non efficiente, non veloce e non abbondante, e non vengono mai termalizzati. Questa produzione dipende da diversi fattori, dalla massa, dal tipo di interazione, e da quale particella li produce.

Essendo molto leggeri, rispetto alle particelle componenti la massa oscura, dovevano dare origine ad una massa oscura calda, invece le loro caratteristiche ne facevano una componente fredda e questo è connesso alla produzione non-termica, quindi di particelle leggere e non calde.

Per correttezza bisogna dire che molti della comunità scientifica nutrono dubbi sulla esistenza di questa particella anche perchè la sua eventuale esistenza potrebbe creare problemi rilevanti per l'astrofisica. La presenza di assioni altererebbe la formazione delle strutture su grandi scale, dato che si addenserebbero in enormi strutture ad anello (che non sono mai state osservate). Se esistessero, in presenza di forti campi magnetici, come vicino alle Magnetar, si avrebbe una conversione estremamente efficiente di fotoni in assioni cosa che produrrebbe dei segnali inequivocabili, come particolari righe di assorbimento nello spettro delle Magnetar. Tutto ciò non è mai stato visto. I problemi di tipo cosmologico, legati all'esistenza degli assioni sono presentati in [29].

## Extradimensioni, stringhe e materia oscura

Uno sconosciuto matematico tedesco Theodor Kaluza mandò ad Einstein un lavoro nel 1919, nel quale presentava una teoria di unificazione della gravità e dell'elettromagnetismo (le due uniche forze conosciute all'epoca), la particolarità era che le dimensioni dello spazio non erano 3 ma 4, per cui lo spazio-tempo era pentadimensionale, ma la quarta dimensione spaziale non era ancora stata vista da nessuno. Kaluza aveva fatto una cosa semplice e cioè quando si consi-

deravano 4 (spazio) + 1 (tempo) dimensioni, le equazioni di Einstein facevano comparire altre equazioni che altro non erano che le equazioni di Maxwell. Il sogno di unificazione di Einstein poteva essere sui binari giusti. Einstein non cestinò il lavoro. C'era un problema non semplice: non vi era traccia empirica della quarta dimensione spaziale. L'articolo fu pubblicato due anni dopo [30] grazie all'interessamento di Einstein. Qualche anno dopo, nel 1926, il fisico Oskar Klein [31] capì dove potesse essere la dimensione nascosta: era una dimensione accartocciata, arrotolata in una dimensione spaziale normale, per cui un ipotetico osservatore si potrebbe muovere avanti o indietro in una dimensione spaziale ordinaria e muoversi circolarmente attorno a questa dimensione. Il raggio della dimensione doveva essere dell'ordine della lunghezza di Planck (non accessibile agli esperimenti). Questo studio dava concretezza alla proposta di Klein per cui la teoria fu chiamata teoria di Kaluza-Klein. Purtroppo questa teoria aveva grosse difficoltà a trovare all'elettrode una giustificazione geometrica, anche Einstein la considerò e studio fino agli inizi degli anni '40. Poi fu messa nel dimenticatoio.

La teoria delle stringhe, nota dal lavoro pionieristico del fisico Gabriele Veneziano nel 1968 [32], cominciò a farsi strada negli anni '70 del secolo scorso. Alla base di questa teoria c'è il fatto che le particelle sono considerate come strutture non più puntiformi ma come cordicelle. C'è un fatto però, e cioè che le interazioni (considerando anche la supersimmetria) possono essere descritte nel modo giusto solo se le stringhe sono considerate in uno spazio pluridimensionale e questo perché i modi di vibrazione delle stringhe, cioè le particelle elementari, sono influenzati dalle dimensioni extra. Le vecchie teorie di Kaluza e Klein ritornano a galla!

Ma che relazione c'è tra le extradimensioni e la materia oscura? Volendo semplificare la questione è questa. Quando si considerano le extradimensioni, quello che accade ad ogni particella nota è che si associano nuove particelle identiche a quelle originali, ma con massa crescente, con regolarità. Alla particella del Modello Standard con massa  $m$ , vi è la corrispondente scala di particelle con massa  $2m, 3m, 4m, \dots$ . Ora il raggio della quarta dimensione spaziale e massa  $m$  sono grandezze correlate, una l'inversa dell'al-

tra. Queste particelle con massa  $2m, 3m, \dots$  sono poco stabili per cui se venissero prodotte decadrebbero, la particella  $B(2m)$  di massa  $2m$  in 2 particelle  $A(m)$  di massa  $m$ , la particella  $C(3m)$  di massa  $3m$  in 3 particelle  $A$  ecc.. Se ad esempio  $A$  fosse un fotone di massa  $m$ , nato dalla supersimmetria e per qualche ragione non potesse decadere, avremmo ottenuto la materia oscura perché non decadendo è stabile, è neutro e ha massa  $m$ . Per onestà bisogna dire che questa è una interessante congettura, non ancora vagliata dagli esperimenti.

### Cosa pensiamo di sapere e... altro...

Elenco sommariamente cosa sappiamo o meglio cosa pensiamo di sapere della materia oscura e delle sue caratteristiche, facendo un sunto schematico delle nostre conoscenze.

- 1) Non ha quasi mai interazione con la materia ordinaria.
- 2) Fino ad ora non è mai stata vista o rivelata da nessuno strumento.
- 3) Interagisce solo con la gravità, in caso contrario l'avremmo già vista da tempo attraverso le tracce lasciate su eventuali rivelatori. Gli effetti gravitazionali ne manifestano la presenza e le caratteristiche.
- 4) È stabile.
- 5) L'individuazione della materia oscura non coinvolge emissione di onde elettromagnetiche,
- 6) Non ha carica di colore perché non interagisce con l'interazione forte.
- 7) L'ottimo accordo con i dati sull'abbondanza dei nuclei prodotti nella nucleosintesi primordiale ottenuto considerando soltanto le particelle a noi note, implica che la materia oscura sia costituita da particelle che ancora non abbiamo identificato.
- 8) La radiazione cosmica di fondo ci dice che il plasma primordiale non poteva avere tra i suoi componenti la materia oscura. Quindi la materia oscura non è composta da particelle con carica elettrica, pertanto non poteva essere un plasma.

9) Deve avere una vita media almeno dell'ordine dell'età dell'universo perchè la percentuale di materia oscura al tempo della nucleosintesi e della ricombinazione è la stessa di adesso.

10) Non ha autointerazione, tantè che vi sono Cluster di galassie come il Bullet Cluster che ci dice che la materia oscura non interagisce con se stessa attraversandosi. È come se la materia oscura fosse oscura a se stessa!

11) Deve essere costituita da particelle pesanti essenzialmente perchè se non fossero tali avrebbero una velocità elevata e questo pregiudicherebbe il fatto di trovare materia oscura in spazi compatti e ci sarebbero problemi seri sulla formazione delle strutture. Pertanto la bassa velocità della materia oscura, non relativistica, ci dice che essa deve essere fredda. Nessuna particella nota però soddisfa a questi requisiti.

12) L'alone sferico che circonda ogni galassia dovrebbe essere esteso per circa 50 mila parsec oltre il disco galattico.

13) L'alone sferico dovrebbe contenere da 2-10 volte più materia di quanto ne contiene la galassia stessa (materia barionica).

14) Gli aloni di materia oscura nei superammassi tendono a formarne uno gigantesco, una sorta di superalone, che potrebbe essere rivelato tramite il fenomeno delle lenti gravitazionali.

La materia oscura presenta diversi aspetti contraddittori, ne citiamo solo qualcuno anche se sono molti di più. Le velocità molto elevate delle stelle periferiche nelle galassie induce a pensare alla presenza di materia oscura nella galassia ma anche alla presenza di aloni esterni molto più grandi della galassia stessa. La quantità di materia oscura e barionica, dovrebbe essere davvero moltissima, tanto da non essere trascurabile nel processo di rallentamento dell'espansione dell'universo, ma di questo non si fa mai menzione.

Un altro aspetto strano è l'inaspettata distribuzione omogenea della materia oscura. La distribuzione della materia oscura nell'alone che circonda la galassia è molto regolare rispetto alla distribuzione della materia visibile.

Un altro aspetto bizzarro riguarda un fenomeno mai chiarito e cioè le galassie ruotano, facendo perno su un nucleo centrale, ma sono avvolte da una gigantesca nube di materia oscura, che stranamente sembra non partecipare al moto di rotazione della galassia. La galassia centrale gira vorticosamente attorno a se stessa mentre l'alone gigantesco che l'avvolge sembra fermo. Abbastanza strano ed illogico come comportamento.

Le perplessità sulla esistenza della materia oscura non sono poche. Forse in parte avevano ragione i contemporanei di Zwicky che ritenevano che molte anomalie viste da Zwicky sarebbero scomparse alla luce di nuove scoperte e affinamenti sperimentali. Cito un recente lavoro, tra i cui autori c'è Francesco Sylos Labini del centro studi E. Fermi, in cui si esaminano i dati del satellite Gaia, lanciato 10 anni fa, ma gli ultimi dati rilasciati sono del 2022 [33]. Questo risultato è straordinario e chiaramente in contrasto con la stima della massa della via Lattea, che secondo questo studio potrebbe mancare all'appello circa mille miliardi di masse solari e quindi ci potrebbe essere molta meno massa di quella che normalmente si richiede per far tornare i conti introducendo la materia oscura. È un forte indizio di non congruità e di profonde implicazioni fuori dal coro.

## Energia oscura: il mistero più fitto

### Così tutto è iniziato

I posti erano tutti occupati quell'8 gennaio 1998 nella sala conferenze del Georgetown Hilton di Washington, c'erano oltre 20 giornalisti anche del New York Times e del Washington Post. Tra i tanti presenti c'erano anche Peter Garnavich per l'High-z teams e Samuel Perlmutter per l'SCP (Supernova Cosmology Project), Ruth Daly con i suoi dati sperimentali su radiogalassie e Neta Bahcall con quelli sugli ammassi di galassie. I quattro scienziati portavoce di quattro collaborazioni diverse con un'unica voce dissero che l'universo di sarebbe espanso per sempre, ma una delle quattro voci fu più altisonante delle altre, era quella di Perlmutter che tenne una minicon-

## La costante di Hubble

L'espansione dell'universo è il risultato di una gigantesca esplosione avvenuta al Big Bang che ha dilatato lo spazio. Il fatto che l'universo si stia espandendo è la conclusione dell'osservazione che le righe dello spettro provenienti da galassie lontane sono affette da uno spostamento verso il rosso (*red shift*). Il *red-shift* è un fenomeno per il quale un corpo celeste in allontanamento da noi emette una radiazione elettromagnetica che quando ci raggiunge ha una lunghezza d'onda maggiore di quella che aveva all'emissione. Si chiama spostamento verso il rosso perché se la radiazione elettromagnetica è la luce visibile, la luce rivelata, di un certo elemento, nelle osservazioni spettroscopiche è spostata verso il rosso dello spettro. In modo analogo se il corpo si avvicina a noi, lo spettro è spostato verso il blu. È il fenomeno noto come "effetto Doppler", in cui si dilatano le lunghezze d'onda di una sorgente che si allontana dall'osservatore e, al contrario, si contraggono quelle di una sorgente che si avvicina. È un dato osservativo che il valore del *red shift* cresce con la distanza della sorgente da noi, e questa è una indicazione dell'espansione dell'universo. In prima approssimazione la distanza tra due corpi celesti e la velocità di allontanamento sono legate da una relazione lineare la cui costante di proporzionalità è la costante di Hubble, che prende il nome da chi l'ha scoperta sperimentalmente.

ferenza di un'ora ai giornalisti parlando alla sua normale velocità e cioè velocissimo!

Il giorno dopo, il cosmologo Michael Turner si avvicinò agli otto poster di Perlmutter, in particolare al sesto che era tratto dall'articolo apparso una settimana prima dove l'SPC aveva pubblicato i risultati di 7 supernovae, ma accanto a destra vi erano i dati di oltre 40 supernovae, non ancora pubblicati, che definivano in modo chiaro la questione.

Ma facciamo un passo indietro. Nel 1995, Perlmutter e Ariel Goobar pubblicarono un lavoro su "The Astrophysical Journal" [34] in cui ritenevano che si potessero usare le supernovae per dimostrare che l'universo era tutta materia e costante cosmologica  $\Lambda = 0$  ( presenteremo in seguito la costante cosmologica).

I risultati delle 7 supernovae riportati in un pannello quell'8 gennaio 1998 davano, secondo la loro interpretazione,  $\Lambda = 0$ ; la sola materia bastava a spiegare tutta la composizione dell'universo. A destra di quel pannello, 40 supernovae, invece, sempre dello stesso gruppo, davano un risultato in profondo contrasto con le 7 supernovae precedenti e quindi in disaccordo totale con le osservazioni fatte dallo stesso gruppo di ricerca! The Astrophysical Journal accettò il lavoro con le 7 supernovae nel febbraio 1997, pubblicandolo a luglio [35]. I risultati di queste supernovae erano stati presi con strumenti a terra e per mi-

gliorare e confermare i risultati, le misurazioni fotometriche furono eseguite con il telescopio spaziale. Purtroppo i risultati furono in contrasto con quelli ottenuti a terra: i segnali erano molto più deboli di ciò che ci si aspettasse, le supernovae erano meno luminose, voleva dire che erano più lontane di quanto ci si attendesse. Infatti nel grafico delle magnitudo (misura standard della luminosità per i corpi celesti) in funzione della distanza, ci si aspettava di vedere una retta con inclinazione di  $45^\circ$ , in sintonia con la legge di Hubble. Invece le supernovae erano distanti, nel grafico, dalla retta.

Peter Nugent studiò le prime due supernovae dell'HST (Hubble Space Telescope), con una attenta analisi fotometrica. Si ipotizzava  $\Omega = 1, \Lambda = 0$ , cioè un universo piatto formato da sola materia, anche perché se l'universo fosse stato riempito di materia e radiazione, allora ci si sarebbe aspettati un rallentamento nella espansione cosmica, rallentamento prodotto dalla gravitazione universale. Con sorpresa, nel grafico magnitudo-*red-shift* Nugent trovò che, posizionando 2 supernovae secondo la loro distanza, le loro magnitudo erano 1.6 volte più deboli di quanto ci si aspettasse. Il tutto faceva pensare che  $\Lambda \neq 0$ , anche se questa informazione era a dir poco straordinaria! Il dubbio nasceva dal fatto che i dati si riferivano solo a due casi. Il gruppo di Nugent si scambiò una serie di *mail* in cui

Nugent invitava a fare molto presto per la pubblicazione. La cosa non fu fatta. In quella estate del 1997, il gruppo di Nugent eliminò 2 delle 7 supernovae perchè una non era una supernova IA e la seconda perchè presentava un forte anomalia. Alla fine, nel settembre del 1997 le supernovae rimaste indicavano un totale disaccordo col lavoro pubblicato da loro stessi due mesi prima. Il gruppo presentò il lavoro a Nature agli inizi di ottobre [36], ma la prosa dell'articolo era infarcita di frasi prudenti, perchè dovevano giustificare la contraddittorietà dei risultati con quelli del loro stesso lavoro precedente.

Anche il gruppo di High-*z* fece un lavoro sulle stesse supernovae [37], però col telescopio spaziale, ed il 13 ottobre con Garnavich primo autore, venne pubblicato *on-line* il lavoro, i cui risultati convergevano col gruppo di Nugent.

Il gruppo di High-*z* era il gruppo concorrente, tra cui spiccava la figura di Adam Riess. La collaborazione era in ritardo rispetto al gruppo SCP, che non poteva esse battuto sulla quantità dei dati ma solo sulla qualità. Nella sua tesi di dottorato Riess si era interessato dei metodi per eliminare il contributo della polvere contenuta nella galassia che ospitava la supernova. Il suo metodo, noto come MLCS Multicolor light-curve shape, consentiva di ripulire i dati. I dati erano relativi a 22 supernovae vicine osservate al telescopio di Mount Hopkins, dati mai pubblicati. C'era un problema però, e cioè quei dati indicavano un universo con massa negativa, ma se si introduceva nei programmi una costante cosmologica,  $\Lambda \neq 0$ , tutto tornava, la massa dell'universo diventava positiva. Riess inviò i dati al direttore del gruppo, Brian Schmidt che ricontrollò tutto il calcolo scrivendo un programma per conto suo.

La storia potrebbe continuare, ma il capitolo finale, quello che conta, è che l'universo sta accelerando, contrariamente a quanto si è sempre pensato. Stranamente, però, il premio Nobel per la fisica è stato assegnato a Riess, al suo capo Schmidt e a Perlmutter. Gli attori decisivi di questa avventura erano molti di più e molto più determinanti. L'assegnazione del premio Nobel è un mistero, più oscuro di quelli dell'universo...

Il lettore si sta chiedendo, ma perchè si sono usate le supernovae IA, cosa c'entra la costante  $\Lambda$ , ma soprattutto, la domanda delle doman-

de è: cosa genera questa forza repulsiva anti-gravitazionale che accelera lo spazio-tempo nel cosmo?

Cerchiamo di fare ordine e partiamo dalla prima domanda.

## Le supernovae IA e le distanze in cosmologia

### Perchè le supernovae IA?

Attraverso catene di reazioni nucleari, una stella come il sole converte l'idrogeno in elementi più pesanti incrementando l'energia cinetica dei nuclei coinvolti. Come conseguenza si ha un incremento della temperatura della stella e, quindi, della pressione del gas che la compone. Questo processo induce un equilibrio tra la pressione gravitazionale della stella, che la farebbe collassare, e la pressione generata dalla fusione dell'idrogeno, che la farebbe espandere. Man mano che vengono prodotti carbonio ed ossigeno nelle stelle, il processo di fusione si arresta perchè servirebbe una temperatura molto più elevata per fondere questi nuclei, quindi la pressione termica non compensa più l'attrazione gravitazionale e si produce il collasso gravitazionale.

Se la massa della stella è maggiore del limite di Chandrasekhar, che è di 1.38 masse solari, il collasso procede aumentando la temperatura fino a permettere di fondere i nuclei di carbonio e ossigeno. Il processo continua attraverso una serie di reazioni nucleari che formano nuclei sempre più pesanti e che producono sempre più energia. Il processo si ferma quando vengono prodotti nuclei di  $^{56}\text{Fe}$ . La fusione di nuclei più pesanti non produce più energia ma la necessita. A questo punto l'equilibrio tra pressione termica e gravitazionale si rompe, ed inizia il collasso, che si interrompe quando il nocciolo della stella raggiunge la densità della materia nucleare. A questo punto si genera un rimbalzo della materia che sta collassando. Lo scontro tra materia che rimbalza e quella che collassa genera un'onda d'urto e quindi l'esplosione da Supernova. Questo è il meccanismo alla base delle Supernovae di tipo IB, IC, o II, nelle cui righe spettrali si trovano tracce anche di elementi leggeri come l'idrogeno e l'elio perché contenuti nella stella progenitrice. A grandi linee, ciò che rimane dopo l'esplosione è un buco nero, se la massa della stella collassata

è di circa una ventina di masse solari. Per masse stellari inferiori si ha una stella di neutroni, individuata come *pulsar*.

Se, invece, la massa della stella progenitrice è inferiore al limite di Chandrasekhar, il collasso si interrompe perché la pressione gravitazionale è compensata da quella prodotta dal gas degenerato di elettroni liberi soggetti al principio di esclusione di Pauli. È un dato di fatto che due fermioni non possono occupare lo stesso stato quantistico, cioè non possono avere la stessa energia, spin, e quantità di moto. Cosicché gli elettroni, che sono fermioni, devono occupare stati con livelli di energia sempre più elevata e questo impedisce di comprimere il gas di elettroni in un unico stato di energia minima. Questo fenomeno produce nella stella una pressione verso l'esterno che bilancia la pressione gravitazionale. La stella rimane in uno stato di equilibrio, ed è una nana bianca.

Se la nana bianca si trova in un sistema binario, magari legata ad una gigante rossa, a causa della estrema volatilità della zona esterna della gigante rossa, la nana bianca attira gli strati esterni della compagna gigante rossa. Questo processo fa aumentare considerevolmente la massa della nana bianca fino a superare il limite di Chandrasekhar, per cui salta l'equilibrio tra pressione gravitazionale e pressione quantistica degli elettroni. In pochissimo si ha il collasso della nana bianca, la temperatura diventa elevatissima, tanto da fondere carbonio ed ossigeno, generando elementi molto più pesanti. Si produce così una gigantesca quantità di energia che induce la nana bianca ad esplodere: la sua luminosità di picco è paragonabile a quella della galassia a cui appartiene se non addirittura di più. È una supernova di tipo IA, e produce questa luminosità per qualche giorno espellendo gran parte della sua massa.

Le supernovae IA (SNIA), che sono quelle che ci interessano, sono caratterizzate dal fatto che i loro spettri di luce non hanno righe di idrogeno e neppure di elio. Questo perché la stella progenitrice è una nana bianca che non contiene questi due elementi. Le SNIA raggiungono quasi tutte lo stesso picco di luminosità nel senso che la curva di luce (di quanto varia nel tempo la luminosità) è identica per tutte queste SNIA. Il motivo di tale uniformità è legato al fatto che la stella progenitrice di questo tipo di supernovae



**Figura 11:** Nana bianca che accresce la sua massa a scapito della stella compagna, di solito una gigante rossa, i cui gas esterni sono gravitazionalmente meno legati e quindi più facilmente catturabili dalla nana bianca. (credit: NASA)

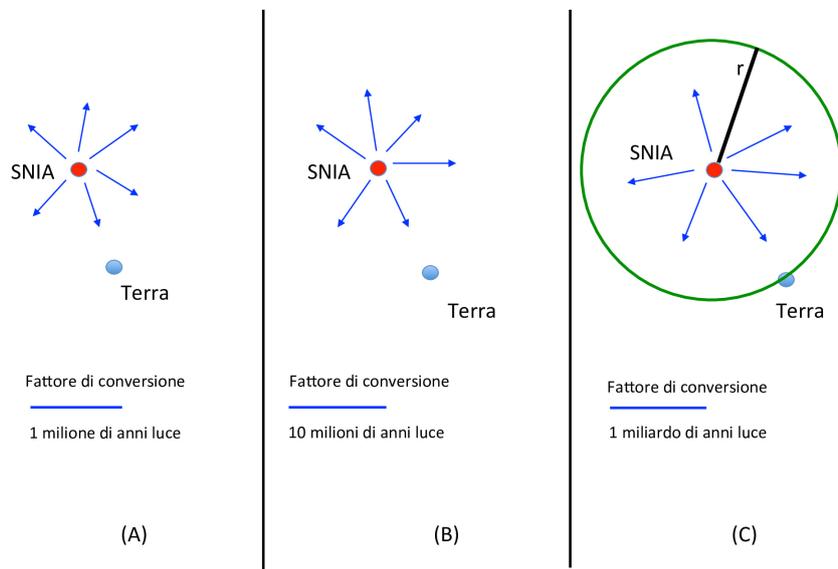
è sempre una nana bianca la cui composizione elementare è ben definita, al contrario delle stelle progenitrici degli altri tipi di supernova, che possono avere masse molto differenti, e quindi composizioni elementari molto differenti.

Vi è un problema, e cioè l'esplosione di queste SNIA è un evento molto raro ed improvviso. Mediamente, in una galassia, ne esplodono 2 o 3 ogni millennio, e, inoltre, le SNIA sono una piccola percentuale delle supernovae. Ma dato l'elevatissimo numero di galassie la frequenza con cui si vedono queste supernovae non è trascurabile.

In cosmologia molta informazione proviene dalla luce emessa da un corpo celeste e su questa si fondano i nostri ragionamenti e le nostre conclusioni.

La determinazione delle distanze dalla Terra di un corpo celeste si basa su una idea molto semplice: quanto più è lontano il corpo celeste da noi, tanto più fioca apparirà la luce emessa. La **luminosità apparente** è la luminosità del corpo se osservata dalla Terra, luminosità che diminuisce come la superficie su cui si diffonde, cioè con l'inverso del quadrato della distanza, quindi molto rapidamente, mentre la **luminosità intrinseca** è la luminosità che il corpo avrebbe se osservato da vicino. Dal confronto delle due luminosità possiamo calcolare la distanza. Naturalmente la difficoltà maggiore sta nel determinare la luminosità intrinseca, e questo è affidato (come vedremo) alle supernovae IA.

Detto in altri termini, se vogliamo determinare il tasso di espansione dell'universo, dobbiamo



**Figura 12:** (A) La luce della SNIA parte e si diffonde. (B) Man mano che la luce viaggia lo spazio si espande, cambia il fattore di scala. (C) La luce della SNIA raggiunge la Terra, il fattore di scala è quello su cui fare i conti. Dal confronto con la luminosità apparente e quella intrinseca riusciamo a risalire al raggio della sfera con centro nella SNIA, passante per la Terra

puntare il nostro telescopio verso un faro illuminato. Dallo spostamento Doppler della luce del faro siamo in grado di determinare la velocità alla quale il faro si sta allontanando o avvicinando a noi. Però non basta, per determinare il tasso di espansione c'è bisogno di sapere quanto è lontano il faro da noi (questo si ricava dalla brillantezza intrinseca della luce del faro). Combinando queste due informazioni, velocità e distanza siamo in grado di risalire al tasso di espansione.

Le SNIA sono ottimi indicatori di distanza e candele standard perchè hanno: 1) una piccola dispersione in prossimità del picco di luminosità e dopo il picco, 2) sono molto luminose, 3) il meccanismo di esplosione è abbastanza noto, 4) le incertezze dovute al *red-shift* sono ben controllate, 5) c'è un gran numero di *test* su SNIA locali.

### Le distanze in cosmologia

È necessario porsi una domanda che spesso si trascura quando ci si occupa di questi argomenti. Che distanza misurano gli astronomi? La distanza tra noi e la SNIA al momento della emissione della luce, oppure la distanza tra la nostra posizione oggi e la SNIA quando essa ha emesso la luce, oppure è la distanza tra le due posizioni attuali tra noi e la posizione della SNIA? Diciamo subito che la risposta giusta è la terza (che in certo qual modo è anche la seconda). Per capire la questione per nulla accademica, facciamo un esempio. Consideriamo due punti sulla superficie di un palloncino che si espande. I due punti

non si muovono, ma la loro distanza aumenta, anche se relativamente al raggio della sfera tutto rimane identico. In modo del tutto analogo, man mano che l'universo si espande, o più correttamente lo spazio tra i corpi celesti si espande, mentre i corpi celesti rimangono fermi, è necessario considerare il fattore di conversione giusto, che i cosmologi chiamano col nome di **fattore di scala**, il quale aumenta all'aumentare della espansione dell'universo.

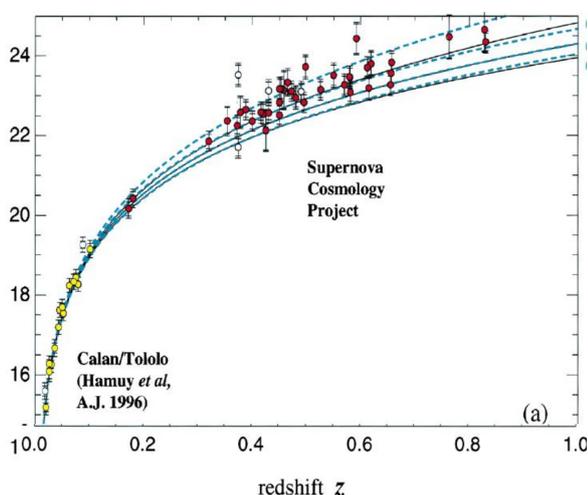
L'attenuazione della luce delle SNIA è legata alla grandezza della sfera su cui si diffonde la luce. Vi è però un'ulteriore complicazione dovuta al fatto che la dilatazione dello spazio, nell'espansione, aumenta la lunghezza d'onda dei fotoni, spostando verso il rosso la lunghezza d'onda  $\lambda$  emessa dalla SNIA. In definitiva l'attenuazione dell'intensità luminosa proveniente dalla SNIA è dovuta non solo alla diminuzione della densità dei fotoni che si sparpagliano su una superficie sempre più grande ma anche all'aumento della lunghezza d'onda dei fotoni emessi fatto che ne diminuisce l'energia secondo la legge di Planck  $E = hc/\lambda$ , con  $c$  velocità della luce e  $h$  costante di Planck. È necessario considerare tutto questo quando si quantificano questi concetti.

### La distanza di luminosità e l'accelerazione dell'universo

I fari erano le SNIA e furono impiegati i telescopi più potenti esistenti, Keck Telescope alle Hawaii, il Cerro Tololo Inter-American Telescope in Cile e l'Hubble Space Telescope (HST). Gli astronomi

lavoravano in due gruppi, il Supernova Cosmology Project (SPC) e l'High-z Supernovae Search Team. Ciò che loro cercavano con le SNIA era con quale tasso di rallentamento l'universo diminuiva la sua espansione cosmica, essendo tutti convinti che l'universo stesse rallentando la sua espansione. Contro ogni attesa le SNIA erano molto meno brillanti di quanto ci si aspettava, in altri termini lo spazio aveva scagliato nell'universo queste SNIA più velocemente di quanto atteso. Il verdetto era uno solo: l'universo sta accelerando!

Fondamentale è la determinazione della distanza di luminosità  $d_L$ <sup>6</sup>, inoltre dallo spettro della galassia ospite possiamo determinare il *red-shift*  $z$ , per cui è facile costruire il grafico  $d_L$  in funzione di  $z$ .



**Figura 13:** Diagramma di Hubble di 42 SNIA da Supernova Cosmology Project (in rosso) e 18 supernovae da Calan/Tololo (in giallo). In ascissa il *red-shift* sulle ordinate il modulo di distanza. Se l'universo non stesse accelerando i puntini rossi seguirebbero la curva più bassa, invece si posizionano al di sopra di essa, su una curva che descrive i dati sperimentali e che considera l'universo composto per il 70% circa di energia oscura e 30% di materia (oscura e non) (figura tratta da [38]).

<sup>6</sup>La distanza di luminosità può essere espressa come  $d_L = \sqrt{L/(4\pi F)}$  con  $F$  flusso ed  $L$  luminosità. Se il corpo celeste è vicino, ad esempio nella nostra galassia,  $d_L$  e la distanza ordinaria nello spazio euclideo sono praticamente la stessa cosa. Se il corpo celeste è lontano da noi bisogna tenere conto di altri fattori quali la dilatazione temporale, il *red-shift* e la curvatura.

La distanza di luminosità è data da

$$d_L(z) = c(1+z) \int_0^z \frac{dz'}{H(z')} \quad (6)$$

con  $c$  velocità della luce,  $z$  *red-shift*,  $H(z)$  parametro di Hubble. Definiamo la **magnitudine apparente**  $m(z)$  come la luminosità di un corpo celeste determinata dalla Terra, la **magnitudine assoluta**  $M$  che è la luminosità apparente che avrebbe il corpo celeste se si trovasse a 10 pc dall'osservatore e la si assume costante per le SNIA (dopo opportune correzioni). Ciò che gli astronomi utilizzano in questi casi è il **modulo di distanza**  $\mu$  che è dato da

$$\mu = m(z) - M = 5 \log_{10} \left[ \frac{d_L(z)}{\text{Mpc}} \right] + 25 \quad (7)$$

dove il termine 25 è determinato dalla scala di riferimento convenzionale assunta per  $M$ . Sperimentalmente, nel diagramma di Hubble si riportano in ascissa il valore del *red-shift*  $z$  ed in ordinata i valori sperimentali del modulo di distanza. Come si vede in Figura 13, nel diagramma di Hubble, i punti delle SNIA si posizionano in punti più in alto di quelli attesi. L'interpretazione è semplice: fissato  $z$ , cioè la distanza dalla terra, le SNIA invece di avere una certa luminosità attesa, risultano molto più flebili. Vuole dire che sono più lontane, ecco perché l'universo in base a questi dati, sta accelerando!

### Come e perché fu introdotta la costante cosmologica $\Lambda$

L'astronomo tedesco Hugo von Seeliger (1849-1924) era professore di Astronomia a Monaco di Baviera dove era anche direttore del locale osservatorio astronomico. Tra i suoi studenti di dottorato c'era Karl Schwarzschild. Seeliger era un forte oppositore della Relatività e della cosmologia che scaturiva dalla applicazione della Relatività Generale. Secondo Seeliger lo spazio nell'universo non poteva essere curvo né la Relatività Generale poteva spiegare l'anomalia del perielio di Mercurio.

Per evitare che in un universo infinito il contributo della gravità newtoniana risultasse infinito, nel 1895 Seeliger modificò la legge di gravità di Newton introducendo il precursore della costante cosmologica. In questo modo, riusciva

ad avere una distribuzione di materia nell'universo infinita, senza alcun problema connesso, rendendo stabile l'universo stesso perché questo termine di repulsione cosmologica riusciva a bilanciare la gravità a grandi distanze. In fondo fece ciò che avrebbe fatto Einstein 22 anni dopo.

Negli stessi anni il matematico Carl Gottfried Neumann (1832-1925) arrivò agli stessi risultati di Seeliger [39]. In questo modo il cosmo descritto dalla meccanica newtoniana era salvo.

Il 15 febbraio 1917 Einstein pubblicò un articolo sulla famosa rivista prussiana delle Scienze della Reale Accademia, dal titolo "Considerazioni cosmologiche sulla teoria della relatività" [40], dove introdusse quella che lui chiamò "fantasticheria" che oggi chiamiamo **costante cosmologica**. In verità Einstein chiamò questa costante col nome "termine cosmologico" e solo dopo prese il nome di costante cosmologica, termine con quale oggi la conosciamo.

Il valore della costante cosmologica è tra i più intriganti, ma allo stesso tempo sconcertanti, problemi aperti connessi con la energia oscura perchè la stima della costante cosmologica, straordinariamente enorme, è calcolata con metodi e strumenti della fisica teorica estremamente consolidati.

Ma perchè Einstein introdusse la costante cosmologica nelle sue equazioni? Quando nel 1915 Einstein formulò le sue equazioni cosmologiche (identiche a quelle che lui stesso aveva trovato e rifiutato nel 1912), voleva ottenere una soluzione, e per farlo, due anni dopo, fece l'ipotesi più semplice, cioè che la materia e l'energia fossero distribuite uniformemente nello spazio in qualunque direzione (queste ipotesi sono utilizzate ancora oggi e prendono il nome di **principio cosmologico**).

Einstein era convinto che l'universo dovesse essere lo stesso ovunque, inoltre l'universo con queste caratteristiche rendeva le equazioni più semplici, ma predicavano un universo molto strano e cioè che tutte le porzioni di materia ed energia avrebbero cominciato a muoversi l'una rispetto all'altra e niente sarebbe rimasto fermo. È bene tenere presente che nel 1916 si aveva una mappa precisa della via Lattea, ma una idea molto vaga di ciò che c'era oltre: ad Einstein il cielo appariva statico.

Nel 1917 fu costretto a ricorrere ad un artificio

matematico e cioè ad introdurre nelle equazioni della Relatività Generale una nuova grandezza che lui stesso chiamò con la lettera greca  $\Lambda$  per controbilanciare il collasso dell'universo che veniva fuori dalle sue stesse equazioni e quindi stabilizzare il tutto, dato che l'azione di questa costante era di spingere in modo contrario alla gravità ed evitare il collasso stesso. Ad Einstein questa costante non piaceva perchè voleva dire, da un punto puramente estetico, rinunciare alla semplicità. Einstein nel 1917 disse ad Ehrenfest che "l'introduzione di  $\Lambda$  mi espone al pericolo di essere rinchiuso in un manicomio" [41].  $\Lambda$  è una costante, da inserire nelle equazioni gravitazionali, ma è un parametro libero nella Relatività Generale che non ne predice il valore. Einstein non sapeva cosa fosse esattamente questa costante (in verità probabilmente non lo sappiamo neanche noi oggi), non l'aveva connessa con la materia, fu aggiunta alla geometria, ma non è abbinata alla curvatura dello spazio-tempo e non dipende da essa, però faceva bene ciò per cui era stata introdotta nelle equazioni della Relatività Generale: controbilanciava la gravità e rendeva l'universo stabile e non in espansione, per cui le due azioni uguali ed opposte rendevano l'universo in equilibrio statico.

Willem de Sitter (1872-1934), astronomo olandese della università di Leida, lesse il modello di universo con  $\Lambda$  ma capì che esisteva anche un universo, con piccolissima quantità di materia o senza materia, da non avere alcun effetto, nè utile a controbilanciare l'azione espansiva di  $\Lambda$ . Questo universo essenzialmente non aveva materia ma solo costante cosmologica. In altri termini de Sitter ipotizzava un universo con spazio-tempo curvo solo con costante cosmologica. L'universo di Einstein e quello di de Sitter erano entrambi statici, ma quello di de Sitter era strano perchè (come notò Hermann Weyl (1885-1955) [42]) se si fossero disseminate in questo universo corpi celesti, allora essi si sarebbero messi in movimento nonostante la geometria di questo universo fosse statica e non variabile nel tempo. Qualche settimana dopo che de Sitter ebbe l'articolo di Einstein (universo con costante cosmologica), trovò la soluzione che prende il suo nome e la inviò ad Einstein che non ne rimase entusiasta (si veda Ref. [43]). Einstein non concepiva che l'universo non potesse avere corpi celesti al suo

interno.

Alexander Friedman (1888-1925), fisico russo, negli anni 1922-1924 dimostrò che a prescindere da  $\Lambda$ , le equazioni di Einstein potevano contenere un universo in espansione, o in contrazione o statico [44, 45]. Tre anni dopo, il matematico e fisico belga, padre Georges Lemaître (1894-1966), fu il primo a intuire che l'espansione dell'universo era correlata con lo spostamento verso il rosso della luce ricevuta dai corpi celesti (proponendo quella che oggi è nota come la legge di Hubble) e conservando nelle sue equazioni la costante cosmologica [46]. Lemaître era profondamente convinto della espansione dell'universo senza limiti e fu il primo a proporre che l'universo avrebbe potuto avere un Big Bang che lui chiamò "ipotesi dell'atomo primigenio".

Dopo che Humanson e Hubble provarono l'espansione cosmica (1929) [47] <sup>7</sup> pescando dal punto di vista teorico nel modello di de Sitter e Friedman. I lavori di de Sitter e Friedman furono del tutto dimenticati e non considerati anche dallo stesso Einstein, che riteneva, ad esempio, che Friedman non avesse ragione e che gli studi di Lemaître fossero "abominevoli".

Einstein abbandonò  $\Lambda$ , dicendo la famosa frase secondo cui fu il suo più grande errore averla considerata. D'altra parte Arthur Eddington nel 1930 dimostrò che il modello di Einstein con costante cosmologica e statico, non era "affidabile" nel senso che sarebbe bastata una piccolissima variazione nella densità di materia che l'universo sarebbe espanso o contratto per sempre.

Riassumiamo per chiarezza:

- a) Einstein: modello di universo statico con materia e costante cosmologica;
- b) de Sitter: il suo universo non aveva materia ma solo costante cosmologica, e si espandeva;
- c) Friedman e Lemaître: il loro universo non aveva costante cosmologica, aveva materia ma poteva espandersi tranquillamente.

La costante cosmologica  $\Lambda$  non fu messa in cantina, nel 1948, Bondi e Gold da un lato e Hoyle dall'altro [49], nel tentativo di introdurre un

modello di universo che non avesse come inizio una singolarità con densità infinita, ma che fosse però in espansione, reintrodussero  $\Lambda$  anche loro come Einstein, non sapendo cosa volesse significare questa costante. In seguito, dopo che si trovò la radiazione cosmica di fondo,  $\Lambda$  fu di nuovo accantonata in quanto era necessario un Big Bang.

La costante  $\Lambda$  rispuntò nel 1967 quando tre cosmologi della Cornell University pubblicarono un articolo su *The Astronomical Journal* dal titolo " *Oggetti quasi stellari in un universo con una costante cosmologica non nulla*" [50], per spiegare i *quasar*. In seguito, capito meglio il comportamento dei *quasar*,  $\Lambda$  fu rimessa a riposo.

Nel 1975 la costante cosmologica riprese ad esistere anche grazie a J.E. Gunn e B.M. Tinsley [51] che intrecciando i dati del diagramma di Hubble, età delle galassie e densità dell'universo trovarono che esiste una costante cosmologica diversa da zero. Nel loro articolo, gli autori presentarono anche i possibili errori legati a queste analisi.

Dopo che alla fine degli anni '80 fu introdotta l'inflazione, il cosmologo Turner diceva spesso che "la costante cosmologica è l'ultimo rifugio dei cosmologi fuorilegge, a partire da Einstein" (si veda [52]). Negli anni successivi lo stesso Peebles aveva una idea di  $\Lambda$  molto seria anche se Turner ne era profondamente contrario. Dopo quasi 90 anni dopo la formulazione della teoria della Relatività Generale il termine  $\Lambda$  ritornava alla luce.

È bene ribadire che  $\Lambda$  non è né geometria né materia, ma Einstein sistemò la costante cosmologica vicino alla geometria e non alla materia, questo storicamente e fisicamente rimane comunque un mistero.

La costante cosmologica  $\Lambda$  ha avuto diverse interpretazioni fisiche, e nelle sezioni seguenti ne presenteremo due. La costante cosmologica è interpretabile come un fluido, ma è anche interpretabile come energia del vuoto secondo la teoria quantistica dei campi.

## $\Lambda$ come un fluido perfetto

Un fluido perfetto è un fluido senza viscosità, con densità costante e senza attriti interni nel senso che non ci sono interazioni tra le componenti del

<sup>7</sup>In realtà il primo ad accorgersi dello spostamento verso il rosso delle nebulose fu l'astronomo Vesto Slipher, nel 1912 [48], alla Lowell Observatory misurò lo *shift* della lunghezza d'onda di M31, che è una delle poche che mostra *blu-shift*. Fino al 1925 misurò le linee spettrali di quasi 40 galassie che per la maggior parte avevano lo spettro spostato verso il rosso.

fluido. Esso è caratterizzato da due quantità: la densità di energia  $\rho$  e la densità di pressione  $p$ . Questo modo di idealizzare il contenuto energetico dell'universo porta a forti semplificazioni, infatti le componenti di questo fluido sono le stelle, le galassie o anche gli ammassi di galassie e questo modo di descrivere rende le equazioni abordabili, in altri termini si imitano i fluidi perfetti per avere una descrizione matematica semplificata. L'equazione di stato del fluido riduce le variabili da due ( $\rho$  e  $p$ ) ad una sola delle due e la relazione che lega il tutto è la seguente

$$p = w \rho. \quad (8)$$

Il valore di  $w$  è abbastanza arbitrario, regola il rapporto tra pressione e densità di energia, ma  $w$  non è una costante universale, infatti differenti osservatori in moto relativo ottengono differenti valori di  $w$ .

Una interessante proprietà di  $\Lambda$  è che è in grado di generare nelle equazioni di Einstein una pressione negativa, come vedremo tra poco. Una pressione positiva vuole dire che le particelle spingono, ad esempio, sulle pareti di un contenitore, invece pressione negativa vuole dire che c'è una tensione del fluido, tensione che ne riduce la capacità attrattiva, facendola diventare repulsiva. Se consideriamo un elastico teso, tutte le sue molecole tendono a tirare verso l'interno esercitando una pressione negativa o tensione. In Relatività Generale la pressione positiva genera una gravità attrattiva, mentre la pressione negativa genera sempre una gravità ma repulsiva. La costante cosmologica fornisce allo spazio una energia uniforme il cui valore è proprio dato dal valore di  $\Lambda$ , ma fornisce allo spazio anche una pressione uniforme negativa che genera una forza gravitazionalmente repulsiva.

Chiaramente, dato che l'eq. (8) dipende dall'osservatore, allora  $w$  dipende non solo da quale fluido stiamo considerando, ma anche dalla cinematica dell'osservatore. Ma allora nasce spontanea la domanda se esiste un particolare valore di  $w$  che sia lo stesso per qualunque osservatore, indipendentemente dal suo stato di moto. Questo valore esiste e fa sì che ogni osservatore formuli la stessa equazione di stato, ed esso è  $w = -1$ . Questo valore caratterizza un unico fluido, particolare, che può associarsi alla densità di energia

della costante cosmologica ed esso è lo stesso per qualunque osservatore.

È bene ribadire questa caratteristica fondamentale, questo particolare fluido con  $w = -1$ , è identico per qualunque osservatore, indipendentemente dal suo stato di moto. Pertanto  $\Lambda$  può essere interpretata come un fluido perfetto cosmico. Tutto ciò che caratterizza questo fluido ci fa venire in mente l'etere, con proprietà assolute e con le stesse caratteristiche simili al fluido appena esaminato. Einstein elimina l'etere con la relatività ristretta ed introduce  $\Lambda$  con proprietà simili. Davvero strano, intrigante e sorprendente tutto ciò.

Però per completezza bisogna dire che l'accelerazione dell'universo viene spiegata per qualunque valore di  $w < -1/3$ , quindi esiste da un punto di vista teorico un infinito ventaglio di possibilità che possono spiegare l'accelerazione dell'universo, a seconda di quanto vale  $w$ . Adirittura esistono anche teorie che considerano una unificazione nella materia oscura ed energia oscura, ritenendo che ci sia una sorta di fluido cosmico che li contempla entrambi. Dato che non ci facciamo mancare nulla, i teorici hanno contemplato anche il caso in cui ci sia una "energia fantasma" con  $w < -1$ , caso questo che fa sì che si possano aprire dei veri e propri squarci (*Big Rip*), che provocherebbero la distruzione di qualunque corpo celeste, dove alla fine di questo processo ogni atomo sarebbe solo con se stesso nell'universo. Insomma la fantasia non manca oltre a scenari molto teorici, forse fin troppo.

## **$\Lambda$ e l'energia del vuoto quantistico dei campi**

Mentre per i relativisti  $\Lambda$  è quel termine aggiunto nelle equazioni di Einstein, per i fisici delle particelle e per i "campisti"  $\Lambda$  ha un significato diverso. Nella teoria quantistica dei campi non esistono particelle ma solo campi, le cui fluttuazioni si identificano con le particelle. È come se ogni particella avesse le sue onde, con la carica, lo spin, la massa ecc..

Andando indietro nel tempo, al 1918, ci si chiese se eliminando la massa dell'universo, la gravità sarebbe scomparsa, e de Sitter rispose, affermando che ci sarebbe stata la gravità anche se tutte le masse fossero state escluse. In altri termi-

ni il vuoto cosmico genera la gravità e questa fu la conclusione a cui giunsero sia Einstein che de Sitter. È una gravità particolare nel senso che è uniforme nello spazio e nel tempo e quindi non è misurabile studiando ad esempio il moto di un corpo celeste.

Il vuoto quantistico è un particolare stato della materia che riesce ad imitare la costante cosmologica. Il problema, sottile, è proprio questo: il vuoto quantistico caratterizza ed imita  $\Lambda$  o è proprio  $\Lambda$ ? Non riusciamo a distinguere  $\Lambda$  da un campo quantistico nel suo stato fondamentale.

Ora, le equazioni originarie di Einstein sono queste (senza specificarne il significato dei simboli)

$$R_{\mu\nu} - \frac{1}{2}R g_{\mu\nu} = \frac{8\pi G}{c^4} T_{\mu\nu} \quad (9)$$

che riscriviamo in modo simbolico come  $G = T$  dove  $G$  (cioè tutto il membro di sinistra) è essenzialmente la geometria e  $T$  (cioè tutto il membro di destra) è la sorgente materia/energia.

Riscriviamo queste equazioni mettendoci la costante cosmologica  $\Lambda$ , abbiamo due casi, con diverse interpretazioni fisiche.

#### Caso 1

$$\mathcal{K} = T + \Lambda \quad (10)$$

in questo caso la sorgente materia/radiazione è sempre  $T$  ma avendo messo a destra della equazione la costante cosmologica abbiamo una ulteriore sorgente che è il vuoto quantistico dei campi.

#### Caso 2

Se invece scriviamo, come ha fatto Einstein

$$\mathcal{K} + \Lambda = T \quad (11)$$

allora abbiamo che come sorgente vi è solo la materia/radiazione mentre questa posizione di  $\Lambda$  ci sta dicendo che vi è associato anche un'altro contributo alla metrica dato appunto da  $\Lambda$  quindi la costante cosmologica viene associata alle proprietà geometriche e non quelle delle sorgenti. I cosmologi hanno sposato questa seconda interpretazione anche se entrambe sono equivalenti (ma sono davvero equivalenti le due descrizioni?).

## Cosa è il vuoto nella fisica moderna?

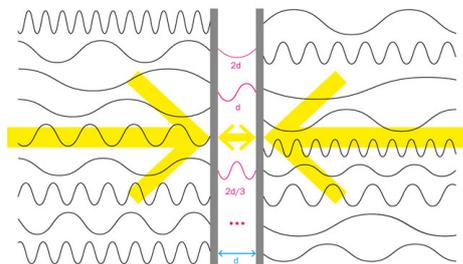
Dato un sistema fisico, tra tutti gli stati possibili, ve ne è uno caratterizzato da avere il minimo dell'energia, esso è detto **stato di vuoto** o **stato fondamentale**.

Si può dimostrare che la distribuzione dell'energia e dell'impulso del vuoto dei campi ha la stessa forma funzionale di  $\Lambda$ , cioè non siamo in grado di distinguere la  $\Lambda$  posta nelle equazioni di Einstein da un campo fisico nello stato fondamentale.

Immaginiamo di considerare una porzione di vuoto nel cosmo, e di eliminare ogni particella. Da un punto di vista classico questa porzione di spazio è stata svuotata completamente, da un punto di vista quantistico no. Il principio di indeterminazione di Heisenberg della meccanica quantistica ci dice che comunque vi è dell'energia, che non è zero ed è detta "energia di punto zero", proposta per la prima volta nel 1913 da Albert Einstein e Otto Stern [53]. L'energia di punto zero non può essere estratta, non può essere usata, non può essere eliminata, ed è infinita. L'energia del vuoto non dà contributo alla formazione delle strutture, anche se, essendo una energia, produce effetti gravitazionali. Il motivo di ciò è legato al fatto che questa energia del vuoto è equamente distribuita nel cosmo per cui non partecipa alla aggregazione di materia, per cui la sua presenza si manifesta a livello cosmologico e non a livello locale.

La meccanica quantistica prevede, nel vuoto, una costante creazione e distruzione di particelle virtuali, per cui risulta, almeno in linea teorica, che si può calcolare l'energia generata dalle fluttuazioni delle particelle virtuali nel vuoto. Da un punto di vista sperimentale questi concetti apparentemente astrusi sono stati messi alla prova nel 1948 dal fisico olandese Hendrik Casimir [54], che usando la meccanica quantistica, calcolò che il campo elettromagnetico poteva produrre, a causa delle fluttuazioni quantistiche, prove di tutto ciò. Considerò due lamine di metallo parallele, non cariche elettricamente, e distanti pochissimi micron tra le quali era stata tolta ogni forma di materia e a temperatura prossima allo zero assoluto. All'esterno delle piastre ci sarebbero state onde elettromagnetiche con tutte le frequenze, mentre tra le due piastre solo quelle

onde la cui lunghezza d'onda sarebbe stata un sottomultiplo intero della lunghezza tra le due lamine, in altri termini all'interno delle lamine vi dovevano essere meno oscillazioni ed esattamente solo quelle che si annullano ai bordi, sulle lamine. Questo in pratica selezionava natural-



**Figura 14:** Effetto Casimir. Tra le lamine le lunghezze d'onda ammesse dei fotoni virtuali sono un sottomultiplo intero della distanza tra le lamine. La maggiore presenza di onde fuori dalle lamine favorisce la pressione esterna generando una forza di attrazione delle lamine. Il vuoto non è vuoto. (Dalla Ref. [55]).

mente il numero di lunghezze d'onda permesse all'interno. Pertanto la differenza di energia tra l'esterno e l'interno avrebbe generato una spinta che avrebbe fatto avvicinare le lastre stesse: le lamine si sarebbero attratte a causa della riduzione delle oscillazioni all'interno delle lamine rispetto a quelle esterne. Era la dimostrazione che il vuoto è pieno di particelle virtuali.

Nel 1958 Marcus Sparnaay misurò ad Eindhoven questa *forza di Casimir* di attrazione [56] e nel 1997 si ebbe l'ulteriore conferma sperimentale grazie a Steven Lamoreaux dell'università di Washington [57]<sup>8</sup>. In seguito l'esperimento fatto da altri ha avuto ulteriori conferme. Nel 1947 Willis Lamb scoprì e misurò un sottile spostamento nel livello di energia dell'atomo di idrogeno, noto come, come Lamb Shift [58]. La velocità dell'elettrone nell'atomo di idrogeno è circa l'1% della velocità della luce. Lo spettro dell'atomo di idrogeno si manifesta quando l'elettrone passa da uno stato quantico all'altro, solo che a causa della interazione tra l'elettrone ed il vuoto si

<sup>8</sup>Questo esperimento di Lamoreaux era tra una lente sferica e una lamina di quarzo. Farla con due lamine parallele era un esperimento difficile perchè mantenere le lamine parallele non è affatto semplice, ma questo è stato fatto da un gruppo di Padova con Gianni Carugno e Roberto Onofrio e collaboratori.

aveva uno spostamento per il livello  $^2S_{1/2}$  che fu verificato sperimentalmente. Il vuoto non era vuoto!

Un campo quantistico si può considerare come una specie di sovrapposizione di onde, piccole, localizzate, con una lunghezza d'onda  $\lambda$ . Le particelle sono onde molto localizzate e con una energia di punto zero che va come l'inverso della lunghezza d'onda  $1/\lambda$ . Man mano che consideriamo valori sempre più piccoli di  $\lambda$ , vuol dire che stiamo considerando valori sempre più grandi di energia, ecco perchè l'energia del vuoto è infinita.

Un altro modo di guardare allo stesso problema è che la meccanica quantistica prevede una costante creazione e distruzione di particelle virtuali che altro non sono, in un linguaggio della teoria quantistica dei campi, che microscopiche oscillazioni. L'energia del vuoto è la risultante di tutte queste oscillazioni.

Il fatto che sia infinita l'energia non è un problema perchè in fisica si misurano solo le differenze di energia, per cui anche se lo stato di vuoto ha energia infinita, ciò non è osservabile. Un modo per stimare l'energia del vuoto è quello di trascurare le oscillazioni con lunghezze d'onda più piccole della lunghezza di Planck<sup>9</sup>  $\lambda_{Pl} = 10^{-33}$  cm per cui le onde con lunghezza d'onda minore di  $\lambda_{Pl}$  vengono trascurate e dato che l'energia del vuoto va come l'inverso della lunghezza d'onda  $E_{vac} \sim 1/\lambda$  si ha che la densità di energia della costante cosmologica è circa  $10^{120}$  volte più grande del valore osservato, questo assicura che la densità di energia del vuoto non sia infinita, ma il valore di  $\Lambda$  è comunque enorme e se fosse corretto avrebbe il potere di distruggere ogni forma di aggregazione di materia nell'universo.

Tutto ciò ci dice che una particolare proprietà del vuoto quantistico ci consente di interpretare la costante cosmologica. Le fluttuazioni dei campi quantistici sono generatori della costante cosmologica, cioè il contributo in energia da parte dei campi quantistici diffusa nel cosmo, porta alla idea di  $\Lambda$ .

<sup>9</sup>La lunghezza di Planck è pari a circa  $1.616252 \times 10^{-35}$  metri. Essa si può ottenere a partire da 3 costanti  $G, c, \hbar$  ed è la più piccola lunghezza sotto la quale perde di significato il concetto stesso di lunghezza, infatti si ritiene che al di sotto di questa lunghezza lo stesso spazio-tempo non segua più le leggi della fisica a noi note.

Fare affidamento sulla teoria quantistica dei campi su scale estremamente piccole, come la scala di Planck, non è mai una cosa buona anche perchè a queste scale la gravità non può essere trascurata. Tutto naturalmente vira nel considerare una futura teoria della gravità e della meccanica quantistica, la cui unificazione risolverebbe anche questo problema.

In ogni caso, bisogna fare attenzione quando si parla di gravità a questi livelli perchè in generale la si trascura sempre in laboratorio, data la sua debolezza. Però, se la si considera, le cose si fanno più complesse perchè secondo la teoria di Einstein anche l'energia genera un campo gravitazionale, pertanto il valore infinito della energia del vuoto crea seri problemi se si introduce la gravità.

Il fatto di associare l'energia del vuoto a  $\Lambda$ , porta a problemi ancora più gravi di quelli che si vuole risolvere: perchè il valore empirico di  $\Lambda$ , quello che proviene dalle osservazioni cosmologiche ed è inserito nella teoria della Relatività Generale, è estremamente piccolo e l'energia del vuoto, calcolata, è estremamente grande! La discrasia è intollerabile, c'è qualcosa di profondo che non abbiamo capito.

La cosa sorprendente è che la stima in energia contenuta nella agitazione quantistica è lontanissima dalla quantità di energia oscura che viene misurata nel nostro universo. Come detto in precedenza, usando una versione semplificata, che utilizza solo particelle del Modello Standard si trova che ci dovrebbe essere  $10^{120}$  volte più energia oscura di quanto ne misuriamo. È necessario dire che questa discrepanza era già nota prima della introduzione della energia oscura e andava sotto il nome di "problema della costante cosmologica".

Un modo per uscirne è quello che i fisici teorici chiamano "effetto compensativo", nel senso che il calcolo di  $\Lambda$  dà un numero enorme che potrebbe essere annullato da contributi opposti, riducendo così la nostra costante cosmologica quasi a zero. I fisici teorici hanno pensato che la supersimmetria potrebbe dare un contributo in questo senso, dato che il contributo alla energia di punto zero di un campo dovrebbe essere annullato dal campo del partner supersimmetrico, ma questo sarebbe stato vero se le coppie di particelle avessero la stessa massa, cosa che non

è <sup>10</sup>.

## Il destino dell'universo, il problema della coincidenza e il principio antropico

Tra i vari problemi che pone la costante cosmologica ve ne è uno molto importante legato alla evoluzione dell'universo. Attualmente la composizione dell'universo è per il 70% di costante cosmologica e il restante 30% di materia (oscura e barionica) Ora, andando indietro nel tempo, essendo  $\Lambda$  costante, ovviamente aveva sempre lo stesso valore nel passato, mentre la densità di energia e materia erano certamente maggiori e sempre più grandi man mano che ci si sposta indietro nel tempo, diminuendo anche il volume a disposizione. Ora però dai dati di SNIA e non solo quelli, sappiamo che l'accelerazione dell'universo è un fatto abbastanza recente (circa 5 miliardi di anni fa, secondo le ultime stime) e da quel momento cominciava a diventare prevalente il contributo delle densità di  $\Lambda$  su quella di materia.

In altri termini, all'inizio e per diverso tempo la materia prevaleva e rallentava l'espansione dell'universo, vinceva sulla energia oscura poi man mano che passava il tempo il suo effetto si esaurì a causa della espansione dell'universo e l'azione della costante cosmologica, che ha aspettato miliardi di anni, si prende la rivincita iniziando una lenta, inesorabile, costante azione acceleratrice, diventando la sua azione predominante sulla materia.

Vi è stato un tempo in cui densità di materia e densità di  $\Lambda$  sono stati uguali. Rispetto alla vita dell'universo questo tempo è un epsilon, un infinitesimo, un battito di ciglia. Ebbene, questo momento particolarissimo è proprio ora! Stranissima storia, davvero sorprendente, incredibile coincidenza temporale!

Per spiegare questa coincidenza temporale, nel 1987 Steven Weinberg (1933-2021) (Nobel per la fisica) fu portato a rifare una proposta degli anni '70 del secolo scorso, dovuta a B. Carter, M.J. Rees, B. Carr, J. Barrow e F. Tipler, nota come *principio*

<sup>10</sup>Il motivo tecnico è semplice: la supersimmetria tiene conto dei bosoni e dei fermioni, ma i bosoni vengono descritti da variabili che commutano mentre i fermioni che anticommutano, da qui il segno opposto nelle oscillazioni quantistiche.

*antropico* [59, 60, 61, 62]. In fondo, questo principio, dal nome altisonante, dice semplicemente che un altro numero di parametri diversi non avrebbe consentito la nostra esistenza, di umani. Weinberg sostiene che per avere un universo in cui ci siamo noi, è necessario che ci sia la coincidenza tra  $\Lambda$  e materia. Quando  $\Lambda$  prevarrà in modo irreversibile, tutto sarà distrutto, qualunque forma di aggregazione di materia nell'universo. Questa spiegazione, anche condita da matematica raffinata, non è affatto soddisfacente, anche se molto di moda, lascia l'amaro in bocca e non sembra neppure molto scientifica.

### Alcuni Problemi su $\Lambda$

Vale la pena a questo punto far una piccola sosta per riprenderci ed elencare per chiarezza e sintesi i problemi connessi con la costante cosmologica.

- 1) Il primo problema è perchè non abbiamo effetti osservabili a causa della gigantesca densità di energia connessa con le fluttuazioni quantistiche.
- 2) Il secondo problema consiste nel chiedersi come si elimina il contributo in energia a causa delle piccole lunghezze d'onda delle fluttuazioni dei campi quantistici.
- 3) Terzo problema, come si spiega questa strana coincidenza tra densità di energia oscura e densità di materia, oggi?
- 4) Quarto problema, forse il più grave di tutti. Trovare che la  $\Lambda$  debba essere  $10^{120}$  volte quella attesa è la peggiore previsione che i fisici teorici abbiano mai potuto fare in tutta la storia della fisica. E questa cosa passa spesso con semplicità ed ineluttabilità, invece potrebbe essere la spia che c'è qualcosa di veramente profondo che non abbiamo capito e che ci sta trascinando in un abisso di incomprensione della realtà.

### Quintessenza

Ci sono modelli, detti di "quintessenza", in cui la densità di energia varia nel tempo. Al modello standard della cosmologia si introduce un nuovo campo  $\phi$ , solo che contrariamente a  $\Lambda$ , esso può variare nello spazio e nel tempo, e questo fa sì che l'energia cinetica sia grande. Se  $\phi$  non varia, la massa associata è nulla, e quindi la sua energia è nulla; in pratica se  $\phi$  rimane ovunque

costante nello spazio e nel tempo, può essere considerato  $\Lambda$ . In questo modello il problema della coincidenza è superato perchè essendo l'energia di  $\phi$  variabile nel tempo, si possono generare dei meccanismi in grado di fornire in modo corretto quel valore che oggi vediamo.

Ora dato che i fotoni, neutrini, barioni e la materia oscura sono essenzialmente le particelle che formano l'universo, P. Steinhardt e R. Caldwell nel 1998 [63] hanno denominato questo campo  $\phi$ , "quintessenza", in analogia al quinto elemento di Aristotele per spiegare e capire il movimento di un corpo.

Senza complicarci la vita, diciamo subito che il campo di quintessenza è la fotocopia dell'inflatone nell'universo inflazionario. La pressione di questo campo  $\phi$  è dovuta a due contributi: energia cinetica (che contribuisce positivamente) ed energia potenziale (che contribuisce negativamente). È chiaro che se l'energia potenziale è di gran lunga superiore a quella cinetica la pressione risultante è negativa, che è ciò di cui abbiamo bisogno come abbiamo visto prima. Per essere in questo caso è necessario che la massa di  $\phi$  debba essere  $10^{33}$  volte più piccola della massa del neutrino.

La pressione negativa di  $\phi$  non è costante nel tempo. Dalla SNIA si trova che  $\phi$  dovrebbe avere una pressione molto vicina a quella di  $\Lambda$  ed essere quasi costante (come  $\Lambda$ ), inoltre non genererebbe semi di strutture a grandi o piccole scale proprio perchè  $\phi$  avrebbe pressione negativa.

Ora però, essendo la massa di  $\phi$  quasi zero, questo campo potrebbe essere un mediatore di una forza a lunghissimo *range* (dato che il raggio di azione di una forza è inversamente proporzionale alla massa della particella mediatrice). Questa analisi fu fatta da Robert Dicke e da Carl Brans nel 1961 [64], infatti  $\phi$  fu chiamato "campo di Brans-Dicke". L'idea fu accantonata perchè non vi erano evidenze sperimentali. Nel 1987 C. Wetterich [65], chiamò  $\phi$  "comon" e cercava di capire quanto valesse  $\Lambda$ .

Gli studi su  $\phi$  sono andati avanti e le cose da un punto di vista teorico si sono complicate. Un ricercatore canadese Gregory Horndesky propose nel 1974 [66] una lagrangiana, nota oggi come "lagrangiana di Horndesky". Egli non era un fisico ma un matematico, per cui non era interessato alla cosmologia ma a studiare una teoria

di campo scalare, la più generale possibile, nel secondo ordine nelle derivate. Il successo di questo approccio è che contempla la “quintessenza”, la teoria di Brans-Dicke e un’ampia gamma di campi scalari.

Come ben scritto nel libro di L. Amendola “L’altra faccia dell’universo” (vedi la bibliografia) il lavoro del 1974 ebbe una sola citazione nel 1976 ed un’altra nel 1978. Poi più nulla fino al 2011 dopo di che fu largamente citato. Il motivo era personale e non fisico, infatti intorno agli anni ’80 del secolo scorso, Horndesky visitò una mostra di Van Gogh, ne rimase colpito a tal punto che lasciò gli studi e l’università dove lavorava in Canada, e si mise lui stesso a dipingere, a Santa Fe, nel Nuovo Messico. Nel 2011, fisici teorici cercarono di trovare il più generale campo scalare al secondo ordine e si accorsero che nel 1974 Horndesky aveva già trovato la risposta a questa domanda.

In ogni caso, il campo di “quintessenza” non è mai stato trovato e rimane tutt’oggi una vaga possibilità teorica.

## Considerazioni generali

L’energia oscura è una forma strana di energia che ha solo un effetto osservabile: accelerare l’espansione dello spazio cosmico.

C’è da dire che  $\Lambda$  è la spiegazione più immediata, e, se vogliamo, la più semplice dell’esistenza della energia oscura.

L’energia oscura non agisce come la massa o come l’energia che conosciamo, perchè queste spingono le componenti dell’universo ad attirarsi, mentre l’energia oscura ha un effetto repulsivo, di anti-gravità.

Ciò che lascia sconcertati non è solo l’origine ignota della energia oscura, ma anche la quantità di energia oscura nel cosmo, dato che la densità di energia oscura è circa  $2/3$  della densità di materia oscura, quasi uguali, e questo di per sè disorienta perchè materia oscura ed energia oscura sembrano completamente non correlate tra loro: una strana coincidenza.

La domanda delle domande è se abbiamo capito davvero gli effetti della gravità dell’energia del vuoto, perchè tutto alla fine si riduce a questo livello di comprensione della realtà della energia oscura.

Inoltre, non abbiamo capito neppure perchè l’energia del vuoto ha quei valori che le osservazioni ci dicono.

C’è anche un’altra osservazione che spesso viene trascurata, e riguarda le due interpretazioni della costante cosmologica e cioè una connessa al fluido e l’altra come energia del vuoto: queste due interpretazioni non si danno fastidio, non cadono in contraddizione e coesistono una indipendentemente dall’altra. Come è possibile questo?

La via scelta dalla maggior parte dei fisici è una scelta con non molto coraggio. O vengono introdotti ingredienti strani, per i quali non c’è uno straccio di evidenza sperimentale oppure forzano in modo davvero incredibile le leggi della natura, però senza il coraggio vero di chi vuole scardinare il sapere consolidato, il tutto da modificare solo poco.

Gli scettici (pochissimi) si chiedono che forse materia oscura ed energia oscura siano la febbre di una malattia, che non quadra a livello di comprensione fondamentale. È come se si cercasse di mantenere a tutti i costi l’impianto di conoscenze acquisite, cercando di non molestare troppo la comprensione della fisica e della cosmologia odierna. Personalmente, credo che probabilmente abbiamo spinto troppo la teoria di Newton ed Einstein, al limite massimo che possiamo ottenere, per cui materia oscura e/o energia oscura sono la manifestazione di una inapplicabilità di quelle teorie, che quindi manifestano la loro eventuale incapacità a descrivere in modo corretto la natura, generando cose che forse potrebbero neppure esistere. A dare forza a questo modo di vedere le cose c’è il fatto che, ad esempio, per la descrizione delle curve di rotazione delle galassie le teorie di Newton ed Einstein producono risultati praticamente indistinguibili.

La materia oscura e l’energia oscura potrebbero essere solo la testimonianza di una nostra profonda incapacità a capire cosa stia accadendo nel cosmo che quindi rappresenterebbero una sorta di calderone di ignoranza con il quale nascondere sotto il tappeto la polvere della nostra incomprendenza di ciò che stiamo osservando di anomalo.

La cosa può essere vista in altro modo e cioè che la descrizione del nostro universo, quindi gravità newtoniana ed einsteiniana siano descri-

zioni non corrette, per cui materia oscura ed energia oscura sono l'espressione non di un mistero ma di una applicazione non corretta di leggi non ultime. Dissacrare le teorie cosmologiche dominanti è considerato un sacrilegio, ma è troppo fitto il mistero per non avere il dubbio che materia oscura ed energia oscura non siano delle stampe della cosmologia necessarie per mantenere lo *status quo* della fisica conosciuta e salvare tutto ciò che teoricamente si può salvare.

Tutte le teorie, o meglio congetture, sulla materia oscura ed energia oscura godono di una rilevanza e privilegio e, se si vuole, di un certificato di esistenza in vita, puramente teorico e congetturale.

La teoria delle stringhe con le dimensioni extra spiega l'accelerazione dell'universo e la materia oscura, ma questi modelli forniscono previsioni teoriche spesso difficili da verificare sperimentalmente, inoltre spiegano l'accelerazione dell'universo ma non il valore piccolissimo di  $\Lambda$ . Spesso queste teorie con dimensioni extra coinvolgono scale talmente piccole da non essere oggetto di osservazione, anche se esistono versioni con dimensioni compatte che potrebbe in futuro essere oggetto di sperimentazione.

Ci sono teorie che ritengono che vada scardinato qualche pilastro, come ad esempio l'omogeneità dell'universo, che essendo ad esempio un frattale, potrebbe mimare l'energia oscura, ipotesi, questa, che L. Pietronero, della Sapienza di Roma ha più volte proposto [67], ed è stata molto osteggiata perchè come molte proposte che non seguono il *mainstream* sono soggette ad attacchi anche violenti dagli addetti ai lavori.

Non sappiamo dove andremo con questa ricerca e linea di pensiero, quello che è certo è che ciò che pensiamo dell'Universo dovrà subire un cambio di paradigma senza precedenti e ci obbligherà a pensare a qualcosa di profondamente diverso rispetto alle nostre conoscenze. Lo stato di confusione è senza precedenti. Certo stanare l'energia oscura non è solo una cosa complessa da un punto di vista sperimentale, ma è forse ancora più complessa da un punto di vista teorico, perchè non ne abbiamo la più pallida idea con cosa abbiamo a che fare.

Si sono portate diverse modifiche alla gravità di Einstein, ma sempre con troppo rispetto per la Relatività Generale, il cui impianto è stato la-

sciato essenzialmente integro. È come ostinarsi a spiegare con la teoria di Newton il problema del perielio di Mercurio, possiamo fare tutte le congetture possibili, ma alla fine dobbiamo abbandonare la teoria della gravità di Newton e affidarci a quella di Einstein per avere chiarezza. Allo stesso modo, la teoria della gravità di Einstein l'abbiamo spinta quasi la massimo del suo rendimento (o meglio di ciò che sappiamo farne) e usandola, con tutta la cosmologia annessa, troviamo delle lacune nella nostra comprensione della realtà.

Personalmente penso che l'approccio condiviso da quasi tutto il mondo scientifico sia poco coraggioso, non può portarci lontano, perchè sarebbe come stare in una strada buia, e perdere le chiavi, e cercarle sotto l'unico lampione che si trova in quella strada solo perchè è l'unico posto illuminato.

La cosa che potrebbe sorprendere in futuro è che la materia oscura e l'energia oscura possano essere espressioni di risposte errate o domande mal poste al cosmo.

O, come dice qualcuno: "se l'universo è la risposta, qual è la domanda?"

## Ringraziamenti

Questo lavoro è parzialmente supportato dall'INFN mediante il programma TAsP: *Theoretical Astroparticle Physics*, e dal progetto di ricerca numero 2022E2J4RK PANTHEON: *Perspectives in Astroparticle and Neutrino THEory with Old and New messengers* sotto il programma PRIN 2022 del Ministero dell'Università e della Ricerca (MUR).

Un effetto collaterale nello scrivere questo articolo è l'aver conosciuto ed apprezzato l'amico e collega Giampalo Co' che ringrazio per aver reso migliore questo articolo con i suoi interessantissimi suggerimenti e le sue preziose correzioni.

## Suggerimenti bibliografici

La bibliografia su materia oscura ed energia oscura è sterminata. Segnalo alcuni testi divulgativi di ottima fattura e qualche testo non divulgativo.

## Testi divulgativi

- L. Amendola, *L'altra faccia dell'universo*, Il Mulino (2018).
- Amedeo Balbi, *Il buio oltre la siepe*, Codice edizioni (2011).
- John David Barrow, *Da zero a infinito*, Mondadori, (2002).
- Andrea Cimatti, *L'universo oscuro*, Carocci editore (2021).
- Marco Cirelli, *La materia oscura*, Ithaca: Viaggio nella Scienza XII, pag. 117 (2018).
- Frank Close, *Nulla*, Codice Edizioni (2011).
- Pedro G. Ferreira, *La teoria perfetta*, Rizzoli (2014).
- Maurizio Gasperini, *Gravità, stringhe e particelle*, Springer iblu (2014).
- Maurizio Gasperini *Teoria gravitazionale e applicazioni cosmologiche: possibili sviluppi*, "Ithaca: Sfide", XXI (2023) ISSN: 2282-8079, ESE (Salento University Publishing).
- Maurizio Gasperini, *L'universo prima del big bang*, Franco Murzio Editore (2002).
- Brian Green, *La trama del Cosmo*, Einaudi (2004).
- Brian Greene *La realtà nascosta*, Einaudi (2012).
- Danis Hooper, *Il lato oscuro dell'universo*, Edizioni Dedalo (2008).
- Lawrence Krauss, *Il mistero della massa mancante*, Raffaello Cortina Editore (2000).
- Mario Novello, *Qualcosa anziché il nulla*, Einaudi (2011).
- Massimo Pietroni, *Energia oscura, il motore dell'universo*, Ithaca: Viaggio nella Scienza XII, pag. 129 (2018).
- Richard Panek, *L'universo oscuro*, La Biblioteca delle Scienze (2011).
- Lisa Randall, *Bussando alle porte del cielo*, il Saggiatore (2012).
- Paul J. Steinhardt e Neil Turok, *Universo senza fine*, il Saggiatore (2008).
- James Owen Weatherall, *La fisica del nulla*, Boringhieri (2017).

## Testi non divulgativi

- Luca Amendola e Shinji Tsujikawa, *Dark energy, theory and observations*, Cambridge University Press (2010).

Lefteris Papantonopoulos Editor (autori vari), *The invisible universe: dark matter and dark energy*, Springer (2007).

Marco Roncadelli, *Aspetti astrofisici della materia oscura*, Bibliopolis (2009).

Steven Weinberg, *Cosmology*, Oxford University Press (2008).



- [1] D. Huterer, M. S. Turner: *Prospects for probing the dark energy via supernova distance measurements*, Phys. Rev. D, 60 (1999) 0831.
- [2] A. Secchi: *Le stelle, saggio di astronomia siderale*, Fratelli Dumolard, Milano (1877).
- [3] H. Poincarè: *The milky way and the theory of gases*, Bulletin de la Société Astronomique de France, 20 (1906) 153.
- [4] Lord Kelvin: Appendice al libro *Baltimore lectures on molecular dynamics and the wave theory of light*, C.J. Clay and Sons, Londra (1904), p. 274.
- [5] J. C. Kapteyn: *First attempt at a theory of the arrangement and motion of the sidereal system*, Astrophysical Journal, 55 (1922) 302.
- [6] K. Lundmark: *Über die Bestimmung der Entfernungen, Dimensionen, Massen und Dichtigkeit für die nächstgelegenen anagalactischen Sternsysteme.*, Meddelanden Fran Lunds Astronomiska Observatorium Serie I, 125 (1930) 1.
- [7] G. Bertone, Dan Hooper: *A History of Dark Matter*, Rev. Mod. Phys., 90 (2018) 45002.
- [8] J. H. Oort: *The Force Exerted by the Stellar System in the Direction Perpendicular to the Galactic Plane and Some Related Problems*, Bulletin of the Astronomical Institute of the Netherlands, 6 (1932) 249.
- [9] F. Zwicky: *The red shift of extragalactic nebulae*, Helvetica Physica Acta, 6 (1933) 651.
- [10] S. van der Bergh: *The stability of clusters of galaxies*, Astrophys. J., 66 (1960) 558.
- [11] L. Amendola: *L'altra faccia dell'universo*, Il Mulino, Bologna (2018).
- [12] H.W. Babcock: *The rotation of the Andromeda Nebula*, Lick Observatory Bulletin, 19 (1939) 41.
- [13] J.H. Oort: *Some Problems Concerning the Structure and Dynamics of the Galactic System and the Elliptical Nebulae NGC 3115 and 4494*, Astrophysical Journal, 91 (1940) 273.
- [14] V.C. Rubin, W. K. Ford: *Rotation of the Andromeda Nebula from a Spectroscopic Survey of Emission Regions*, Astrophysical Journal, 159 (1970) 379.
- [15] M. Roncadelli: *Aspetti astrofisici della materia oscura*, Bibliopolis, Napoli (2009).
- [16] E. Asencio, I. Banik, P. Kroupa: *The El Gordo Galaxy Cluster Challenges  $\Lambda$ CDM for Any Plausible Collision Velocity*, Astrophysical Journal, 954 (2023) 162.

- [17] F. Zwicky: *On the Masses of Nebulae and of Clusters of Nebulae*, The Astrophysical Journal, 86 (1937) 3.
- [18] F. De Paolis et al.: *Macro / micro / retro lensing gravitazionale*, Ithaca, V (2015) 19.
- [19] H. C. van de Hulst: *Radiostraling uit het wereldruim. II. Herkomst der radiogolven*, Nederlandsch Tijdschrift voor Natuurkunde, 11 (1945) 210.
- [20] H. I. Ewen, E. M. Purcell: *Observation of a Line in the Galactic Radio Spectrum: Radiation from Galactic Hydrogen at 1,420 Mc./sec*, Nature, 168 (1951) 356.
- [21] H.C. van de Hulst: *Light scattering by small particle*, Wiley, Hoboken, New Jersey, Stati Uniti (1957).
- [22] R.S. Morton: *A high resolution 21 cm hydrogen-line survey of the Andromeda nebula*, Astrophysical Journal, 159 (1966) 639.
- [23] S. Gershtein, Y. a. Zeldovich: *Rest mass of muonic neutrinos and cosmology*, JETP Lett., 4 (1966) 120.
- [24] J. F. Navarro, C. S. Frenk, S. D. M. White: *The Structure of Cold Dark Matter Halos*, The Astrophysical Journal, 462 (1996) 563.
- [25] B. W. Lee, S. Weinberg: *Cosmological lower bound on heavy-neutrino masses*, Phys. Rev. Lett., 39 (1977) 165.
- [26] R. D. Peccei, H. R. Quinn: *CP Conservation in the Presence of Pseudoparticles*, Phys. Rev. Lett., 38 (1977) 1440.
- [27] S. Weinberg: *A New Light Boson?*, Phys. Rev. Lett., 40 (1978) 223.
- [28] F. Wilczek: *Problem of Strong P and T Invariance in the Presence of Instantons*, Phys. Rev. Lett., 40 (1978) 279.
- [29] K.J. Mack, P.J. Steinhard: *Cosmological problems with Multiple Axion-like fields*, Journal of Cosmology and Astroparticle Physics, 1105 (2011) 001.
- [30] T. Kaluza: *Unitätsproblem in der Physik*, Sitzungsberrichte der Koniglich Akademieder Preussischen Akademie der Wissenschaften, 1 (1921) 966.
- [31] O. Klein: *Quantentheorie und fünfdimensionale Relativitätstheorie*, Z. Physik, 37 (1926) 895.
- [32] G. Veneziano: *Construction of a crossing-symmetric, Regge-behaved amplitude for linearly rising trajectories*, Nuovo Cim. A, 57 (1968) 190.
- [33] Z. Chrobáková., M. López-Corredoira, F. Sylos Labini, H.F. Wang, R. Nagy: *Gaia-DR2 extended kinematical maps. III. Rotation curves analysis, dark matter*, Astronomy & Astrophysics, 642 (2020) 95.  
F. Sylos Labini, G. De Marzo, M. Straccamore, S. Comeron: *The Tully-Fisher relation and the Bosma effect*, ArXiv:2310.1573.
- [34] A. Goobar, S. Perlmutter: *Feasibility of Measuring the Cosmological Constant Lambda and Mass Density Omega Using Type IA Supernovae*, Astrophysical Journal, 450 (1995) 14.
- [35] S. Perlmutter et al.: *Measurements of the Cosmological Parameters  $\Omega$  and  $\Lambda$  from the First Seven Supernovae at  $z \geq 0.35$* , The Astrophysical Journal, 483 (1997) 565.
- [36] S. Perlmutter et al.: *Discovery of a supernova explosion at half the age of the universe and its cosmological implications*, Nature, 391 (1998) 51.
- [37] P. M. Garnavich et al.: *Constraints on cosmological models from Hubble Space telescope observations of high  $z$  supernovae*, Astrophys. J. Lett., 493 (1998) L53.
- [38] S. Perlmutter et al.: *Measurements of  $\Omega$  and  $\Lambda$  from 42 high-redshift supernovae*, The Astrophysical Journal, 517 (1999) 565.
- [39] C. G. Neumann: *Allgemeine Untersuchungen über das Newton'sche Princip der Fernwirkungen mit besonderer Rücksicht auf die elektrischen Wirkungen*, Monatsh. f. Mathematik und Physik, 7 (1896) A50.
- [40] A. Einstein: *Kosmologische Betrachtungen zur allgemeinen Relativitätstheorie*, Sitz. König. Preuss. Akad., (1917) 142. -152.
- [41] A. Einstein: Lettera a Paul Ehrenfest, 14 febbraio 1917 CPAE 8 (Doc. 298).
- [42] H. Weyl: *Temp, Espace, Matière*, Libraire Scientifique Albert Blanchad, Parigi (1922).
- [43] P. Ferreira: *La teoria perfetta*, Rizzoli, Bologna (2014).
- [44] A. Friedman: *Über die krümmung des raumes*, Z. Phys., 10 (1922) 377.
- [45] A. Friedman: *Über die Möglichkeit einer Welt mit konstanter negativer Krümmung des Raumes*, Z. Phys., 21 (1924) 326.
- [46] G. Lemaître: *Un Univers homogène de masse constante et de rayon croissant rendant compte de la vitesse radiale des nébuleuses extra-galactiques*, Annales de la Société Scientifique de Bruxelles, 47 (1927) 49.
- [47] E. Hubble: *A relation between distance and radial velocity among extra-galactic nebulae*, Proc. Natl. Acad. Sci. USA, 15 (1929) 168.
- [48] V. Slipher: *The radial velocity of the Andromeda Nebula*, Lowell Observatory Bulletin, (1912) 2.56.
- [49] H. Bondi, T. Gold: *The steady-state of the expanding Universe*, Monthly Notice Royal Astronomical Society, 108 (1948) 3.
- [50] V. Petrosian, E. Salpeter, P. Szekeres: *Quasi-Stellar Objects in Universes with Non-Zero Cosmological Constant*, Astrophys. J., 147 (1967) 1222.
- [51] J.E. Gunn, B.M. Tinsley: *An accelerating universe*, Nature, 247 (1975) 454.
- [52] Richard Panek: *L'universo oscuro* La Biblioteca delle Scienze (2011).
- [53] A. Einstein, O. Stern: *Einige Argumente für die Annahme einer molekularen Agitation beim absoluten Nullpunkt*, Annalen der Physik, 40 (1913) 551.
- [54] H.B.G. Casimir: *On the attraction between two perfectly conducting plates*, Proc. 'kon. Ned. Akad. Wetenschap., ser. B,, 51 (1948) 793.
- [55] A. Urbano: *La ricchezza del niente*, Asimmetrie, 24 (2018) 3.
- [56] M. J. Sparnaay: *Measurements of attractive forces between flat plates*, Physica, 24 (1958) 751.
- [57] S. Lamoreaux: *Demonstration of the Casimir Force in the 0.6 to 6  $\mu\text{m}$  Range*, Phys. Rev. Lett., 78 (1997) 5.  
Phys. Rev. Lett., 81 (1998) 5475 (erratum).

- [58] W. E. Lamb, R.C. Retherford: *Fine Structure of the Hydrogen Atom by a Microwave Method*, Phys. Rev., 72 (1947) 241.
- [59] B. Carter: *Large Number Coincidences and the Anthropic Cosmological Principle*, "Confrontation of Cosmological Theories with Observational Data", a cura di M.S. Longair, Reidel, Dordrecht (1974) 291.
- [60] B. Carr, M. Rees: *The Anthropic Principle and the Structure of the Physical World*, Nature, 278 (1979) 605.
- [61] J. Barrow: *Anthropic Definitions*, Quarterly Journal of the Royal Astronomical Society, 24 (1983) 146.
- [62] J. Barrow, F. Tipler: *The Anthropic Cosmological Principle*, Clarendon Press, Oxford (1986).
- [63] R. R. Caldwell, R. Dave, P. J. Steinhardt: *Cosmological Imprint of an Energy Component with General Equation-of-State*, Phys. Rev. Lett., 80 (1998) 1582.
- [64] C. Brans, R. H. Dicke: *Mach's principle and a relativistic theory of gravitation*, Phys. Rev., 124 (1961) 925.
- [65] C. Wetterich: *Cosmology and the fate of dilatation symmetry*, Nucl. Phys. B, 302 (1988) 668.
- [66] G. W. Horndesky: *Second-order scalar-tensor field equations in a four dimensional space*, International Journal of Theoretical Physics, 10 (1974) 363.
- [67] L. Cosmai, G. Fanizza, F. Sylos Labini, L. Pietronero, L. Tedesco: *Fractal universe and cosmic acceleration in a Lemâitre-Tolman-Bondi scenario*, Class. Quantum Grav., 36 (2019) 045007.



**Luigi Tedesco:** è professore di Fisica teorica presso il Dipartimento Interateneo di Fisica di Bari. Si occupa nelle sue ricerche di Relatività e Cosmologia.

---

# Euclid

**Stefano Dusini, Luca Stanco**

*Istituto Nazionale di Fisica Nucleare, Sez. di Padova, Padova, Italy*

---

## Introduzione

Le origini dell'Universo e la sua evoluzione sono sempre stati uno dei quesiti più affascinanti della scienza e della filosofia. Non c'è cultura antica che non abbia formulato una narrazione sulla nascita dell'Universo o che abbia fatto congetture sulla sua evoluzione. Ma è soltanto nel secolo scorso, con la Teoria della Relatività, che la scienza inizia a porre le prime basi per la costruzione di un modello capace di descrivere la storia del cosmo.

La teoria di Einstein ci dice che la forza di gravità è una conseguenza della geometria dello spazio-tempo, la cui forma dipende dalla materia ed energia presente nello spazio. Ecco che la Teoria della Relatività diventa la base per costruire un modello che descriva l'evoluzione dell'Universo. Infatti passano solo pochi anni dalla pubblicazione delle equazioni di Einstein, che il matematico russo Alexander Friedmann trova una soluzione che descrive l'espansione di un universo omogeneo e isotropo popolato di materia. Friedmann trova che la curvatura dello spazio-tempo dipende da quanta materia è presente nell'universo. Se questa è poca allora l'Universo si espande indefinitamente. Se questa invece è maggiore di una certa quantità critica, il campo gravitazionale prodotto dalla materia è in grado di fermare l'espansione per poi generare una successiva contrazione.

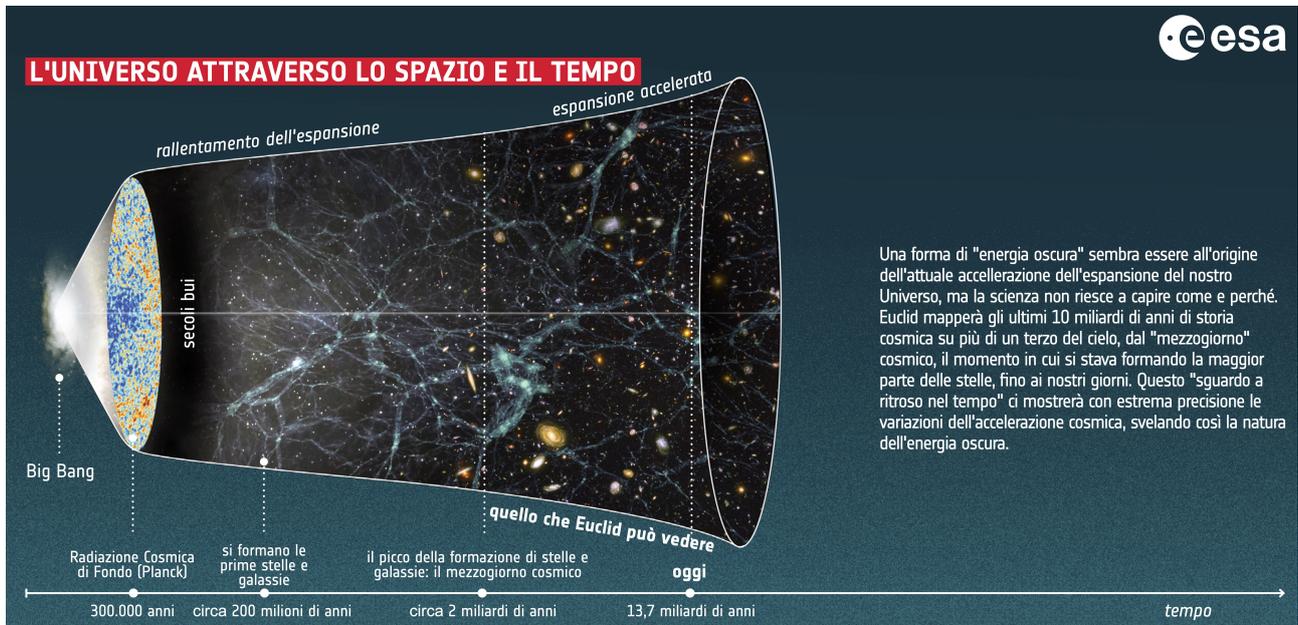
Ma quando Friedmann scrive le sue equazioni non si sa se l'Universo sia in espansione. Non è nemmeno chiaro che esistano altre galassie al di fuori della nostra, per cui guardando alla Via Lattea è naturale pensare che l'Universo

sia statico e quindi l'idea che la Teoria della Relatività predica un Universo o in espansione o in contrazione non piace. In primis ad Einstein, che per risolvere quest'apparente problema introduce nelle equazioni un termine costante tale da annullare il termine cinetico ed ottenere quindi un Universo statico. Così è nata la costante cosmologica.

Ma nel 1929 arriva un'importante scoperta, una di quelle che fanno voltare pagina alla storia della scienza. Edwin Hubble scopre che le galassie non hanno un moto erratico per cui alcune si avvicinano a noi e altre si allontanano. No! tutte le galassie, sufficientemente lontane da non sentire l'attrazione gravitazionale della nostra galassia, si allontanano da noi e la loro velocità è proporzionale alla distanza. In altre parole, l'Universo non è statico ma si sta espandendo e la velocità apparente delle galassie, osservata da Hubble attraverso lo spostamento verso il rosso degli spettri di emissione atomica, non è altro che lo spazio che si dilata.

Questa importante scoperta insieme alle equazioni di Friedmann hanno gettato le basi per la costruzione del modello del Big Bang, secondo cui l'Universo ha avuto origine 13.8 miliardi di anni fa a partire da uno stato iniziale di elevata densità e temperatura per poi espandersi fino all'Universo che oggi conosciamo. Da questo quadro rimaneva aperta la domanda se l'Universo si sarebbe espanso indefinitamente, o se ad un certo punto avrebbe cominciato a contrarsi, sotto l'azione della forza di gravità, per generare quello che in gergo viene chiamato un Big Crunch.

Per trovare una risposta a questa domanda



**Figura 1:** Rappresentazione artistica dell'evoluzione dell'Universo dal Big Bang a oggi. Crediti: Esa/Euclid CC BY-SA 3.0 IGO

gli scienziati dovranno aspettare la fine del '900, quando dalle misure dell'anisotropia della radiazione cosmica di fondo – la radiazione residua del Big Bang – emerge che le fluttuazioni di temperatura osservate sono compatibili con un universo piatto, cioè un universo in cui la densità di energia e materia è pari a quella critica. Ovvero nel nostro Universo non c'è sufficiente energia per frenare l'espansione e generare un collasso (Universo chiuso) ma neanche troppo poca perchè l'espansione non continui all'infinito (Universo aperto). Il nostro è un Universo con una geometria piana che, in assenza di altri effetti, dovrebbe rallentare la sua espansione fino a raggiungere, asintoticamente, uno stato statico.

Come spesso accade nella scienza quando si trova una risposta, questa ne apre altre dieci. Infatti dalla teoria del Big Bang gli scienziati hanno calcolato le abbondanze relative degli elementi leggeri presenti nell'Universo e le hanno confrontate con le osservazioni astronomiche per stimare la quantità totale di materia barionica presente nell'Universo. Il calcolo mostra però che la densità di materia visibile è di molto inferiore alla densità critica. Deve quindi esistere una grande quantità di materia non visibile, chiamata appunto materia oscura, per far sì che la densità totale sia prossima a quella critica.

Per gli astronomi il concetto di materia oscura non era del tutto nuovo. Le osservazioni sulla

velocità di rotazione delle galassie a spirale, già dal lontano 1933 [1] e successive altre lungo un arco di decenni, fino alle prossime osservazioni del Vera Rubin Observatory [2], unite alle osservazioni delle lenti gravitazionali [3] hanno già evidenziato l'esistenza di una materia non visibile.

Ma la sorpresa più grande arriverà nel 1998 quando due gruppi di astronomi e fisici, capitanati da Saul Perlmutter, Brian Schmidt e Adam Riess [4], pubblicano i risultati di una ricerca sulle supernove (SN) di tipo Ia (Premio Nobel per la Fisica 2011). Le SN Ia sono delle sorgenti luminose molto intense la cui luminosità è pressoché costante e indipendente dalla particolare esplosione che le ha generate. Questo le rende delle *candele standard* per le quali è possibile misurarne la distanza direttamente dalla loro luminosità apparente. Gli scienziati vogliono confrontare questa distanza, chiamata distanza luminosa, con lo spostamento verso il rosso (redshift) dello spettro di emissione delle SN. Infatti il redshift  $z$ , definito come lo spostamento relativo della lunghezza d'onda della luce emessa  $\lambda_e$  ed osservata  $\lambda_o$  di una sorgente lontana

$$z = \frac{\lambda_o - \lambda_e}{\lambda_e}, \quad (1)$$

è direttamente proporzionale all'espansione relativa dell'Universo tra l'istante di emissione e di

rivelazione della luce. A seconda di come è avvenuta questa espansione, se a velocità costante o in maniera (de)accelerata, cambia la distanza percorsa dal raggio luminoso e quindi la luminosità apparente della sorgente che lo ha emesso. I ricercatori vogliono cercare una indicazione di un rallentamento nell'espansione dell'Universo compatibile con un universo, chiuso, piatto o aperto. Contro ogni attesa, i risultati non mostrano un rallentamento ma una espansione in piena accelerazione.

Da dove nasce questa accelerazione, qual è la forza che la genera? Per capirlo dobbiamo ritornare alla famosa costante cosmologica introdotta da Einstein e guardare un po' più nel dettaglio le equazioni di Friedmann.

In cosmologia, l'espansione dell'Universo è descritta dal parametro di scala  $a(t)$  della metrica dello spazio-tempo

$$ds^2 = c^2 dt^2 - a^2(t)(dx^2 + dy^2 + dz^2) \quad (2)$$

che ci dice come la metrica evolve nel tempo. In (2) la distanza spazio-temporale  $ds$  è data dalla distanza temporale  $c^2 dt^2$ , essendo  $c$  la velocità della luce nel vuoto, e quella spaziale  $(dx^2 + dy^2 + dz^2)$  opportunamente scalata dal parametro  $a(t)$ . Le equazioni di Friedmann ci dicono come la densità di energia e materia dell'Universo influiscono sull'evoluzione del parametro di scala  $a(t)$ :

$$H^2 = \frac{1}{a} \frac{da(t)}{dt} = \frac{8\pi G}{3c^2} \epsilon - \frac{kc^2}{a^2} + \frac{\Lambda}{3}, \quad (3)$$

$$\frac{1}{a} \frac{d^2 a(t)}{dt^2} = -\frac{4\pi G}{3c^2} (\epsilon + 3P) + \frac{\Lambda}{3}, \quad (4)$$

dove  $H$  è il parametro di Hubble,  $\epsilon$  e  $P$  la densità totale di energia e materia e la sua pressione,  $\Lambda$  la costante cosmologica e  $G$  è la costante di gravitazione universale di Newton, mentre  $k$  è il parametro di curvatura e vale 0, +1, -1 nel caso la geometria dello spazio sia, rispettivamente, piana, a curvatura positiva o chiusa, a curvatura negativa o aperta. Dall'Eq. (3) si vede che l'aggiungere la costante cosmologica equivale ad aggiungere una nuova componente di energia che, a seconda del suo valore, può annullare l'attrazione gravitazionale, come era stato voluto da Einstein per avere un Universo statico, o determinare una sua espansione accelerata. Un aspetto

importante dell'energia oscura è che la sua densità è costante e non decresce come la densità di materia o radiazione al crescere del volume dell'Universo. Questo vuol dire che in passato, quando l'Universo era più piccolo di adesso, il suo effetto era trascurabile, ma con l'espansione dell'Universo il suo contributo è cresciuto molto, tant'è che ad oggi l'energia oscura, ovvero la componente associata alla costante cosmologica, rappresenta circa il 69% dell'energia totale dell'Universo, mentre il restante è composto da  $\sim 25\%$  di materia oscura e  $\sim 4\%$  di materia ordinaria. Una conseguenza importante è che l'energia oscura continuerà ad accelerare l'espansione indefinitamente.

Il modello che abbiamo appena descritto è chiamato  $\Lambda$ CDM ( $\Lambda$  Cold Dark Matter) ed è considerato il modello standard della cosmologia. Nonostante il suo grande successo nel descrivere le osservazioni fino ad ora fatte, rimane un modello efficace incapace di descrivere la natura della materia ed energia oscura. Anche il Modello Standard delle particelle elementari e la Meccanica Quantistica non ci aiutano molto. Sebbene la costante cosmologica possa essere interpretata come una manifestazione dell'energia associata alle fluttuazioni quantistiche del vuoto, il valore che il Modello Standard delle particelle elementari prevede risulta essere molte decine di ordini di grandezza più grande del valore attualmente misurato dalla cosmologia.

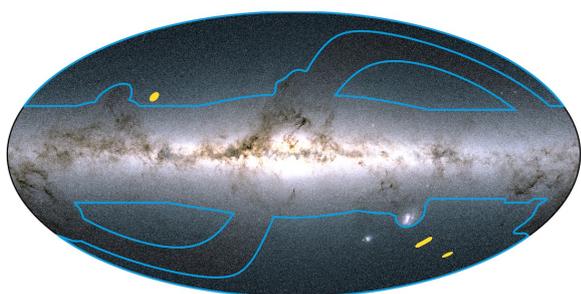
Per cercare di rispondere a queste domande sono stati formulati diversi modelli alternativi a  $\Lambda$ CDM che ipotizzano l'esistenza di nuove forze che si manifestano solo a scale cosmologiche o modelli che prevedono delle modifiche della Teoria della Relatività e che sono comunemente chiamate teorie di gravità modificata. Purtroppo la precisione e l'accuratezza dei dati che abbiamo in questo momento a disposizione non ci permettono di discriminare tra questi modelli.

## La Missione Euclid

Per far luce su questo lato oscuro dell'Universo nel 2008 l'ESA ha approvato la missione spaziale Euclid [5] con l'obiettivo di misurare con estrema accuratezza l'evoluzione dell'Universo e delle strutture a larga scala per comprendere la

## Weak gravitational Lensing

Il *Weak gravitational Lensing* (WL) è l'apparente distorsione della forma delle galassie dovuta alla non omogeneità del campo gravitazionale attraversato dai fotoni nel loro viaggio dalla sorgente a noi. L'effetto è simile a quello che si ha guardando attraverso il fondo di un bicchiere. L'immagine sullo sfondo risulta distorta e dal modo come è distorta possiamo capire la forma del bicchiere. Allo stesso modo guardando la distorsione della forma delle galassie possiamo ricostruire la distribuzione della materia oscura e del potenziale gravitazionale attraversato dai fotoni. Non conoscendo però la forma a priori delle galassie che osserviamo, ma solo la distribuzione statistica della loro forma, il segnale di WL è un segnale statistico che si manifesta come una sistematica distorsione in un campione composto da migliaia di galassie.



**Figura 2:** La figura mostra la porzione di cielo che sarà coperta dalla missione spaziale Euclid. Il contorno blu indica la regione coperta dalla "Wide-survey" mentre le due piccole regioni gialle sono due regioni che verranno osservate ripetutamente e più profondamente per stimare la purezza e completezza del catalogo prodotto da Euclid.

natura dell'energia oscura e capire se questa sia dovuta a una nuova forza o a un comportamento differente della gravità su scala cosmica.

L'energia oscura influenza l'evoluzione dell'Universo in due modi: modificando il tasso di espansione dell'Universo e quindi modificando la relazione tra distanza e *redshift*, ma anche modificando la formazione delle strutture su larga scala come gli ammassi di galassie. Infatti l'energia oscura agisce sulla materia come una sorta di anti-gravità, o come preferiscono dire i fisici con una pressione negativa, opponendosi al collasso gravitazionale e quindi riducendo, per esempio, il numero e la dimensione degli ammassi di galassie. Quindi per studiare l'energia oscura dobbiamo ricostruire la storia dell'universo negli ultimi 10 miliardi di anni e capire come, nelle varie fasi della sua evoluzione, materia ed energia oscura abbiano agito per creare gli am-

massi di galassie che oggi vediamo partendo da una distribuzione uniforme di materia, quella dei primi anni di vita dell'universo.

Per raggiungere questo obiettivo la natura ci mette a disposizione alcuni strumenti che sono utilizzati da Euclid per studiare la storia dell'espansione dell'Universo. Il primo va sotto il nome di *Weak gravitational Lensing* (WL) e consiste nel misurare la distorsione osservata della forma delle galassie causata dalla inhomogeneità del campo gravitazionale lungo il cammino dei fotoni dalla galassia al punto di osservazione. Questa distorsione è sensibile sia a come l'Universo si è espanso,  $H(t)$ , che alla quantità di materia oscura attraversata. Non conoscendo però la forma a priori delle singole galassie e misurandone invece solo la loro distribuzione statistica, il segnale di WL è un segnale statistico che si manifesta come una sistematica distorsione in un campione composto da migliaia di galassie. Il secondo strumento è il *Galaxy Clustering* che consiste nello studio di grandi agglomerati di galassie tenute insieme dal campo gravitazionale prodotto dalla materia oscura contenuta al loro interno. Questi ammassi nascono come evoluzione di piccole fluttuazioni di materia nell'Universo primordiale, che sono cresciute attraverso la forza di gravità prodotta dalla sovra densità, fino a contenere centinaia se non migliaia di galassie. La loro distribuzione nel cielo non è uniforme, ma segue un pattern lasciato dalle oscillazioni acustiche di materia (BAO) presenti nel plasma primordiale (vedi box dedicato).

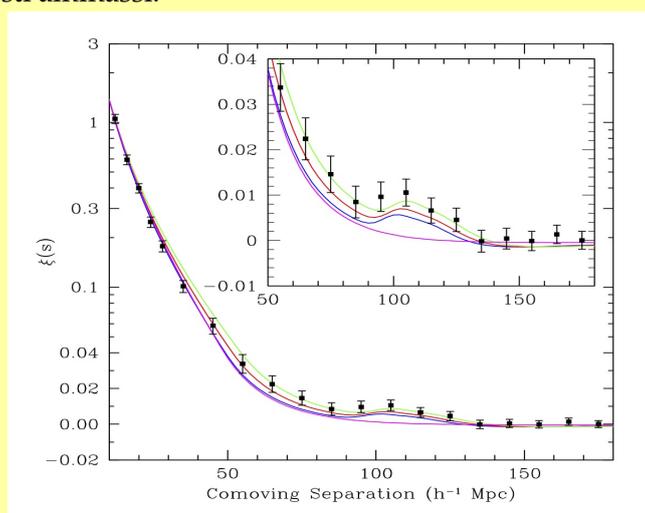
Misurando queste increspature nella distribuzione degli ammassi di galassie al variare del *redshift*, possiamo ricostruire la storia dell'evolu-

## Galaxy Clustering

Il Galaxy Clustering (GC) consiste nello studio di grandi agglomerati di galassie tenute insieme dal campo gravitazionale prodotto dalla materia oscura contenuta al loro interno. Sono tra le più grandi strutture che conosciamo e sono l'evoluzione delle piccole fluttuazioni di materia ed energia presenti nell'Universo primordiale. La loro distribuzione nel cielo non è uniforme, ma segue un *pattern* lasciato dalle oscillazioni acustiche di materia (BAO) presenti nel plasma primordiale.

Nei primi anni di vita l'Universo era un plasma molto caldo in cui la materia era in equilibrio termico con la radiazione. Il plasma era percorso da onde di materia a causa dell'azione opposta della forza di gravità che faceva collassare la materia nelle regioni di sovra densità riscaldando il plasma, e la pressione prodotta dall'interazione dei fotoni con gli elettroni liberi del plasma che invece si opponeva al collasso. Ma quando a causa del raffreddamento del plasma i protoni hanno iniziato a ricombinarsi con gli elettroni per produrre gli atomi di idrogeno, non c'erano più elettroni liberi con cui la radiazione poteva interagire e quindi la pressione di radiazione ha cessato di alimentare le oscillazioni di materia, congelando per sempre queste onde di materia separate da una distanza caratteristica. Questa distanza caratteristica si è evoluta a causa dell'espansione dell'Universo diventando un metro standard da utilizzare per capire di quanto si è espanso l'Universo. Misurando queste increspature nella distribuzione degli ammassi di galassie al variare del *redshift*, possiamo ricostruire la storia dell'evoluzione dell'Universo.

Il GC ci permette inoltre di studiare il tasso di crescita degli ammassi al variare del *redshift*, ovvero dell'epoca evolutiva dell'Universo, e capire il contributo dell'energia oscura nel rallentare la formazione di questi ammassi.



**Figura 3:** Le funzione di correlazione a due punti delle posizioni dei cluster di galassie nel catalogo SDSS. Il picco a  $100 h^{-1} \text{ Mpc}$  è dovuto alle BAO.

zione dell'Universo. Il *Galaxy clustering* ci permette inoltre di studiare il tasso di crescita degli ammassi al variare del *redshift*, ovvero dell'epoca evolutiva dell'Universo, e capire il contributo dell'energia oscura nel rallentare la formazione di questi ammassi.

Per sfruttare a pieno le potenzialità del WL and del GC è fondamentale disporre di un catalogo di galassie il più ampio possibile in termini di

copertura del cielo e profondità di esposizione. Per questo motivo la missione spaziale Euclid fotograferà  $\sim 15000$  gradi-quadrati di cielo extragalattico sul totale dei  $\sim 45000$  di tutto l'Universo (si veda Fig. 2) per costruire il più grande catalogo di galassie fino ad ora realizzato.

Il catalogo conterrà la posizione angolare di miliardi di galassie osservate sia nella banda del visibile che in quella del vicino infrarosso. Per

circa 1.5 miliardi di queste galassie sarà possibile ricostruirne con grande accuratezza la forma e misurarne il *redshift* fino a  $z = 2$  che corrisponde a circa 10 miliardi di anni fa. La misura del *redshift* verrà fatta sia in maniera spettroscopica guardando lo spostamento della riga di emissione  $H_\alpha$  dell'idrogeno, sia in maniera fotometrica confrontando la luce emessa dalla galassia con tre filtri a banda larga nel vicino infrarosso.



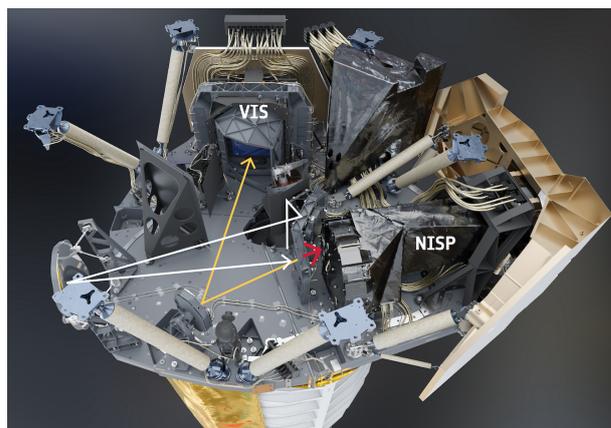
**Figura 4:** Il satellite Euclid poco prima di essere integrato nel razzo Falcon9 di SpaceX.

## Il satellite Euclid

Per poter raggiungere gli obiettivi scientifici di Euclid, la scelta di un telescopio spaziale è stata quasi obbligatoria. Infatti, la necessità di osservare una grande parte di cielo nell'infrarosso per ricostruire il *redshift* delle galassie, e la necessità di ricostruire in maniera accurata la loro forma per misurarne il WL, non hanno lasciato dubbi; bisognava andare nello spazio. Nello spazio la qualità dell'immagine è limitata solo dalla qualità delle ottiche e del rivelatore che la catturano. Per questo motivo il *design* del telescopio è stato particolarmente curato per raggiungere tre importanti requisiti: un grande campo visivo in modo da poter osservare grandi porzioni di cielo in un'unica esposizione, nessun tipo di aberrazione ottica per non falsare il profilo di luce delle galassie e una bassissima luce diffusa all'interno del telescopio in modo da ottenere immagini molto nitide. Il design adottato dall'ESA è stato quello di un telescopio a tre specchi, secondo la configurazione brevettata da D. G. Korsch [6], con lo specchio primario di 1.2 m di diametro. Il campo visivo è di 0.57 gradi quadrati, 180 vol-

te quello dell'Hubble Space Telescope, ma con una qualità dell'immagine paragonabile se non migliore.

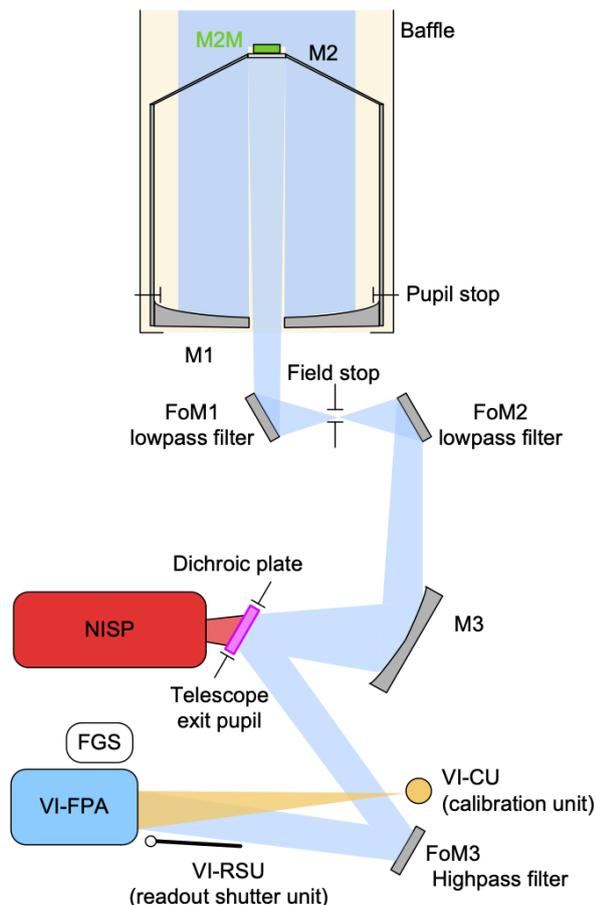
La struttura meccanica del telescopio è realizzata interamente in carburo di silicio (SiC). Il SiC è un materiale ceramico molto innovativo che si presta ad applicazioni spaziali. Ha una densità e una conducibilità termica paragonabile a quella dell'alluminio ma è 6 volte più rigido. Inoltre alla temperatura operativa del telescopio Euclid, circa 150 K, il suo coefficiente di dilatazione termica è di soli  $0.2 \cdot 10^{-6} K^{-1}$  a tutto vantaggio della stabilità termica delle ottiche. Le superfici del carburo di silicio possono essere lucidate fino ad ottenere specchi con ottime prestazioni ottiche, in questo modo la struttura meccanica del telescopio e le ottiche hanno le medesime proprietà meccaniche riducendo gli stress meccanici a tutto vantaggio della qualità delle immagini. Al di sotto dello specchio primario si trovano i due strumenti: una camera sensibile alla luce visibile (VIS [7]) e uno spettro-fotometro nel vicino infrarosso (NISP [8]) (si veda la Figura 5).



**Figura 5:** La figura mostra il piano ottico dove sono montati gli strumenti VIS e NISP e il percorso fatto dalla luce proveniente dal telescopio. Questa entra nella cavità attraverso un foro al centro dello specchio primario e viene deflessa per mezzo di una rete di specchi fino ad un filtro dicroico che separa la componente visibile, riflessa verso VIS, dalla componente infrarossa trasmessa a NISP. (Credit: Airbus Defense and Space/ESA)

La luce del telescopio arriva ai due strumenti per mezzo di un filtro dicroico che separa la componente visibile da quella infrarossa. In questo modo entrambi gli strumenti vedono il mede-

simo campo di vista ed è possibile acquisire le immagini in parallelo (Fig 6). Il campo di vista comune dei due strumenti ha un'ampiezza angolare di 0.53 gradi–quadrati. Lo specchio secondario

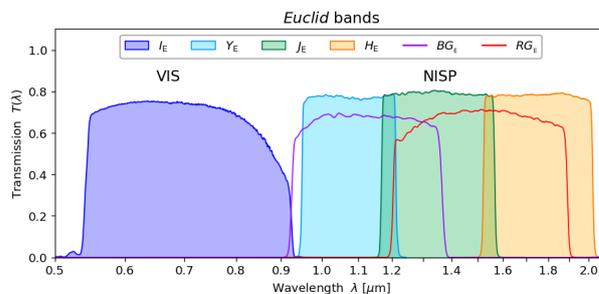


**Figura 6:** Rappresentazione schematica del telescopio di Euclid.

dario M2 è montato su un meccanismo comandabile da terra (M2M) che permette di muovere lo specchio su tre gradi di libertà ed eseguire la messa a fuoco del telescopio una volta raggiunta la stabilità termica del sistema dopo il lancio. Lo strumento VIS (VISible Instrument) è una camera sensibile alla luce visibile tra 550 nm e 900 nm, disegnata per ricostruire con estrema accuratezza e precisione la forma delle galassie e quindi la distorsione indotta dalle lenti gravitazionali presenti lungo il cammino di luce. La camera è composta da 36 rivelatori CCD, ognuno dei quali composto da 4096x4096 pixel. La dimensione di ogni pixel è di  $12 \mu\text{m}^2$  che si traduce in una risoluzione angolare nel cielo di 0.1 arco–secondi, sufficiente per risolvere bene galassie dell'ordine di 0.3 arco–secondi. Con i suoi 604 milioni di pixel VIS è il secondo più grande piano focale

su un satellite spaziale, dopo quello del satellite Gaia dell'ESA. Ma a differenza di Gaia il segnale di tutti i pixel di VIS è trasmesso a terra. I rivelatori sono operati ad una temperatura di circa 150 K per massimizzare l'efficienza di trasferimento della carica raccolta dai CCD, ma l'elettronica di lettura dei CCD e le unità di alimentazione, che sono posti dietro il piano focale, devono lavorare ad una temperatura molto più alta, 280 K. Questa differenza di temperatura è ottenuta in maniera passiva accoppiando termicamente la struttura di supporto dei CCD a quella del telescopio, mentre l'elettronica calda dissipa il calore prodotto nello spazio per mezzo di un radiatore dedicato. Lo strumento VIS è inoltre dotato di un otturatore meccanico per oscurare il piano focale e da una unità di calibrazione che permette di illuminare in maniera uniforme i CCD per determinare la loro risposta alle varie lunghezze d'onda.

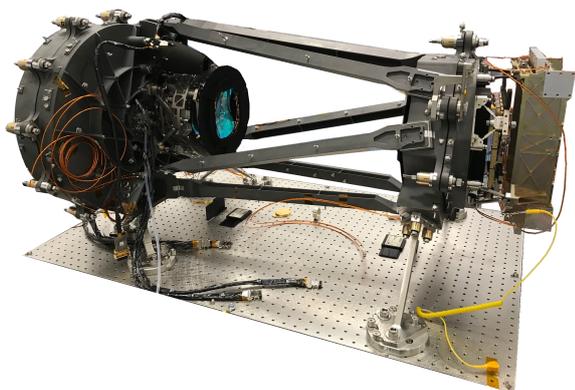
NISP è uno strumento abbastanza complesso perché può operare in due modalità differenti: come fotometro per l'acquisizione delle immagini con tre filtri a banda larga ( $Y_E$ ,  $J_E$  e  $H_E$ ), o come spettrometro per misurare lo spettro della luce dispersa da 4 differenti GRISM. I filtri e i GRISM sono montati su due ruote porta filtri in modo da posizionare alternativamente un filtro o un grism lungo il cammino ottico. Per poter



**Figura 7:** Sensibilità spettrale totale dello strumento VIS e NISP. Le quattro aree colorate si riferiscono a VIS e i tre filtri  $Y_E$ ,  $J_E$ ,  $H_E$ , mentre le due curve si riferiscono al grism "Blu" e "Rosso".

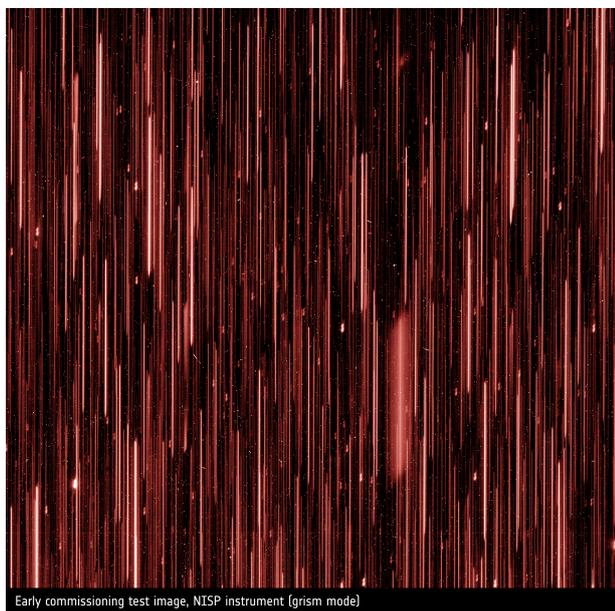
misurare più spettri nel medesimo campo di vista, le immagini spettroscopiche sono acquisite senza alcuna fenditura.

Ne consegue che tutte le sorgenti nel campo visivo sono disperse consentendo di poterle acquisire contemporaneamente. In regioni di cielo con un'alta densità di galassie può succedere che



**Figura 8:** Lo strumento NISP durante la sua fase di test. Sulla sinistra è visibile l'involucro che contiene le due ruote porta filtri e grism, e il sistema di lenti per focalizzare l'immagine su piano focale, posto sulla destra dell'immagine.

gli spettri di queste si sovrappongono generando confusione nella ricostruzione delle linee spettrali. Per questo NISP acquisisce il medesimo campo di vista con 4 differenti direzioni di dispersione che una volta combinanti riducono notevolmente la probabilità di confondere le linee spettrali.



**Figura 9:** Una delle prime immagini acquisite dallo strumento NISP in modalità spettroscopica dove ogni "riga" di luce è lo spettro di emissione di una stella o di galassia. L'ordine zero dello spettro coincide con la posizione della galassia nelle immagini fotometriche. ESA/Euclid/Euclid Consortium/NASA, CC BY-SA 3.0 IGO



**Figura 10:** Una delle prime immagini acquisite dallo strumento NISP in modalità fotometrica nell'infrarosso in banda Y. Nell'immagine è visibile anche la traccia lasciata da un raggio cosmico. ESA/Euclid/Euclid Consortium/NASA, CC BY-SA 3.0 IGO

Il piano focale di NISP è composto da una matrice 4x4 di rivelatori a pixel CMOS HR2G sensibili alla luce infrarossa fino ad una lunghezza d'onda di 2000 nm. Ogni rivelatore è composto da 2048x2048 pixel con un passo di 18  $\mu\text{m}$  per una dimensione totale del piano focale di circa 15 cm di lato. I rivelatori sono operati ad una temperatura di  $\sim 96\text{ K}$  per ridurre il rumore di lettura. Il raffreddamento dei rivelatori è ottenuto con un radiatore passivo che scambia calore con lo spazio. Siccome il piano focale di NISP è più piccolo di quello di VIS, un sistema di lenti poste all'ingresso dello strumento NISP ne adatta la focale.

L'elevato numero di pixel e quindi l'elevata mole di dati prodotti giornalmente dai due strumenti hanno posto una sfida importante nella gestione e trasmissione dei dati a terra. Le immagini acquisite da VIS e NISP sono processate e parzialmente ridotte direttamente a bordo da due unità di processamento dei dati realizzate da OHB-Italia. La trasmissione a terra è fatta quotidianamente attraverso un link in banda-K in grado di trasmettere i 100 Gbyte di dati prodotti giornalmente in circa 4 ore di tempo.



**Figura 11:** Le prime cinque immagini a colori di Euclid: la galassia a spirale Ic 342 (in alto a sinistra), la Nebulosa Testa di Cavallo (in alto al centro), l'ammasso globulare Ngc 6397 (in alto a sinistra), la galassia irregolare Ngc 6822 (in basso a sinistra) e l'ammasso di galassie del Perseo (in basso a destra). Crediti: Esa/Euclid/Euclid Consortium/Nasa, image processing by J.-C. Cuillandre (Cea Paris-Saclay), G. Anselmi; CC BY-SA 3.0 IGO

Un'altra sfida che ha messo a dura prova gli ingegneri è stato lo sviluppo di un sistema di puntamento del satellite in grado di garantire l'elevata qualità delle immagini richieste per la misura di WL. Euclid è dotato di un sofisticato sistema di controllo d'assetto in grado di mantenere una precisione di puntamento migliore di 75 milli-arco-secondo su un arco di tempo di 700 sec. Questa accuratezza è stata ottenuta realizzando il sistema di guida fine (FGS) direttamente sul piano focale del telescopio. In questo modo il sistema può tracciare le stelle con la medesima risoluzione delle immagini di VIS.

## Il lancio e le prime fasi operative

Il satellite Euclid è stato lanciato l'1/7/2023 dalla base di Cape Canaveral, a bordo di un Falcon9 di SpaceX. E poche ore dopo la separazione la navicella è stata messa sulla traiettoria verso la sua destinazione: il punto lagrangiano secondo (L2) del sistema terra-sole a 1.5 milioni di chilometri dalla Terra. Lì orbiterà per 6 anni per mappare i 15000 gradi quadrati di cielo previsti dalla missio-

ne. Durante il suo viaggio verso L2, durato circa 30 giorni, sono stati attivati tutti i componenti del satellite e monitorato il raffreddamento del telescopio. Una volta raggiunta la temperatura operativa si sono accesi gli strumenti VIS e NISP in modo da poter acquisire le immagini e mettere a fuoco il telescopio. A fine luglio, dopo quasi 10 anni di lavoro per la costruzione del satellite e dei suoi strumenti, Euclid mandava a terra le prime immagini. E lo stupore di tutti è stato grande. Le immagini mostravano una nitidezza e una risoluzione veramente impressionanti. La moltitudine di galassie che si vedeva in ogni singola immagine lasciava a bocca aperta. Per mostrare alla comunità scientifica e non le prestazioni del telescopio Euclid, sono state prese alcune immagini iconiche riportate in Fig. 11. Ogni immagine è ottenuta da un unico puntamento combinando le immagini nel visibile con quelle nelle tre bande dell'infrarosso per ottenere gli effetti di colore. La cosa che impressiona di più in queste immagini è la possibilità di acquisire grandi porzioni di cielo, mantenendo la risoluzione e la sensibilità per risolvere oggetti o dettagli molto piccoli. L'immagine dell'ammasso

## Cosa è un GRISM

Un GRISM è la combinazione di un reticolo di diffrazione con un prisma disposti in modo tale che la luce di una certa lunghezza d'onda vi passi attraverso senza essere deflessa. Il reticolo di diffrazione disperde la luce nelle sue componenti mentre il prisma è costruito in maniera tale da deflettere la luce per riportare i raggi paralleli a quelli incidenti. In questo modo si può usare un unico rivelatore per fare sia *imaging* che spettroscopia senza dover spostare il rivelatore quando si

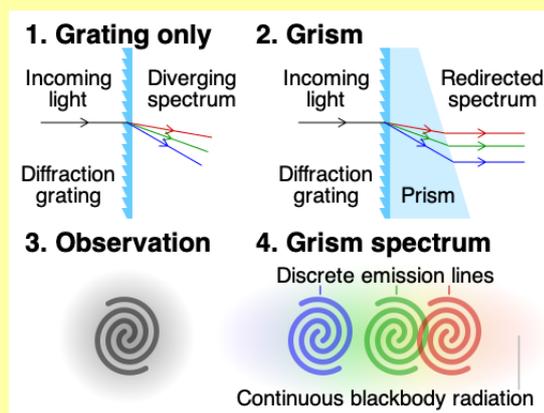


Figura 12: By Cmglee - Own work, CC BY-SA 4.0, <https://l.infn.it/109>

di galassie del Perseo è particolarmente interessante perché mostra un cluster di galassie a 240 milioni di anni luce da noi, tenute insieme dalla materia oscura presente al suo interno, visibile solo attraverso l'attrazione gravitazionale che esercita sulle galassie dell'ammasso.

Finita la fase di commissioning, ad Agosto è cominciata una fase di calibrazione degli strumenti che sarebbe dovuta terminare a fine settembre. Ma a causa di un problema nel sistema di puntamento fine del satellite, che ha richiesto un aggiornamento del software di bordo, questa fase terminerà a fine novembre. Dopodiché inizierà la vera campagna di mappatura del cielo. I primi risultati della missione Euclid arriveranno nel 2025 con l'analisi dei dati acquisiti nel primo anno di osservazione, ma saranno molto preliminari e ci diranno ancora poco sull'energia e la materia oscura. Per questo dovremo aspettare l'analisi completa dei dati, fra circa 7 anni. Nel frattempo Euclid osserverà con questo dettaglio porzioni di cielo mai osservate prima fornendo una mole incredibile di dati per la comunità astronomica. Possiamo veramente dire che con Euclid si apre una nuova finestra sull'Universo che ci porterà scoperte inimmaginabili.



[1] F. Zwicky: *Astrophysics and Dark Matter Theory*, Helvetica Physica Acta, 6 (1933) 110.

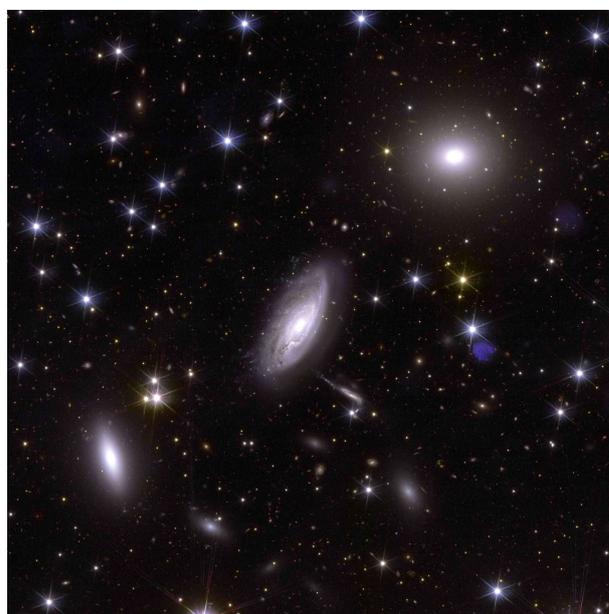


Figura 13: L'ingrandimento di alcune galassie dell'ammasso del Perseo dove si può apprezzare la risoluzione con la quale sono state ricostruite le immagini. Crediti: Esa/Euclid/Euclid Consortium/Nasa, image processing by J.-C. Cuillandre (Cea Paris-Saclay), G. Anselmi; CC BY-SA 3.0 IGO

[2] Vera Rubin Observatory. Il nuovo sito della collaborazione si trova in <https://rubinobservatory.org>

[3] Una buona sintesi si trova in R. Massey, T. Kitching, J. Richard: *The dark matter of gravitational lensing* Rep. Prog. Phys. 73 (2010) 086901. <https://doi.org/10.1088/0034-4885/73/8/086901>

[4] F. Perlmutter et al.: *Discovery of a supernova explosion*

at half the age of the Universe. *Nature*, 391 (1998) 51, (erratum 392, 311) (1998)

A. Riess et al.: *Observational Evidence from Supernovae for an Accelerating Universe and a Cosmological Constant* *Astrophysical Journal*, 116 (1998) 1009.

R. Schmidt et al.: *The High-Z Supernova Search: Measuring Cosmic Deceleration and Global Curvature of the Universe Using Type IA Supernovae* *Astrophysical Journal*, 507 (1998) 46.

- [5] R. Laureijs et al. *Euclid Definition Study Report* arXiv 1110.3193 (2011) <https://doi.org/10.48550/arXiv.1110.3193>
- [6] R. A. Frosch, D. G. Korsch: NASA, *Anastigmatic three-mirror telescope*, 4101195A, United States Patent Office, USA [1977-07-29] (18 luglio 1978).
- [7] M. Cropper et al. *VIS: the visible imager for Euclid* Proceedings SPIE, Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series vol. 10698, p. 10698282018 <https://oro.open.ac.uk/56606/1/56606.pdf>
- [8] T. Maciaszek et al.: *Euclid Near Infrared Spectrometer and Photometer instrument flight model presentation, performance and ground calibration results summary* arXiv 2210.10112 (2022) <https://doi.org/10.48550/arXiv.2210.10112>



**Stefano Dusini:** è Primo Ricercatore dell'Istituto Nazionale di Fisica Nucleare, Sez. di Padova. È responsabile nazionale dell'INFN della missione spaziale Euclid e è stato responsabile delle attività di integrazione e test dell'elettronica calda dello strumento NISP della missione Euclid.

**Luca Stanco:** è Dirigente di Ricerca dell'Istituto Nazionale di Fisica Nucleare, Sez. di Padova. È stato promotore del coinvolgimento INFN in Euclid, coordinando e perfezionando negli anni le attività delle sedi INFN coinvolte. È stato responsabile nazionale dell'INFN della missione spaziale Euclid fino alla data del lancio.



---

# La Computazione Quantistica

*Nature isn't classical dammit, and if you want to make a simulation of Nature you better make it quantum mechanical, and by golly it's a wonderful problem because it doesn't look so easy*

R. Feynman

---

**Luigi Martina**

Dipartimento di Matematica & Fisica "Ennio De Giorgi" - Università del Salento  
Istituto Nazionale di Fisica Nucleare, Sez. di Lecce, Lecce, Italy

---

**I**nformazione Quantistica: sembra la formula stregonesca di un qualche personaggio poco affidabile. In realtà è un corpus di attività scientifiche che sta ricevendo sempre più attenzione, soprattutto da parte dei governi che aspirano ad ottenere la supremazia quantistica, come chiave di quella politica. Qui cercheremo di indicare le sue basi scientifiche e le sue possibili prospettive.

## Fisica e Informazione

Lo studio dei fenomeni naturali si inquadra in un modello teorico chiamato Meccanica Quantistica (MQ) che, per quanto poco intuitiva per gli esseri umani, risponde molto efficacemente alle domande relative al comportamento dei sistemi fisici. Lo fa molto meglio (in senso tecnico) della più intuitiva Meccanica Classica e, nelle sue varie estensioni, include anche il comportamento della radiazione (la luce) e delle forze fondamentali della natura ad esclusione, finora, della teoria della gravitazione. Quindi possiamo affermare con una certa confidenza che l'Universo sia in gran parte descritto dagli strumenti fornitici

dalla MQ. Tra i concetti che dominano la nostra concezione del mondo moderno c'è sicuramente quello di Informazione. Abbiamo bisogno spasmodico di informazioni, al fine di prendere decisioni, preferire un tipo di studi ad un altro, decidere dove e come allocare del denaro ed altre risorse finanziarie e materiali, sapere se si vuole trascorrere del tempo libero o fare la guerra e via dicendo. Ma come ci giungono le informazioni? Esse devono essere catturate e trasformate opportunamente per permettere la loro trasmissione e diffusione. Per quanto l'informazione costituisca la base della valorizzazione dei beni immateriali, essa è codificata negli stati di certi sistemi fisici. La sua elaborazione, spesso intesa come calcolo, si esplica attraverso azioni di controllo ben precisi su degli opportuni sistemi materiali. Quindi essa corrisponde allo stato fisico di certi supporti materiali. Nemmeno essa quindi può sfuggire alla Fisica. In particolare, il celebre esempio del diavoleto di Maxwell ci ricorda che l'Informazione è associata al concetto di entropia e ad una qualche formulazione della seconda Legge della Termodinamica. In effetti, sappiamo che una quantificazione della qualità dell'Informazione trasmessa è descritta dall'Entropia di

Shannon, che ha indubbie relazioni matematiche con il concetto termodinamico introdotto da Boltzmann. Ancor più, il Principio di Landauer ci ricorda che in corrispondenza di un processo di cancellazione di informazione, si verifica una precisa crescita dell'entropia termodinamica ed una corrispondente dissipazione di calore nell'ambiente. In definitiva, per quanto affermato inizialmente sulla natura quantistica dell'Universo, dobbiamo porci nell'ottica di affrontare il calcolo e l'elaborazione delle informazioni utilizzando sistemi quanto-meccanici e tecniche coerenti con la MQ.

## Retrospectiva

La MQ ha già prodotto nel mondo moderno una prima rivoluzione molto più incisiva di quelle sociali, costituendo la base teorica per lo sviluppo della globale civiltà delle comunicazioni.

Essa ha consentito invenzioni come il laser e il transistor, gli elementi costitutivi di base dei computer, e gli scienziati che costruiscono tali dispositivi seguono le regole della MQ. Ma molto più in generale la MQ ha fornito una chiave di lettura di gran parte dei fenomeni naturali: dalla struttura stellare alle origini della vita. Lo studio del comportamento dei semiconduttori, in particolare, ha prodotto i metodi e le tecniche per produrre quei dispositivi elettronici a risposta rapida, che consentono di memorizzare ed elaborare imponenti quantità di informazione, come mai in precedenza nella storia umana. Tuttavia, la codifica dell'informazione avviene distinguendo valori alto/basso di corrente, o di potenziale elettrico. Cioè la codifica avviene sulla base di un alfabeto binario classico: 0 - 1, sì - no, vero - falso, acceso - spento. Espressioni queste del concetto di **bit** come unità base dell'informazione. Questo codice di rappresentazione finito non può essere utilizzato per una ragione intrinseca in MQ: i possibili stati di un sistema fisico si possono sovrapporre linearmente con coefficienti complessi arbitrari. Non esiste più qualcosa del tipo la traiettoria di un corpo, ma si può parlare solo di posizioni più o meno probabili per esso. Tali probabilità si compongono secondo delle regole specifiche, differenti da quelle abituali, diciamo, quelle del gioco dei dadi. Questo aspetto è all'origine di lunghe discussioni, equivoci e in-

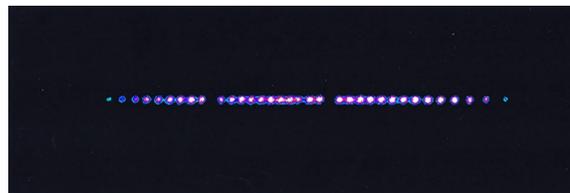
comprensioni, anche tra i fondatori della teoria stessa, tuttora in corso. Inoltre, i vari tentativi teorici di ricondurre questo problema a quello di un modello statistico classico (teoria delle variabili nascoste), ammettendo in definitiva che l'attuale formulazione della MQ sia incompleta, non ha portato i frutti desiderati. Anzi, escogitati opportuni test per dirimere la questione (disuguaglianza di Bell e simili), i dati sperimentali sostengono i postulati della MQ. Questi, a loro volta, implicano delle correlazioni non locali (spesso dette "entanglement") tra parti differenti di un sistema fisico, che non hanno alcun analogo classico. L'esistenza di queste correlazioni svolge allora un ruolo importante, quando il sistema fisico considerato funge anche da supporto alla memorizzazione e al trattamento dell'informazione. Per avere un'idea sommaria del concetto di *entanglement*, utilizziamo l'analogia con un libro. Se si tratta di un normale libro classico, per ogni pagina letta si impara una frazione del contenuto totale ed è necessario leggerle tutte singolarmente, per conoscerlo completamente. Supponiamo invece che esista un libro quantistico, le cui le pagine siano fortemente collegate tra loro: nelle singole pagine si trovano solo parole che formano frasi senza senso e, leggendole tutte una ad una, si saprà molto poco del contenuto totale. Bisogna quindi fare un'osservazione collettiva su più pagine contemporaneamente. Una caratteristica di questo tipo rende le informazioni contenute nei sistemi quantistici molto diverse da quelle elaborate dai normali computer digitali. Nel seguito di questo scritto si darà una definizione più tecnica e precisa del concetto.

D'altro canto, la poderosa progressione delle tecnologie informatiche in tutti i campi della nostra vita dipende in larga misura dalla capacità di miniaturizzare i circuiti elettronici. Attualmente la lunghezza della più piccola struttura circuitale riconoscibile raggiunge i 4 nanometri (circa 15 strati di atomi di silicio impilati). Ma a scale prossime a quelle atomiche, gli effetti quantistici cominciano a interferire nel funzionamento dei dispositivi elettronici. Quindi gli approcci progettuali attuali tendono a confliggere con i propri presupposti, quali la certezza della sequenzialità dei processi di calcolo. Ancora una volta siamo di fronte alla necessità di trovare una strada alternativa per elaborare l'informazione.

Naturalmente accanto ai problemi tecnologici si sovrappongono, come si dice, aspetti geopolitici: i detentori di tecnologie così spinte si riducono ad un numero di colossi industriali, nessuno in Europa, che si contano sulle dita di una mano. Non entreremo in queste questioni, ma il lettore dovrebbe tenerle presenti.

## Prospettiva

Per affrontare le problematiche esposte sopra si sta proponendo un passaggio all'ambito dell'**Informazione Quantistica**; la scienza che si basa sull'idea di utilizzare dispositivi puramente quantistici per immagazzinare, manipolare e trasmettere informazioni [1],[2], [3]. Essa sintetizza i due campi della MQ e della teoria dell'Informazione, fornendo un punto di vista unificante, sia sul piano applicativo che teorico. L'Informazione quantistica studia la preparazione e il controllo degli stati quantistici dei sistemi fisici ai fini della trasmissione e della manipolazione dell'informazione. Comprende la computazione, la comunicazione e la crittografia quantistiche. Questo campo si basa su una ampia gamma di nuovi dispositivi, tenuto conto sia della varietà di osservabili fisici che possono essere usati per la computazione, sia dello sviluppo di tecniche raffinate di preservazione della fase relativa degli stati in sovrapposizione: la cosiddetta **coerenza** degli stati. Quindi non si misureranno solo correnti elettriche, ma stati di carica, di spin, di cammino, di eccitazione interna, di numeri di occupazione e altri osservabili. Non più solo elettroni, per esempio confinati in *quantum dots* [9], ma nuclei con tecniche di Risonanza Magnetica Nucleare (NMR) [3], [10], atomi in cavità elettromagnetiche [11], [12], catene di ioni [13], [14],[15], fotoni [16], fononi [17] e anioni [18]. Infatti, l'unità di informazione quantistica, il **qubit** può essere realizzato e trasportato fisicamente in molti modi diversi: può esserlo da un singolo atomo, o da un singolo elettrone, o da un singolo fotone. Oppure un qubit può essere realizzato utilizzando un sistema più complicato, come un circuito elettrico superconduttore, a bassa temperatura, nel quale si muovono molti elettroni [19]. L'area di ricerca dei supporti materiali richiesti ed il loro controllo è indica-



**Figura 1:** Immagine in fluorescenza di diversi ioni atomici di mercurio  $^{199}\text{Hg}^+$  intrappolati. Gli ioni sono distanziati di  $\approx 15 \mu\text{m}$  e le due lacune sono isotopi differenti del mercurio, che non rispondono alla sorgente laser. (NIST)

ta genericamente come **tecnologie quantistiche**: per un quadro sinottico si veda Fig. 20 e [20, 21].

Poiché la MQ è fondamentalmente probabilistica, la casualità e l'incertezza sono profondamente radicate nel calcolo e nell'informazione quantistica. Di conseguenza, gli algoritmi quantistici sono di natura casuale, nel senso che forniscono soluzioni solo con una una associata distribuzione di probabilità. Il compito di massimizzare le distribuzioni attorno alle soluzioni desiderate costituisce il compito fondamentale di un buon algoritmo quantistico. In prospettiva quindi siamo in presenza di una seconda rivoluzione quantistica, che riguarda fondamentalmente il controllo dei singoli sistemi quantistici in misura molto più marcata rispetto a prima [22].

## In che senso un computer quantistico dovrebbe essere più potente

### La frontiera dell'*entanglement*

Per un fisico come me, ciò che è entusiasmante dell'informatica quantistica è che abbiamo buone ragioni per credere che un computer quantistico sia in grado di simulare in modo efficiente qualsiasi processo che avviene in Natura. Vorremmo sondare più a fondo le proprietà di molecole complesse e dei materiali esotici, esplorare la fisica fondamentale simulando le proprietà delle particelle elementari o il comportamento quantistico di un buco nero, o l'evoluzione dell'universo subito dopo il Big Bang.

Non pensiamo che ciò non sia possibile grazie ai computer digitali classici, ma che essi (per quanto ne sappiamo) non possono simulare siste-

mi quantistici altamente correlati. Tali situazioni costituiscono la frontiera dell'entanglement. La nostra fiducia che l'esplorazione della frontiera dell'entanglement sarà gratificante si basa in gran parte su due principi:

1. la teoria della complessità quantistica: una tecnica per esprimere l'efficacia dell'informatica quantistica;
2. la teoria della correzione dell'errore quantistico: una tecnica per consentire ai computer quantistici di rimanere affidabili, proteggendoli dalla perdita di coerenza dei qubit, ed efficienti, anche se il numero degli stessi qubit e delle operazioni di controllo dovessero aumentare di diversi ordini di grandezza.

## Complessità computazionale

Quando parliamo di complessità quantistica, ciò che ci viene in mente è la sconcertante mole di dati classici ordinari necessari per descrivere stati quantistici altamente correlati. Infatti, le correlazioni in un dato insieme di qubit sono espresse da una quantità di numeri complessi esponenzialmente crescente con la numerosità dell'insieme stesso. Tuttavia, per quanto questo suggerisca una inimmaginabile potenza di immagazzinamento ed elaborazione dell'informazione, non c'è garanzia di per sé che i computer quantistici siano più efficienti di quelli classici. In effetti, ci sono almeno tre buone ragioni per pensare che questo sia il caso.

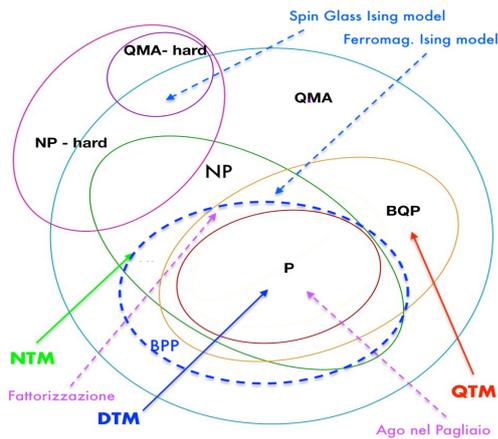
- Conosciamo problemi che riteniamo siano difficili da affrontare per i computer classici, ma per i quali sono stati scoperti algoritmi quantistici che potrebbero risolverli molto più facilmente.

L'esempio più noto consiste nel trovare i fattori primi di un grande intero composito  $N$  [4]. Discuteremo successivamente con maggiore dettaglio questo problema ma, in genere, si ritiene che la fattorizzazione sia classicamente difficile, perché non è stato trovato alcun algoritmo in grado di farlo per tutti i numeri interi in un tempo, o con una quantità di risorse computazionali, che crescano secondo una legge del tipo  $O(b^k)$ , essendo  $b = \log_2 N$  i bit rappresentativi e  $k$  una certa

## Complessità a confronto

La complessità computazionale è riferita a modelli digitali di calcolo comparabili con una macchina di Turing (TM): TM deterministica (DTM), TM quantistica (QTM) cioè che processa un algoritmo quantistico su una memoria quantistica, TM classica non deterministica (o probabilistica) (NTM), essa è anche detta Oracolo, non essendo sequenziale. Le classi di complessità sono definite dal tempo di esecuzione che una TM impiega per un certo calcolo in funzione delle dimensioni dell'input.  $P$  denota quei problemi che sono risolvibili in modo efficiente con un computer classico in un tempo crescente come la potenza intera del numero di bit in ingresso.  $P$  è un sottoinsieme di  $NP$ , che è la classe dei problemi le cui soluzioni sono verificabili in modo efficiente da un computer classico. Essi potrebbero essere risolti efficientemente da una NTM. I problemi  $NP$ -hard sono i problemi difficili almeno quanto il più generico problema  $NP$ . Quindi nemmeno una NTM potrebbe risolverli efficientemente. I  $BQP$  sono problemi che potrebbero essere risolti in un tempo polinomiale da una QTM. Poiché l'esito di un calcolo in questo ambito ha un carattere probabilistico, tali algoritmi vanno confrontati con i problemi  $BPP$ , cioè quelli risolvibili con algoritmi probabilistici a tempo polinomiale con errore limitato, contenente problemi decisionali risolti da famiglie di circuiti uniformi randomizzati di dimensione polinomiale. QTM non sembra contenere interamente  $NP$  e  $NP$ -hard ed inoltre non si è dimostrata neanche la disuguaglianza  $BPP \neq BQP$ .  $QMA$  denota i problemi verificabili efficientemente da un computer quantistico. I problemi  $QMA$ -hard sono i problemi difficili almeno quanto un qualsiasi problema in  $QMA$ .

costante positiva, che caratterizza i problemi di classe  $P$ . Non è stata dimostrata la non esistenza di tali algoritmi, quindi si sospetta che il problema non sia di classe  $P$ , mentre è chiaramente di classe  $NP$ , cioè ipotizzando



**Figura 2:** Diagramma delle Complessità Computazionale. Alcuni problemi celebri sono collocati nelle loro classi di complessità.

una soluzione la sua verifica è facile. Per una introduzione alla *Teoria della Complessità Computazionale* si può fare riferimento a [5]. Una sintesi estrema è contenuta nel riquadro "Complessità a confronto". In generale, gli algoritmi quantistici possono accelerare le procedure di calcolo. Il tipico esempio è costituito dal cosiddetto algoritmo di Grover [6] per la ricerca in un database disordinato, o problema dell'Ago nel Pagliaio. La sua implementazione sarà descritta con un certo dettaglio nel seguito, ma qui ci basti avere un'idea generale di quale sia il concetto di fondo. Ad esempio, si immagini una rubrica telefonica contenente  $N$  nomi disposti in ordine completamente casuale. Per trovare il numero di telefono di qualcuno con una probabilità del 50% un algoritmo classico (sia deterministico che probabilistico) dovrà accedere al database un minimo di  $\frac{1}{2}N$  volte. Memorizzando il database su un sistema quantistico, che si trovi in una sovrapposizione di stati, si possono esaminare simultaneamente più nomi. Regolando adeguatamente le fasi relative dei qubit durante le varie operazioni, si ottiene una amplificazione di certe specifiche ampiezze di probabilità, mentre altre interferiscono in

modo casuale quasi azzerandosi. Di conseguenza, si può dimostrare che il numero di telefono desiderato può essere ottenuto con  $O(\sqrt{N})$  accessi al database. Il che rappresenta un certo guadagno in velocità rispetto alle  $O(N)$  del metodo classico.

- Argomenti della teoria della complessità mostrano (sotto presupposti ragionevoli) che la misura di tutti i qubit in uno stato *entangled* avviene con una distribuzione di probabilità correlata, che non può essere campionata efficientemente con alcuna procedura classica [7] [8].
- Nessun algoritmo classico conosciuto può simulare un computer quantistico. Ciò rimane vero anche dopo molti decenni di sforzi da parte dei fisici indirizzati a trovare modi migliori per simulare i sistemi quantistici.

Per un fisico, l'ambito naturale in cui cercare problemi che siano classicamente difficili, ma in principio facili per un *quantum computer*, è simulare un sistema quantistico a molte particelle. Una serie di modelli di riferimento sono costituiti dai vetri di spin (Spin Glass Ising model, vedi Fig. 2), la cui classe di complessità è stata dimostrata essere NP-complete [24], [25]. Anche se B. Laughlin e D. Pines [26] sollevarono molte perplessità sulla possibilità teorica di risolvere le equazioni che descrivono molte particelle tra loro *entangled*, circa 40 anni dopo la proposta di Feynman [1] stiamo appena iniziando a raggiungere la fase in cui i computer quantistici possono fornire soluzioni utili a problemi quantistici complessi. Questo senza essere necessariamente riduzionisti ad ogni costo.

## Scogli e Criteri

Il nocciolo del problema deriva da una caratteristica fondamentale del mondo quantistico a volte noto come Principio di Indeterminazione di Heisenberg: non possiamo osservare un sistema quantistico senza produrvi un disturbo incontrollabile. Allora, per archiviare ed elaborare informazioni in modo affidabile su un supporto quantistico, dobbiamo mantenere tale sistema quasi perfettamente isolato dal mondo esterno. Allo stesso tempo, però, vogliamo che i qubit

interagiscano fortemente tra loro, in modo da poter correlare le informazioni tra di essi. Inoltre, dobbiamo essere in grado di controllare il sistema dall'esterno ed eventualmente leggere i qubit, in modo da estrarre il risultato del nostro calcolo. Ci sono troppe condizioni in conflitto nel realizzare e utilizzare un sistema quantistico. La prospettiva tecnologica entro la quale l'informazione quantistica si muove è definita dai cosiddetti criteri di Di Vincenzo [27], che costituiscono la principale linea guida per fisici e ingegneri che costruiscono computer quantistici. Essi sono:

1. Trovare qubit ben caratterizzati e scalabili. Molti dei sistemi quantistici che troviamo in natura non sono qubit, quindi dobbiamo trovare un modo per farli comportare come tali. Inoltre, dobbiamo mettere insieme molti di questi sistemi.
2. Determinare procedure di inizializzazione del qubit. Dobbiamo essere in grado di preparare ripetutamente lo stesso stato entro un margine di errore accettabile.
3. Garantire tempi di coerenza lunghi rispetto all'esecuzione del calcolo. I qubit perderanno le loro proprietà quantistiche dopo aver interagito con l'ambiente. Vorremmo che durino abbastanza a lungo da poter eseguire tutte le operazioni quantistiche richieste.
4. Realizzare l'insieme universale delle Porte Logiche Quantistiche. Dobbiamo eseguire operazioni arbitrarie sui qubit. Per fare ciò, sono necessarie sia porte a qubit singolo che porte a due qubit. Questo aspetto deve essere appropriatamente approfondito.
5. Avere la capacità e le procedure di misurazione dei singoli qubit. Per leggere il risultato di un algoritmo quantistico, dobbiamo misurare accuratamente lo stato finale di un insieme prescelto di qubit.

Oltre alla produzione di materiali e metodi di controllo appropriati, sarà cruciale il ricorso alla correzione degli errori quantistici [28], il che permetterà di aumentare anche il numero di qubit utilizzabili. L'idea base è che per proteggere un sistema quantistico da disturbi, l'informazione va codificata in uno stato altamente *entangled*.

Questo stato *entangled* ha la proprietà che l'ambiente, interagendo con le parti del sistema, non sia in grado di leggere le informazioni correlate e quindi non può danneggiarle. Sfortunatamente, la correzione degli errori quantistici comporta costi generali significativi: scrivere le informazioni quantistiche protette in un libro altamente correlato richiede molti qubit fisici aggiuntivi, quindi è improbabile che computer quantistici affidabili che utilizzino la correzione degli errori quantistici siano disponibili a breve. Anche se dispositivi basati su circuiti superconduttori sono stati recentemente resi operativi rispettivamente da Google con 53 qubit [29] e con 127 da IBM [30], rimane comunque una scala limitata di possibili risorse computazionali. Questi sono i numeri con i quali ci si dovrà confrontare e possiamo considerare l'attuale stato dell'arte, che Preskill [31] ha battezzato *NISQ era*: epoca della Scala Quantistica Intermedia Rumorosa. Nonostante tutto, sembra che alcuni importanti test di efficienza (alcuni basati sullo studio di modelli di Ising in 3d) siano stati dimostrati [32], [33]. Questo sembra valere anche per i sistemi nanofotonici, come dimostra la Xanadu [34] nel lavoro [35].

Per approfondimenti dei vari aspetti sia della teoria dell'informazione quantistica, che delle realizzazioni concrete di *quantum computers* si rimanda ai testi base, ormai dei classici, [36]-[41], oppure ai più recenti [42, 43].

## Richiami di MQ

### Quadro

La differenza più significativa tra la Fisica Classica e la MQ risiede nel fatto che quest'ultima permette di ottenere soltanto previsioni probabilistiche delle varie grandezze. Nonostante essa appaia controintuitiva, non solo fornisce una spiegazione plausibile e coerente dei fenomeni che avvengono a scala atomica, o subatomica, ma anche molte proprietà della fisica a scala macroscopica possono essere pienamente interpretate e comprese alla sua luce. Basti pensare a tutta la Fisica dei metalli e dei semiconduttori. È noto che fenomenologicamente le onde luminose, in certe condizioni, si comportano come particelle, mentre le particelle si comportano come

onde (dualità onda-particella). La MQ fornisce una descrizione matematica di tale dualità onda-particella e dell'interazione tra materia ed energia a livello di processi elementari microscopici. Essa descrive i sistemi fisici e la loro evoluzione temporale con l'ausilio di entità matematiche (funzioni d'onda, operatori di stato, etc.), che non necessariamente corrispondono a quantità fisicamente osservabili, ma che incapsulano le distribuzioni di probabilità relative agli esiti delle misure di ogni possibile grandezza osservabile sul sistema.

Dal punto di vista della MQ i singoli eventi non sono riproducibili. Tuttavia i risultati delle Misurazioni di uno stesso Osservabile, su una sequenza (idealmente infinita) di Preparazioni uguali dello stesso Sistema, hanno distribuzioni di frequenza limite ben definite. Ogni specifica Preparazione determina le distribuzioni di probabilità di tutti i possibili Osservabili del Sistema. Quindi uno Stato del dato Sistema è identificato con l'insieme di tutte le Distribuzioni di Probabilità degli esiti di ogni possibile Misurazione. Per tal motivo è impossibile dedurre lo Stato iniziale del sistema dal risultato di una Misurazione. Infine, esistono Osservabili Incompatibili. Il che equivale a dire che le distribuzioni di probabilità degli esiti di Misurazioni su Osservabili distinti sono in generale correlate. Questo postulato è privo di un analogo classico. Pertanto l'atto di acquisire informazioni su un sistema misurando l'Osservabile  $\mathcal{A}$  disturba lo Stato, talché l'esito della Misura di un altro Osservabile  $\mathcal{B}$  ne verrà influenzato in modo casuale. Infine, è un fatto che più stati si possano sommare linearmente con coefficienti complessi, che nel dar luogo alle nuove distribuzioni di probabilità intervengono in maniera quadratica. Per gli approfondimenti relativi a queste tematiche si vedano i manuali [44, 45, 46]. Alcune idee fondanti della MQ sono presentate nell'Appendice.

## Qubit

Il qubit è il più semplice sistema quantistico, realizzato da un qualsiasi sistema fisico che abbia un osservabile dicotomico, cioè con uno spettro costituito da due valori reali non degeneri. Ad essi corrispondono due autostati ortogonali. Esempio

### Matrici di Pauli.

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} ; \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} ; \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

pi fisici di qubit sono gli stati di polarizzazione dei fotoni, un atomo con due livelli energetici, lo spin dell'elettrone o quello del protone e simili sistemi che posseggono due stati ben distinti.

In ossequio al bit classico, che assume i valori logici 0 e 1, esistono due vettori  $\{|0\rangle, |1\rangle\}$ , che costituiscono una base ortonormale nello spazio di Hilbert associato al qubit

$$\mathcal{H} \equiv \mathbb{C}^2 = \{ |\psi\rangle = a|0\rangle + b|1\rangle \}_{a,b \in \mathbb{C}}$$

$$\langle \psi | \psi \rangle = |a|^2 + |b|^2. \quad (1)$$

Tale spazio è invariante rispetto alle trasformazioni unitarie

$$U(\hat{n}, \theta) = e^{-i\frac{\theta}{2}\hat{n} \cdot \vec{\sigma}}$$

$$= \mathbf{1}_2 \cos \frac{\theta}{2} - i\hat{n} \cdot \vec{\sigma} \sin \frac{\theta}{2}, \quad (2)$$

espresse dalle matrici di Pauli  $\{\sigma_0 = \mathbf{1}_2, \vec{\sigma}\} = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$  (vedi riquadro). Gli operatori  $\sigma_i$  sono hermitiani e rappresentano Osservabili Fisici corrispondenti, per esempio allo stato di polarizzazione di spin/momenti magnetici elementari lungo tre direzioni ortogonali nello spazio [44, 45, 46]. Le componenti 1, 2, 3 di questi Osservabili sono incompatibili tra loro che, come si è detto in precedenza, è una delle caratteristiche specifiche di MQ. Questo schema può essere generalizzato a qualsiasi sistema fisico, che ammetta tre osservabili dicotomiche, che godono delle stesse proprietà delle matrici di Pauli. Nel quadro teorico della MQ, facendo eventualmente riferimento alla sintesi dei suoi postulati riportata in Appendice, lo stato fisico di un qubit è descritto da un operatore di stato hermitiano positivo a traccia 1 (per brevità, da qui in poi, si userà stato per indicare un operatore di stato)

$$\rho(\vec{p}) = \frac{1}{2}(\mathbf{1} + \vec{p} \cdot \vec{\sigma}), \quad (3)$$

dove  $\vec{p} \in \mathbb{R}^3$ ,  $0 \leq \vec{p}^2 \leq 1$ . Quindi tutti

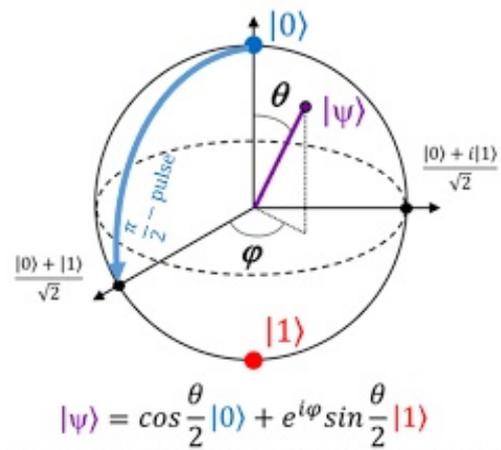
gli stati sono in corrispondenza biunivoca con i punti contenuti in una sfera di raggio unitario, detta **la Sfera di Bloch**. Se un qubit è nello stato  $\rho$ , le misure di una qualunque pertinente grandezza fisica  $\mathcal{O}$  hanno come loro valor medio  $\langle \mathcal{O} \rangle = \text{tr} \rho \mathbf{O}$  (vedi la Regola di Born in Appendice), avendo denotato con  $\mathbf{O}$  il corrispondente operatore osservabile hermitiano su  $\mathcal{H}$ . La proprietà cruciale degli stati, immediatamente verificabile, è che si possono sommare secondo la combinazione lineare convessa  $\rho(\lambda) = \lambda \rho_1 + (1 - \lambda) \rho_2$ ,  $0 \leq \lambda \leq 1$ . Questa formula connette tutti gli stati che si trovano sulla corda tra  $\rho_1$  e  $\rho_2$ , rappresentati come punti nella Sfera di Bloch. È evidente che, in generale, ogni singolo stato può avere un numero infinito di queste rappresentazioni, ad eccezione di quelli che si trovano esattamente sulla superficie della Sfera di Bloch. Dall' espressione in (3) si deduce che gli stati puri sono operatori di Proiezione, cioè della forma

$$\rho = |\psi\rangle\langle\psi|, \quad |\psi\rangle \in \mathcal{H}, \quad \langle\psi|\psi\rangle = 1,$$

dove  $|\psi\rangle$  è detto **vettore di stato**. A loro volta, essendo i vettori di stato elementi di  $\mathcal{H}$ , si possono sommare tra loro con coefficienti complessi come, per esempio, riportato in (1). Combinazioni lineari di vettori di stato sono dette **coerenti** e, una volta normalizzate a 1, corrispondono univocamente a nuovi stati puri  $\rho$  collocati sulla superficie della Sfera di Bloch. Da un punto di vista fisico gli stati puri rappresentano tutti e soli gli stati di un qubit isolato. Pertanto, ogni coppia di essi può essere connessa da una trasformazione unitaria, del tipo indicato in (2).

Invece, i punti interni alla Sfera rappresentano **Stati Misti**, cioè miscele statistiche classiche degli stati puri (non di vettori di stato, attenzione!). Come visto in precedenza, queste combinazioni, dette **incoerenti**, sono convesse e, in una opportuna scelta di base in  $\mathcal{H}$ , possono essere espresse con coefficienti reali positivi di somma 1.

I punti interni della Sfera di Bloch possono essere raggiunti da uno stato puro iniziale tramite trasformazioni non unitarie. Pertanto si è nella condizione di descrivere con un unico quadro teorico sia il qubit come sistema isolato, evoluzione unitaria, sia quando esso è parte di un sistema aperto, con evoluzione non unitaria, ma che pre-



**Figura 3:** La sfera di Bloch.

serva la traccia e la positività di  $\rho$  (si veda la sezione Decoerenza nel seguito). Questo si realizza, per esempio, quando il qubit è in interazione con un ambiente esterno, comunque modellato, che non si possa o non si voglia controllare.

Chiaramente le trasformazioni non unitarie fanno perdere, in generale, la correlazione di fase tra i coefficienti complessi dei vettori di base, nella quale è espresso il vettore di stato iniziale. Questo fenomeno è chiamato **Decoerenza** ed è il principale ostacolo alla computazione quantistica, che intende basarsi esattamente sul controllo dei vettori di stato e della loro evoluzione. Ricordiamo a tal proposito il criterio 3. di Di Vincenzo nella sezione precedente.

In conclusione il qubit costituisce un modello elementare, sia in sovrapposizione coerente di stati puri, che in quelli incoerenti degli stati misti in presenza di decoerenza e rumore.

Tuttavia è abbastanza chiaro che ben poco si possa fare con un solo qubit, quindi è necessario passare a Sistemi Composti, il cui modello minimale è quello del 2-qubit, descritto nello spazio di Hilbert

$$\begin{aligned} \mathcal{H}_A \otimes \mathcal{H}_B & \\ \equiv \text{Span} \{ |0_A\rangle, |1_A\rangle \} \otimes \{ |0_B\rangle, |1_B\rangle \} & \\ = \text{Span} \{ |0_A 0_B\rangle, |0_A 1_B\rangle, |1_A 0_B\rangle, |1_A 1_B\rangle \} & . \end{aligned}$$

Questa struttura della base suggerisce subito la notazione computazionale

$$\mathcal{H}_A \otimes \mathcal{H}_B \equiv \text{Span} \{ |0\rangle, |1\rangle, |2\rangle, |3\rangle \}.$$

Ovviamente tale spazio ha dimensione  $4 = 2^2$ .

Ma se si mettono assieme 3 qubit il loro spazio è

$$\begin{aligned} \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C &= (\mathbb{C}^2)^{\otimes 3} \\ &= \text{Span} \{ |0_A 0_B 0_C\rangle, |0_A 0_B 1_C\rangle, \\ &\quad |0_A 1_B 0_C\rangle, \dots \} \end{aligned}$$

che è a  $8 = 2^3$  dimensioni e così via all'aumentare del numero di qubit. Lo spazio di Hilbert di  $n$  qubit è  $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$  con dimensioni  $2^n$ .

Si consideri, ora, un sistema bipartito AB in un particolare stato puro, specificato dal vettore di stato

$$|\psi\rangle_{AB} = a|0_A 1_B\rangle + b|1_A 0_B\rangle \quad (4)$$

con  $|a|^2 + |b|^2 = 1$ . Si supponga, inoltre, che un osservatore esegua una misura dell'osservabile locale  $\sigma_{3A}$ , che considera solo il qubit A rimanendo ininfluenza sullo stato di B. I possibili esiti si verificano secondo la seguente distribuzione di probabilità  $\mathcal{P}$  (si veda l'Appendice):

$$\begin{cases} \text{valore} & \mathcal{P} & \text{Stato ridotto} \\ 0 & |a|^2 & |0_A 1_B\rangle, \\ 1 & |b|^2 & |1_A 0_B\rangle. \end{cases} \quad (5)$$

Dalla tabella deduciamo che l'esito della misura sul sottosistema A comporta immediatamente informazione sullo stato del sottosistema B. Lo stato considerato stabilisce una correlazione interna tra i sottosistemi A e B. Tale correlazione è il prototipo del concetto di *Entanglement*.

## Entanglement

### EPR

Nel 1935 Einstein, Podolski e Rosen considerarono un sistema analogo a quello descritto sopra per presentare un esperimento mentale, con lo scopo di dimostrare la non completezza della MQ come teoria della Natura [48]. La loro convinzione era che in qualsiasi teoria fisica completa ogni elemento di realtà dovesse essere rappresentato. Essi ritenevano che una condizione sufficiente affinché una proprietà fisica sia un elemento di realtà consista nella possibilità di prevederla con certezza il suo valore immediatamente prima della misurazione. Le precedenti misurazioni condotte dall'osservatore A gli consentono di prevedere con certezza quale possa

essere il valore dell'osservabile locale  $\sigma_{3B}$  effettuata dal suo omologo osservatore B. Riuscendo A a prevedere il valore dell'osservabile adottato da B, esso deve corrispondere a un elemento della realtà, il quale a sua volta dovrebbe essere rappresentato in qualsiasi teoria fisica completa. In particolare, la riduzione (o collasso) dello stato puro (4) nello stato ridotto in (5) dovrebbe avvenire istantaneamente per tutto il sistema composto, indipendentemente dalla distanza relativa tra A e B. In tal modo verrebbe introdotta una *spooky action at a distance*, incompatibile con la Relatività Speciale, che invece impone una condizione di località: l'influenza di un corpo su un altro non può manifestarsi ad una velocità superiore a quella della luce. Tuttavia, la MQ dice semplicemente come calcolare le probabilità dei possibili risultati di un osservabile, quando esso viene misurato, e non include alcun altro elemento più fondamentale.

### Bell & Co.

Quasi trent'anni dopo la pubblicazione dell'articolo EPR [48] è stato proposto un test, noto come disuguaglianza di Bell [49], utilizzabile per verificare sperimentalmente la validità dell'ipotesi di località di Einstein (o realismo locale) in MQ: se A e B sono sistemi quantistici spazialmente separati, un'azione eseguita sul sistema A non deve modificare la descrizione del sistema B. L'idea fruttuosa di Bell fu quella di testare la località di Einstein, tradotta nella cosiddetta "teoria delle variabili nascoste". Il test si basa sulla stima quantitativa delle correlazioni tra gli esiti delle misure effettuate, rispettivamente, dall'osservatore Alice su A e dall'osservatore Bob su B, i quali condividono un 2-qubit A-B. Un ausiliario preparatore Cao fornisce una sequenza, idealmente infinita, di copie del 2-qubit preparate sempre nello stesso stato.

Se i valori delle variabili nascoste fossero esattamente noti, allora i risultati di qualsiasi misurazione potrebbero essere previsti con certezza. Ma in realtà bisogna continuare a descriverli probabilisticamente, perché di fatto possiamo solo fissare il dominio delle variabili nascoste. In secondo luogo si presume che tali variabili siano locali, cioè ogni decisione di Bob sul tipo di misura da effettuare, non ha alcun effetto sulle variabili

nascoste che regolano le misure di Alice, purché tali osservatori siano causalmente disconnessi. Questo significa i due osservatori sono tanto lontani tra loro, che un segnale luminoso non potrà giungere dall'uno all'altro prima che entrambe le rispettive misure siano state eseguite.

Per ipotesi Alice può decidere di misurare casualmente uno dei due osservabili  $\mathbf{Q}$  o  $\mathbf{R}$  e, analogamente, Bob può misurare  $\mathbf{S}$  o  $\mathbf{T}$ , essendo  $\{\pm 1\}$  lo spettro di ognuno degli osservabili. Allora, sotto le ipotesi della teoria delle variabili nascoste, si può dimostrare la disuguaglianza di (tipo) Bell

$$\Delta_{CHSH} = \mathcal{E}(\mathbf{Q}\mathbf{S}) + \mathcal{E}(\mathbf{R}\mathbf{S}) + \mathcal{E}(\mathbf{R}\mathbf{T}) - \mathcal{E}(\mathbf{Q}\mathbf{T}) \leq 2 ,$$

dove  $\mathcal{E}$  rappresenta il valor medio rispetto all'ipotetica distribuzione di probabilità delle variabili nascoste, qualunque essa sia. Il pedice CHSH nella precedente relazione fa riferimento alle iniziali dei ricercatori J.F.Clauser, M.A.Horne, A.Shimony, R.A.Holt, che diedero la formulazione della disuguaglianza qui presentata [50].

Si supponga ora che il sistema considerato sia un 2-qubit con vettore di stato  $|\psi_{AB}\rangle$  e segua la sola MQ, senza alcun riferimento a variabili nascoste. Gli osservabili presi in considerazione siano

$$\begin{aligned} \mathbf{Q} &= \vec{\sigma}_A \cdot \hat{\mathbf{q}}, & \mathbf{R} &= \vec{\sigma}_A \cdot \hat{\mathbf{r}}, \\ \mathbf{S} &= \vec{\sigma}_B \cdot \hat{\mathbf{s}}, & \mathbf{T} &= \vec{\sigma}_B \cdot \hat{\mathbf{t}}, \end{aligned}$$

dove i simboli con il cappuccio indicano versori nello spazio, lungo i quali si misurano le componenti di spin  $\vec{\sigma}$ . È immediato valutare la CHSH usando la MQ, specificamente la formula di Born (si veda l'Appendice). Per esempio, se detti versori sono coplanari e sono separati da angoli di  $45^\circ$  e lo stato  $|\psi\rangle_{AB}$  dell'equazione (4) è determinato dalle ampiezze  $a = -b = 1/\sqrt{2}$ , si ottiene  $\Delta_{CHSH} = 2\sqrt{2} \geq 2$ , che viola chiaramente la CHSH. Si scopre quindi che le correlazioni previste dalla MQ sono, in generale, incompatibili con le ipotesi di una teoria di variabili nascoste.

Nel 1982, Aspect e collaboratori [51] condussero un esperimento che dimostrava la violazione di CHSH e affrontando la questione della separazione causale tra le azioni di A e B. Per questo la-

voro Aspect ha ricevuto il premio Nobel nel 2022 [52], assieme a J. Clauser e A. Zeilinger, anch'essi "per esperimenti con fotoni *entangled*, per stabilire la violazione delle disuguaglianze di Bell e per aprire la strada alla scienza dell'informazione quantistica".

Rimane da verificare che la teoria delle variabili nascoste non rientri in gioco controllando lo stato dei rivelatori, oppure la stessa tecnica decisionale delle osservazioni da effettuare. In ogni caso, si avrebbe una causa di inapplicabilità della condizione CHSH. Perciò la verifica sperimentale di tale disuguaglianza, o simili, è un'attiva area di ricerca. Per esempio, molto recentemente è stato pubblicato un articolo su Physical Review X [53], nel quale si riporta di un esperimento EPR con due condensati di Bose-Einstein spazialmente separati, ciascuno contenente circa 700 atomi di rubidio. L'*entanglement* tra i condensati si manifesta in forti correlazioni dei loro spin collettivi. Tali esperimenti mostrano che il conflitto tra la MQ e il realismo locale non scompare quando le dimensioni del sistema aumentano.

## Da Enigma a Risorsa

Dopo il lavoro di Bell, l'*entanglement* quantistico divenne oggetto di studio intensivo da parte di coloro che erano interessati ai fondamenti della teoria quantistica. Ma a poco a poco si è evoluto un nuovo punto di vista: l'*entanglement* è anche una risorsa potenzialmente preziosa. Sfruttando gli stati quantistici *entangled*, possiamo svolgere compiti altrimenti difficili o impossibili. Questa caratteristica essenziale della MQ è vista oggi come una risorsa fisica, che può essere spesa per risolvere compiti di elaborazione delle informazioni in modi nuovi, ma anche per descrivere nei dettagli gli stati della teoria dei campi quantistici [54].

Il primo obiettivo è definire quando un sistema si trova in uno stato *entangled*. L'idea di base consiste nel comprendere quale informazione si riesca ad ottenere effettuando misure soltanto sul sottosistema A, ignorando quanto si verifichi in B. Da un punto di vista matematico, lo strumento che realizza questo concetto consiste nella **traccia parziale**. Considerando uno stato puro  $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$ , la sua traccia parziale rispetto a B

è lo stato di A fornito dalla relazione

$$\begin{aligned}\rho_A &= \text{tr}_B (|\psi_{AB}\rangle\langle\psi_{AB}|) \\ &= \sum_{\pi\mu\nu} c_{\pi\nu}^* c_{\mu\nu} |\mu_A\rangle\langle\pi_A|,\end{aligned}$$

dove il vettore di stato

$$|\psi_{AB}\rangle = \sum_{\mu,\nu} c_{\mu\nu} |\mu_A\rangle \otimes |\nu_B\rangle$$

è stato sviluppato in una generica base di  $\mathcal{H}_{AB}$ . Questa decomposizione è utile quando si considerano osservabili locali solo di A, in quanto si dimostra che il valor medio di ogni osservabile  $\mathbf{O}_{AB} = \mathbf{O}_A \otimes \mathbf{1}_B$  si scrive come

$$\langle \mathbf{O}_{AB} \rangle = \text{tr} (\mathbf{O}_A \rho_A).$$

Questa relazione caratterizza tutti gli osservabili e le trasformazioni locali su A (analogamente su B). Per un generico sistema bipartito si dice che  $\rho_{AB}$  è uno **stato entangled** se

$$\rho_{AB} \neq \sum_{\mu} p_{\mu} \rho_A^{\mu} \otimes \rho_B^{\mu}.$$

dove  $\rho_A^{\mu}$  e  $\rho_B^{\mu}$  sono stati puri per ogni  $\mu$ . L'insieme complementare è costituito dagli **stati separabili**, per i quali effettivamente si verifica che

$$\rho_{AB} = \sum_{\mu} p_{\mu} \rho_A^{\mu} \otimes \rho_B^{\mu}.$$

con  $\rho_A^{\mu}$  e  $\rho_B^{\mu}$  stati puri.

Un esempio di vettore di stato che rappresenta uno stato puro separabile è dato da

$$|\psi_{AB}\rangle = |1_A 1_B\rangle.$$

Infatti si ha  $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}| = |1_A\rangle\langle 1_A| \otimes |1_B\rangle\langle 1_B|$ . Differentemente, il vettore di stato

$$|\phi_{AB}^+\rangle = \frac{1}{\sqrt{2}} (|0_A 0_B\rangle + |1_A 1_B\rangle) \quad (6)$$

corrisponde ad uno stato puro *entangled* dato da

$$\begin{aligned}\rho_{AB} &= |\phi_{AB}^+\rangle\langle\phi_{AB}^+| \\ &= \frac{1}{2} [ |0_A\rangle\langle 0_A| \otimes |0_B\rangle\langle 0_B| \\ &\quad + |1_A\rangle\langle 1_A| \otimes |1_B\rangle\langle 1_B| \\ &\quad + |0_A\rangle\langle 1_A| \otimes |0_B\rangle\langle 1_B| \\ &\quad + |1_A\rangle\langle 0_A| \otimes |1_B\rangle\langle 0_B| ],\end{aligned}$$

dove gli ultimi due termini in parentesi non sono proiettori, né esiste una diversa base in  $\mathcal{H}_A \otimes \mathcal{H}_B$  che consenta di eliminare tale tipo di termini.

In generale, un vettore di stato che corrisponde ad uno stato puro bipartito separabile è un prodotto diretto di vettori di stato di  $\mathcal{H}_A$  e  $\mathcal{H}_B$ , cioè  $|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\chi\rangle_B$ . Corrispondentemente gli stati ridotti  $\rho_A = |\phi\rangle_A\langle\phi_A|$  e  $\rho_B = |\chi\rangle_B\langle\chi_B|$  sono sempre puri.

Ogni vettore di stato che non può essere espresso come prodotto tensoriale corrisponde ad uno stato *entangled* e, in tal caso,  $\rho_A$  e  $\rho_B$  sono stati misti. Non esistendo alcun analogo classico di questa situazione, sembra quasi che la peculiarità della MQ sia contenuta negli stati *entangled*. In particolare, si può dimostrare che la CHSH è violata da tutti gli stati *entangled*, mentre è soddisfatta da tutti gli stati separabili. Inoltre l'*entanglement* tra le due parti di un sistema non può essere creato agendo localmente, ma solo attraverso una effettiva interazione tra di esse. Per convenienza, conviene definire gli **stati puri massimalmente entangled** come

$$\rho_{AB} = |\Psi\rangle\langle\Psi|, \quad |\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{\mu} |\mu_A\rangle \otimes |\mu_B\rangle$$

se accade che

$$\text{tr}_A \rho_{AB} = \frac{\mathbf{1}_B}{d}, \quad \text{tr}_B \rho_{AB} = \frac{\mathbf{1}_A}{d},$$

essendo  $d$  la dimensione dei rispettivi spazi di Hilbert.

Una maniera equivalente di caratterizzare l'*entanglement* degli stati può essere fatta attraverso il concetto di Numero di Schmidt, oppure tramite il concetto di Entropia di *Entanglement*  $S_A = -\text{tr} [\rho_A \log \rho_A]$ , particolarmente utile in teoria dei campi, ma non tratteremo questi aspetti nella presente discussione (vedi [37]).

## Non Super-Luminale

Il primo impulso che si potrebbe avere nel manipolare uno stato *entangled* sarebbe quello di utilizzare il carattere non locale delle sue correlazioni per inviare messaggi a velocità superluminale (idea aborrita da Einstein in primis).

Si supponga d'aver preparato una serie copie di un particolare stato puro massimalmente

*entangled* rappresentato dal vettore

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}} \left[ |\uparrow_{\hat{n}_A} \uparrow_{\hat{n}'_B}\rangle + |\downarrow_{\hat{n}_A} \downarrow_{\hat{n}'_B}\rangle \right] \quad (7)$$

specificato dalle direzioni  $\hat{n}, \hat{n}'$ . Il vettore di stato (6) è chiaramente un caso particolare di (7). Come in precedenza si suppone che gli osservatori Alice e Bob che posseggono il sottosistema A e B, rispettivamente, siano causalmente disconnessi. Per inviare un messaggio ad Alice, Bob lo codifica misurando l'osservabile  $\sigma_{1B}$ , oppure  $\sigma_{3B}$ , su ogni qubit in suo possesso, inducendo una corrispondente preparazione del qubit A nella base  $\{|\uparrow_{\hat{x}_A}\rangle, |\downarrow_{\hat{x}_A}\rangle\}$ , oppure in  $\{|\uparrow_{\hat{z}_A}\rangle, |\downarrow_{\hat{z}_A}\rangle\}$ . Tuttavia, sebbene le due preparazioni siano sicuramente differenti, l'operatore di stato che effettivamente possiede Alice è  $\rho_A = \mathbf{1}_A/2$ . Pertanto, non esiste alcuna misurazione che Alice possa effettuare per distinguere quale riduzione Bob abbia operato. Il messaggio è illeggibile, non c'è possibilità di comunicazioni superluminali. Solo nel caso in cui Alice e Bob effettuassero la misura lungo uno stesso asse, giungerebbero a una concordanza.

Analogamente, se Bob misurasse il suo insieme di qubit, scegliendo a caso una delle due direzioni dello spazio, diciamo  $x$  e  $y$ , e comunicasse ad Alice anche solo la successione dei valori da lui ottenuti, allora con misure su A Alice potrebbe distinguere quale degli osservabili sia stato effettivamente misurato. In ogni caso ci deve essere una comunicazione convenzionale, quindi non più veloce della luce.

## Usare l' Entanglement

### Informazioni e Cancellazioni

Lasciatoci alle spalle questo sogno fantascientifico, ci sono altri aspetti sorprendenti su cui far leva. Ad esempio, sappiamo che gli operatori di stato formano un insieme convesso e gli stati puri sono i punti estremi dell'insieme. Uno stato misto di un sistema A può essere preparato come un insieme di stati puri in molti modi diversi, tutti però sperimentalmente indistinguibili. D'altra parte, per ogni dato stato misto  $\rho_A$  si può trovare una sua purificazione, cioè un vettore di stato *entangled*  $|\Phi_{AB}\rangle$  per un appropriato si-

stema bipartito A-B, tale che la traccia parziale di  $|\Phi_{AB}\rangle\langle\Phi_{AB}|$  in B produca esattamente  $\rho_A$ .

Inoltre, è possibile trovare un osservabile in B che riproduca, in corrispondenza di ogni esito, il corrispondente stato puro presente nella miscela rappresentata da  $\rho_A$ . Infine, a seguito di un ulteriore cambiamento di base in B, si può ottenere una nuova rappresentazione degli stati puri che costituiscono  $\rho_A$  differenti dai precedenti. Questo risultato è noto come teorema di Gisin-Hughston-Jozsa-Wootters e costituisce la formulazione più generale della procedura detta della **cancellazione quantistica** [36, 37]. Risulta quindi che a seconda dell'informazione acquisita sul sistema B, viene cambiata anche la descrizione fisica dello stato di A.

Tutte queste proprietà dei sistemi bipartiti si possono sfruttare in applicazioni nell'ambito delle telecomunicazioni: il **dense coding**, il **teletrasporto quantistico** e la **crittografia quantistica**.

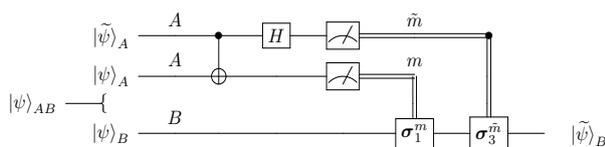
### Dense Coding

In primo luogo supponiamo che Alice possieda due bit di informazione, che desidera inviare a Bob in un modo particolarmente efficiente. In effetti, se Alice condividesse con Bob un 2-qubit in uno stato *entangled* puro, ad esempio rappresentato da (6), lei potrebbe spedirli con un solo qubit (*dense coding*). Sul qubit A, quello in possesso di Alice, si possono eseguire solo trasformazioni unitarie locali: per esempio tre rotazioni di  $\pi$  attorno a tre assi ortogonali tra loro, oltre alla rotazione identica. Esse possono cambiare il vettore di stato  $|0_A\rangle$  in  $|1_A\rangle$  e viceversa, con un eventuale fattore di fase. I corrispondenti stati del 2-qubit complessivo formano i quattro elementi di una base ortonormalizzata di stati massimalmente *entangled* (base di Bell) dello spazio di Hilbert. Dopo una simile preparazione, il qubit A viene inviato lungo un canale classico a Bob, il quale esegue una misura collettiva, per esempio di  $(\vec{\sigma}_A + \vec{\sigma}_B)^2$  e di  $\sigma_{A3} + \sigma_{B3}$  che commutano tra loro. Essa permette di distinguere inequivocabilmente quale delle quattro trasformazioni sia stata eseguita. Questo equivale alla trasmissione di due bit classici. In conclusione, per comunicare più efficientemente i loro messaggi Alice e Bob hanno sfruttato un pre-esistente stato *entan-*

gled come una risorsa computazionale quantistica, per ottenere la trasmissione di due bit classici. Realizzazioni sperimentali pionieristiche sono riportate in [55].

## Teletrasporto

Ci si chiede ora se sia possibile avere l'effetto inverso, cioè inviare due bit classici per trasmettere un qubit. Si supponga, come prima, che Alice e Bob posseggano ciascuno uno dei qubit che si trovano in uno stato *entangled*  $|\psi_{AB}\rangle$ , per semplicità (7). Inoltre, Alice è in possesso di un secondo qubit, che per convenienza si denota con  $|\tilde{\psi}_A\rangle$ , del quale vuole trasmettere lo stato a Bob attraverso un canale di comunicazione classico. A questo scopo, in primo luogo ella provvede a produrre un nuovo stato *entangled* tra i qubit  $|\psi_A\rangle$  e  $|\tilde{\psi}_A\rangle$  in suo possesso, facendoli opportunamente interagire. A questo stadio ci sono ben tre qubit in un unico stato *entangled*. Su quelli in suo possesso Alice esegue una misura locale, per esempio di  $\sigma_{A3}$ , separatamente su ciascuno dei due qubit. Questa doppia misura produce la coppia di esiti  $(m, \tilde{m})$ . Ora, su un canale classico Alice invia tali dati numerici a Bob, il quale possiede un opportuno protocollo di codifica: ad ogni coppia di valori ricevuti corrisponde una ben precisa trasformazione locale sul suo qubit  $|\psi_B\rangle$ , che gli consente di porlo esattamente nello stato originario definito da  $|\tilde{\psi}\rangle$ .

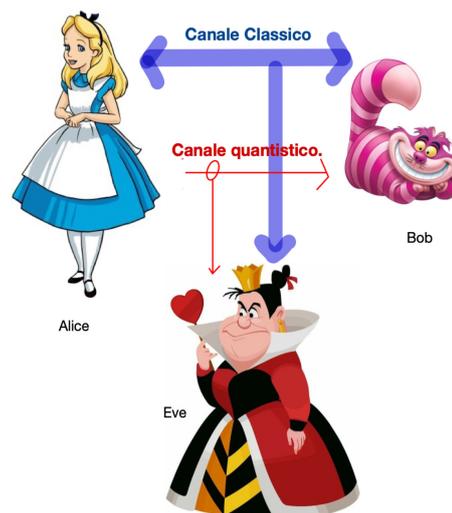


**Figura 4:** Il Teletrasporto attraverso una rappresentazione circuitale, che verrà discussa più dettagliatamente nel seguito. Gli elementi essenziali sono i due qubit entangled suddivisi tra B ed A, che ne possiede anche un terzo in uno stato specifico. Ogni qubit procede lungo un filo del circuito. Il simbolo che collega i due fili di A rappresenta una specifica forma di interazione tra i due qubit e che li pone in *entanglement*. Le altre operazioni unitarie locali sul singolo qubit vengono rappresentate con dei simboli a scatola. Infine le misure vengono rappresentate con un simbolo di misuratore e i canali di comunicazione classici con un doppio filo.

La procedura è stata ideata dal gruppo di McGill University [56] ed implementata sperimentalmente in molti modi [57, 59, 60]. In particolare la tecnologia fotonica dal gruppo di Roma [59] è diventata uno standard in questo ambito. Questo sorta di magia è spesso chiamata **Teletrasporto Quantistico**, ma in effetti il termine sembra piuttosto enfatico: 1) nulla di materiale viene trasportato, 2) ma solo informazione su un canale classico a velocità non superiore a quella della luce, 3) inoltre viene distrutto lo stato *entangled* originario per generare un solo qubit in B, quindi c'è un costo in questa operazione, 4) infine il qubit  $|\tilde{\psi}\rangle$  non viene copiato: in primo luogo l'originario viene distrutto dalla misura e solo dopo di ciò il nuovo qubit è prodotto. Queste ultime osservazioni sono conformi al cosiddetto Teorema di No Cloning.

## Crittografia Quantistica

L'impossibilità di copiare stati quantistici, oltre all'effetto perturbativo di ogni misura su di essi, ha stimolato un'area piuttosto importante di applicazioni chiamata Crittografia Quantistica. Si è sviluppata così una grande area di ricerca, sia per quanto riguarda i protocolli di codifica che le tecniche di implementazione. Tra i più noti esempi vi è il protocollo di distribuzione di



**Figura 5:** Alice e Bob possono accordarsi su una comune chiave crittografica sia su un canale classico che uno quantistico. In questo caso, il tentativo di spionaggio da parte di Eve incontra difficoltà legate allo stabilirsi di uno stato correlato con i qubit A e B.

chiavi quantistico (QKD) denominato BB84 dal nome dei suoi inventori [61] (Si veda l'articolo di Samuele Altilia, Michele Notarnicola e Stefano Olivares e quello di Taira Giordani, Alessia Suprano, Fabio Sciarrino in questo numero di **Ithaca**).

Lo scopo del protocollo è quello di stabilire una chiave segreta, cioè una sequenza casuale di bit, nota solo alle due parti Alice e Bob, che possono utilizzarla per eseguire lo scambio di messaggi criptati o rilevamento di eventuali manomissioni. Se non si dovessero rilevare problemi durante il tentativo di stabilire tale chiave, con alta probabilità essa si potrà ritenere segreta, anche se non c'è garanzia che si riesca a stabilire una chiave privata, nota a solo una delle parti.

Immaginiamo che Alice e Bob siano collegati da due canali pubblici: un canale classico bidirezionale e un canale quantistico unidirezionale. Il canale quantistico consente ad Alice di inviare a Bob una sequenza di singoli qubit. Per esempio, supponiamo che essi condividano una scorta di coppie *entangled* descritte dal vettore di stato  $|\phi_{AB}^+\rangle$  di (6). Alice e Bob decidono di misurare  $\sigma_1$  o  $\sigma_3$  sui qubit in loro possesso con un criterio pseudo-casuale di probabilità 1/2. Una volta eseguite le misurazioni, sia Alice che Bob annunciano sul canale classico quali osservabili abbiano misurato, ma non rivelano i risultati ottenuti. Per quei casi (circa la metà) in cui abbiano misurato i loro qubit lungo assi diversi, i loro risultati vengono scartati. Invece, nei casi in cui abbiano misurato lungo lo stesso asse, i loro risultati sono perfettamente correlati, ma mantenuti segreti. In questo modo stabiliscono una chiave condivisa, cioè una QKD.

Ci si chiede se questo protocollo sia davvero invulnerabile ad un subdolo attacco da parte di una terza parte Eve. In particolare, Eve potrebbe aver manomesso clandestinamente le coppie in qualche occasione nel passato. Il significa che le coppie che Alice e Bob possiedono potrebbero essere (a loro insaputa) non perfette, ma piuttosto *entangled* con i qubit in possesso di Eve. Se così fosse, Eve può attendere che Alice e Bob facciano i loro annunci pubblici e procedere a misurare i propri qubit, in modo tale da acquisire la massima informazione possibile dagli scambi tra i due. Di fatto il vettore di stato quantistico

complessivo a tre con Eve è del tipo

$$\begin{aligned} |\Psi\rangle_{ABE} = & |00_{AB}\rangle |\phi_{0E}\rangle + |10_{AB}\rangle |\phi_{1E}\rangle \\ & + |01_{AB}\rangle |\phi_{2E}\rangle + |11_{AB}\rangle |\phi_{3E}\rangle \end{aligned}$$

Si osservi, ora, che  $|\phi_{AB}^+\rangle$  è autostato sia di  $\sigma_1^A \otimes \sigma_1^B$  che di  $\sigma_3^A \otimes \sigma_3^B$  con lo stesso autovalore 1, mentre si può verificare facilmente che  $|\Psi\rangle_{ABE}$  a tre qubit non gode di questa proprietà. Quindi, con una misura di integrità di questo tipo il tentativo di spionaggio da parte di Eve può essere facilmente svelato.

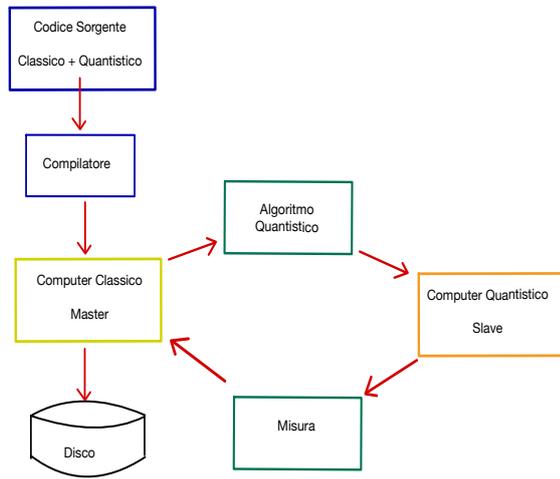
Fin dalla sua concezione la QKD si è evoluta da una semplice curiosità teorica a un'industria prolifica all'avanguardia nelle tecnologie quantistiche. Oggigiorno si stanno costruendo reti QKD sia metropolitane [62], [63], [64], [65] che satellitari [66], [67], culminati nello sviluppo e nel lancio del satellite Micius dell'Accademia cinese delle Scienze, che ha dimostrato la realizzabilità collegamenti QKD intercontinentali [68].

I vari dispositivi e i protocolli offrono buone prestazioni in termini di stabilità e di tasso di qubit errati, ma ulteriori studi hanno evidenziato che una implementazione completamente sicura può essere ancora una sfida impegnativa.

## Algoritmi Quantistici

### Architettura di un Computer Quantistico

In tutti gli esempi precedentemente esposti si è potuto notare che ogni operazione a livello quantistico deve necessariamente essere accompagnata dall'uso di un canale classico di comunicazione. Questo tipo di struttura si deve riflettere nell'architettura di un computer quantistico, che assume una struttura ibrida nella quale i processori classici e quantistici funzionano in modalità *master/slave*. In questo caso, il codice classico effettua chiamate a un dispositivo esterno quantistico. Inoltre, il codice quantistico, scritto in un linguaggio adeguato, fornisce le istruzioni che devono essere eseguite dal processore quantistico. Una volta che le istruzioni inviate dal computer classico sono state eseguite nel processore quantistico, viene eseguita una misurazione e il risultato viene rinviato al processore classico. Tale processo può essere ripetuto più volte. Tale architettura viene chiamata QRAM [69].



**Figura 6:** Architettura QRAM per un computer quantistico.

In questa architettura rimangono alcuni colli di bottiglia, quali l'eventualità di un possibile sovraccarico del trasferimento dati, fatto comune anche per i processori grafici e vettoriali. Oltre a queste limitazioni, il processore quantistico ne introduce potenzialmente altre: potrebbe, nello specifico, esserci un limite alla quantità di tempo a disposizione, durante la quale è possibile mantenere una sovrapposizione quantistica prima che si dissipi per interazioni con l'ambiente circostante. Questo è il già menzionato tempo di decoerenza, il quale rappresenta un vincolo senza analogo nella progettazione degli algoritmi classici.

## Porte Logiche e Circuiti Quantistici

Passiamo ora ad analizzare le operazioni elementari di un computer quantistico. Come già discusso in precedenza, mentre un computer classico elabora bit, un computer quantistico elabora i qubit. Per l'elaborazione dei bit, un computer classico utilizza un insieme finito di porte logiche, cioè di funzioni booleane  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ , dove  $n$  è il numero di bit in ingresso ed  $m$  quello dei bit in uscita. Ma nel caso quantistico questo non è un fatto scontato. In primo luogo, le porte logiche classiche sono tipicamente irreversibili (dissipative): a due ingressi corrisponde in genere una sola uscita, come ad esempio per la porta  $AND : (a, b) \in \mathbb{Z}_2^2 \rightarrow ab \in \mathbb{Z}_2$ . Ma nel manipolare più qubit non ci debbono essere dissipazioni, perderemmo rapidamente la coerenza degli stati. Solo manipolazioni reversibili sono

quindi ammesse: cioè rappresentate da trasformazioni unitarie. Dal punto di vista classico la teoria booleana consente un calcolo reversibile a patto di utilizzare porte logiche con un numero uguale di ingressi e uscite, come ad esempio la porta NOT :  $x \leftrightarrow \bar{x}$ , oppure quella di Toffoli:  $(x, y, z) \leftrightarrow (x, y, z \oplus xy)$ , avendo indicato con  $\oplus$  la somma tra interi mod 2. Si può dimostrare che, facendo uso della porta di Toffoli, ogni porta logica classica irreversibile a più ingressi può essere emulata da una reversibile, purché siano disponibili dei bit ausiliari.

In generale, nella teoria booleana si introduce il concetto di circuito booleano, con  $n$  ingressi e  $m$  uscite, definito come un grafo aciclico, monodirezionale e finito. In ogni vertice (o nodo) di tale grafo possiamo collocare una porta logica, tratta da un insieme finito di esse, ad eccezione di  $n$  nodi riservati agli input ed  $m$  agli output. Inoltre gli archi di connessione devono avere un qualche ordinamento, per distinguere tra diversi argomenti che puntano alla stessa funzione. Ad esempio, un circuito potrebbe contenere solo porte binarie AND e OR e porte unarie NOT, oppure essere interamente descritto da porte binarie NAND. A queste bisogna aggiungere INPUT e COPY, che consentono di assegnare i valori di ingresso e leggere i risultati. In definitiva, nel caso di circuiti booleani irreversibili è possibile far corrispondere dei circuiti equivalenti reversibili, cioè costruiti solo con porte reversibili. Per esempio un insieme siffatto è dato da: INPUT, NOT, Toffoli e COPY. Ma quello che preme sottolineare è che esso realizza un insieme universale finito di porte logiche, con le quali costruire ogni altra possibile funzione o circuito booleano.

Nel caso quantistico, le trasformazioni unitarie costituiscono, invece, un insieme infinito, operanti sul prototipo di spazio di Hilbert  $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$  qui adottato. Anche se può sembrare superfluo, la situazione ideale nella quale ci stiamo ponendo consente di far agire tutte le porte logiche quantistiche solo su stati puri producendo stati puri, rappresentabili in termini dei soli vettori di stato corrispondenti. Gli eventuali effetti di decoerenza non vengono inclusi a questo livello di trattazione e considerati in maniera perturbativa: si suppone che in un computer quantistico esista un tempo minimo di decoerenza, entro il

quale lo stato complessivo dei qubit rimane puro. Nella Figura 20 sono riportati i tempi di decoerenza  $T_1$  medi tipici per diversi sistemi di calcolo quantistico reali. Come ultima avvertenza ai fini di alleggerire la notazione, le porte logiche verranno indicate con lettere maiuscole, e non in grassetto, per quanto rappresentino sempre operatori unitari. In linea di principio, una sola di esse realizzerebbe il passaggio dallo stato iniziale a quello finale, simbolicamente

$$|i_1 i_2 i_3 \dots i_n\rangle \xrightarrow{U} |i'_1 i'_2 i'_3 \dots i'_n\rangle$$

con  $i_j, i'_j = 0, 1$ . Ma questo vorrebbe dire costruire un apparato apposito per ogni singolo calcolo, il che non porterebbe nessun vantaggio!

L'idea è che la generica trasformazione unitaria su un  $n$ -qubit si possa costruire, almeno in forma approssimata, combinando un numero finito di trasformazioni unitarie standard. A loro volta, ognuna di esse agisce su un sottoinsieme di qubit di fissato numero, relativamente piccolo rispetto ad  $n$ . Con questa idea si propone di sostituire le porte logiche classiche con delle porte logiche quantistiche. Esse debbono costituire un insieme universale finito, nel senso che, a meno di casi eccezionali, ogni trasformazione unitaria si possa scrivere con un circuito, analogo a un circuito booleano, nei cui nodi sono collocati gli elementi dell'ipotetico insieme universale. Ovviamente indipendentemente dall'implementazione fisica specifica, ogni porta compie sempre la stessa operazione logica.

Per perseguire questi scopi si possono utilizzare vari teoremi, il primo dei quali è quello detto di Solovay-Kitaev per le trasformazioni  $U \in SU(2)$ , cioè su 1-qubit. Usando la compattezza del gruppo, si mostra che 1) esiste almeno una famiglia finita  $G$  di suoi elementi che generano sotto-insiemi densi in esso, 2) che per qualsiasi porta  $U$  è possibile trovare una sua approssimazione  $U_\epsilon$ , con precisione  $\epsilon$  in norma traccia, utilizzando al più  $O(\log^4(1/\epsilon))$  elementi tratti da  $G$  [70]. Questo teorema ci consente di costruire una qualunque trasformazione su un qubit a partire, per esempio, dall'insieme finito di porte costituito come segue.

Le tre porte di Pauli

$$X = \sigma_1, Y = \sigma_2, Z = \sigma_3,$$

tra le quali  $X$  è l'analogo della porta NOT e le altre cambiano le fasi relative tra gli stati di base. La porta di Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad (8)$$

la cui azione sugli elementi della base computazionale è data da

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle), \quad |1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle).$$

Infine si aggiungono le porte di fase

$$S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix} = \sqrt{Z},$$

e

$$T = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} = \sqrt{S}.$$

Fatto questo, si deve passare alla costruzione di trasformazioni unitarie di dimensioni superiori. Un altro teorema ci viene in soccorso: esso afferma che, a meno di un insieme di misura nulla in norma traccia, una trasformazione unitaria di  $n$ -qubit può essere costruita da porte a due qubit. Questo risultato è particolarmente importante, perché ci consente di approssimare ogni possibile trasformazione solo con porte a 1 qubit e a 2 qubit. Non c'è la necessità di coinvolgere porte con 3 qubit, analoghe a quella di Toffoli nel caso classico. Da un punto di vista fisico esse realizzano lo scopo di porre in *entanglement* i due qubit coinvolti. Procedendo ad accoppiamenti di questo tipo, l'intero insieme di qubit può essere correlato. In realtà, si può far vedere che basta un solo tipo di porta a 2-qubit. Ad esempio la porta NOT controllata cNOT, definita da

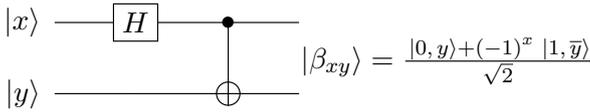
$$cNOT = |0\rangle\langle 0|_c \mathbf{1}_t + |1\rangle\langle 1|_c X_t,$$

dove i pedici indicano rispettivamente il qubit di controllo  $c$  e  $t$  per *target*. Una sua rappresentazione grafica è

$$\begin{array}{ccc} |a\rangle & \text{---} \bullet \text{---} & |a\rangle \\ |b\rangle & \text{---} \oplus \text{---} & |a \oplus b\rangle \end{array}$$

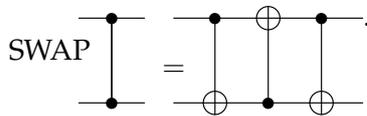
cNOT consente di realizzare la base degli stati di Bell, tutti massimalmente *entangled*, secondo la

relazione circuitale



nella base computazionale  $\{|0\rangle, |1\rangle\}$ .

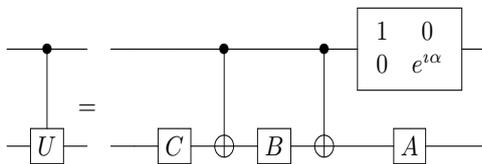
Per il ruolo cruciale che questa porta svolge nello sviluppo dell'idea di computazione quantistica, essa è stata anche la prima ad essere considerata da un punto di vista implementativo ad opera di Cirac e Zoller [71], che proposero l'utilizzo di una trappola ionica. Altro aspetto importante è che essa consente di realizzare, in combinazione con porte a 1-qubit, ogni porta logica a 2-qubit. Ad esempio, la porta SWAP che esegue la permutazione di  $c$  con  $t$ , secondo l'equivalenza circuitale



Così anche per ogni porta controllata

$$cU = |0\rangle\langle 0|_c \mathbf{1}_t + |1\rangle\langle 1|_c U_t,$$

che, usando  $U = e^{i\alpha} AXBXC$  con  $ABC = \mathbf{1}$ , in forma circuitale è espressa come:

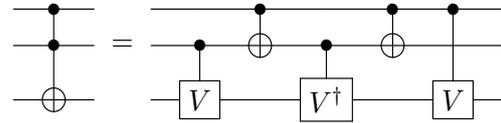


Procedendo in maniera analoga si possono costruire porte logiche per ogni numero di qubit. Ad esempio l'analoga della porta Toffoli a 3 qubit

$$\begin{aligned} cc\text{NOT} &= (\mathbf{1}_{c_1} \mathbf{1}_{c_2} - |1\rangle\langle 1|_{c_1} |1\rangle\langle 1|_{c_2}) \mathbf{1}_t \\ &+ |1\rangle\langle 1|_{c_1} |1\rangle\langle 1|_{c_2} X_t \end{aligned}$$

si rappresenta con il circuito di porte a 1 e 2 qubit presentato dalla Fig. 7.

In definitiva, estendendo il precedente teorema di Solovay-Kitaev per elementi  $U \in U(2^n)$ , è possibile dimostrare che, usando un circuito quantistico costituito da un insieme universale di porte (chiuso rispetto all'inversione), si può realizzare una trasformazione approssimata  $U_\epsilon$  con un numero di risorse computazionali che



**Figura 7:** Rappresentazione circuitale della porta a 3 qubit ccNOT in termini di porte a 1- e 2-qubit. La porta indicata con  $V$  rappresenta l'operatore  $V = (1 - i)(1 + iX)/2$ .

crece al più come una potenza di  $\log_2 1/\epsilon$ . Il che ci rende confidenti che in linea di principio sia possibile calcolare concretamente, con una successione ordinata di operazioni tipiche, implementabili fisicamente con un certo numero fisso di dispositivi scelti in partenza, una data funzione booleana. Intuitivamente, l'utilizzo efficiente di un algoritmo quantistico è possibile perché qualsiasi circuito può essere costruito da un insieme universale di porte logiche. Ma, essendo vero che esistono operazioni unitarie non approssimabili efficientemente (si veda la discussione precedente), è possibile immaginare sistemi quantistici che non possono essere simulati efficientemente su un computer quantistico. Forse tali sistemi non sono realizzati in Natura, altrimenti saremmo in grado di sfruttarli per elaborare informazioni oltre il modello del circuito quantistico.

L'ultimo passaggio che ci rimane è leggere il risultato del calcolo, che consiste in una misurazione ortogonale di tutti i qubit (o un sottoinsieme di essi), proiettando ciascun qubit sulla base  $\{|0\rangle, |1\rangle\}$ . L'esito di questa misurazione è il risultato del calcolo, ma ovviamente esso compare con una certa probabilità, la cui distribuzione statistica si può calcolare conoscendo il circuito. In definitiva il risultato di una computazione quantistica ha un valore probabilistico, non è certo nel senso di un algoritmo classico sequenziale. Pertanto, in generale, si dovrà ripetere il calcolo più volte, per essere confidenti che si sia ottenuto il risultato corretto. In alternativa, si potrebbe procedere ad una verifica a posteriori del risultato ottenuto, almeno per certe classi di problemi.

Con queste premesse, oltre alle applicazioni indicate nel precedente paragrafo, si possono riconoscere e sviluppare alcune aree algoritmiche generali, per le quali il modello quantistico sembra offrire vantaggi sostanziali rispetto alle

alternative classiche più conosciute.

- **Trasformata quantistica di Fourier e Stima della Fase**

La QFT è un algoritmo di generale utilizzo che consente di calcolare la trasformata di Fourier di una funzione in maniera più efficiente di quanto non faccia il corrispondente classico *Fast Fourier Transform*. Dettagli su questo punto saranno discussi in una prossima Sezione. Anche l'algoritmo della Stima della Fase è una sorta di *subroutine*, in quanto può essere applicato in tutti i casi si debbano valutare gli autovalori di operatori unitari.

- **Amplificazione di ampiezza**

Questa procedura consente di aumentare (amplificare) il peso associato a uno stato desiderato all'interno di una sovrapposizione quantistica, in modo che sia più probabile che esso venga misurato. L'amplificazione dell'ampiezza può essere utilizzata come strumento generico per trovare in modo efficiente la soluzione per un'ampia varietà di problemi di ricerca e ottimizzazione. Una discussione di questa tecnica verrà illustrata nella sezione riguardante l'algoritmo di Grover.

- **Quantum Random Walk (QRW)**

Essa può essere applicata per risolvere un'ampia varietà di problemi di stima statistica in modo più efficiente di quanto non possa fare l'analogo classico. Un'introduzione molto dettagliata all'uso QRW in informatica può essere trovata in [72].

- **Simulazione di sistemi fisici**

Non dovrebbe sorprendere che i fenomeni quantistici possano essere simulati in modo più efficiente sull'*hardware* quantistico di quanto sia possibile classicamente, che si è già detto motivò Feynman. Tra i diversi approcci alle simulazioni, negli ultimi anni si è sviluppato un grande interesse verso gli algoritmi quantistici adiabatici, cioè che si basano sul teorema delle perturbazioni adiabatiche [73]. Essi sono stati utilizzati per risolvere problemi impegnativi in bioinformatica, come la conformazione e il ripiegamento delle proteine [74], ed in Fisica

del nucleo. [23, 75]. Sebbene queste applicazioni promettono progressi rivoluzionari in una varietà di settori scientifici e ingegneristici, non è chiaro fino a che punto una simulazione possa rappresentare fedelmente il comportamento di un sistema reale esteso, tornando così alle osservazioni di [26].

- **Correzione degli errori quantistici**  
La QEC è analoga alle classiche tecniche di correzione degli errori, tranne per il fatto che può riconoscere e correggere errori di qubit, al contrario della sola negazione di bit [36]. Le sue applicazioni risiedono nell'implementazione dell'architettura complessiva del sistema di calcolo (sia quantistica che classica di controllo), anche con la progettazione di algoritmi ibridi.

Non avendo lo scopo di trattare in dettaglio tutte le menzionate vaste aree di ricerca ed applicazioni, si rimanda il lettore alla manualistica già citata [36]-[43], ad altri articoli presenti su **Ithaca** e alla letteratura specialistica. A titolo esemplificativo, qui si riportano le idee di fondo di alcune delle tecniche citate.

## Simulazioni Quantistiche

Come sappiamo da molto tempo ormai, una delle applicazioni pratiche più importanti del calcolo è la simulazione di sistemi fisici, sia a scopo progettuale/ingegneristico, che di scoperta di base là dove la comprensione e l'immaginazione umana non riesce ancora spingersi. Il cuore delle simulazioni è la ricerca di soluzioni alle equazioni che esprimono le leggi dinamiche di un dato sistema fisico. Le soluzioni vengono solitamente ottenute approssimando le equazioni ed eventuali altre informazioni, quali condizioni iniziali o al bordo o vincoli al sistema, tramite una loro rappresentazione digitale. Intrinseca alla procedura di discretizzazione è la comparsa di un margine di errore, che cresce per propagazione ai passi successivi di una iterazione algoritmica. Perciò è importante che l'errore in questa procedura sia limitato e che non cresca più velocemente di una piccola potenza del numero di iterazioni. Inoltre, non tutti i sistemi dinamici possono essere simulati efficientemente: generalmente, solo quei sistemi per i quali si conosca

l'esistenza della soluzione globale, per ogni dato iniziale.

Focalizzandosi sui sistemi quantistici isolati, in accordo al postulato di evoluzione riportato in Appendice, il problema centrale consiste nel risolvere l'equazione di Schrödinger per la matrice di stato  $\rho$ . Questo comporta che per un sistema di  $n$  qubit si debba determinare l'evoluzione temporale di  $4^n - 1$  componenti reali (vedi l'Eq. (3)). Quindi la difficoltà base consiste nella crescita esponenziale nel numero di equazioni che si debbono risolvere.

Si sa che esistono molti importanti sistemi quantistici per i quali la simulazione con algoritmi classici è computazionalmente proibitiva, tra i quali il già citato modello di Heisenberg/Ising (vedi Fig. 2) o il più complesso modello di Hubbard. Tali modelli sono utili nello studio della superconduttività, del magnetismo e di molte altre proprietà fisiche dei materiali. Ad essi si affiancano modelli più sofisticati, come la cromodinamica quantistica (QCD), i quali possono essere utilizzati per calcolare le proprietà dei costituenti elementari dell'Universo. Pertanto in Fisica si è ben presto compreso il potenziale della nuova tecnologia della computazione quantistica, intraprendendo l'esplorazione di semplici modelli nucleari [76],[77], modellando la fisica del neutrino [78] e la preparazione degli stati di input [79]. Tuttavia, l'analisi fatta in [80] suggerisce che calcoli accurati delle strutture molecolari possono essere effettuati con certi algoritmi classici efficienti, nel senso che hanno un costo computazionale crescente con una potenza (e non esponenzialmente) delle dimensioni del sistema. Perciò i computer quantistici non necessariamente costituiscono una alternativa vantaggiosa. Tuttavia, rimane il fatto che la simulazione di processi dinamici in tempo reale ponga ancora sfide formidabili all'informatica classica, e molti sforzi sono stati dedicati ad esplorare le proposte provenienti da quella quantistica [81]. Una rassegna sinottica delle varie idee e simulazioni riguardante questo settore di ricerca si può reperire in [82].

La situazione più semplice da considerare è costituita dalla simulazione [83] dell'equazione di Schrödinger mono-dimensionale, nell'intervallo  $-d \leq x \leq d$ , per la funzione d'onda  $|\psi(t)\rangle$  di una particella soggetta ad potenziale, definita

dall'operatore Hamiltoniano

$$\mathbf{H} = \frac{\mathbf{p}_x^2}{2m} + V(x).$$

In rappresentazione di posizione significa che la funzione d'onda  $\psi(x, t) = \langle x | \psi(t) \rangle$ , con condizioni al bordo  $\psi(-d, t) = \psi(d, t) = 0$  e condizione iniziale  $\psi(x, 0) = \psi_0(x)$ , è soggetta alla arcinota equazione di Schrödinger

$$i \frac{\partial}{\partial t} \psi(x, t) = \left[ -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} + V(x) \right] \psi(x, t).$$

La soluzione formale del problema è data dall'azione unitaria dell'operatore di evoluzione

$$|\psi(t)\rangle = e^{-\frac{i}{\hbar} \mathbf{H}t} |\psi(0)\rangle.$$

Come di consueto, per ottenere una soluzione numerica si procede discretizzando lo spazio ed il tempo. La regione del moto viene suddivisa in  $2^n$  sottointervalli di lunghezza  $\Delta = d/2^{n-1}$ , dove  $n$  è stabilito dalle risorse computazionali disponibili. Ora, all' $i$ -esimo intervallo è associato il vettore della base computazionale  $|i\rangle$  ( $i = 0, \dots, 2^n - 1$ ) di un sistema di  $n$  qubit. Si è così realizzata una approssimazione dello spazio di Hilbert originario,  $\infty$ -dimensionale, a  $\mathbb{C}^{2^n}$  costituito da funzioni d'onda discretizzate della forma

$$\psi_d(t) = C \sum_{i=0}^{2^n-1} \psi(x_i, t) |i\rangle,$$

con

$$x_i = -d + (i + \frac{1}{2}) \Delta,$$

dove  $C$  è la costante di normalizzazione. Nel contempo l'Hamiltoniano originario del sistema continuo assume implicitamente la forma discretizzata  $\mathbf{H}_d = \sum_{i=0}^{2^n-1} \mathbf{H}_i$ . Come noto gli operatori momento e posizione sono soggetti alla disuguaglianza di Heisenberg, ovvero  $\mathbf{p}_x$  e  $\mathbf{x}$  sono osservabili incompatibili. Questo si riflette nel fatto che  $[\mathbf{H}_i, \mathbf{H}_j] \neq 0$ . A sua volta per calcolare l'operatore di evoluzione approssimato non può valere una espressione ingenua, per esempio

$$e^{-\frac{i}{\hbar} \mathbf{H}_d t} \neq \prod_{i=0}^{2^n-1} e^{-\frac{i}{\hbar} \mathbf{H}_i t}.$$

Qui viene in soccorso la cosiddetta formula di Trotter per una coppia  $\mathbf{A}, \mathbf{B}$  di operatori

hermitiani:

$$\lim_{k \rightarrow \infty} \left( e^{i\mathbf{A}t/k} e^{i\mathbf{B}t/k} \right)^k = e^{i(\mathbf{A}+\mathbf{B})t}$$

che, a meno di contributi di secondo ordine nel passo temporale  $\Delta t$ , consente di scrivere

$$e^{-\frac{i}{\hbar} \left( \frac{\mathbf{p}_x^2}{2m} + V(\mathbf{x}) \right) \Delta t} \approx e^{-\frac{i}{\hbar} \frac{\mathbf{p}_x^2}{2m} \Delta t} e^{-\frac{i}{\hbar} V(\mathbf{x}) \Delta t} = U_F^\dagger e^{-\frac{i}{\hbar} \frac{\mathbf{p}_x^2}{2m} \Delta t} U_F e^{-\frac{i}{\hbar} V(\mathbf{x}) \Delta t},$$

dove nel secondo passaggio si è usata la rappresentazione di posizione e  $U_F$  rappresenta l'operatore unitario Trasformata di Fourier Quantistica, che sarà discussa in dettaglio in una successiva sezione. Di fatto essa rappresenta l'analogo sullo spazio dei qubit dell'abituale Trasformata di Fourier, la quale produce il cambiamento dalla base di posizione  $\{|x\rangle\}$  in quella di momento  $\{|p\rangle\}$ .

Gli altri operatori presenti agiscono diagonalmente sugli stati di qubit, cioè come  $e^{-\frac{i}{\hbar} V(\mathbf{x}) \Delta t} |i\rangle = e^{-\frac{i}{\hbar} V(x_i) \Delta t} |i\rangle$  e analogamente per l'operatore nello spazio dei momenti.

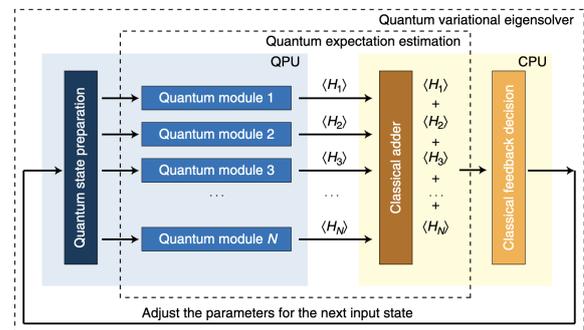
Tutti questi operatori possono essere implementati per mezzo di  $2^{n-1}$  porte di fase controllate  $n - 1$  volte, descritte nelle precedenti sezioni. Da questo punto di vista il metodo risulta ancora inefficiente, perché le risorse computazionali necessarie crescono esponenzialmente con la precisione desiderata nel calcolo. D'altra parte lo stato è descritto ed evoluto in parallelo con solo  $n$  qubit, piuttosto che dai  $2^n$  valori della funzione d'onda. Per potenziali non troppo complessi, i primi studi hanno dimostrato che un simulatore quantistico con una decina di qubit è abbastanza robusto contro gli errori, ma per eseguire il calcolo occorrerebbero  $O(10^4)$  porte quantistiche elementari, che sono ancora una sfida per un vero computer quantistico. Sviluppi in quest'area di ricerca sono ancora attuali [84, 85].

La lezione appresa dalla precedente procedura suggerisce che esiste un ampio spettro di tecniche quantistiche per lo studio di equazioni e modelli di Fisica, ma che esse stesse vanno studiate per coglierne gli aspetti più vantaggiosi per gli scopi ai quali sono destinate. Questo ha portato ad una nuova classe di algoritmi ibridi.

Per citare un esempio sappiamo che per trovare l'autovalore di un Hamiltoniano, potremmo usare l'algoritmo di Stima della Fase

Quantistica, che analizzeremo nel seguito. In linea di principio con tale metodo si potrebbe ottenere l'intero spettro degli autovalori e i corrispondenti autostati. Inoltre, per i problemi di Materia Condensata o di Teoria dei Campi, nella maggior parte dei casi siamo interessati principalmente allo stato fondamentale. Tuttavia, per un'Hamiltoniano generico l'implementazione di una porta  $U$  controllata potrebbe non essere semplice. Per problemi realistici, la stima della fase quantistica richiede una grande profondità del circuito, il che implica la necessità di un lungo tempo di coerenza dei qubit, non disponibile con la tecnologia della NISQ era.

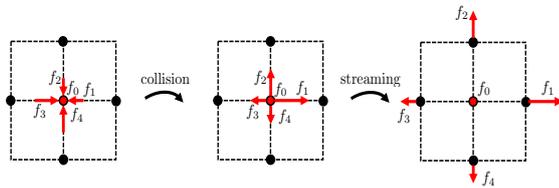
Per superare queste limitazioni, è stato recentemente introdotto il metodo Variazionale agli autovalori quantistici (VQES) [86, 87]. Esso è un algoritmo ibrido, la cui idea di base è quella di sfruttare i vantaggi sia dei computer quantistici che di quelli classici, facendo risolvere al computer quantistico la parte di calcolo che esso può eseguire efficientemente, mentre si assegnano al computer classico compiti risolvibili con algoritmi di per sé efficienti.



**Figura 8:** Diagramma di flusso dell'implementazione del risolutore di autovalori VQES, che utilizza un circuito ibrido classico-quantistico. La figura è adottata da [88]

In un contesto di Fisica Classica è noto che le simulazioni di fluidodinamica richiedono le nostre più potenti risorse computazionali e i computer quantistici offrono l'opportunità di accelerare gli algoritmi tradizionali. È stato mostrato [89, 90] che i metodi numerici su mesoscala, del tipo Automa di Gas Reticolare (LGA) o il metodo del Reticolo di Boltzmann (LBM), possono essere eseguiti con algoritmi quantistici efficienti. L'algoritmo è stato validato simulando

due equazioni alle derivate parziali (PDE) canoniche: l'equazione di Diffusione e quella di Burgers (un analogo semplificato dell'equazione di Navier-Stokes, comunque nonlineare) con diversi simulatori quantistici. È naturale in questo



**Figura 9:** Le principali operazioni consentite su un Gas Reticolare di Boltzmann: collisione flusso. Esse possono essere rappresentate in un circuito quantistico che agisce su un insieme di qubit. La figura è ripresa da [89]

contesto cercare di risolvere anche equazioni differenziali classiche con metodi quantistici, il che ha prodotto una messe di risultati ancora da approfondire, per quanto riguarda la loro efficienza e robustezza rispetto agli errori [91, 92]. D'altro canto si è già citato in precedenza che si stanno sviluppando tecnologie di calcolo di multi-fisica basati su queste idee.

## L'algoritmo di Deutsch

Il prototipo ed anche il più semplice algoritmo quantistico è quello di Deutsch [93], che consiste nel risolvere il seguente problema decisionale: data una funzione booleana

$$f : \{0, 1\} \rightarrow \{0, 1\}$$

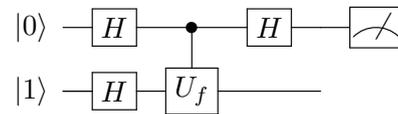
stabilire se essa sia costante o **bilanciata**. Con questo termine si intende dire che la funzione assume i valori 0 o 1 in uguale numerosità. È chiaro che nel caso delle classe delle funzioni considerate la risposta è immediata, perché esistono in totale quattro di esse :

$$f_1(x) \equiv 1, f_2(x) \equiv 0, f_3(x) = x, f_4(x) = \bar{x} ,$$

cioè due costanti e due bilanciate. Tuttavia, volendo esercitarsi a sviluppare un algoritmo apposito si deve inventare una opportuna porta logica

$$U_f : |x\rangle |y\rangle \rightarrow |x\rangle |y \oplus f(x)\rangle , \quad (9)$$

detta **oracolo**, perché fornisce una risposta al problema senza che entri in una successione di verifiche sui singoli argomenti  $x$ . Per vedere come agisce l'algoritmo, si osservi in primo luogo che dalla sua definizione l'oracolo dipende dalla funzione  $f$  e la sua azione, su una coppia di qubit, produce uno stato da essa dipendente. Precisamente, realizzando il seguente circuito



lo stato inizialmente separato evolverà in un altro, anch'esso separato, secondo i seguenti passaggi

$$\begin{aligned} & |0\rangle |1\rangle \xrightarrow{H \otimes H} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) (|0\rangle - |1\rangle) \\ & \xrightarrow{U_f} \frac{1}{\sqrt{2}} (|0\rangle |f(0)\rangle - |0\rangle |\overline{f(0)}\rangle + |1\rangle |f(1)\rangle - |1\rangle |\overline{f(1)}\rangle) = \\ & \frac{1}{\sqrt{2}} ( (-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle ) (|0\rangle - |1\rangle) \\ & \xrightarrow{H} \frac{1}{\sqrt{2}} [ ( (-1)^{f(0)} + (-1)^{f(1)} ) |0\rangle + \\ & ( (-1)^{f(0)} - (-1)^{f(1)} ) |1\rangle ] \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) . \end{aligned}$$

Si osservi che i valori della funzione  $f$  sono stati calcolati in parallelo su tutti gli argomenti  $x \in \{0, 1\}$  e trasferiti nelle fasi delle ampiezze del vettore di stato nel primo registro <sup>1</sup>.

Procedendo ora ad effettuare una misurazione sul primo qubit, evidenziato dal simbolo di misura nella rappresentazione circuitale, si ottengono le due alternative

$$\begin{cases} |0\rangle \Rightarrow f(0) = f(1) & f \text{ costante} \\ |1\rangle \Rightarrow f(0) \neq f(1) & f \text{ bilanciata} \end{cases} ,$$

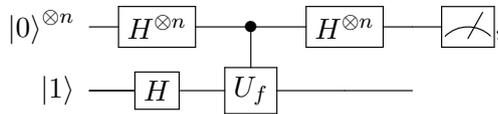
il che fornisce una risposta univoca al problema posto.

Il punto da sottolineare qui è che per ottenere questo risultato è stato sufficiente applicare una sola volta l'algoritmo quantistico, mentre classicamente avremmo dovuto calcolare  $f$  due volte. Questo dà un senso al termine oracolo: il calcolo della funzione  $f$  è effettuato in parallelo su tutti i possibili input descritti dal registro dei qubit di ingresso.

<sup>1</sup>Per registro si intende un gruppo di qubit i cui stati iniziale e finale sono separati da quelli dei restanti qubit. In questo caso il primo qubit da sinistra verso destra nella notazione di Dirac, o dall'alto verso il basso nella notazione circuitale.

## Variazioni sul tema

Il vantaggio computazionale è modesto nell'esempio di Deutsch, ma si può enfatizzare nel caso si debba decidere se una funzione booleana sia costante o bilanciata su  $\mathbb{Z}_2^n$ , ovvero  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ . Il corrispondente algoritmo di Deutsch - Josza, rappresentato dal circuito



produce uno stato finale (prima della misura) della forma

$$\frac{1}{2^n} \sum_{x, y=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} |y\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}},$$

con

$$x \cdot y = (x_1 y_1) \oplus (x_2 y_2) \oplus \dots \oplus (x_n y_n).$$

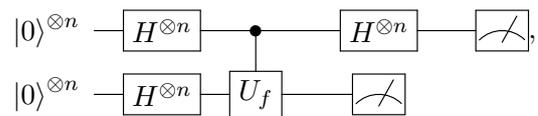
Come nel caso precedente, i valori della funzione  $f$  su  $\mathbb{Z}_2^n$  simultaneamente calcolati vanno a definire le fasi dei coefficienti di tutti gli elementi del primo registro di qubit, inizialmente posti a  $|0\rangle^{\otimes n} = |0\rangle$ . Nello stato finale essi potrebbero assumere tutti i possibili valori della base computazionale  $|y\rangle = |0\rangle, \dots, |2^n - 1\rangle$ . Se a questo punto si procedesse alla misura di tale registro, potrebbe accadere di ottenere  $y = 0$ . Ma, da un'analisi delle ampiezze, questo si verifica solo se la funzione  $f$  è costante, mentre non può ottenersi nel caso fosse bilanciata, perché in questo caso i contributi alla sua ampiezza sarebbero in egual numero  $\pm 1$ .

Osserviamo ora che in un algoritmo classico, verificato che per due valori diversi dell'argomento una funzione  $f$  assume valori distinti, se ne conclude con certezza che essa non è costante. Ma per verificare che la funzione sia effettivamente costante, dovremo calcolarla per tutti i  $2^n$  valori dell'argomento. Diversamente, il calcolo quantistico fornisce una risposta definita in un solo passaggio. In questo senso (se pretendiamo la certezza assoluta) potremmo dichiarare di essere di fronte ad un'accelerazione esponenziale della procedura quantistica.

In realtà la questione è più sottile, perché è possibile trovare algoritmi classici probabilistici, che risolvono questo problema con probabilità  $1 - \epsilon$

con un numero di verifiche  $k = O(-\log_2 \epsilon)$ , cioè di complessità crescente a potenza con il numero di input in ingresso (classe BPP). Il problema non è in effetti veramente difficile e l'algoritmo quantistico fornisce solo un incremento relativo in velocità di computazione.

Sulla linea concettuale di Deutsch si sono sviluppati algoritmi di maggiore complessità computazionale. Qui basti citare quello di Simon [94], che consiste nel determinare il periodo  $a \in \{0, 1\}^n$  di una funzione booleana  $f_a : \{0, 1\}^n = \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ . Da un punto di vista classico questo è un problema NP, cioè difficile, ma consideriamo il circuito quantistico



dove si usa l'oracolo (9) secondo la relazione

$$\left[ \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle \right] |0\rangle \xrightarrow{U_f} \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |f(x)\rangle.$$

Applicandolo un numero sufficiente di volte ed effettuando la seguente misura sul primo registro, il problema si riduce a risolvere un sistema lineare omogeneo di  $n$  equazioni per l'incognita  $a$ . Quindi abbiamo trovato un esempio in cui, trovato un particolare oracolo quantistico, possiamo risolvere un problema in tempo polinomiale sfruttando il parallelismo quantistico, mentre è necessario un tempo esponenziale con algoritmi classici. In termini di classi di complessità computazionale si è dimostrato che  $\text{BQP} \neq \text{BPP}$ .

## La Trasformata di Fourier Quantistica e la Stima di Fase

### La QFT

L'algoritmo di Simon offre un ottimo esempio di tecnica basata sull'amplificazione di ampiezza per ridurre un problema effettivamente difficile. Allora ci si può chiedere se sia possibile formulare analoghi algoritmi anche per problemi più complessi, quali la determinazione del periodo di funzioni definite su  $\mathbb{Z}_{2^n}$ . In questo caso, l'algoritmo classico ben noto, ed ampiamente utilizzato in tutti i domini della Scienza, è la Trasformata di Fourier, nella sua versione discreta, nota come Fast Fourier Transform (FFT). Ora, l'i-

dea chiave è che la trasformata di Fourier può essere valutata anche da un circuito quantistico efficiente [95, 96, 97]. La trasformata quantistica di Fourier (QFT) sfrutta la potenza del parallelismo quantistico per ottenere un'accelerazione esponenziale della FFT.

La QFT è definita dalla trasformazione unitaria

$$U_F |x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \exp[2\pi i x y / 2^n] |y\rangle, \quad (10)$$

per cui agisce su un generico vettore di stato secondo la regola

$$U_F \sum_x a(x) |x\rangle = \sum_x A(x) |x\rangle,$$

dove

$$A(x) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} a(k) \exp\left(2\pi i \frac{kx}{N}\right).$$

Esattamente producendo la trasformata di Fourier di una data funzione  $a(x)$ . Inoltre, ricordando la corrispondenza tra numeri in notazione binaria ed elementi della base computazionale data da

$$x = \sum_{k=0}^n \xi_k 2^k \leftrightarrow |x\rangle = |\xi_n, \dots, \xi_1, \xi_0\rangle,$$

e introducendo la notazione abbreviata

$$\bigotimes_{\ell=0}^n |i_\ell\rangle = |i_0\rangle \otimes |i_1\rangle \otimes \dots \otimes |i_n\rangle,$$

l'azione di  $U_F$  può essere espressa anche nella forma

$$U_F |x\rangle = \frac{1}{2^{n/2}} \bigotimes_{\ell=0}^n \left[ |0\rangle + e^{2\pi i \sum_{k=0}^{\ell-1} \frac{\xi_k}{2^{\ell-k}}} |1\rangle \right].$$

In altre parole la QFT porta ogni stato della base computazionale in uno stato non *entangled* di  $n$  qubit. Non sembra quindi un'impresa così difficile implementarlo.

La QFT per 1-qubit coincide con la porta di Hadamard  $H$ , definita in (8). Per calcolare la QFT per un sistema multi-qubit si può adottare una procedura ricorsiva, già nota per la FFT, della

forma

$$U_F^{(k)} = (H \otimes \mathbf{1}_{2^{k-1}}) \left( |0\rangle\langle 0| \otimes \mathbf{1}_{2^{k-1}} + |1\rangle\langle 1| \otimes D^{(k-1)} \right) \left( \mathbf{1}_2 \otimes U_F^{(k-1)} \right) R^{(k)},$$

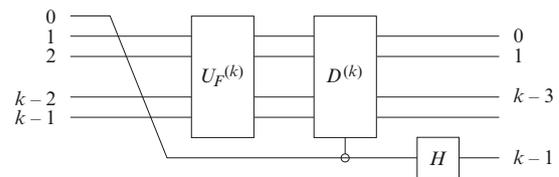
dove sono ora coinvolti gli operatori

$$D^{(k)} = D^{(k-1)} \otimes \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^{k+1}}\right) \end{pmatrix},$$

e

$$R^{(k)} = \sum_{i=0}^{2^k-1} \left( |i\rangle\langle 2i| + |i+2^k\rangle\langle 2i+1| \right).$$

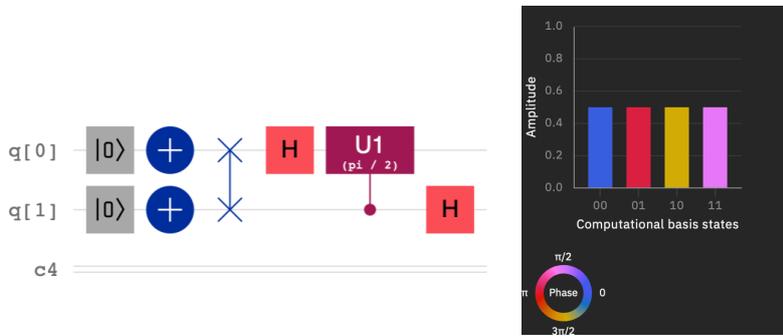
Quest'ultimo operatore è interpretabile come una successione di permutazioni tra qubit e, pertanto, si può implementare con delle porte SWAP. Il corrispondente circuito quantistico è



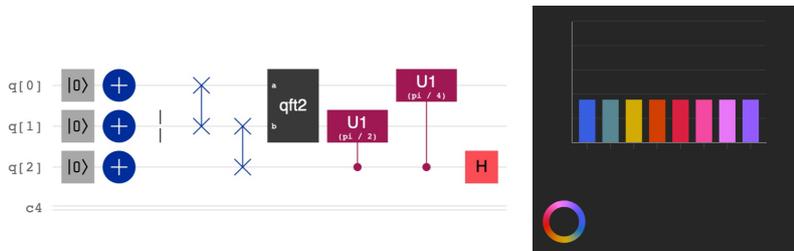
In conclusione la QFT può essere implementata con un numero di risorse computazionali  $O(n^2)$ , contro le  $O(n2^n)$  richieste da FFT. Questo naturalmente non può che aumentare significativamente l'impatto sulle capacità di calcolo in tutte le innumerevoli applicazioni in cui la Trasformata di Fourier svolga un ruolo importante.

## La Stima della Fase

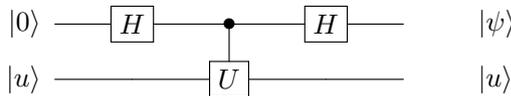
Consideriamo ora il problema della Stima della Fase discusso in [97]. In generale, gli autovalori di un operatore unitario sono della forma  $e^{2\pi i \phi}$ . A meno che esso non sia anche hermitiano, come gli operatori di Pauli, tali autovalori non sono direttamente misurabili. Tuttavia, si può considerare il seguente circuito dove  $|u\rangle$  denota il corrispondente autovettore di  $U$  e  $|\psi\rangle = \cos(\pi\phi)|0\rangle + i \sin(\pi\phi)|1\rangle$ . Come abbiamo discusso nel problema di Deutsch, questa procedura distingue con certezza tra  $\phi = \pm 1$ , ma per altri suoi valori si ha una minore confidenza



**Figura 10:** La  $U_F^{(2)}$  applicata allo stato  $|\bar{0}, \bar{0}\rangle = |1, 1\rangle$ . Nel pannello a destra si riportano le ampiezze dei vettori della base computazionale, di modulo  $1/2$ , e le corrispondenti fasi. La porta H a sinistra svolge il ruolo di  $QFT^{(1)}$ . La porta NOT è simboleggiata da  $\oplus$  in blu.



**Figura 11:** The  $QFT^{(3)}$  applicata  $|\bar{0}, \bar{0}, \bar{0}\rangle = |111\rangle$ . Nel pannello a destra si riportano le ampiezze dei vettori della base computazionale, di modulo  $2^{-3/2}$ , e le corrispondenti fasi. Si osservi che essa è costruita ricorsivamente su  $QFT^{(2)}$ . La porta NOT è simboleggiata da  $\oplus$  in blu.

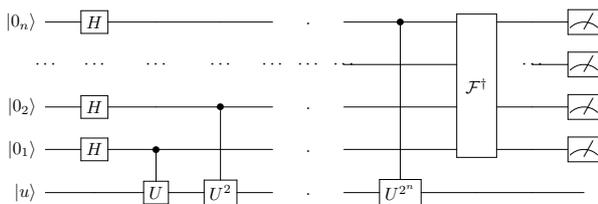


Se la rappresentazione binaria

$$\phi = \sum_{k=1}^{\infty} \frac{\phi_k}{2^k} ,$$

statistica e sarà necessario ripetere molte volte il calcolo. C'è una maniera per evitarlo.

Supponiamo di avere un registro di  $n$  qubit e si ricordi che se  $|u\rangle$  è un autovettore di un operatore  $U$  unitario, lo è anche di  $U^{2^j}$  con autovalore  $e^{2^j 2\pi i \phi}$ . Ora si implementa il circuito tracciato in Fig. 12 Nei primi  $n$ -qubit di controllo viene



**Figura 12:**

generata la sovrapposizione

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle .$$

A loro volta, ogni  $c = U^{2^j}$  produce il contributo

$$\frac{1}{\sqrt{2}} (|0_j\rangle + |1_j\rangle) |u\rangle$$

$$\xrightarrow{c=U^{2^j}} \frac{1}{\sqrt{2}} (|0_j\rangle + e^{2\pi i 2^j \phi} |1_j\rangle) |u\rangle .$$

con  $\phi_k \in \{0, 1\}$ , si troncasse ai primi  $n$  termini, o la si assumesse come una approssimazione accettabile, tenendo conto che eventuali termini nella somma con potenze positive di 2 non contribuiscono alla fase, l'intero registro si porrebbe nello stato

$$|0_n \dots, 0_2, 0_1\rangle \longrightarrow$$

$$\frac{1}{2^{n/2}} \left( |0_n\rangle + e^{2\pi i \frac{\phi_n}{2}} |1_n\rangle \right) \otimes \dots$$

$$\dots \otimes \left( |0_1\rangle + e^{2\pi i \sum_{k=1}^n \frac{\phi_k}{2^k}} |1_1\rangle \right) ,$$

analogo allo sviluppo per la trasformata di Fourier  $U_F$  visto in precedenza. Quindi, usando l'inverso della QFT (indicato con  $\mathcal{F}^\dagger$  in Fig. 12, si può ottenere lo stato  $|\phi\rangle = |\phi_n, \dots, \phi_1\rangle$ , che rappresenta la fase  $\phi$  se avesse solo  $n$  cifre significative. In generale, una misurazione di tutti gli  $n$  qubit di controllo fornirà i valori  $\phi_k$  con  $k = 1, \dots, n$  e, quindi,  $\phi$  con accuratezza  $2^{-(n+\log_2 2\epsilon)}$ , dove  $1 - \epsilon$  è la probabilità di ottenere un'approssimazione con precisione  $2^{-n}$ .

## Ordine, Fattorizzazione e algoritmo di Shor

Gli algoritmi appena presentati possono essere utilizzati per risolvere una grande varietà di problemi interessanti. Tra di essi il problema di fattorizzazione degli interi e quello, ad esso collegato, del problema della ricerca dell'ordine di un intero nell'aritmetica modulare. Al di là dell'interesse strettamente matematico per essi, c'è anche quello applicativo legato alla possibile violazione dei sistemi crittografici a chiave pubblica tipo RSA [98].

L'obiettivo è valutare efficientemente la funzione esponenziale negli interi di base  $a$ , co-primo di  $M$ , nell'aritmetica  $\text{mod } M$

$$f_{M,a}(x) = a^x \text{ mod } M, \quad \text{GCD}(a, M) = 1,$$

avendo indicato con  $\text{GCD}$  il Massimo Comune Divisore.

Per esemplificare, riportiamo l'insieme dei valori delle seguenti funzioni:

$$\{f_{15,7}(x)\} = \{7, 4, 13, 1, 7, 4, 13, 1, 7, 4, 13, 1, 7, 4\}$$

$$\{f_{17,3}(x)\} = \{3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1\}$$

L'insieme dei valori di  $f_{M,a}(x)$  è un gruppo rispetto alla moltiplicazione  $\text{mod } M$ , il che comporta che deve esistere un qualche intero  $r$  per il quale

$$a^r = 1 \text{ mod } M.$$

Il più piccolo di tali numeri  $r$  è chiamato l'**ordine** di  $a \text{ mod } M$  ed è evidentemente il periodo della funzione  $f_{M,a}(x)$ . Riferendoci agli esempi precedenti, per ispezione l'ordine di  $f_{15,7}$  è 4, mentre quello di  $f_{17,3}$  è 16. Ma se i numeri  $M$  ed  $a$  sono molto grandi, il compito di determinare  $r$  può essere arduo nel senso NP.

A questo stadio può essere stabilita la connessione tra il calcolo dell'ordine e il problema della Fattorizzazione di un intero  $M$ , sintetizzandola nella procedura generale di risoluzione presentata nel riquadro sopra.

I Passi 1, 2 e 3 si possono eseguire con un dispendio di risorse computazionali che crescono con una potenza del numero in input, quindi efficientemente, da un algoritmo classico. Il punto cruciale è quindi il calcolo di  $r$  al Passo 4.

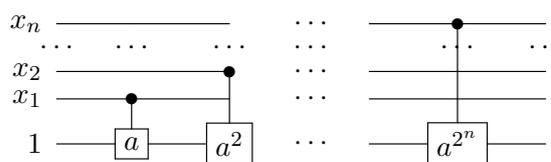
### Passi dell'algoritmo di Shor

Passo	Operazione
1	Se $M$ Pari, ritorna 2.
2	Se $M = p^m$ con $p$ Primo, ritorna $p$ .
3	Scegliere a caso $3 \leq a \leq M - 1$ : se $\text{GCD}(a, M) > 1$ ritorna $\text{GCD}(a, M)$ .
4	Calcolare l'ordine $r$ di $f_{M,a}$
5	Se $r$ è Pari e $f_{M,a}\left(\frac{r}{2}\right) \neq M - 1$ , ritorna $\text{GCD}(a^{r/2} \pm 1, M) \neq 1$
6	Se $r$ è Dispari, oppure $f_{M,a}\left(\frac{r}{2}\right) = M - 1$ , tornare al Passo 3

Tornando al calcolo della funzione  $f_{M,a}$  e usando ancora una volta la rappresentazione binaria  $x = \sum_{k=0}^n \xi_k 2^k$ , esso può essere espresso anche nella forma

$$f_{M,a}(x) = (a^{2^n})^{\xi_n} (a^{2^{n-1}})^{\xi_{n-1}} \dots (a^{2^0})^{\xi_0} \text{ mod } M.$$

Questa formula è efficientemente implementabile anche su un computer classico. Si può dimostrare che il numero di potenze da calcolare è dell'ordine  $m \sim O(\log_2 M)$  e, in definitiva, la funzione  $f_{M,a}(x)$  può essere valutata con un circuito classico di dimensione  $O((\log_2 M)^3)$  avente la struttura simbolica presentata in Fig. 13. Ma esso non rappresenta un algoritmo quanti-



**Figura 13:** Circuito classico per calcolare l'esponentiale modulare di  $a^x$

stico, in quanto non è costituito da trasformazioni unitarie. D'altra parte, per trovare l'ordine  $r$  si dovrebbero calcolare tutti i possibili valori di  $f_{M,a}(x)$  ed estrarlo poi con la tecnica della Trasformata di Fourier.

Ora siamo nelle condizioni per illustrare l'algoritmo di Shor [95], la cui prima realizzazione sperimentale fu riportata in [96]. L'idea è di as-

sociare ad un intero  $a$  coprìmo di  $M$  di ordine  $r$ , per ora incognito, l'operatore unitario

$$U_a : |x\rangle \rightarrow |ax \pmod M\rangle, \\ x \in \{0, 1, \dots, M-1\}.$$

Per esso si dimostra che la famiglia di vettori di stato

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[-\frac{2\pi i s k}{r}\right] |a^k \pmod M\rangle,$$

con  $0 \leq s \leq r-1$ , è costituita da suoi autovettori, con autovalori

$$\exp\left[-\frac{2\pi i s}{r}\right],$$

analoghi agli stati in (10) e indicativi della riduzione del problema dell'ordine a quello della stima della fase. Ma per quest'ultima ci sono due importanti requisiti da rispettare: 1) si devono avere procedure efficienti per implementare le operazioni di tipo  $c-U^{2^j}$  per qualsiasi intero  $j$ , 2) bisogna essere in grado di preparare in modo efficiente un autostato  $|u_s\rangle$ , o almeno una sovrapposizione di essi. Il primo requisito può essere soddisfatto ispirandosi alla procedura riportata nelle Figure 13 e 14. Usando un certo numero di qubit ausiliari è semplice costruire un circuito quantistico con due registri con almeno  $L = \log_2 M$  qubit, che calcolano la trasformazione

$$c-U_a : |z\rangle |y\rangle \rightarrow |z\rangle |a^z y \pmod M\rangle.$$

Il secondo requisito è più difficile da soddisfare, poiché dipende dalla conoscenza di  $r$ . L'idea si basa sull'osservazione che

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_k\rangle = |1\rangle,$$

e lo stato  $|1\rangle$  è semplice da realizzare. Quindi, utilizzando

$$t = 2L + 1 + \log\left[2 + \frac{1}{(2\epsilon)}\right]$$

qubit nel primo registro (con riferimento alla Figura 13) e preparando il secondo registro nello stato  $|1\rangle$ , con probabilità  $(1 - \epsilon)/r$  si ottiene una stima della fase  $\phi \approx s/r$  per ogni  $0 \leq s \leq r-1$  con l'accuratezza di  $2L + 1$  bit. Non abbiamo

ancora  $r$ , ma sappiamo che a priori  $\phi$  è un numero razionale con  $r$  al denominatore. Perciò se potessimo calcolare la frazione più vicina a  $\phi$  potremmo anche ottenere  $r$ . Poiché ottenere la stima della fase con l'accuratezza di  $2L + 1$  bit significa che

$$|\phi - s/r| \leq 2^{-(2L+1)},$$

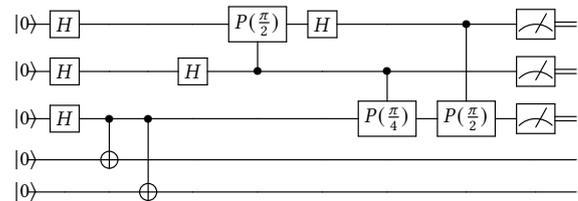
e, poiché  $r \leq M \leq 2^L$ , si ha anche che  $1/2r^2 \geq 2^{-(2L+1)}$ , ovvero

$$|\phi - s/r| \leq \frac{1}{2r^2}.$$

Questa relazione è sufficiente per garantire che  $s/r$  sia un convergente dello sviluppo in frazioni continue di

$$\phi = \frac{1}{p_1 + \frac{1}{p_2 + \frac{1}{\dots}}}.$$

Quindi, dallo sviluppo in frazione continue di  $\phi$  è possibile estrarre un convergente  $s'/r'$  costituito da coprìmi tra loro, per i quali vale anche  $s'/r' = s/r$ . Se si verifica che  $a^{r'} = 1 \pmod M$ , allora  $r' = r$  è l'ordine ricercato. Se così non fosse,  $s$  ed  $r$  devono avere un fattore comune. Ma è possibile dimostrare che se si ripete l'algoritmo almeno  $2 \log M$  si otterrà con alta probabilità  $s/r$  co-primi tra loro.



**Figura 14:** Il circuito ottimizzato in [96] che realizza l'algoritmo di Shor per fattorizzare  $M = 15$  con  $a = 11$ .

L'algoritmo di Shor è un caso particolare di un più generale algoritmo quantistico, discusso da Kitaev per la prima volta [97] e poi esteso ed ottimizzato in [99], che risolve il problema di Sottogruppo Nascosto. Senza entrare in nessun dettaglio, ma solo per mostrare il suo carattere generale, tale problema può essere enunciato come segue:

“sia  $f$  una funzione da un gruppo  $G$  a un insieme finito  $X$ , tale che essa sia

costante sui coset di un sottogruppo  $K$  e distinta su ciascuno di essi. Trovare il sottoinsieme generatore di  $K$ , usando un oracolo quantistico che esegue la trasformazione unitaria  $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$ , per  $g \in G$  e  $h \in X$ . ”

## L' algoritmo di Grover

L' algoritmo di Grover [6] consente di trovare (con probabilità  $> 1/2$ ) uno specifico elemento all'interno di un database disordinato, costituito da  $N$  oggetti, usando  $O(\sqrt{N})$  operazioni, mentre un computer classico richiederebbe  $O(N)$  operazioni per raggiungere lo stesso obiettivo. Pertanto, l' algoritmo di Grover fornisce un' accelerazione quadratica rispetto a un algoritmo classico ottimale. È stato anche dimostrato [100] che l' algoritmo di Grover è ottimo, nel senso che nessuna macchina di Turing quantistica può farlo con un numero inferiore di operazioni.

Sebbene l' algoritmo di Grover sia comunemente considerato utile per la ricerca in un database, le idee di base di questo algoritmo sono applicabili in un contesto molto più ampio. Questo approccio può essere utilizzato per accelerare gli algoritmi di ricerca in cui si potrebbe costruire un oracolo quantistico che distingue l' ago dal pagliaio. L' implementazione dell' oracolo può es-

sere ridotta alla costruzione di un circuito quantistico che cambia lo stato di un qubit ausiliario, se esiste una certa funzione  $f$ , definita sull' insieme  $\{x_1, x_2, \dots, x_N\}$ , tale che  $f_*(x) = 0 \forall x_i \neq x^*$  e  $f_*(x) = 1$  se  $x = x^*$ , essendo  $x^*$  l' elemento da trovare.

Si costruisca uno spazio di Hilbert, le cui dimensioni siano  $N = 2^n$  pari al numero di elementi del database, in particolare  $|x^*\rangle$  faccia parte della base computazionale. L' elemento chiave dell' algoritmo di Grover è l' operatore definito da

$$U_\Psi = 2|\Psi\rangle\langle\Psi| - \mathbf{1},$$

dove

$$|\Psi\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle.$$

L' azione di  $U_\Psi$  su un generico elemento dello spazio  $\sum_i a_i |i\rangle$  è

$$U_\Psi \sum_i a_i |i\rangle = \sum_i (2\langle a \rangle - a_i) |i\rangle,$$

dove

$$\langle a \rangle = \frac{1}{N} \sum_i a_i$$

è l' ampiezza media degli stati di base. Questo ci dice che l' ampiezza di ogni singolo stato  $|i\rangle$  è riflessa attorno a tale valor medio.

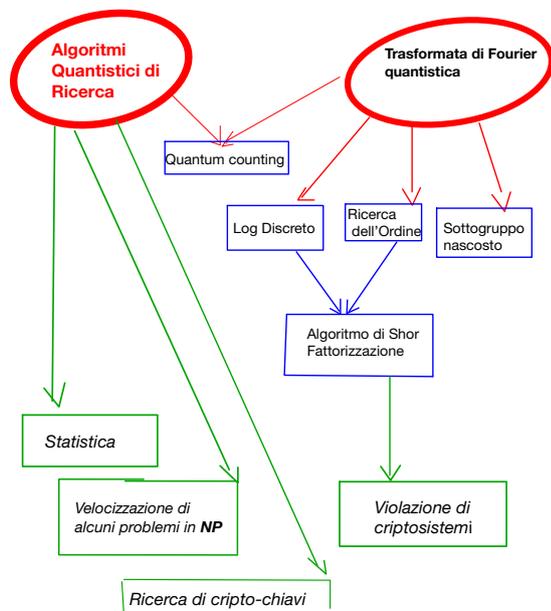
Per poter utilizzare l' operatore di Grover con successo in una ricerca, è necessario che il registro dei qubit di input sia opportunamente inizializzato. Esso viene posto nello stato  $\Psi$  precedentemente introdotto, mentre un qubit ancillare è posto nello stato  $H|1\rangle$ . A questo stadio viene applicato l' oracolo

$$U_{f_*} : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f_*(x)\rangle,$$

il quale lascia immutati tutti gli stati della base computazionale, eccetto che per  $x^*$  per il quale vale

$$U_{f_*} |x^*\rangle \otimes H|1\rangle = -|x^*\rangle \otimes H|1\rangle,$$

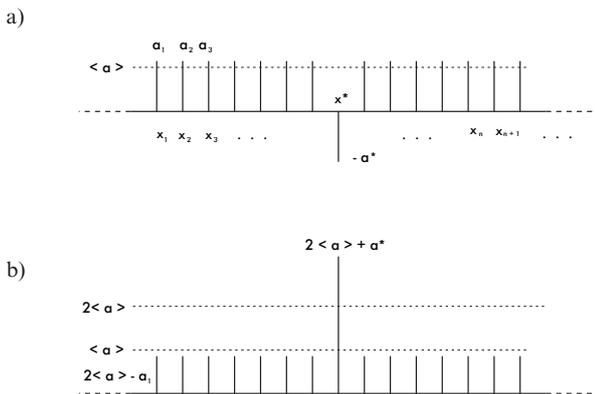
cambiando la fase del qubit ancillare. Combinando questo risultato con l' azione successiva di  $U_\Psi$  si esalta l' ampiezza dello stato  $|x^*\rangle$ , decrementando quelle degli altri elementi di base. Una misura del registro principale di qubit darà  $x^*$



**Figura 15:** Due dei principali Algoritmi Quantistici e le loro relazioni, incluse alcune notevoli applicazioni.

con probabilità vicina a 1, se la precedente successione di operatori è ripetuta un numero circa uguale a  $(\pi\sqrt{N})/4$  volte. Un algoritmo classico assolverebbe allo stesso compito con  $O(N)$  tentativi, quindi Grover costituisce un significativo aumento di efficienza computazionale.

Il metodo di Grover è stato applicato in vari problemi di analisi topologica, quale quello della ricerca di triangoli in grafi costituiti da un fissato numero di nodi [101], o di Intelligenza Artificiale e Machine Learning [102].

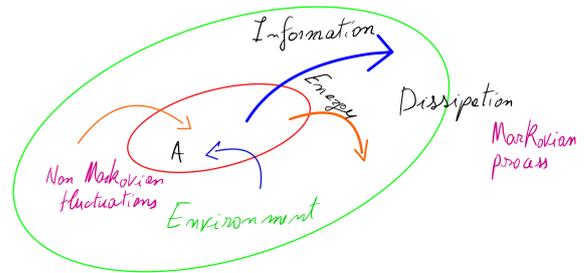


**Figura 16:** Descrizione grafica di un passo di iterazione dell'algoritmo di Grover. L'elemento da trovare è  $x^*$ . In (a) si è cambiato il segno della sua ampiezza attraverso l'azione dell'oracolo  $U_{f_x}$ . In (b) si è eseguita l'inversione rispetto alla media usando  $U_{\Psi}$ .

## Decoerenza

In pratica è impossibile isolare completamente un computer quantistico dal suo ambiente. Si pensi, ad esempio, alle inevitabili fluttuazioni quantistiche del Campo Elettromagnetico interagenti con un dipolo magnetico, che potrebbe fisicamente costituire un qubit utilizzato in un computer quantistico. Questo va visto come un sottosistema di un sistema più ampio, costituito da esso stesso e dall'ambiente in cui è immerso, che sia termico, elettromagnetico o nucleare. Per ambiente si intende un sistema fisico sul quale non abbiamo alcun controllo: non possiamo ricavarne informazioni di dettaglio, mediante misurazioni o applicarvi azioni di controllo, ma al più valori medi statistici di alcune grandezze interpretate macroscopicamente. In alcuni casi, l'effetto di un'interazione ambientale sul sottosistema

computazionale è reversibile, ma in generale produce l'effetto irreversibile della decoerenza. Nella decoerenza, l'informazione codificata nello stato del sottosistema computazionale viene persa nell'ambiente. Pertanto tali errori sono gravi e varie strategie di correzione degli errori, come la ridondanza tripla da un punto di vista computazionale, o comunque l'estensione per quanto possibile del tempo di decoerenza.



**Figura 17:** L'insieme dei qubit utilizzati nella computazione è rappresentato da A, mentre *Environment* è l'ambiente con il quale essi vengono a contatto. L'Energia è certamente scambiata in maniera incoerente tra A ed *Environment*, ma anche l'Informazione può fluire irreversibilmente da A verso *Environment*, a causa della decoerenza degli stati puri. Nella situazione più semplice si avranno processi Markoviani. Se le interazioni A-*Environment* godono di una certa memoria si avranno processi non Markoviani e fenomeni di revival degli stati precedenti in A.

Sono state sviluppate varie tecniche per la descrizione dei processi di decoerenza nei sistemi computazionali, per comprenderne le caratteristiche e verificare la tolleranza, o robustezza, dei sistemi rispetto ad essa. Nonché per concepire metodi di correzione degli errori quantistici ad essa dovuti e contrastarne gli effetti.

L'idea base consiste nel pensare A e *Environment* come un unico sistema isolato *entangled* (vedi Fig. 17), a causa delle interazioni reciproche, le cui azioni sono espresse da operatori unitari. Allo stesso tempo l'*Environment* può essere anche visto come un osservatore del sistema computazionale A, saggiandone costantemente tutta una serie di proprietà osservabili. L'*entanglement* però modifica le probabilità di osservare un certo esito in una misura sul sottosistema A. Il che, per essere descritto correttamente, richiede una generalizzazione del-

lo schema consueto delle proiezioni ortogonali sugli autostati (vedi Appendice). Questa generalizzazione si esplica nell'esistenza di una famiglia  $\{\mathbf{E}_m\}_{m \in \sigma(\mathbf{O}_A)}$  di Operatori di Misura generalizzati (POVM) associati ad un certo osservabile  $\mathbf{O}_A$ . Gli elementi di tale famiglia godono delle seguenti proprietà:

1. Hermitianità:  $\mathbf{E}_m^\dagger = \mathbf{E}_m$
2. Positività:  $\langle \psi | \mathbf{E}_m | \psi \rangle \geq 0 \quad \forall |\psi\rangle \in \mathcal{H}_A$
3. Completezza:  $\sum_m \mathbf{E}_m = \mathbf{1}_A$

Data una POVM  $\{\mathbf{E}_m\}$  esistono sempre degli operatori, detti di Kraus, che godono delle proprietà

$$\mathbf{Q}_m = \mathbf{U}_m \sqrt{\mathbf{E}_m}, \quad \sum_m \mathbf{Q}_m^\dagger \mathbf{Q}_m = \mathbf{1}_A$$

dove  $\mathbf{U}_m$  sono unitari. Gli operatori di Kraus producono gli stati post-misura. Questo significa che se a seguito della misura si ottiene  $m \in \sigma(\mathbf{O}_A)$ , allora a riduzione del pacchetto d'onda è data da

$$|\psi\rangle \xrightarrow{m} \frac{\mathbf{Q}_m |\psi\rangle}{|\sqrt{\mathbf{E}_m} |\psi\rangle|},$$

o più in generale

$$\rho_m = \frac{\mathbf{Q}_m \rho \mathbf{Q}_m^\dagger}{\text{tr}(\mathbf{Q}_m \rho \mathbf{Q}_m^\dagger)},$$

Una POVM attribuisce probabilità a priori

$$\mathcal{P}_m = \text{tr}(\mathbf{Q}_m \rho \mathbf{Q}_m^\dagger)$$

di ottenere  $m$  nella misura di un dato operatore sullo stato  $\rho$ . Inoltre, c'è completa libertà di scegliere l'operatore  $\mathbf{U}_m$  per ogni  $m$ .

L'introduzione delle POVM consente di studiare, senza riferimento a quanto avvenga in *Environment*, le possibili trasformazioni finite in  $A$  secondo la mappa

$$\rho_A \rightarrow \mathcal{E}(\rho_A) = \sum_m \mathbf{Q}_m \rho_A \mathbf{Q}_m^\dagger.$$

In tal modo, ogni trasformazione finita dello stato di un sistema quantistico in contatto con un *Environment* viene descritta da una mappa lineare completamente positiva e che preserva la traccia (TPCP)  $\mathcal{E}$ . Essa agisce solo sullo stato  $\rho_A$  del sistema computazionale  $A$  e viene detta

**Canale Quantistico.** Si può dimostrare che più Canali Quantistici possono comporsi tra di loro. A differenza degli operatori unitari, in genere i canali quantistici non sono invertibili, quindi essi formano dei semi-gruppi. Per la stessa ragione non è detto che  $\mathcal{E}$  rappresenti una trasformazione unitaria, il che implica la decoerenza e la possibilità di descrivere trasformazioni irreversibili in MQ.

Per fare un semplice esempio, si consideri un modello elementare costituito da un qubit che può subire, per cause non specificate e con uguale probabilità  $p$ , uno dei tre tipi di errore:

1. Bit flip:  $|\psi\rangle \rightarrow \sigma_1 |\psi\rangle$
2. Phase flip:  $|\psi\rangle \rightarrow \sigma_3 |\psi\rangle$
3. Bit-Phase flip:  $|\psi\rangle \rightarrow \sigma_2 |\psi\rangle$

Naturalmente c'è una probabilità  $1-p$  che il qubit rimanga nel suo stato originale. Allora, con una opportuna argomentazione, si possono trovare quattro operatori di Kraus:

$$\begin{aligned} \mathbf{Q}_0 &= \sqrt{1-p} \mathbf{1}_2 & , & \quad \mathbf{Q}_1 = \sqrt{\frac{p}{3}} \sigma_1, \\ \mathbf{Q}_2 &= \sqrt{\frac{p}{3}} \sigma_2 & , & \quad \mathbf{Q}_3 = \sqrt{\frac{p}{3}} \sigma_3 \end{aligned}$$

i quali verificano la condizione di normalizzazione  $\sum_m \mathbf{Q}_m^\dagger \mathbf{Q}_m = \mathbf{1}_2$ . Inoltre, il corrispondente canale quantistico è fornito dalla mappa nella sfera di Bloch

$$\begin{aligned} \rho \rightarrow \rho' &= (1-p) \rho \\ &+ \frac{p}{3} (\sigma_1 \rho \sigma_1 + \sigma_2 \rho \sigma_2 + \sigma_3 \rho \sigma_3) . \end{aligned}$$

Quindi anche se lo stato originario poteva essere puro, la mappa lo fa diventare misto, facendogli perdere coerenza.

Moltissimi altri esempi si possono studiare, quali, ad esempio, singoli qubit accoppiati ad ambienti costituiti da altri qubit, o da oscillatori armonici, oppure da bagni termici variamente specificati. Si possono studiare oscillatori armonici quantistici smorzati, oppure a contatto con bagni termici. Molti esempi e tecniche di studio sono riportati in [47, 106, 105].

Il passaggio successivo consiste nel determinare le equazioni di evoluzione, a tempo continuo, degli stati di sotto-sistemi quantistici a contatto

con un Environment. Sotto le ipotesi di markovianità si ottiene la cosiddetta Master Equation di Lindblad [37, 103, 104]

$$\frac{d\rho}{dt} = -i[\mathbf{H}, \rho] + \sum_{m>0} \left( \mathbf{L}_m \rho \mathbf{L}_m^\dagger - \frac{1}{2} \left\{ \mathbf{L}_m^\dagger \mathbf{L}_m, \rho \right\} \right)$$

dove  $\mathbf{H}$  è l'operatore Hamiltoniano se  $A$  fosse isolato dall'Environment, quindi il primo termine del membro di destra è ovviamente lo stesso dell'equazione di Schrödinger. Gli altri termini invece provengono da operatori di Kraus infinitesimi, chiamati Salti Quantici, e descrivono l'effetto di Environment su  $A$ . Sono essi i responsabili della decoerenza dello stato di  $A$ .

Di questa equazione esiste anche una versione in rappresentazione di Heisenberg per gli osservabili di  $A$ .

Con l'equazione di Lindblad si possono studiare effetti di smorzamento e di depolarizzazione di sistemi quantistici soggetti a dissipazione e/o decoerenza e, quindi, estremamente rilevanti per l'effettiva dinamica di un computer quantistico. A titolo di esempio si consideri l'evoluzione libera di un qubit sotto l'azione di un effetto di smorzamento di ampiezza (una combinazione degli errori 1. e 3. sopra descritti) definito dal salto quantico  $L_1 = \gamma(\sigma_1 + i\sigma_2)/2$  dove  $\gamma > 0$  parametrizza l'intensità della perturbazione esterna. L'evoluzione delle popolazioni (gli elementi diagonali) e delle coerenze (gli elementi fuori diagonale) di  $\rho(t)$  è rappresentato dal grafico di Fig. 18, dove i tempi di decoerenza sono  $T_1 = 1/\gamma$  e  $T_2 = 2/\gamma$  rispettivamente. Come si nota, mentre gli elementi fuori diagonali si annullano, quelli sulla diagonale vanno a dei valori costanti, che debbono sommare a 1. Quindi lo

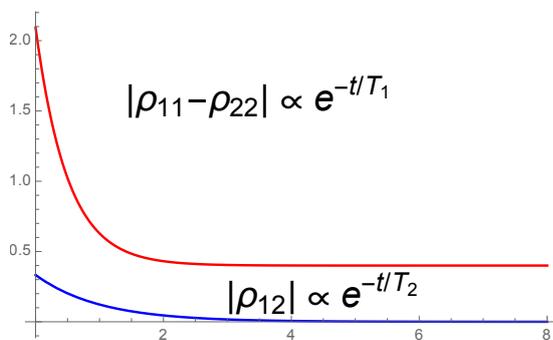


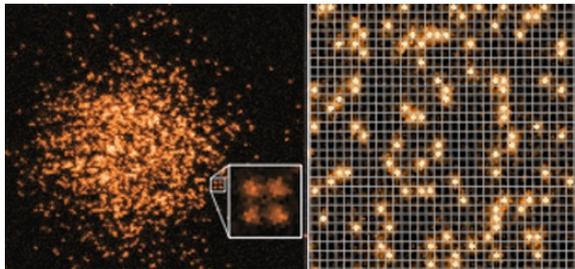
Figura 18

stato finale si decompone solo nelle due possibili configurazioni, senza possibilità di considerare sovrapposizioni quantistiche. Il sistema si è ridotto al comportamento classico.

## Qual è il valore economico della ricerca nelle Tecnologie Quantistiche?

Le tecnologie quantistiche hanno gridato vittoria grazie ad alcuni riconoscimenti di alto profilo nel 2022, quando Alain Aspect, John Clauser e Anton Zeilinger, che hanno lavorato sull'entanglement quantistico nei loro gruppi di ricerca, hanno ricevuto il Premio Nobel per la Fisica. Mentre il loro lavoro scientifico si è svolto effettivamente decenni fa, il progresso tecnologico si è sviluppato poi progressivamente negli anni seguenti. Negli ultimi anni, gli investimenti globali nelle tecnologie quantistiche sono aumentati da poche centinaia di milioni di dollari di dieci anni fa a quasi 2,5 miliardi nel 2022 [108]. Anno in cui IBM ha presentato un processore quantistico da 433 qubit, la macchina Osprey, e prevede di costruire un processore da 4.000 qubit entro il 2025. Un altro esempio è costituito dalla canadese Xanadu [34], che ha utilizzato il suo computer quantistico fotonico, per dimostrare il vantaggio quantistico nel campionamento dei bosoni gaussiani, seguendo i risultati ottenuti in precedenza da altre due squadre.

Tuttavia, accanto a questi riconoscimenti e risultati duramente conquistati si nota un rallentamento della ricerca sulla tecnologia quantistica. In tutto il mondo, nel 2022 sono stati concessi 1.589 brevetti relativi alla tecnologia quantistica, il 61% in meno rispetto al 2021. In effetti, dal 2021 al 2022, il numero di articoli pubblicati sulla tecnologia quantistica è diminuito del 5%. Queste tendenze potrebbero essere un segnale che le sfide rimanenti sono più difficili da risolvere. Forse perché il problema più pertinente e urgente resta tuttora irrisolto: costruire un computer quantistico con un numero e una qualità di qubit sufficienti per garantire che il calcolo non sia compromesso da rumore, ovvero un computer tollerante agli errori. Sebbene le dimensioni dei computer quantistici (in termini di numero di qubit al loro interno) e la fedeltà dei qubit siano



**Figura 19:** Atomi fermionici ripresi utilizzando un microscopio a gas. Il dispositivo consente di trovare la disposizione dei singoli atomi nel reticolo, nonché il loro spin. (K. Wright, Physics 12, 76 (2019) )

cresciute costantemente, ciò non è ancora avvenuto in tandem. In altre parole, un computer quantistico più grande avrà solitamente una fedeltà inferiore rispetto a uno più piccolo. È di questi giorni [107] la notizia che Atom Computing ha realizzato il primo computer quantistico con 1180 qubit, utilizzando lo spin nucleare di atomi neutri di itterbio intrappolati in un reticolo ottico bidimensionale. La compagnia sostiene di poter decuplicare la quantità di qbit in due anni. Inoltre, si afferma che l'insieme di qbit riesca a mantenere un tempo di coerenza dell'ordine del minuto, contro i 70-80  $\mu\text{sec}$  dei sistemi a superconduttore. Se fosse vero, ci troveremmo di fronte ad una pietra miliare nella storia di questa tecnologia.

In ciascuno dei cinque approcci principali ai computer quantistici, permangono sfide impegnative. Ad esempio, i dispositivi basati sulla fotonica continuano a perdere fotoni, con conseguenti errori di calcolo. I dispositivi basati su trappola ionica e atomi neutri non hanno ancora dimostrato la capacità di condurre rapidamente calcoli man mano che il numero di qubit aumenta. I dispositivi a superconduttori devono ancora adattare i propri sistemi di controllo e raffreddamento per gestire potenzialmente migliaia di qubit.

## Appendice: postulati della MQ

Ad un dato sistema fisico sia associato un opportuno spazio lineare (vettoriale)  $\mathcal{H} = \{|\psi\rangle\}$  su  $\mathbb{C}$ ,  $\dim(\mathcal{H}) = d$ , dotato di prodotto scalare hermitiano  $\langle \cdot | \cdot \rangle$ , separabile, completo e di opportuna

dimensione (detto spazio di Hilbert). In questa esposizione supporremo sempre  $d$  finito, anche se in molte circostanze è necessario adottare spazi di dimensione infinita numerabili. Valgono i seguenti postulati:

- Ad ogni stato fisico del sistema corrisponde un unico operatore di **stato**  $\rho$ : hermitiano su  $\mathcal{H}$ , semipositivo e a traccia 1. In letteratura è anche chiamato *Matrice Densità*.

Nel testo si userà spesso solo la parola **stato** per riferirsi all'operatore di stato.

- Combinazioni lineari convesse di stati sono ancora stati  $\rho(\lambda) = \lambda \rho_1 + (1 - \lambda) \rho_2$ ,  $0 \leq \lambda \leq 1$ .

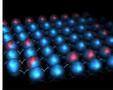
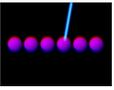
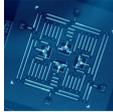
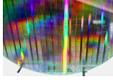
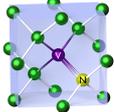
- Gli stati che sono anche proiettori sul sottospazio generato dal vettore  $|\psi\rangle$  (detto **vettore di stato**) sono espressi nella forma  $\rho = |\psi\rangle\langle\psi|$  ( $\langle\psi|\psi\rangle = 1$ ) e sono chiamati **stati puri**. Inoltre, data una qualunque base ortonormalizzata  $\{|\phi_i\rangle\}$ ,  $\langle\phi_i|\phi_j\rangle = \delta_{ij}$ ,  $i, j = 1, \dots, d$  di  $\mathcal{H}$ , i coefficienti  $a_i = \langle\phi_i|\psi\rangle$  di  $|\psi\rangle$  rispetto ad essa sono detti **ampiezze di probabilità**, o collettivamente **funzione d'onda**.

- Ad ogni grandezza fisica  $\mathcal{O}$  corrisponde un **osservabile**, cioè un operatore lineare hermitiano  $\mathbf{O}$  su  $\mathcal{H}$ . Il suo **spettro**  $\sigma(\mathbf{O}) = \{\mu : \mathbf{O}|\psi_\mu^h\rangle = \mu|\psi_\mu^h\rangle\} \subseteq \mathbb{R}$  costituisce l'insieme dei valori che si possono ottenere a seguito di una misura di  $\mathcal{O}$ .

- Osservabili per i quali  $[\mathbf{O}, \mathbf{O}'] \neq 0$  si dicono **incompatibili**. Le loro distribuzioni di probabilità sono correlate. In particolare, si dimostra che per coppie di osservabili canonicamente coniugati  $[\mathbf{p}_i, \mathbf{x}_i] = i\hbar$  vale la disuguaglianza  $\Delta p_i \Delta x_i \geq \hbar/2$  (principio di Heisenberg)

- (Teorema di Decomposizione Spettrale) Ogni osservabile  $\mathbf{O}$  possiede una famiglia completa di **proiettori ortogonali**  $\mathbf{P}_\lambda^\dagger = \mathbf{P}_\lambda$ ,  $\sum_{\sigma(\mathbf{O})} \mathbf{P}_\lambda = \mathbf{1}_{\mathcal{H}}$ ,  $\mathbf{P}_\lambda \mathbf{P}_\mu = \delta_{\lambda,\mu} \mathbf{P}_\lambda$ ,  $\mathbf{P}_\lambda = \sum_g |\psi_\lambda^g\rangle\langle\psi_\lambda^g|$  tali che  $\mathbf{O} = \sum_{\sigma(\mathbf{O})} \lambda \mathbf{P}_\lambda$ .

- (**Regola di Born**) Introdotta la *traccia* di un operatore su  $\mathcal{H}$  come l'applicazione  $\text{tr}(\cdot) : \text{End}(\mathcal{H}) \rightarrow \mathbb{C}$  che sia lineare, indipendente dalla base scelta e ciclica, essa consente di

	Cold atoms	Trapped Ions	Superconducting	Silicon	NV centers	Photons
						
Number of physical qubits	324	32	433	15	10	216
Best two-qubit gate fidelity (%)	99.4	99.9	99.97	>99	99.2	98
Best readout fidelity (%)	99.1	99.9	99.4	99	98	50
Best gate time (ns)	1	$10^5$	20	$5 * 10^3$	10	<1
Best $T_1$ (s)	>1	0.2	$4 * 10^{-4}$	$1.2 * 10^{-4}$	$2.4 * 10^{-3}$	$\infty$
Temperature (mK)	<1	<1	15	100	$4 * 10^3$	Room Temperature
Scalability (# qubits)	up to $10^4$	<50	$\sim 10^3$	$\sim 10^6$	$\sim 10^2$	$\sim 10^6$

**Figura 20:** Confronto tra diversi tipi di implementazioni fisiche di qubit. La tabella ripresa da [23] è stata ottenuta raccogliendo i dati di numerosi altri lavori ivi citati. La Fedeltà di porta è definita da  $F = |\langle \psi_N | \psi \rangle_I|^2$  tra gli stati evoluti attraverso un porta sperimentale rumorosa e la corrispondente ideale. La Fedeltà in lettura misura la precisione, compresa tra 0.5 e 1, con cui è possibile determinare lo stato di un qubit. Il tempo di porta è il tempo necessario per eseguire la corrispondente operazione.  $T_1$  è il tempo di rilassamento di un qubit, cioè la costante di decadimento nella probabilità di permanenza  $p \propto e^{-t/T_1}$  del qubit nello stato  $|1\rangle$ . La temperatura si riferisce alla quella tipica alla quale devono funzionare i computer quantistici basati sulla data tecnologia. La scalabilità riporta una stima della capacità di aumentare il numero di qubit in un computer quantistico senza compromettere la qualità dei qubit con le attuali tecnologie. Il numero 216 di qubit fisici nella piattaforma fotonica corrisponde al numero di modalità GBS (Gaussian Boson Sampling). Le immagini sono indicative della tecnologia adottata.

calcolare il valore medio dell'osservabile  $\mathbf{O}$  sullo stato  $\rho$  dalla formula

$$\langle \mathbf{O} \rangle = \text{tr}(\rho \mathbf{O}).$$

- Nel caso della misura di un osservabile  $\mathcal{O}$  su uno Stato Puro  $\rho = |\psi\rangle\langle\psi|$ , la probabilità di ottenere l'autovalore  $m$  è data da

$$\mathcal{P}_m = \langle \psi | \mathbf{P}_m | \psi \rangle.$$

- Se un sistema, preparato in uno stato puro specificato da  $|\psi\rangle$ , è sottoposto alla misura di un osservabile  $\mathbf{O}$ , a seguito della quale si ottiene  $m \in \sigma(\mathbf{O})$ , lo stato conseguente è puro ed è il proiettato del vettore di stato

$$|\psi\rangle \xrightarrow{m} \frac{\mathbf{P}_m |\psi\rangle}{\sqrt{\langle \psi | \mathbf{P}_m | \psi \rangle}},$$

detto anche **stato ridotto**.

- Dato un sistema isolato che a  $t = 0$  si trovi nello Stato  $\rho(0)$ , esso evolverà **unitariamente** nel tempo, in accordo all'equazione di Schrödinger

$$\dot{\rho}(t) = -i [\mathbf{H}(t), \rho(t)],$$

dove l'operatore hermitiano  $\mathbf{H}(t)$  è detto **Hamiltoniano**.

- La descrizione dei sistemi quantistici non isolati richiede l'introduzione di alcune ipotesi aggiuntive e una apposita estensione dei precedenti concetti [36, 37, 47].



- [1] R. P. Feynman: *Simulating physics with computers*. Int. J. Theoret. Phys., 21 (1981) 467.
- [2] D. Deutsch: *Quantum theory, the Church-Turing principle and the universal quantum computer*. Proc. R. Soc. Lond. Ser. A Math. Phys. Sci., 400 (1985) 97.
- [3] D. P. Di Vincenzo: *Two-bit gates are universal for quantum computation*. Phys. Rev. A, 50 (1995) 1015.
- [4] P. W. Shor: *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer* SIAM Rev., 41 (1999) 303.
- [5] A. Sanjeev; B. Boaz: *Computational complexity* Cambridge University Press, Cambridge UK, (2009) p. 230.
- [6] L. K. Grover: *Quantum mechanics helps in searching for a needle in a haystack*. Phys. Rev. Lett., 79 (1997) 325.
- [7] A. P. Lund, M. J. Bremner, T. C. Ralph: *Quantum sampling problems, Boson Sampling and quantum supremacy*. Quantum Inf., 3 (2017) 15.

- [8] A. Harrow, A. Montanaro: *Quantum computational supremacy*. Nature, 549 (2017) 203.
- [9] D. Loss, D. P. Di Vincenzo: *Quantum computation with quantum dots.*, Phys. Rev. A, 57 (1998) 120.
- [10] N. Gershenfeld, I. L. Chuang: *Bulk spin resonance quantum computation*. Science, 275 (1997) 350.
- [11] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble. *Measurement of conditional phase shifts for quantum logic*. Phys. Rev. Lett., 75 (1995) 4710.
- [12] P. Domokos, J. M. Raimond, M. Brune, S. Haroche: *Simple cavity-QED two-bit universal quantum logic gate: The principle and expected performances*. Phys. Rev. Lett., 52 (1995) 3554.
- [13] D. Kielpinski, C. Monroe, D. Wineland: *Architecture for a large-scale ion-trap quantum computer*. Nature, 417 (2002) 709.
- [14] H. Häffner, C.F. Roos, R. Blatt: *Quantum computing with trapped ions*. Phys. Rep., 469 (2008) 155.
- [15] <https://www.nist.gov/programs-projects/quantum-computing-trapped-ions>
- [16] S. Slussarenko, G. J. Pryde: *Photonic quantum information processing: A concise review*. Appl. Phys. Rev., 6 (2019) 041303.
- [17] C. W. Fink, C. Salemi, B. A. Young, D. I. Schuster, N. A. Kurinsky: *The Superconducting Quasiparticle-Amplifying Transmon: A Qubit-Based Sensor for meV Scale Phonons and Single THz Photons*. <https://doi.org/10.48550/arXiv.2310.01345>
- [18] A. Stern, N. H. Lindner: *Topological Quantum Computation—From Basic Concepts to First Experiments*. Science, 339 (2013) 1179.
- [19] G. Wendin: *Quantum information processing with superconducting circuits: a review*. Rep. Progr. Phys., 80 (2017), 106001.
- [20] G. T. Byrd and Y. Ding: *Quantum Computing: Progress and Innovation*. Computer, 56 (2023) 20.
- [21] H. Sahu, D. H. Gupta: *Quantum Computing Toolkit From Nuts and Bolts to Sack of Tools*. (2023). arXiv preprint arXiv:2302.08884
- [22] L. Jaeger: *The second Quantum Revolution* Springer Nature Switzerland AG (2018).
- [23] E. A. Ruiz Guzman: *Symmetry breaking and restoration for many-body problems treated on quantum computers*. PhD Thesis, Paris-Saclay (2023).
- [24] F. Barahona: *On the computational complexity of Ising spin glass models*. J. Phys. A 15 (1982) 3421.
- [25] S. Istrail, *Statistical Mechanics, Three-Dimensionality and NP-Completeness: I. Universality of Intracatability for the Partition Function of the Ising Model across Non-Planar Surfaces*. Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, Portland, Oregon, USA, (2000), 87. <https://doi.org/10.1145/335305.335316>.
- [26] R. B. Laughlin and D. Pines: *The theory of everything*. Proc. Natl. Acad. Sci., 97 (2000) 28.
- [27] D. DiVincenzo: *The Physical Implementation of Quantum Computation*. Fortschritte der Physik, 48 (2000) 771.
- [28] D. Gottesman: *An introduction to quantum error correction and fault-tolerant quantum computation*. Proceedings of Symposia in Applied Mathematics, 68 (2010).
- [29] <https://quantumai.google>
- [30] [https://www.ibm.com/quantum?mhsrc=ibmsearch\\_a&mhq=quantum%20computer](https://www.ibm.com/quantum?mhsrc=ibmsearch_a&mhq=quantum%20computer)
- [31] J. Preskill: *Quantum Computing in the NISQ era and beyond*. Quantum, 2 (2018) 79.
- [32] F. Arute et al. *Quantum supremacy using a programmable superconducting processor*. Nature, 574 (2019) 505.
- [33] Y. Kim et al.: *Evidence for the utility of quantum computing before fault tolerance*. Nature, 618 (2023) 500.
- [34] <https://www.xanadu.ai>
- [35] J. M. Arrazola et al.: *Quantum circuits with many photons on a programmable nanophotonic chip*. Nature, 591 (2021) 54.
- [36] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge, UK (2000).
- [37] J. Preskill, *Quantum Computation*. Lecture Notes Physics 219/CS219, [http://theory.caltech.edu/~preskill/ph219/ph219\\_2023.html](http://theory.caltech.edu/~preskill/ph219/ph219_2023.html)
- [38] E. Rieffel, W. Polak: *Quantum Computing: a gentle introduction*. The MIT Press Cambridge, Massachusetts (2011).
- [39] M. Lanzagorta, J. Uhlmann: *Quantum Computer Science*. Morgan & Claypool, San Rafael, USA (2009).
- [40] M. M. Wilde: *Quantum information theory*. Cambridge Univ. Press, Cambridge UK (2017).
- [41] G. Benenti, G. Casati, D. Rossini, G. Strini: *Principles of Quantum Computation and Information*. World Scientific, Singapore (2018).
- [42] J. D. Hidary: *Quantum Computing: An Applied Approach*. Springer Nature Switzerland AG (2019).
- [43] J., Abhijith et al.: *Quantum Algorithm Implementations for Beginners*. ACM Transactions on Quantum Computing, 3 (2022) 18.
- [44] C. Cohen-Tannoudji, B. Diu, F. Laloe: *Quantum Mechanics* John Wiley and Sons, New York (1977).
- [45] L. E. Ballentine: *Quantum Mechanics, A Modern Development* 2nd Edition, World Scientific, Singapore, (2014).
- [46] J. J. Sakurai: *Modern Quantum Mechanics* Addison-Wesley, Reading, Mass. (1995).
- [47] U. Weiss: *Quantum dissipative Systems* World Scientific, Singapore (2022).
- [48] A. Einstein, B. Podolsky, and N. Rosen: *Can quantum-mechanical description of physical reality be considered complete?* Phys. Rev., 47 (1935) 777.
- [49] J. S. Bell: *On the Einstein-Podolsky-Rosen paradox*. Physics, 1 (1964) 195. Reprinted in J. S. Bell, *Speakable and Unsayable in Quantum Mechanics*. Cambridge University Press, Cambridge, (1987).

- [50] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt: *Proposed experiment to test local hidden-variable theories*. Phys. Rev. Lett., 49 (1969) 1804.
- [51] A. Aspect, P. Grangier, G. Roger: *Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bell's inequalities* Phys. Rev. Lett., 49 (1982) 91.
- [52] <https://www.nobelprize.org/prizes/physics/2022/summary/>
- [53] P. Colciaghi, Y. Li, Yifan, P. Treutlein, T. Zibold, *Einstein-Podolsky-Rosen Experiment with Two Bose-Einstein Condensates*. Phys. Rev. X, 13(2023) 021031.
- [54] P. Calabrese, J. Cardy: *Entanglement entropy and quantum field theory*. J. Stat. Mech., 0406 (2004) P06002.
- [55] K. Mattle, H. Weinfurter, P. G. Kwiat, A. Zeilinger: *Dense coding in experimental quantum communication*. Phys. Rev. Lett., 76 (1996) 4656.
- [56] C. H. Bennett et al. *Purification of noisy entanglement and faithful teleportation via noisy channels*. Phys. Rev. Lett., 76 (1996) 722.
- [57] D. Bouwmeester et al. *Experimental quantum teleportation*. Nature, 390 (1997) 575.
- [58] M. A. Nielsen, E. Knill, and R. Laflamme: *Complete quantum teleportation using nuclear magnetic resonance*. Nature, 396 (1998) 52.
- [59] D. Boschi et al.: *Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolski-Rosen channels*. Phys. Rev. Lett., 80 (1998) 1121.
- [60] N. Lee et al., *Teleportation of nonclassical wave packets of light*. Science, 332 (2011) 330.
- [61] C. H. Bennett, G. Brassard: *Quantum cryptography: Public key distribution and coin tossing*. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pages 175–179, IEEE, New York, 1984. Bangalore, India, (1984).
- [62] M. Sasaki et al. *Field test of quantum key distribution in the Tokyo QKD Network*. Opt. Express, 19 (2011) 10387.
- [63] D. Stucki et al., *Long-term performance of the Swiss Quantum quantum key distribution network in a field environment*. N. J. Phys., 13 (2011) 123001.
- [64] J. F. Dynes et al.: *Cambridge quantum network*. NPJ Quantum Inf., 5 (2019) 101.
- [65] Y. H. Yang et al. *All optical metropolitan quantum key distribution network with post-quantum cryptography authentication*. Opt. Express, 29 (2021) 25859.
- [66] S.-K. Liao et al. *Satellite-to-ground quantum key distribution*. Nature, 549 (2017) 43.
- [67] Y.-A. Chen et al. *An integrated space-to-ground quantum communication network over 4600 kilometres*. Nature, 589 (2021) 214.
- [68] S. K. Liao et al.: *Satellite-relayed intercontinental quantum network*. Phys. Rev. Lett., 120 (2018) 030501.
- [69] R. Nagarajan, N. Papanikolaou, D. Williams: *Simulating and Compiling Code for the Sequential Quantum Random Access Machine*. In P. Selinger, Proceedings of the 3rd International Workshop on Quantum Programming Languages (QPL 2005), Electronic Notes in Theoretical Computer Science 170 (2007) 101.
- [70] A. W. Harrow B. Recht, I. L. Chuang: *Efficient discrete approximations of quantum gates*. J. Math. Phys., 43 (2002) 4445.
- [71] J. I. Cirac, P. Zoller: *Quantum Computations with Cold Trapped Ions* Phys. Rev. Lett., 74 (1995) 4091.
- [72] S. Venegas: *Quantum Walks for Computer Scientists*. Morgan and Claypool. (2008) DOI: 10.1145/1062261.1062335
- [73] E. Farhi et al., *A Quantum Adiabatic Evolution Algorithm Applied to Random Instances of an NP-Complete Problem*. Science, 292 (2001) 472.
- [74] A. Robert et al.: *Resource-efficient quantum algorithm for protein folding*. Quantum Inf., 7 (2021) 38.
- [75] A. Pardomo et al.: *On the construction of model hamiltonians for adiabatic quantum computing and its application to finding low energy conformations of lattice protein models*. Phys. Rev. A, 78 (2008) 012320.
- [76] E. F. Dumitrescu et al.: *Cloud Quantum Computing of an Atomic Nucleus* Phys. Rev. Lett., 120 (2018) 210501.
- [77] A. Perez-Obiol et al. *Nuclear shell-model simulation in digital quantum computers*. Scientific Reports, 13 (2023) 12291.
- [78] V. Amitrano, A. Roggero, P. Luchi, F. Turro, L. Vespucci, F. Pederiva, *Trapped-ion quantum simulation of collective neutrino oscillations*. Phys. Rev. D, 107 (2023) 023007.
- [79] D. Lacroix: *Symmetry-assisted preparation of entangled many-body states on a quantum computer*. Phys. Rev. Lett., 125 (2020) 230502.
- [80] S. Lee et al.: *Evaluating the evidence for exponential quantum advantage in ground-state quantum chemistry*. Nature Commun., 14 (2023) 1952.
- [81] S. Barison, F. Vicentini, G. Carleo: *An efficient quantum algorithm for the time evolution of parameterized circuits*. Quantum, 5 (2021) 512.
- [82] I. M. Georgescu, S. Ashhab, F. Nori *Quantum simulation*. Rev. Mod. Phys., 86 (2014) 153.
- [83] G. Benenti, G. Strini: *Quantum simulation of the single-particle Schrödinger equation*. Am. J. Phys., 76 (2008) 657.
- [84] R. D. Somma: *Quantum Simulations of One Dimensional Quantum Systems*. Quantum Info. Comput., 16 (2016) 1125.
- [85] Y. I. Bogdanov et al.: *Solution of the Schrödinger Equation on a Quantum Computer by the Zalka–Wiesner Method Including Quantum Noise*. J. Phys.: Conf. Ser., 114 (2021) 354.
- [86] J. R. McClean, J. Romero, R. Babbush, and A. Aspuru-Guzik, *The theory of variational hybrid quantum-classical algorithms*. New Journal of Physics, 18 (2016) 023023.
- [87] A. Montanaro. *Quantum algorithms: an overview*. Quantum Information, 2 (2016) 15023.
- [88] A. Peruzzo et al.: *A variational eigenvalue solver on a photonic quantum processor*. Nat. Commun., 5 (2014) 4213.

- [89] F. E. Chrit et al. *Fully quantum algorithm for lattice Boltzmann methods with application to partial differential equations*, arXiv 2305.07148 (2023).
- [90] L. Budinski: *Going deeper into the quantum lattice Boltzmann method: exploring multiphysics applications in 2D*. Quantum Science, (2023), <https://quanscient.com>
- [91] P. C. Costa, S. Jordan, A. Ostrander *Quantum algorithm for simulating the wave equation*. Phys. Rev. A, 99 (2019) 012323.
- [92] A. Suau, G. Staffelbach, H. Calandra *Practical Quantum Computing: Solving the Wave Equation Using a Quantum Approach*. ACM Transactions on Quantum Computing 2 (2021). <https://doi.org/10.1145/3430030>
- [93] D. Deutsch, R. Jozsa: *Rapid solution of problems by quantum computation*. Proc. R. Soc. London A, 439 (1992) 553.
- [94] D. Simon: *On the power of quantum computation*. In Proceedings, 35th Annual Symposium on Foundations of Computer Science (1994) 116.
- [95] P. W. Shor: *Algorithms for quantum computation: discrete logarithms and factoring*. In Proceedings, 35th Annual Symposium on Foundations of Computer Science, IEEE Press, Los Alamitos, CA, (1994).
- [96] L. M. K. Vandersypen et al.: *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*. Nature, 414 (2001) 883.
- [97] A. Y. Kitaev: *Quantum measurements and the Abelian stabilizer problem*. (1995). arXiv e-print quant-ph/9511026
- [98] N. Koblitz: *A Course in Number Theory and Cryptography*. Springer-Verlag, New York, (1994).
- [99] R. Cleve, A. Ekert, C. Macchiavello, M. Mosca: *Quantum algorithms revisited*. Proc. R. Soc. London A, 454 (1969) 339.
- [100] C. H. Bennett, E. Bernstein, G. Brassard, U. Vazirani: *Strengths and weaknesses of quantum computing*. SIAM journal on Computing, 26 (1997) 1510.
- [101] F. Magniez, M. Santha, M. Szegedy: *Quantum algorithms for the triangle problem*. SIAM J. Comput., (2007) 413.
- [102] M. Schuld, I. Sinayskiy, F. Petruccione: *An introduction to quantum machine learning*. Contemporary Physics, 56 (2015) 172.
- [103] G. Lindblad: *On the generators of quantum dynamical semigroups*, Comm. Math. Phys., 48 (1976) 119.
- [104] V. Gorini, A. Kossakowski, E. C. G. Sudarshan: *Completely positive dynamical semigroups of N-level systems*, J. Math. Phys., 17 (1976) 821.
- [105] H.-P. Breuer, F. Petruccione: *The Theory of Open Quantum Systems*. (Oxford, 2007; online edn, Oxford Academic), <https://doi.org/10.1093/acprof:oso/9780199213900.001.0001>
- [106] D. A. Lidar: *Lecture Notes on the Theory of Open Quantum Systems*. arXiv: Quantum Physics, (2019). <https://api.semanticscholar.org/CorpusID:119477176>
- [107] [https://www.newscientist.com/article/2399246-record-breaking-quantum-computer-has-more-than-1000-qubits/?utm\\_source=nsday&utm\\_medium=email&utm\\_campaign=nsday\\_251023&utm\\_term=Newsletter%20NSDAY\\_Daily](https://www.newscientist.com/article/2399246-record-breaking-quantum-computer-has-more-than-1000-qubits/?utm_source=nsday&utm_medium=email&utm_campaign=nsday_251023&utm_term=Newsletter%20NSDAY_Daily)
- [108] [https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-technology-sees-record-investments-progress-on-talent-gap?utm\\_source=nsqp&utm\\_medium=email&utm\\_campaign=nsqp\\_071123&utm\\_term=Newsletter%20NSQP\\_Lost%20in%20Space%20Time](https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-technology-sees-record-investments-progress-on-talent-gap?utm_source=nsqp&utm_medium=email&utm_campaign=nsqp_071123&utm_term=Newsletter%20NSQP_Lost%20in%20Space%20Time)

---

**Luigi Martina:** è Professore Associato di Fisica Teorica presso l'Università del Salento. Si occupa di sistemi integrabili e, più recentemente, di algoritmi quantistici.



---

# La distribuzione quantistica di chiavi

“La scienza non è nient’altro che una perversione se non ha come suo fine ultimo il miglioramento delle condizioni dell’umanità.”

Nikola Tesla

**Samuele Altia**

Dipartimento di Fisica “Aldo Pontremoli”, Università degli Studi di Milano

**Michele N. Notarnicola**

Dipartimento di Fisica “Aldo Pontremoli”, Università degli Studi di Milano

**Stefano Olivares**

Dipartimento di Fisica “Aldo Pontremoli”, Università degli Studi di Milano

---

**T**ra le tecnologie che hanno beneficiato delle proprietà quantistiche della natura, particolare spazio è riservato alla comunicazione quantistica e alla cosiddetta “distribuzione quantistica di chiavi”, che sta tuttora avendo un notevole sviluppo anche a livello commerciale. In queste pagine illustreremo gli aspetti fisici che stanno alla base della distribuzione quantistica di chiavi (*Quantum Key Distribution, QKD*) e illustreremo le principali applicazioni a variabili discrete e a variabili continue che utilizzano i fotoni per codificare e condividere in modo sicuro l’informazione.

La teoria che chiamiamo comunemente “Meccanica Quantistica” permette di descrivere con grande accuratezza il mondo che ci circonda. Questa teoria ha altresì alcuni aspetti peculiari che non solo la rendono affascinante e, per così dire, strana rispetto al senso comune, ma che spianano la strada ad applicazioni tecnologiche che vanno ben oltre quelle permesse dal-

la fisica classica, ovvero dalla meccanica, dalla termodinamica e dall’elettromagnetismo.

Nel seguito introdurremo i concetti di sovrapposizione ed *entanglement* quantistici su cui si fondano la comunicazione e la computazione quantistica. Ma non solo, in quanto il loro studio ha condotto allo sviluppo di tecnologie quantistiche, che sono l’oggetto della seconda rivoluzione quantistica di cui siamo spettatori in questi anni.

Nelle prossime pagine illustreremo come queste proprietà dei sistemi fisici possano permettere di condividere informazioni in modo più sicuro rispetto a quanto sia possibile fare con mezzi classici.

## Tra teoria e realtà fenomenologica

La fisica è la scienza che studia i fenomeni naturali e le leggi che li governano.

Partendo dall’osservazione del mondo che ci circonda, vengono identificate alcune leggi (o paradigmi) fondamentali grazie alle quali è possibile dare una descrizione scientifica di quanto

accade nel mondo intorno a noi. Grazie a quelle leggi è anche possibile prevedere nuovi fenomeni che devono essere verificati progettando ed eseguendo esperimenti più o meno sofisticati per validare o meno la teoria stessa. Questo permette il progresso della scienza [1].

Da una parte troviamo teorie ormai assodate che vengono ulteriormente perfezionate e completate (si pensi, ad esempio, alla meccanica classica di Newton e Galileo e quella relativistica di Einstein). Dall'altra possono emergere indizi che mostrano l'inadeguatezza delle teorie note, conducendo alla nascita di nuove teorie, come nel caso del lavoro di Max Planck che ha portato al quanto d'azione e, infine, alla fisica quantistica [2, 3, 4].

Così come la meccanica classica si fonda sulle leggi di Newton, la termodinamica sui suoi tre principi (ma è possibile anche riformularla in modo prettamente assiomatico [5, 6]) e l'elettromagnetismo sulle equazioni di Maxwell, anche la meccanica quantistica ha i suoi postulati. C'è però una differenza sostanziale tra quella che chiamiamo comunemente fisica classica e quella quantistica, che anche i non esperti osservano quotidianamente senza a volte esserne consapevoli.

Le leggi della fisica classica descrivono i fenomeni con cui abbiamo a che fare ogni giorno: il cadere di una foglia, il raffreddarsi di una tazza di caffè o il ronzare di un motore elettrico. La descrizione quantitativa dei fenomeni che abbiamo menzionato può richiedere modelli matematici molto complicati, ma il risultato finale non ci stupirebbe in quanto la nostra esperienza li rende comunque intuitivi.

Non è così per le previsioni della meccanica quantistica che spesso si riferiscono al comportamento di sistemi microscopici (ma non solo!) che non sono direttamente accessibili alla nostra esperienza sensoriale. Ed ecco che spesso si parla di stranezze e misteri: niente di più fuorviante! Tutto nasce dal voler inquadrare ostinatamente nella nostra esperienza quotidiana fenomeni naturali che non abbiamo mai sperimentato. Si pensi all'esibizione di un bravissimo prestidigitatore che ci lascia a bocca aperta davanti ad una sua magia spettacolare: spesso il risultato va contro il nostro senso comune, ed ecco che ci appare magico. Tuttavia, una volta svelato il meccani-

simo a volte ingegnoso che sta dietro a quanto abbiamo visto (e quindi percepito con i nostri sensi), la nostra mente inquadra l'esibizione in una serie di passaggi logici che rendono tutto nuovamente intuitivo e, per così dire, naturale.

Possiamo affermare che qualcosa di simile valga anche per la Meccanica Quantistica. Certamente i suoi postulati ci permettono di descrivere in modo accurato il mondo microscopico, quello a cui appartengono atomi, molecole e fotoni, i quanti di luce; ma grazie a questi possiamo anche dare una descrizione accurata e quantitativa, ad esempio, del perché il nostro cielo sia così azzurro oppure utilizzare tecnologie altrimenti inesistenti, come la risonanza magnetica nucleare o il GPS, che si basa sulla estrema precisione degli orologi atomici.

È possibile introdurre gli assiomi della Meccanica Quantistica partendo da alcune chiare situazioni sperimentali e qui ne consideriamo una specifica e, passateci il termine, paradigmatica: l'interferenza. Per un approfondimento divulgativo ma comunque sufficientemente rigoroso sui postulati fondamentali della meccanica quantistica con questo tipo di approccio si veda, ad esempio, la Ref. [7].

## Sovrapposizione e interferenza

Vi sarà capitato di osservare quello che accade quando le onde su uno specchio d'acqua si sovrappongono: quando due creste passano contemporaneamente nello stesso punto si ha un aumento dell'altezza complessiva, quando una cresta incontra un ventre di un'altra onda, si ha una diminuzione dell'altezza. Si parla di "interferenza costruttiva e distruttiva", rispettivamente. Lo stesso fenomeno si ha quando si illuminano con una sorgente LASER due fenditure praticate su uno schermo: al di là dello schermo di osserva una figura di interferenza. In questo caso l'elettromagnetismo ci spiega che ogni fenditura genera dei fronti d'onda analoghi a quelli generati da un sasso gettato in uno stagno. Quando le onde provenienti dalle due fenditure (o sorgenti) si sovrappongono si ha, appunto, interferenza.

Se consideriamo un dato punto  $x$  al di là delle fenditure e indichiamo con  $E_1(x)$  ed  $E_2(x)$  i campi elettrici in tale punto delle onde provenienti dalle fenditure 1 e 2, l'intensità totale della

luce in  $x$  è data da (per semplicità assumiamo che i campi abbiano la stessa polarizzazione e frequenza):

$$I_{\text{tot}}(x) = |E_1(x) + E_2(x)|^2, \quad (1)$$

in quanto il campo in quel punto è fornito dalla combinazione lineare  $E_{\text{tot}} = E_1 + E_2$ . Ricordiamo che, in generale, il campo elettrico è rappresentato da un numero complesso, quindi se poniamo  $E_1(x) = A_1 e^{i\phi_1(x)}$  e  $E_2 = A_2 e^{i\phi_2(x)}$ , otteniamo:

$$I_{\text{tot}}(x) = A_1^2 + A_2^2 + 2A_1A_2 \cos [\phi_1(x) - \phi_2(x)], \quad (2)$$

e l'ultimo termine è responsabile dell'interferenza osservata.

Così come accade per un fascio di luce, anche quando si inviano fasci di particelle materiali (elettroni, atomi, fullereni, ...) opportunamente preparati si ottiene un risultato simile: interferenza! I postulati della meccanica quantistica ci dicono che per descrivere quanto accade dobbiamo associare una **funzione d'onda** complessa  $\psi$  ad ogni particella che passa dallo schermo in cui sono praticate le fenditure. Dal momento che ci sono due fenditure, la funzione d'onda in un dato punto  $x$  al di là dello schermo sarà (si veda la referenza [7] per i dettagli):

$$\psi(x) \propto \psi_1(x) + \psi_2(x), \quad (3)$$

dove i pedici 1 e 2 si riferiscono alle due fenditure come sopra.

Si nota l'analogia con quanto fatto per le onde elettromagnetiche (la luce), analogia che svanisce nel momento in cui consideriamo il modulo quadro di  $\psi(x)$ . I postulati della Meccanica Quantistica, infatti, affermano che la quantità:

$$p(x) \propto |\psi(x)|^2 \quad (4)$$

corrisponde alla densità di probabilità di trovare nel punto  $x$  la particella che proviene dallo schermo con le due fenditure [7]. Anche in questo caso possiamo scrivere  $\psi_1(x) = A_1 e^{i\varphi_1(x)}$  e  $\psi_2(x) = A_2 e^{i\varphi_2(x)}$  e ricaviamo:

$$p(x) \propto A_1^2 + A_2^2 + 2A_1A_2 \cos [\varphi_1(x) - \varphi_2(x)], \quad (5)$$

## Il qubit

Un **qubit**, o bit quantistico, è un sistema fisico che può esistere in due soli stati ben distinti (ortogonali), che possiamo indicare con  $|0\rangle$  e  $|1\rangle$ , mimando il bit classico che è associato ai simboli "0" e "1". Lo stato generico di un qubit può essere scritto come la sovrapposizione:

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

ed ecco ancora il termine di interferenza!

Quello che abbiamo visto all'opera, responsabile dell'interferenza quantistica, è il cosiddetto "principio di sovrapposizione", conseguenza della linearità della teoria quantistica: una combinazione lineare di funzioni d'onda (opportunamente normalizzata) è ancora una legittima funzione d'onda del sistema in questione [7].

## Il qubit

Supponiamo di avere un sistema fisico che possa avere solo due configurazioni particolari, o stati. Abbiamo diversi esempi in natura di un tale sistema: una lampadina accesa o spenta, un condensatore carico o scarico, oppure, passando al mondo microscopico, un atomo in un livello fondamentale o eccitato, un fotone polarizzato orizzontalmente o verticalmente ...

Per essere più generali possibili, indichiamo i due stati utilizzando la ben nota codifica binaria che si serve dei simboli "0" e "1" associati ad un *bit* di informazione. Per passare alla descrizione quantistica, possiamo dire che al sistema che si trovi nello stato "0" associamo la funzione d'onda  $\psi_0$  e, analogamente, associamo la funzione d'onda  $\psi_1$  a quello che si trova nello stato "1". Dal momento che abbiamo a che fare con un sistema binario, è utile associare a  $\psi_0$  e  $\psi_1$  due vettori colonna bidimensionali ortogonali che indicheremo con i simboli introdotti da Paul M. Dirac:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{e} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (6)$$

detti **ket**, e i corrispondenti vettori riga:

$$\langle 0| = (1, 0) \quad \text{e} \quad \langle 1| = (0, 1), \quad (7)$$

chiamati **bra**. In questo modo diventa possibile rappresentare il **prodotto interno** riga per colonna tra i vettori come segue:

$$\begin{aligned} \langle 0|0\rangle &= (1, 0) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1, \\ \langle 1|1\rangle &= (0, 1) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 1, \\ \langle 0|1\rangle &= (1, 0) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0, \\ \langle 1|0\rangle &= (0, 1) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0, \end{aligned} \quad (8)$$

Dati gli stati  $|0\rangle$  e  $|1\rangle$ , la sovrapposizione:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right) |1\rangle \quad (9)$$

rappresenta il generico stato di quello che comunemente si chiama bit quantistico o **qubit** (*quantum bit*). Osserviamo che lo stato  $|\psi\rangle$  è normalizzato:

$$|\langle \psi | \psi \rangle|^2 = 1, \quad (10)$$

mentre le quantità

$$P_0 = |\langle 0 | \psi \rangle|^2 = \cos^2\left(\frac{\theta}{2}\right), \quad (11)$$

e

$$P_1 = |\langle 1 | \psi \rangle|^2 = \sin^2\left(\frac{\theta}{2}\right), \quad (12)$$

che seguono della linearità del prodotto interno e dalle (8), corrispondono alla probabilità che misurando il qubit utilizzando la base  $\{|0\rangle, |1\rangle\}$  si ottenga come risultato "0", ovvero qubit nello stato  $|0\rangle$ , oppure "1", qubit nello stato  $|1\rangle$ .

Una sovrapposizione particolare è quella che si ha quando i due simboli,  $|0\rangle$  e  $|1\rangle$ , hanno la stessa probabilità. In particolare, nel seguito ci focalizzeremo sui due stati:

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}. \quad (13)$$

Analogamente a quanto accade per i bit classici, i qubit permettono di codificare, trasmettere ed elaborare informazione. Tuttavia, mentre con

$n$  bit si può codificare una sola delle  $2^n$  successioni di bit possibili, con lo stesso numero di qubit diventa possibile creare una sovrapposizione di tutte le  $2^n$  possibilità. Ad esempio, nel caso di 2 bit, possiamo codificare volta per volta una sola delle coppie "00", "01", "10" e "11", mentre con 2 qubit è possibile creare la sovrapposizione:

$$\begin{aligned} |\Psi\rangle &= \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle \\ &\quad + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle \end{aligned} \quad (14)$$

dove  $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$  e la scrittura " $|x\rangle|y\rangle$ " indica che il primo qubit si trova nello stato  $|x\rangle$  e il secondo in  $|y\rangle$ .

In particolare, gli stati di due qubit:

$$|\Psi^{(\pm)}\rangle = \frac{|0\rangle|1\rangle \pm |1\rangle|0\rangle}{\sqrt{2}}. \quad (15)$$

e

$$|\Phi^{(\pm)}\rangle = \frac{|0\rangle|0\rangle \pm |1\rangle|1\rangle}{\sqrt{2}}. \quad (16)$$

sono chiamati "stati di Bell", in onore di J. S. Bell scopritore delle celebrate "disuguaglianze", e sono stati *entangled*. In questo luogo non abbiamo modo di approfondire il concetto di *entanglement* e le sue implicazioni, vi rimandiamo perciò alla Ref. [7] per maggiori dettagli e per un'introduzione alle disuguaglianze di Bell, che hanno portato all'assegnazione dei premi Nobel per la Fisica del 2022 [8].

Abbiamo ora tutti gli elementi per comprendere il funzionamento del principale protocollo quantistico di distribuzione di chiavi, proposto da Charles H. Bennett e Gilles Brassard nel 1984 e noto come "BB84" [9].

## Il problema della distribuzione quantistica di chiavi

L'importanza della *privacy* e della sicurezza delle comunicazioni è cruciale in molti contesti, sia privati, si pensi alla protezione dei dati sensibili personali o alle transazioni online, sia pubblici, come le comunicazioni governative e militari.

Per garantire che un messaggio inviato tra due parti, che chiameremo Alice e Bob, sia al sicuro durante il suo trasferimento, si può ricorrere alla tecnica della cifratura: questa consiste nel manipolare in modo opportuno il messaggio stes-

so per mezzo di una sequenza o stringa di dati detta **chiave**. In questa maniera l'informazione diventa incomprensibile a chiunque non posseda la chiave e solo chi la possiede può, appunto, decifrare correttamente il messaggio. L'indecifrabilità del messaggio cifrato da parte di una spia, che chiameremo Eve, è garantita da un teorema matematico, noto come teorema di Vernam [10], a patto che la chiave sia completamente casuale, lunga quanto il messaggio stesso e utilizzata una sola volta (il cosiddetto *one-time pad*, OTP) [11].

Il problema della crittografia diventa quindi quello della distribuzione di chiave, ossia di far sì che Alice e Bob condividano una stessa chiave casuale sicura. Esistono vari protocolli classici di scambio di chiave, i quali tipicamente sfruttano la complessità computazionale di specifici problemi matematici. Un esempio rilevante tra questi è l'algoritmo RSA (dalle iniziali di Rivest, Shamir e Adleman, che lo hanno introdotto nel 1977 [12]), la cui sicurezza si fonda sulla notevole difficoltà nel fattorizzare in tempi brevi numeri interi molto, molto grandi; difficoltà che si traduce in tempi estremamente lunghi se paragonati a quelli di effettivo utilizzo della chiave stessa [12]. Tuttavia, pur non essendoci attualmente un algoritmo efficiente per la fattorizzazione, non esiste nemmeno una prova matematica definitiva che escluda la possibilità di scoprirne uno in futuro. Inoltre, il progresso della computazione quantistica costituisce una minaccia crescente per la sicurezza delle attuali tecnologie di crittografia. I computer quantistici, infatti, potrebbero in futuro comprometterne la robustezza grazie alla loro potenziale capacità di risolvere specifici problemi in tempi significativamente più brevi rispetto ai computer tradizionali sfruttando algoritmi quantistici, quale quello per la fattorizzazione proposto da Shor [13].

Se da una parte i principi della fisica quantistica rischiano di mettere in discussione i protocolli di crittografia attualmente in uso, dall'altra costituiscono anche una preziosa risorsa per risolvere in modo definitivo il problema dello scambio di chiave. Sistemi che implementano distribuzione quantistica di chiavi (*quantum key distribution*, QKD) sono già sufficientemente maturi dal punto di vista tecnologico da essere prodotti a livello commerciale e applicati in diversi contesti. Diversi protocolli di QKD sono stati disegna-

ti sfruttando sia sistemi a variabili discrete, i.e. qubit, sia sistemi a variabili continue, come ad esempio impulsi LASER. Nel seguito presentiamo i principali risultati per ciascuna delle due piattaforme.

## Sistemi a variabili discrete: il protocollo BB84

Il primo protocollo per la QKD ad essere stato introdotto, nonché ora il più diffuso a livello commerciale, è il BB84 [9]. Per realizzarlo sono necessari due canali di comunicazione: uno quantistico e uno classico. Attraverso il canale quantistico vengono inviati singoli fotoni e il grado di libertà fisico su cui viene tipicamente codificata l'informazione è la loro polarizzazione. Il canale classico, invece, deve essere autenticato per garantire la corretta provenienza dei messaggi scambiati, ma questi sono trasmessi in chiaro, quindi accessibili a chiunque possa intercettarli.

Utilizzando il formalismo introdotto nel paragrafo precedente, indicheremo con  $|0\rangle$  e  $|1\rangle$  gli stati con polarizzazione orizzontale e verticale, e con  $|-\rangle$  e  $|+\rangle$  le loro combinazioni lineari definite nella (13), che corrispondono fisicamente ai due stati di polarizzazione a  $-45^\circ$  e  $+45^\circ$ . Chiameremo la base formata dai due stati  $\{|0\rangle, |1\rangle\}$  "base  $\oplus$ " e quella degli stati  $\{|-\rangle, |+\rangle\}$  "base  $\otimes$ ". In questa codifica, possiamo ad esempio associare agli stati  $|0\rangle$  e  $|-\rangle$  il valore logico "0", e agli stati  $|1\rangle$  e  $|+\rangle$  il valore logico "1".

Elemento chiave del protocollo è che gli stati quantistici codificati in una base e misurati in un'altra non forniscono alcuna informazione deterministica. Infatti, se per esempio Alice invia a Bob lo stato  $|+\rangle$  e Bob lo misura sulla base  $\otimes$ , il risultato ottenuto sarà sempre "1"; viceversa, se Bob lo misura sulla base  $\oplus$  egli otterrà con uguale probabilità pari a  $1/2$ , i risultati "0" oppure "1", come si può ricavare facilmente ricordando le (11) e (12) e adattandole al nostro caso. In altre parole, se uno stato viene codificato in una base specifica e successivamente misurato in nell'altra base, il risultato della misura sarà totalmente casuale e non consentirà di ottenere alcuna informazione utile circa il segnale effettivamente inviato.

## Il protocollo BB84

Nel protocollo BB84 Alice codifica su qubit una sequenza di bit casuali servendosi con il 50% di probabilità due basi differenti (non ortogonali tra loro). Gli stati vengono quindi inviati a Bob che li misura utilizzando di volta in volta una delle due basi scegliendole casualmente: solamente gli stati misurati con la medesima base della codifica porteranno ad ottenere con certezza il valore corretto del bit inviato da Alice. Per questo motivo, Alice e Bob comunicano pubblicamente (su un canale pubblico autenticato) le basi di codifica e di misura, rispettivamente, in modo da conservare solamente i bit in cui queste coincidono, scartando i rimanenti (*sifting*). In assenza di una spia le sequenze di bit ottenute dalle due parti, le cosiddette *sifted key*, coincidono. Nel momento in cui Eve interviene sul canale, intercettando gli stati inviati da Alice prima che arrivino a Bob, introduce inevitabilmente un rumore, come previsto dalle leggi della Meccanica Quantistica. In particolare, tale rumore si manifesta introducendo degli errori nelle *sifted key*, che possono essere rivelati confrontando direttamente una frazione delle chiavi finali (si parla di fase di riconciliazione). Se la percentuale di errori, il QBER, è minore di una determinata soglia è possibile ritenere lo scambio di chiavi sicuro: diventa possibile distillare una chiave finale che Eve spia non sarebbe in alcun modo in grado di recuperare.

In questo modo, il protocollo BB84 si avvale della natura intrinsecamente probabilistica della meccanica quantistica per garantire la sicurezza della comunicazione tra Alice e Bob.

Più nel dettaglio, nel protocollo BB84 lo scambio di chiave è realizzato attraverso i seguenti passaggi principali:

1. Alice genera casualmente una sequenza di  $N$  bit. Per ogni bit, sceglie poi in maniera indipendente e casuale una delle due basi  $\oplus$  o  $\otimes$ , e invia a Bob un fotone codificando bit grazie alla polarizzazione nella base scelta. Se, per esempio, il bit fosse "1" e la base scelta  $\otimes$ , il fotone inviato a Bob sarebbe nello stato  $|+\rangle$ . Essendo sia i bit che le basi scelte in modo completamente casuale, la probabilità di mandare ciascuno degli stati  $|0\rangle$ ,  $|1\rangle$ ,  $|+\rangle$  e  $|-\rangle$  è la stessa. Ognuno di questi viene quindi inviato approssimativamente  $N/4$  volte.
2. Per ogni fotone (bit) inviato da Alice, Bob sceglie in modo casuale una delle due basi su cui effettuare la sua misura: un semplice conto mostra che, statisticamente, i due utilizzeranno la stessa base circa  $N/2$  volte. Nel caso ideale di un canale di comunicazione non rumoroso, ossia tale per cui lo stato che giunge a Bob è esattamente lo stesso inviato da Alice, tutte le misure effettuate da Bob sulla stessa base utilizzata da Alice per codificare l'informazione daranno come risultato il valore del bit scelto originariamente da Alice. Al contrario, nelle misure in cui le basi scelte dai due sono diverse, i bit di Alice e di Bob saranno completamente scorrelati.
3. Il passo successivo consiste nell'eliminare i bit scorrelati. Al termine della trasmissione sul canale quantistico, Alice e Bob utilizzano il canale classico autenticato per dichiarare la base scelta per codificare e misurare ciascun fotone (ma non il valore codificato e misurato!). Quindi, conservano solamente i bit che sono stati codificati e misurati nella stessa base, scartando gli altri. Questo processo è chiamato *sifting* ("setacciamento") e bit rimanenti costituiscono la cosiddetta *sifted key*, che sarà quindi lunga circa  $N/2$  bit.
4. Infine, una parte statisticamente significativa della sifted key viene rivelata pubblicamente sul canale classico — e quindi successivamente scartata — per valutare la percentuale di eventuali errori presenti nella sequenza finale di bit (*quantum bit error rate*, QBER). Come vedremo fra poco, dal QBER è possibile rilevare la presenza di una possibi-

		bit	1	0	0	1	1	0	1	0	0	1
ALICE	base codifica	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$
	stato inviato	$ 1\rangle$	$ -\rangle$	$ 0\rangle$	$ +\rangle$	$ +\rangle$	$ 0\rangle$	$ +\rangle$	$ -\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$
BOB	base misura	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$
	risultato misura	1	0	1	1	0	0	1	1	0	1	1
chiave finale (sifted key)		1	0				0	1		0		

**Figura 1:** Esempio di attuazione del protocollo BB84 nel caso ideale di un canale senza rumore. Quando la base di codifica e quella di misura coincidono, il bit ottenuto da Bob ha lo stesso valore di quello spedito da Alice (colonne evidenziate in giallo): condividono la stessa chiave. Si veda il testo per i dettagli.

		bit	1	0	0	1	1	0	1	0	0	1
ALICE	base codifica	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$
	stato inviato	$ 1\rangle$	$ -\rangle$	$ 0\rangle$	$ +\rangle$	$ +\rangle$	$ 0\rangle$	$ +\rangle$	$ -\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$
EVE	base misura	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\oplus$
	risultato misura	1	1	0	1	0	0	0	0	0	1	1
	stato inviato	$ 1\rangle$	$ 1\rangle$	$ -\rangle$	$ +\rangle$	$ 0\rangle$	$ +\rangle$	$ 0\rangle$	$ -\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$
BOB	base misura	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$
	risultato misura	1	1	0	0	0	0	0	0	0	0	0
chiave finale (sifted key)		1	1				0	0		0		

**Figura 2:** Esempio di attuazione del protocollo BB84 identica alla figura 1, ma con una spia nel canale che effettua un attacco di tipo intercept-resend. Ora può accadere che pur avendo la stessa base di codifica e di misura, il bit spedito da Alice non coincida con quello misurato da Bob, indice, questo, della presenza di una spia, Eve, che ha intercettato il segnale di Alice prima che giungesse a Bob misurandolo con la base sbagliata (celle della tabella evidenziate in rosso). Si veda il testo per i dettagli.

le spia nel canale e, di conseguenza, abortire la comunicazione se necessario.

Al termine del protocollo, se questo va a buon fine, Alice e Bob condividono una chiave casuale segreta di lunghezza approssimativamente  $N/2$  bit, a cui vanno però tolti i bit resi noti sul canale classico per il calcolo del QBER. Questa chiave può essere utilizzata per crittografare un messaggio della stessa lunghezza utilizzando la tecnica del *one-time pad*, come precedentemente menzionato. Dopodiché, il messaggio può essere trasmesso attraverso un canale pubblico senza alcun rischio che l'informazione contenuta possa essere decifrata da terzi.

Nella Figura 1 è riportato un esempio di implementazione del BB84 su  $N = 10$  bit, nel caso di un canale quantistico non rumoroso sul quale, cioè, non si sia introdotta nessuna spia. Nella figura abbiamo evidenziato in giallo le colonne in cui la base scelta da Alice per la codifica corrisponde a quella scelta da Bob per la sua misura. Si nota come i bit della chiave finale, la *sifted key*,

siano perfettamente correlati a quelli inviati da Alice.

Passiamo ora a vedere come si comporta il protocollo BB84 in presenza di una spia. Questa situazione è rappresentata nella Figura 2, dove la spia, Eve, si è intromessa nel canale quantistico, attuando una tecnica nota come *intercept-resend*: Eve intercetta il fotone mandato da Alice, lo misura e rispedisce un nuovo fotone a Bob codificando l'informazione che ha acquisito. Non conoscendo la base utilizzata da Alice per codificare ciascun bit (la dichiarazione delle basi avviene, infatti, solo alla fine del flusso di stati sul canale quantistico), Eve non può fare altro che scegliere la base di misura in modo casuale. In seguito invia a Bob lo stato corrispondente al risultato misurato codificandolo con la stessa base di cui si è servita per la sua misura.

Per valutare il QBER dovuto in questo caso alla presenza della spia, dobbiamo contare il numero di bit errati nella sifted key. Le basi scelte da Alice e Bob quindi sono da considerarsi sempre

uguali per tutti i bit, dal momento che le misure in cui questo non è vero sono comunque scartate. Nel 50% dei casi, la base scelta da Eve sarà la stessa utilizzata da Alice e Bob (si vedano le colonne gialle della Figura 2): gli stati inviati da Eve a Bob saranno quindi identici a quelli originariamente prodotti da Alice, senza che alcun errore venga introdotto (si vedano le colonne gialle della Figura 2). Nel restante 50% dei casi, in cui invece la base scelta da Eve non coincide con quella utilizzata da Alice e Bob (le celle rosse nella tabella della Figura 2), le misure di quest'ultimo risulteranno completamente casuali e, quindi, fedeli ai bit originali di Alice solamente la metà delle volte. Nella Figura 2 abbiamo evidenziato in arancione con un bordo rosso i bit della sifted key che differiscono da quelli inviati da Alice (per maggior chiarezza si paragonino anche le chiavi finali riportate nelle figure 1 e 2 in assenza e in presenza della spia, rispettivamente).

In un attacco di tipo *intercept-resend*, quindi, viene introdotto un QBER del 25%: ciò significa che, durante la procedura di riconciliazione, Alice e Bob scopriranno che circa il 25% dei bit della *sifted key* non coincide e, di conseguenza, interromperanno immediatamente la trasmissione, in quanto questa discrepanza manifesta chiaramente la presenza di una spia.

Se il rumore introdotto da un canale reale rimane al di sotto del 25%, allora è possibile considerare lo scambio di chiave come intrinsecamente sicuro rispetto a un attacco di tipo *intercept-resend*. La soglia sul QBER può essere innalzata al 27.6% [14] modificando opportunamente il protocollo iniziale e applicando metodi di *information reconciliation* e *privacy amplification* [15].

In linea di principio, Eve potrebbe lanciare anche attacchi più sofisticati, ottenendo un QBER inferiore. In tal modo, si dimostra che il protocollo BB84 è sicuro contro qualsiasi tipo di attacco fisicamente realizzabile a condizione che il rumore del canale sia inferiore all'11% [16]. Questo significa che, indipendentemente dalla particolare strategia adottata da Eve, la sicurezza del protocollo è garantita purché la qualità del canale (il livello di rumore) soddisfi quest'ultima condizione.

In vista di una realizzazione pratica, è bene sottolineare che il BB84 originale qui descritto richiede che Alice generi un singolo fotone per

ogni bit inviato. Tuttavia, la costruzione di sorgenti a singolo fotone è un problema non banale. Con le attuali tecnologie, infatti, una delle tecniche più efficienti utilizzate per generare singoli fotoni richiede processi di ottica non lineare e misure condizionate, capaci di generare i fotoni solamente in maniera probabilistica [17]. Per questa ragione, nelle realizzazioni sperimentali di BB84 vengono impiegati impulsi LASER attenuati, la cui energia media è dell'ordine di un fotone. Tale scelta non è priva di conseguenze. Infatti, come verrà discusso nelle sezioni successive, lo stato quantistico che descrive un impulso LASER, detto stato coerente, è una sovrapposizione quantistica di stati con diverso numero di fotoni. Dunque, con tale codifica, esiste sempre una probabilità non nulla di avere più di un fotone per impulso, con potenziali conseguenze sulla sicurezza del protocollo, in quanto la spia potrebbe sottrarne solo uno senza farsi scoprire [18, 19]. Per superare tali limitazioni e ripristinare la sicurezza intrinseca, diverse varianti di BB84 sono state proposte, tra cui la principale richiede l'utilizzo dei cosiddetti **stati decoy**, che significa "esca" [20, 21, 22].

La prima implementazione di decoy BB84, utilizzando un singolo stato decoy, è stata ottenuta nel 2006, modificando un sistema di QKD commerciale con una distanza di trasmissione di 15 km [23]. In seguito, nel 2007 tre gruppi sperimentali diversi hanno realizzato BB84 con due stati decoy, raggiungendo distanze di trasmissione pari a 102 km [24] e 107 km [25] in fibra ottica, e 144 km [26] in spazio aperto.

I sempre più avanzati progressi nel campo hanno portato nel 2018 a raggiungere la distanza di 421 km: un risultato ottenuto dal gruppo di H. Zbinden realizzando BB84 con un solo stato decoy attraverso una fibra ottica a perdite ultrabasse [27].

## Introduzione ai sistemi a variabili continue

Storicamente i primi protocolli di QKD hanno riguardato sistemi a variabili discrete (discrete variables, DV), in cui l'informazione viene codificata su un insieme discreto di simboli, ad esempio un qubit. D'altra parte, l'implementazione su larga

## Il protocollo GG02

Nel protocollo GG02 Alice invia a Bob una serie di stati coerenti con i valori medi delle quadrature generati campionando una distribuzione Gaussiana. Bob effettua una misura di quadratura, scegliendo con uguale probabilità se misurare l'osservabile  $q$  oppure  $p$ . A seguito della misura, Alice e Bob condividono un'informazione mutua  $\mathcal{I}(A : B)$ .

Dopo lo scambio dei segnali, avviene la fase riconciliazione, che richiede che Alice e Bob si scambino una parte dei loro dati su un canale classico pubblico. Tipicamente si effettua la riconciliazione inversa, in cui è Bob a rivelare i suoi dati ad Alice. D'altro canto, anche Eve è in grado di estrarre un'informazione mutua non nulla a seguito di tale riconciliazione, pari a  $\mathcal{I}(B : E)$ .

Il KGR risulta, dunque, uguale alla differenza delle due informazioni mutue:

$$K = \mathcal{I}(A : B) - \mathcal{I}(B : E),$$

espressa in numero di bit per impulso. In un protocollo realistico, tale quantità deve essere moltiplicata per la larghezza di banda, ovvero il numero di simboli al secondo generati da Alice, il cui valore tipico è dell'ordine del MHz.

scala di BB84 e di altri schemi più avanzati di DV-QKD risulta non banale per una duplice ragione. Come ricordato in precedenza, il principale ostacolo è rappresentato dalla generazione di singoli fotoni, sulla cui polarizzazione codificare i bit "0" e "1". In secondo luogo, le tecnologie richieste dalla DV-QKD non sono compatibili con i sistemi di comunicazione in fibra ottica impiegati attualmente nelle comunicazioni classiche, basati invece sullo scambio di impulsi LASER tra trasmettitore e ricevitore e su misure omodine o eterodine in grado di misurarne il campo elettrico [28]. Per queste ragioni, in tempi più recenti l'interesse è stato rivolto a sistemi a variabili continue (continuous variables, CV) che codificano l'informazione su un parametro continuo, come, per esempio, l'ampiezza o la fase

di un segnale elettromagnetico. L'esempio paradigmatico di un sistema CV è rappresentato, per l'appunto, da un campo ottico, ossia un campo elettromagnetico monocromatico oscillante prodotto localmente da una sorgente (ad esempio un generatore di segnali) e in propagazione nello spazio libero. In questo scenario, gli impulsi LASER tipicamente impiegati nelle comunicazioni sono descritti dai cosiddetti stati "coerenti", indicati con  $|\alpha\rangle$ , caratterizzati da un'ampiezza complessa  $\alpha \in \mathbb{C}$  proporzionale all'ampiezza media del campo elettrico. Osserviamo che anche in questo caso siamo in presenza di una sovrapposizione quantistica: lo stato coerente è, infatti, una sovrapposizione di infiniti stati  $|n\rangle$ , detti stati di Fock, contenenti ciascuno un numero  $n \in \mathbb{N}$  di fotoni e con una ben determinata relazione di fase:

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (17)$$

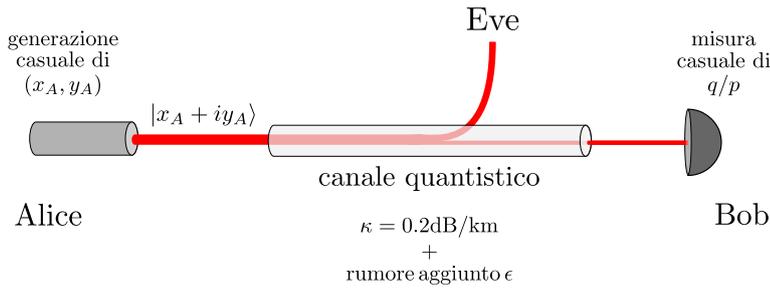
A proposito di campo elettrico, è bene ricordare un risultato fondamentale, valido anche nella teoria classica della radiazione. Per ricostruire il valore del campo elettrico  $E(x)$  in un punto dello spazio  $x$  è necessario misurare due osservabili fisiche distinte, dette "quadrature", tradizionalmente identificate dai simboli  $q$  e  $p$ . Il campo elettrico di una qualunque sorgente risulta infatti essere proporzionale ad una combinazione lineare delle sue quadrature [29, 30]:

$$E(x) \propto q \cos\left(\frac{2\pi x}{\lambda}\right) + p \sin\left(\frac{2\pi x}{\lambda}\right) \quad (18)$$

dove  $\lambda$  è la lunghezza d'onda della radiazione.

Tuttavia, a differenza del caso classico, per un campo ottico in regime quantistico descritto dallo stato coerente  $|\alpha\rangle$  non è possibile conoscere il valore delle due quadrature con precisione arbitraria. Si tratta di una conseguenza delle relazioni di indeterminazione di Heisenberg. Nel caso specifico, a causa delle proprietà quantistiche degli stati coerenti [29], misurando le osservabili  $q$  e  $p$  si registrano valori che fluttuano secondo una distribuzione Gaussiana. Le probabilità  $P(q)$  e  $P(p)$  di misurare i valori  $q$  e  $p$ , rispettivamente, risultano quindi pari a [29, 30]:

$$\begin{aligned} P(q) &= \mathcal{N}_{\sigma_0}(q; \Re(\alpha)), \\ P(p) &= \mathcal{N}_{\sigma_0}(p; \Im(\alpha)). \end{aligned} \quad (19)$$



**Figura 3:** Schema del protocollo GG02. Alice invia a Bob una sequenza di stati coerenti generati secondo una distribuzione normale. I segnali viaggiano lungo il canale quantistico dove vengono attenuati e acquistano un rumore aggiunto  $\epsilon > 0$ . Bob misura una delle due quadrature  $q$  o  $p$  del segnale ricevuto, estraendo l'informazione mutua  $\mathcal{I}(A : B)$ . Il protocollo è sicuro se tale informazione mutua è maggiore di quella potenzialmente estratta da una spia, Eve.

dove:

$$\mathcal{N}_{\sigma_0}(z; \mu) = \frac{\exp\left\{-\frac{(z - 2\sigma_0 \mu)^2}{2\sigma_0^2}\right\}}{\sqrt{2\pi\sigma_0^2}}. \quad (20)$$

Si osserva innanzitutto che il valor medio delle quadrature per uno stato coerente risulta proporzionale alla sua ampiezza:  $\langle q \rangle \propto \Re(\alpha)$  e  $\langle p \rangle \propto \Im(\alpha)$ . Inoltre le distribuzioni di probabilità (19) hanno una varianza non nulla  $\sigma_0^2 > 0$ , conseguenza diretta della quantizzazione del campo e che va sotto il nome di rumore di vuoto. Si noti, infatti, che anche il campo elettrico nello stato di vuoto, corrispondente al caso  $\alpha = 0$ , mostra delle fluttuazioni non nulle nelle due quadrature, che ora hanno entrambe valore medio pari a 0.

A differenza dei sistemi DV, una codifica di questo tipo basata sull'ampiezza (e la fase) del campo risulta compatibile con le tecniche comunemente usate per le comunicazioni classiche, rivelandosi di interesse per un'estensione degli attuali sistemi di comunicazione ottica in regime quantistico.

La presenza del rumore di vuoto rende due segnali coerenti distinti  $|\alpha\rangle$  e  $|\beta\rangle$  aventi ampiezze sufficientemente vicine, cioè  $|\alpha - \beta| \sim \sigma_0$ , indistinguibili dalla sola misura di una quadratura. Questa proprietà torna estremamente utile per la crittografia. Infatti, codificando dei simboli su stati coerenti è possibile trasmettere dell'informazione sicura tra un ricevitore e un trasmettitore, in modo che un'eventuale terza parte non sia in grado di intromettersi e inferire il partico-

lare simbolo generato dalla sorgente. È questo il principio base dei protocolli di distribuzione quantistica di chiave a variabili continue (CV-QKD), il cui esempio paradigmatico è costituito dal protocollo proposto da Frédéric Grosshans e Philippe Grangier nel 2002 e noto come GG02 [31].

## Il protocollo GG02

Lo schema del protocollo GG02 è riportato in Figura 3. Il trasmettitore, Alice, estrae una coppia  $(x_A, y_A)$  di numeri casuali reali campionando una distribuzione Gaussiana  $\mathcal{N}_{\Sigma}(z; 0)$ . Quindi genera un impulso LASER, i.e. uno stato coerente  $|\alpha_A\rangle$ , con ampiezza  $\alpha_A = x_A + iy_A$  e lo invia al ricevitore, Bob, attraverso un canale quantistico [31].

Con il termine "canale" ci si riferisce al supporto fisico, tipicamente rumoroso, che connette Alice e Bob e nel quale propagano i segnali generati. In contesti pratici, il canale quantistico descrive sistemi fisici differenti a seconda della piattaforma utilizzata. Lo scenario tipico è rappresentato dalle comunicazioni in fibra, in cui il canale descrive la fibra ottica che connette Alice e Bob, caratterizzata da un tasso di perdita  $\kappa$  dovuto alla propagazione del segnale nel dielettrico di cui è composta la fibra e da un rumore aggiunto  $\epsilon > 0$  causato dalle imperfezioni del generatore di segnali impiegato da Alice [32].

Possono comunque presentarsi situazioni più complesse. Ad esempio, nelle comunicazioni in spazio aperto o sottomarine, il canale descrive il mezzo stesso di propagazione, rispettivamente

aria o acqua, e, oltre alle perdite, modella anche i fenomeni di assorbimento e dispersione che possono verificarsi in questi ambienti.

Qualunque sia il supporto fisico modellizzato, il canale introduce delle distorsioni dello stato coerente in ingresso e, per questa ragione, viene considerato non fidato, assumendo che tali distorsioni siano opera di una spia, Eve, interessata ad estrarre in tutto o in parte la chiave sicura generata Alice e Bob (si veda la Figura 3). Nel caso di comunicazioni in fibra, ad esempio, si suppone che Eve intercetti la frazione di segnali persa durante la propagazione, e che sia lei stessa a generare il rumore aggiunto  $\epsilon > 0$  osservato sugli impulsi coerenti in uscita [32].

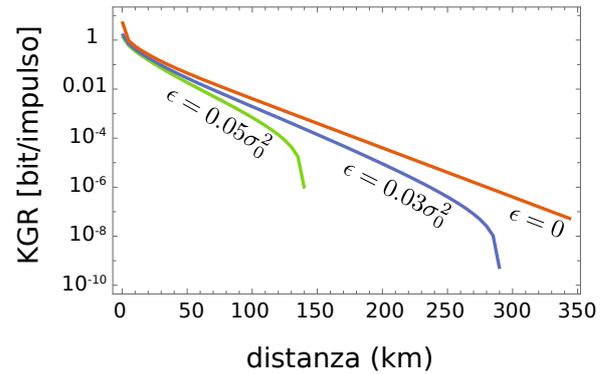
Una volta ricevuti i segnali uscenti dal canale, il ricevitore, Bob, effettua una misura di una delle due quadrature del corrispondente campo elettrico, scegliendo casualmente l'osservabile  $q$  o  $p$  con uguale probabilità. Il risultato della misura è un numero reale  $z_B$  distribuito secondo le Eq. (19) con  $q = x_A$  e  $p = y_A$  ma con una varianza  $\sigma_\epsilon^2$  maggiore del rumore del vuoto,  $\sigma_\epsilon^2 > \sigma_0^2$ . Il valore di  $z_B$  risulta, dunque, correlato alla coppia di simboli in ingresso  $(x_A, y_A)$ . Attraverso un processo di *post-processing* detto "riconciliazione", Bob è in grado di estrarre una parte dell'informazione codificata da Alice nella fase di preparazione del protocollo. Questa quantità, vale a dire la quantità di informazione che Alice e Bob riescono a condividere dopo la misura, prende il nome di "informazione mutua"  $\mathcal{I}(A : B)$ .

Considerazioni analoghe valgono anche per l'azione di Eve, la quale attacca il canale, raccogliendone le perdite e nascondendosi dietro il rumore aggiunto, ed è, dunque, in grado di estrarre un'informazione mutua  $\mathcal{I}(B : E)$  non nulla tramite una misura opportuna.

Pertanto, si conclude che il protocollo è sicuro fintanto che l'informazione mutua estratta da Eve sia inferiore all'informazione mutua scambiata tra Alice e Bob. In tal caso, a seguito del processo di riconciliazione, Alice e Bob possono applicare una serie di tecniche numeriche di *privacy amplification* volte ad estrarre una chiave casuale sicura a partire dalle rispettive liste di dati  $(x_A, y_A)$  e  $z_B$ .

La differenza tra le due informazioni mutue definisce il **tasso di generazione della chiave**

(*key generation rate, KGR*), che rappresenta la lunghezza della chiave estratta, ossia il numero di bit sicuri generati per unità di tempo.



**Figura 4:** KGR in funzione della distanza di trasmissione in km per diversi valori del rumore aggiunto  $\epsilon$ . La presenza del rumore aggiunto introduce una distanza massima di trasmissione oltre la quale non è più possibile distillare una chiave sicura.

Nella Figura 4 è riportato il valore del KGR (in presenza di *reverse reconciliation*) in funzione della distanza di trasmissione espressa in km per alcuni valori realistici dei parametri. Il tasso di perdita delle comuni fibre ottiche è pari a  $\kappa = 0.2$  dB/km, mentre il rumore aggiunto è tipicamente compreso tra  $0.01\sigma_0^2 < \epsilon < 0.05\sigma_0^2$ . Come si osserva, solamente in assenza di rumore aggiunto ( $\epsilon = 0$ ) è possibile effettuare comunicazione sicura a distanze arbitrariamente grandi, mentre per  $\epsilon > 0$  esiste una distanza massima di trasmissione oltre la quale il KGR diventa nullo.

Le potenzialità mostrate dalla CV-QKD sono state anche verificate sperimentalmente. Sino ad oggi, diverse realizzazioni di GG02 sono state testate in laboratorio, analizzando il livello di sicurezza sotto diversi paradigmi. I primi esperimenti *proof-of-principle* risalgono al 2003, in cui è stata impiegata luce visibile a 780 nm e la presenza del canale è stata simulata attraverso un *beam splitter* di transmissività variabile [33]. Tuttavia, le tecniche impiegate in questo lavoro e nei suoi successivi sviluppi [34, 35, 36], pur costituendo una prima dimostrazione pratica, risultano inadatte per un'applicazione in fibra ottica a causa della radiazione utilizzata (incompatibile con le lunghezze d'onda infrarosse impiegate per la comunicazione in fibra, che comunemente sono in tre finestre attorno a 850 nm, a 1300 nm oppure a 1550 nm, lunghezze d'onda *telecom*) e la scarsa

efficienza dei componenti del *setup* e dei codici di riconciliazione.

La prima vera CV-QKD a lunghezze d'onda *telecom* è stata ottenuta solo nel 2007 dal gruppo di Jérôme Lodewyck [37], riuscendo a raggiungere distanze di trasmissione superiori a 25 km. A partire da quella data, nel 2013 e 2016 sono state raggiunte le distanze di 80 km [38] e 100 km [39], rispettivamente. Infine, attraverso l'utilizzo di fibre ottiche a perdite ultrabasse, nel 2020 è stato possibile distillare una chiave sicura a distanze superiori ai 200 km [40]. Parallelamente al tentativo di raggiungere distanze di trasmissione sempre maggiori, le più recenti innovazioni nel campo delle lunghezze *telecom* hanno fatto sì che si potesse anche incrementare il KGR a più basse distanze, riuscendo a estrarre un maggior numero di bit sicuri al secondo. Sui 25 km si è passati dai 2 kbps (kilobit al secondo) dello schema di Lodewyck [37] a 1 Mbps (megabit al secondo) [41], mentre sui 50 km sono stati ottenuti KGR pari a 7.57 kbps [42] e 52 kbps [43].

## Conclusione

Da un lato, la descrizione della natura data dalla Meccanica Quantistica ha permesso di comprendere i suoi meccanismi in maniera più profonda, meccanismi altrimenti elusivi in quanto spesso molto lontani dalla nostra intuizione e dal senso comune. D'altro canto, lo studio approfondito di questa teoria ha aperto la strada a progressi tecnologici irraggiungibili e inimmaginabili nell'ambito della sola fisica classica. A tal riguardo ci piace ricordare la risonanza magnetica nucleare, potente tecnica diagnostica con molteplici sfaccettature, gli orologi atomici che scandiscono il nostro tempo ma, soprattutto, sono fondamentali per il funzionamento del sistema GPS, ma anche tutta la tecnologia basata sul silicio e sui semiconduttori.

In queste pagine vi abbiamo mostrato, seppure in modo semplificato, come la fisica quantistica permetta di dare un contributo rilevante anche alla trasmissione sicura di informazione, focalizzandoci sul problema della distribuzione di chiavi quantistica. Si tratta di un esempio in cui gli sforzi teorici e sperimentali hanno permesso di trasformare le previsioni quantistiche in siste-

mi funzionanti e ormai integrati in alcuni scenari della nostra società fino al livello commerciale.

Un esempio tra tanti della "seconda rivoluzione quantistica" che stiamo vedendo e vivendo in questi anni e che, si spera, possa concorrere a migliorare le condizioni dell'umanità come affermava Nikola Tesla.



- [1] T. S. Kuhn: *La struttura delle rivoluzioni scientifiche*, Einaudi, Torino (2009).
- [2] L. Belloni e S. Olivares: *Planck – La rivoluzione quantistica*, Pelago, (2021).
- [3] P. Ball: *Beyond Weird*, Vintage, Redding, CA (2018).
- [4] L. Branchetti, A. Cattabriga and O. Levrini: *Interplay between mathematics and physics to catch the nature of a scientific breakthrough: The case of the blackbody*, Phys. Rev. Phys. Educ. Res., 15 (2019) 020130.
- [5] H. B. Callen: *Thermodynamics and an Introduction to Thermostatistics*, John Wiley & Sons, Hoboken, NJ (1985).
- [6] S. Olivares: *Appunti di Termodinamica*, Milano University Press, Milano (2023).
- [7] M. L. Giliberti, L. Loviseti, S. Olivares e M. G. A. Paris: *Meccanica quantistica, entanglement e nonlocalità*, Giornale di Fisica, LXIV (2023) 161.
- [8] The Nobel Prize in Physics 2022: <https://www.nobelprize.org/prizes/physics/2022/>
- [9] C. H. Bennett and G. Brassard: *Quantum cryptography: Public key distribution and coin tossing*, Theor. Comput. Sci., 560 (2014) 7.
- [10] G. S. Vernam: *Cipher printing telegraph systems for secret wire and radio telegraphic communications*, Trans. AIEE, XLV (1926) 295.
- [11] C. E. Shannon: *Communication theory of secrecy systems*, Bell Syst. Tech. J., 28 (1949) 656.
- [12] R. L. Rivest, A. Shamir, and L. Adleman: *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM, 21 (1978) 120.
- [13] P. W. Shor: *Algorithms for quantum computation: Discrete logarithms and factoring*, Proceedings 35th Annual Symposium on Foundations of Computer Science, (1994) 124.
- [14] H. F. Chau: *Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate*, Phys. Rev. A, 66 (2002) 60302.
- [15] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin: *Experimental Quantum Cryptography*, J. Cryptol., 5 (1992) 3.
- [16] D. Mayers: *Unconditional security in quantum cryptography*, J. ACM, 48 (2001) 351.
- [17] G. S. Buller and R. J. Collins: *Single-photon generation and detection*, Meas. Sci. Technol., 21 (2010) 012002.

- [18] D. Gottesman, H. K. Lo, Lütkenhaus and J. Preskill: *Security of quantum key distribution with imperfect devices*, *Quant. Inf. Comput.*, 5 (2004) 325.
- [19] V. Scarani, A. Acin, G. Ribordy and N. Gisin: *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak LASER Pulse Implementations*, *Phys. Rev. Lett.*, 92 (2004) 057901.
- [20] X.-B. Wang: *Beating the photon-number-splitting attack in practical quantum cryptography*, *Phys. Rev. Lett.*, 94 (2005) 230503.
- [21] H.-K. Lo, X. Ma and K. Chen: *Decoy State Quantum Key Distribution*, *Phys. Rev. Lett.*, 94 (2005) 230504.
- [22] X.-B. Wang: *Decoy-state protocol for quantum cryptography with four different intensities of coherent light*, *Phys. Rev. A*, 72 (2005) 012322.
- [23] Y. Zhao, B. Qi, X. Ma, H.-K. Lo and L. Qia: *Experimental Quantum Key Distribution with Decoy States*, *Phys. Rev. Lett.*, 96 (2006) 070502.
- [24] C.-Z. Peng et al.: *Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding*, *Phys. Rev. Lett.*, 98 (2007) 2.
- [25] D. Rosenberg et al.: *Long-Distance Decoy State Quantum Key Distribution in Optical Fiber*, *Phys. Rev. Lett.*, 98 (2007) 010503.
- [26] T. Schmitt-Manderbach et al.: *Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km*, *Phys. Rev. Lett.*, 98 (2007) 010504.
- [27] A. Boaron et al.: *Secure Quantum Key Distribution over 421 km of Optical Fiber*, *Phys. Rev. Lett.*, 121 (2018) 190502.
- [28] G. Cariolaro: *Quantum Communications*, Springer International Publishing, Berlino (2015).
- [29] S. Olivares: *Introduction to generation, manipulation and characterization of optical quantum states*, *Phys. Lett. A*, 418 (2021) 127720.
- [30] S. Olivares: *Quantum optics in the phase space: A tutorial on Gaussian states*, *Eur. Phys. J. Special Topics*, 203 (2012) 3.
- [31] F. Grosshans and P. Grangier: *Continuous Variable Quantum Cryptography Using Coherent States*, *Phys. Rev. Lett.*, 88 (2002) 057902.
- [32] F. Laudenbach et al.: *Continuous-Variable Quantum Key Distribution with Gaussian Modulation – The Theory of Practical Implementations*, *Adv. Quantum Technol.*, (2018) 1800011.
- [33] F. Grosshans et al.: *Quantum key distribution using gaussian-modulated coherent states*, *Nature*, 421 (2003) 238.
- [34] S. Lorenz, N. Korolkova and G. Leuchs: *Continuous variable quantum key distribution using polarization encoding and post selection*, *App. Phys. B*, 79 (2004) 273.
- [35] A. Lance et al.: *No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light*, *Phys. Rev. Lett.*, 95 (2005) 180503.
- [36] J. Lodewyck et al.: *Controlling excess noise in fiber-optics continuous-variable quantum key distribution*, *Phys. Rev. A*, 72 (2005) 050303.
- [37] J. Lodewyck et al.: *Quantum key distribution over 25 km with an all-fiber continuous-variable system*, *Phys. Rev. A*, 76 (2007) 042305.
- [38] P. Jouguet et al.: *Experimental demonstration of long-distance continuous-variable quantum key distribution*, *Nat. Photonics*, 7 (2013) 378.
- [39] D. Huang, P. Huang, D. Lin and G. Zeng: *Long-distance continuous-variable quantum key distribution by controlling excess noise*, *Sci. Rep.*, 6 (2016) 19201.
- [40] Y. Zhang et al.: *Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber*, *Phys. Rev. Lett.*, 125 (2020) 010502.
- [41] D. Huang et al.: *Continuous-variable quantum key distribution with 1 Mbps key rate*, *Opt. Express*, 23 (2015) 17511.
- [42] Y. Zhang et al.: *Continuous-variable QKD over 50 km commercial fiber*, *Quantum Sci. Technol.*, 4 (2019) 035006.
- [43] C. Wang et al.: *25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel*, *Sci. Rep.*, 5 (2015) 14607.



**Samuele Altilia:** è un fisico sperimentale, dottorando presso il Dipartimento di Fisica “Aldo Pontremoli” dell’Università degli Studi di Milano. Attualmente si occupa di sistemi ottici per la generazione e la rivelazione di stati quantistici per applicazioni nella comunicazione quantistica.

**Michele N. Notarnicola:** è un fisico teorico, dottorando presso il Dipartimento di Fisica “Aldo Pontremoli” dell’Università degli Studi di Milano. I suoi principali interessi sono la comunicazione quantistica e la distribuzione di chiave quantistica a variabili continue.

**Stefano Olivares:** è un fisico teorico e si occupa di ottica quantistica, informazione quantistica con interesse particolare per la comunicazione quantistica e le sue realizzazioni fotoniche. È Professore Associato presso il Dipartimento di Fisica “Aldo Pontremoli” dell’Università degli Studi di Milano e docente degli insegnamenti di Termodinamica e di Teoria Quantistica della Computazione. Collabora attivamente con diversi gruppi sperimentali ed è anche impegnato nella divulgazione scientifica.



---

# La seconda rivoluzione quantistica: il computer quantistico e la crittografia.

*Taira Giordani, Alessia Suprano, Fabio Sciarrino*

*Dipartimento di Fisica, Sapienza Università, Roma*

---

## Introduzione

La meccanica quantistica, ovvero quell'insieme di straordinarie intuizioni che furono e sono considerate come una vera e propria rivoluzione, è ormai una teoria affermata quasi un secolo fa. Eppure, se ci si sofferma su questo ultimo dettaglio, risulta ancora più sorprendente constatare quanto, rispetto ad altre teorie del passato, essa sia percepita anche a distanza di tanti anni come un qualcosa di nuovo, o di non completamente assimilato, e quindi di difficile comunicazione ad un pubblico non tecnico.

Ancora più sorprendente potrà sembrare il dover parlare di quella che viene definita come la seconda rivoluzione quantistica, ovvero la storia più recente delle applicazioni della teoria che riguardano più da vicino le tecnologie dell'informazione. Ogni rivoluzione, infatti, è figlia dei suoi tempi e non è un caso che questa seconda tappa sia nata non troppo successivamente, se non contemporaneamente, all'affermazione dei primi calcolatori, ai quali da qui in avanti ci ri-

feriremo come computer classici. Infatti, perché non utilizzare proprio un sistema controllato da effetti genuinamente quantistici, ovvero su scale e condizioni fisiche tali da rendere questi effetti evidenti e misurabili, per poter investigare la natura, o tradotto, per poter ampliare la capacità di elaborazione di un computer? Questo fu il primo quesito, attribuito a Richard Feynman, da cui si partì per formalizzare una teoria dell'informazione che tenesse conto dei principi della meccanica quantistica.

In analogia con l'informatica, si definisce un'unità fondamentale, il **qubit**, un sistema costituito da due stati logici 0,1, mutualmente esclusivi. Il qubit descrive però un sistema quantistico per il quale saranno validi sia il principio di sovrapposizione, per cui saranno possibili stati in sovrapposizione dei due livelli logici come stati in sovrapposizione di più qubit, quanto il principio del collasso dello stato durante il processo di misura, ovvero, di estrazione dell'informazione in esso codificata. L'impalcatura teorica dell'informazione quantistica che si sviluppò a partire

dagli anni '80 aveva lo scopo di individuare per quali problemi un paradigma di computazione basato sulla meccanica quantistica potesse effettivamente offrire dei vantaggi, da cui sviluppare appunto protocolli di informazione e algoritmi puramente quantistici [1]. Quanta informazione si può processare e quanta se ne può estrarre da un qubit? Uno stato quantistico può essere copiato senza conoscerne in precedenza l'espressione negli stati logici? Questi sono solo due esempi di domande un po' più tecniche ma molto istruttive inerenti ai fondamenti della teoria dell'informazione quantistica. Esse, infatti, mostrano implicitamente vantaggi e potenziali limiti del paradigma quantistico. L'impossibilità di copiare uno stato quantistico è il principio alla base della sicurezza intrinseca dei protocolli di crittografia quantistica. Come vedremo in seguito più nel dettaglio, essi hanno lo scopo di ottenere uno scambio di una chiave di cifratura sicura tra due interlocutori attraverso comunicazione dell'informazione codificata nei qubit. Il principio di indeterminazione e il processo di misura in meccanica quantistica, si traducono infatti nel no-cloning theorem, la cui conseguenza in un protocollo crittografico è quella di proibire ad un terzo interlocutore di poter accedere all'informazione sui qubit scambiati senza alterarne lo stato [1]. Questo permette ai due comunicanti di individuare in linea di principio la presenza di un terzo nella comunicazione. Per quanto riguarda la computazione quantistica, la possibilità di avere stati o qubit in sovrapposizione fa intuire la possibilità di poter processare l'informazione in parallelo. Questo è indubbiamente uno dei fondamentali vantaggi che hanno motivato negli anni la ricerca nel campo. Ma i teoremi sopra citati e il processo stesso di misura che di fatto limita la quantità di informazione che può essere estratta da un sistema quantistico, spesso pongono dei paletti alle dimensioni del ventaglio dei problemi computazionali per cui si può ottenere un vantaggio. Per vantaggio è utile chiarificare che si indica un miglioramento di come le risorse computazionali quali il tempo di calcolo o il numero di operazioni e qubit, scalino rispetto alla taglia del problema da risolvere. Si ha un vantaggio quantistico se l'algoritmo richiede risorse che aumentano più favorevolmente rispetto all'equivalente classico con la dimensione del dato in

ingresso al processo. Tra gli algoritmi quantistici più famosi che appartengono a questa classe figurano sicuramente quello di scomposizione degli interi in fattori primi, algoritmi di ricerca, algoritmi di ottimizzazione e più recentemente algoritmi quantistici di apprendimento. In questo articolo si vuole riassumere lo sviluppo e l'impatto della seconda rivoluzione quantistica nella teoria e nelle tecnologie dell'informazione. Pertanto, nel seguito, si illustreranno più nel dettaglio i possibili paradigmi di computazione e crittografia quantistica proposte fino ad oggi, insieme alla presentazione delle possibili realizzazioni di tali tecnologie quantistiche. Stato dell'arte, limiti e prospettive saranno infine discusse per capire in quale stagione di questa seconda rivoluzione siamo ormai giunti.

## Computazione quantistica

I principali schemi di computazione quantistica universali proposti nel corso di questi ultimi decenni sono essenzialmente tre, che possono essere riassunti nel modello circuitale [1], il modello measurement-based [2] e il modello di computazione di tipo blind [3, 4]. Uno schema invece totalmente alternativo rispetto ai precedenti è quello di tipo analogico [5]. Nel seguito tratteremo brevemente di ciascuno.

Il modello circuitale è quello storicamente introdotto per primo. Lo spirito di questo modello è di trasporre lo schema classico di computazione che prevede un set di bit e porte logiche elementari per costituire un computer universale. Alla stessa maniera, il modello circuitale quantistico prevede un registro di qubit e un insieme di porte logiche quantistiche con cui operare su di essi. Le porte quantistiche sono delle operazioni unitarie nello spazio di Hilbert che descrive il registro dei qubit. Il qubit, essendo uno stato quantistico, può essere considerato un oggetto matematico equivalente ad un vettore. Le porte logiche che operano sul singolo qubit saranno dunque delle rotazioni in tale spazio vettoriale. Il modello prevede anche delle porte logiche che operano su due qubit, le quali permettono le interazioni tra di essi e di creare stati di sovrapposizione tra più qubit. Esempi di questo tipo sono le porte controllate, come la negazione controllata (controlled-not) oppure la rotazione

controllata (*controlled-phase*), le quali operano sul secondo qubit in maniera condizionata allo stato del primo. La combinazione di rotazioni sul singolo qubit e porte controllate permette di avere uno schema universale per il computer quantistico.

Sebbene il modello circuitale sia il più naturale ed immediato per costruire un computer quantistico, esso può presentare alcune limitazioni nella sua realizzazione fisica. Allo stato attuale i qubit vengono generati e manipolati con un certo grado di rumore, il quale si propaga e si amplifica nelle varie operazioni logiche. In questo schema è quindi necessario introdurre tecniche di correzione degli errori, dette di *error-correction*, per mitigare la loro propagazione e tenere l'accuratezza di calcolo entro una data soglia di tolleranza [6]. In termini di risorse computazionali questo si traduce nell'impiego di qubit e porte ancillari che potrebbero limitare l'effettivo vantaggio dell'impiego di un algoritmo quantistico rispetto alla controparte classica.

Un possibile approccio alternativo di più recente introduzione rispetto al modello circuitale è quello chiamato *measurement-based*. Questo modello prevede la generazione di uno stato di diversi qubit in sovrapposizione tra di loro. In altre parole, anziché preparare tutti i qubit separatamente e farli interagire attraverso un circuito di porte logiche, in questo schema la complessità della costruzione del dispositivo risiede nel generare uno stato di qubit altamente correlati, detto stato *cluster*. La computazione viene svolta da una sequenza di opportune misure su determinate basi di altrettanti determinati qubit del cluster. Il vantaggio dell'approccio *measurement-based* risiede proprio nell'essere per costruzione più robusto al rumore e agli errori. Inoltre, risulta una valida alternativa per tutte quelle piattaforme quantistiche nelle quali la realizzazione del modello circuitale risulta complessa, quali le architetture fotoniche [2] e gli ioni intrappolati [7].

Un terzo schema molto recente è quello noto come *blind quantum computing*. Rispetto ai precedenti, utilizza un paradigma totalmente diverso, che unisce elementi sia di comunicazione che di computazione. Nell'approccio *blind*, la computazione viene delegata dall'utente ad un server che svolge l'algoritmo. Un importante det-

taglio è che non è richiesta da parte del server la conoscenza dello stato iniziale del cliente. Infatti, gli stati scambiati tra i server e gli utenti sono sempre codificati in maniera tale che né il server e né il cliente conosce lo stato quantistico dell'altro, rendendo il processo sicuro da eventuali intromissioni di un terzo interlocutore come in un protocollo crittografico. Pertanto, è richiesto che le operazioni computazionali del server vengano svolte a prescindere dallo stato che arriva dal cliente, al quale, di contro, viene solo richiesto di generare e preparare i qubit. Anche questo protocollo per la computazione quantistica offre dei vantaggi rispetto al numero di risorse quantistiche necessarie per la sua realizzazione. Chiaramente richiede che i qubit possano essere scambiati tra più parti attraverso canali di comunicazione quantistici. Questo elemento aggiuntivo restringe il campo delle piattaforme fisiche che si prestano alla realizzazione dello schema. Infatti, ad oggi, figurano solo primi esperimenti basati su qubit fotonici, i quali, non a caso, sono quelli che ben più si adattano a protocolli che prevedono comunicazione, come vedremo nella sezione dedicata alla crittografia.

L'approccio analogico alla computazione quantistica è fondato su principi completamente diversi. I parametri della computazione non sono le operazioni unitarie sui qubit, ma bensì l'energia di interazione tra di essi, descritti dall'*hamiltoniana* del sistema. La computazione quantistica analogica risulta vantaggiosa quando si vogliono realizzare, algoritmi di simulazione di una data *hamiltoniana* di cui è difficile individuare autovalori e autovettori, oppure, algoritmi di ottimizzazione in cui si fa coincidere la soluzione del problema con il livello fondamentale dell'*hamiltoniana* del processore quantistico [8]. Questo modello alternativo può favorire alcune piattaforme rispetto ad altre, come ad esempio quelle che sfruttano sistemi di atomi neutri.

## Crittografia quantistica

Come introdotto nella precedente sezione, stabilire canali quantistici di comunicazione che siano sicuri rispetto ad eventuali intromissioni di un terzo interlocutore è un ingrediente fondamentale per lo sviluppo di *blind quantum computer*. Inoltre, nell'era digitale in cui viviamo, la sicurezza

za delle comunicazioni è diventata una preoccupazione sempre più rilevante che ha reso fondamentale trovare soluzioni avanzate per proteggere le informazioni sensibili. I sistemi tradizionali di crittografia, si basano su algoritmi matematici complessi la cui risoluzione richiede un numero di risorse computazionali troppo elevato per poter essere raggiunta con i computer classici. Conseguentemente, l'impiego di nuove tecnologie, come quelle quantistiche, per sviluppare calcolatori in grado di risolvere efficientemente tali algoritmi, potrebbe inficiare la sicurezza dei sistemi di crittografia classica. In questo contesto, la crittografia quantistica si è rivelata una tecnologia rivoluzionaria in grado di garantire una comunicazione intrinsecamente sicura.

Il concetto chiave della crittografia quantistica è la distribuzione di una chiave crittografica segreta tra due parti che desiderano comunicare in modo sicuro. Tale distribuzione avviene attraverso protocolli di Quantum Key Distribution (QKD), in cui la chiave viene codificata nello stato di particelle quantistiche e la sicurezza è garantita dal *no-cloning theorem*, che proibisce ad un terzo interlocutore di estrarre informazioni sulla chiave senza alterare lo stato delle particelle stesse. Sebbene, diverse particelle quantistiche potrebbero essere utilizzate per codificare informazioni, l'alta trasmissibilità e la bassa interazione dei singoli fotoni con l'ambiente, rendono questi ultimi particolarmente adatti alla trasmissione a distanza. Conseguentemente, nella maggior parte delle implementazioni sperimentali, la trasmissione delle chiavi crittografiche avviene inviando singoli fotoni e codificando l'informazione nei suoi gradi di libertà, come la polarizzazione.

I diversi protocolli di QKD si possono dividere in due categorie principali: i protocolli di preparazione e misura e i protocolli basati sull'entanglement [9].

Per quanto riguarda la prima categoria, uno dei più conosciuti ed utilizzati è il protocollo BB84, sviluppato da Charles Bennett e Gilles Brassard nel 1984 [10]. In quest'ultimo, i bit costituenti la chiave segreta sono codificati in fotoni polarizzati e il mittente (Alice) può scegliere tra due basi di codifica, di solito lineare o diagonale. Allo stesso modo, il destinatario (Bob) sceglierà casualmente la base di misura. Successivamente,

confrontando le loro basi attraverso un canale pubblico, Alice e Bob sono in grado di individuare la presenza di un terzo interlocutore e selezionando solamente i bit non compromessi riescono a distribuire una chiave sicura.

D'altra parte, il protocollo E91, sviluppato da Artur Ekert nel 1991 [11], è il primo protocollo basato sull'entanglement. In questo caso, Alice e Bob, condividono una coppia di fotoni entangled. Entrambi i partecipanti misurano lo stato delle loro particelle in diverse basi e successivamente confrontano i risultati tramite un canale pubblico non sicuro. Sapendo che le correlazioni quantistiche tra la coppia di fotoni assicurano che chiunque intercetti uno dei due oggetti altera il sistema complessivo, Alice e Bob possono rilevare la presenza di terze parti e trasmettere una chiave crittografica sicura.

Oltre ai protocolli illustrati diverse varianti sono state sviluppate e implementate in piattaforme che sfruttano comunicazioni in fibre ottiche, nello spazio libero o tramite satelliti [12]. Un esempio degno di nota riguarda il lancio del satellite cinese Micius nel 2016. Quest'ultimo, generando fotoni entangled e trasmettendoli a stazioni terrestri distanti 1203 km, ha permesso di superare i limiti di distanza legati alla comunicazione terrestre [13].

## Piattaforme computer quantistico

Sebbene teoricamente si è dimostrato che lo sfruttamento delle proprietà quantistiche in computazione permetterebbe di risolvere problemi complessi in modo molto più efficiente, la realizzazione sperimentale del computer quantistico è ancora in una fase di sviluppo in quanto presenta delle sfide significative. Per far fronte a tali sfide, sono state sviluppate diverse implementazioni basate su superconduttori, atomi, ioni o fotoni.

Il computer quantistico a superconduttori sfrutta circuiti superconduttori per manipolare e memorizzare informazioni quantistiche. In particolare, sono realizzati utilizzando dispositivi microelettronici a temperature vicine allo zero assoluto (-273,15 °C). I qubit sono implementati come giunzioni Josephson in grado di generare e controllare gli stati di sovrapposizione e l'interferenza quantistica [14]. Tale tecnologia, permette di manipolare velocemente lo stato dei qubit, ave-

re un elevato controllo su quest'ultimo e propone una piattaforma altamente scalabile. Tuttavia, i computer a superconduttore sono sensibili alle perturbazioni ambientali e necessitano un raffreddamento a basse temperature per sfruttare le proprietà superconduttive dei materiali [15].

Un'altra possibilità nell'implementare i computer quantistici si basa sullo sfruttamento di atomi neutri [16, 17] o ioni intrappolati [18] e raffreddati a temperature molto basse. Questi ultimi, conosciuti come computer quantistici ad atomi freddi, memorizzano l'informazione codificando i qubit negli stati quantistici degli atomi o degli ioni intrappolati. La manipolazione degli stati degli atomi o ioni avviene, rispettivamente, utilizzando laser o campi elettromagnetici.

Un'altra possibile codifica dei qubit risiede nello sfruttamento degli spin di singole particelle. In tali computer quantistici a qubit di spin, la manipolazione avviene attraverso campi magnetici, impulsi di microonde e altre tecniche di controllo per modificare gli stati di spin. Per la realizzazione di tali calcolatori, diverse piattaforme continuano ad essere esplorate, come i qubit di spin di ioni intrappolati [19], dei centri NV [20], molecolari [21] e basati su semiconduttori [22].

Infine, diverse piattaforme fotoniche sono state utilizzate per sviluppare computer quantistici che sfruttano la luce (fotoni) al fine di rappresentare e manipolare l'informazione quantistica. Sia le variabili discrete che continue possono essere sfruttate per codificare i qubit [23]. Nel primo caso, si utilizzano solitamente gli stati di polarizzazione dei fotoni o i loro stati di cammino (modalità spaziali), mentre nel secondo gli osservabili del campo elettromagnetico. Tramite l'ottica integrata è possibile proporre piattaforme scalabili, in cui la generazione, manipolazione e rivelazione dei singoli fotoni avviene attraverso elementi ottici integrati in una singola piattaforma oppure attraverso un approccio ibrido [24]. In questo caso, la sfida principale è di riuscire a scalare in maniera significativa il numero di elementi integrati e di minimizzare le diverse perdite del sistema.

## Stato dell'arte e prospettive future

Nelle sezioni precedenti abbiamo introdotto i concetti chiave della computazione e della crittografia quantistica e discusso i possibili sistemi fisici che vengono oggi investigati per poter sviluppare tecnologie nei suddetti campi. Attualmente l'informazione quantistica sta vivendo una stagione di transizione, ovvero da una situazione in cui la maggior parte della ricerca si svolge in ambito accademico ad uno scenario in cui grandi aziende e grandi investimenti incentivano lo sviluppo di tali tematiche, allo scopo di realizzare prototipi performanti da introdurre sul mercato.

Tra le piattaforme più mature per quanto riguarda la computazione quantistica figura quella che sfrutta qubit superconduttori e il modello circuitale. Google, Rigetti e IBM sono le più grandi aziende che hanno deciso di sviluppare un computer quantistico con questa tecnologia. In particolare, IBM mette a disposizione sul suo cloud [25] diversi dispositivi che contano fino a centinaia di qubit e prevede di aumentare la capacità di calcolo dei suoi processori raggiungendo i 100000 qubits nei prossimi 10 anni. Inoltre, recentemente, la start-up francese Alice & Bob sta proponendo una variante nel controllo dei qubit superconduttori allo scopo di mitigare il rumore e le procedure di error-correction nelle varie porte logiche.

Un approccio sempre di tipo circuitale è utilizzato dalla start-up IonQ che propone però processori basati su ioni intrappolati fino a 20 qubit. Il processore di IonQ è disponibile sul cloud di Amazon Braket [26], la piattaforma gestita da Amazon che permette l'utilizzo da remoto di diversi processori quantistici delle diverse aziende e start-up del settore.

Le piattaforme basate su atomi neutri intrappolati stanno raggiungendo livelli di complessità e performance significative. La start-up americana QuEra mette a disposizione sul cloud di Amazon Braket un computer ad atomi neutri che conta 250 qubit, mentre la start-up francese PASQAL commercializza processori con 100 qubit. Questi dispositivi sono basati sulla computazione analogica, in cui le operazioni logiche vengono realizzate cambiando l'hamiltoniana di

interazioni tra gli atomi.

In ambito fotonico le principali start-up, ovvero l'americana Psi Quantum e la canadese Xanadu, stanno procedendo verso un computer quantistico basato sull'approccio measurement-based. Più precisamente, Psi Quantum sta puntando su qubit processati attraverso fotonica integrata. La start-up Xanadu invece sta utilizzando il cosiddetto schema a variabili continue, nel quale l'informazione viene codificata nei valori attesi degli osservabili del campo elettromagnetico, che possono assumere, per l'appunto, valori continui. Xanadu ha a disposizione due dispositivi sul proprio cloud [27], compreso Borealis (disponibile fino allo scorso 2 giugno 2023), il processore quantistico non universale che ha dimostrato recentemente la possibilità di superare un computer classico nella risoluzione di uno specifico problema di campionamento [28]. In ambito europeo, segnaliamo le startup Quandela e QuiX, la prima impegnata principalmente nella produzione di sorgenti di singoli fotoni performanti e commercializzabili, mentre la seconda si occupa del design e dello sviluppo della parte circuitale dei dispositivi fotonici integrati. Come anticipato nelle precedenti sezioni, i qubit fotonici sono impiegati soprattutto nell'ambito delle comunicazioni e della crittografia. Le aziende Toshiba e ID Quantique sono impegnate nel produrre strumenti e dispositivi per la crittografia quantistica. Un prototipo di rete di comunicazione quantistica su grande scala è stato realizzato in Cina, il quale comprende canali di comunicazione in fibra ottica tra le città di Beijing, Hefei, Shanghai e Jinan e il canale satellitare tra gli osservatori di Nanshan e Xinglong [29]. Altre reti quantistiche basate su fibre sono in sviluppo nel Regno Unito [30] e in Europa [31], compresa l'Italia.

Dal quadro appena fornito risulta evidente quanto le tecnologie quantistiche siano ad oggi di centrale interesse. Gli investimenti fatti da diverse aziende e nazioni in queste tematiche hanno subito un vistoso incremento negli ultimi 5 anni. La sfida dei prossimi anni sarà quindi di riuscire a sviluppare quella svolta tecnologica necessaria per rendere tali dispositivi utilizzabili e performanti in problemi concreti. Ovvero, in altre parole, di poter considerare conclusa la stagione della seconda rivoluzione quantistica, per aprire la strada alla terza, quella dello sviluppo

tecnologico vero e proprio.

## Ringraziamenti

Questo lavoro è supportato dalla sovvenzione ERC Advanced QU-BOSS (Grant Accordo n. 884676) e dal progetto PNRR MUR PE0000023-NQSTI.



- [1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge (UK) (2010).
- [2] H. Briegel et al.: *Measurement-based quantum computation*, *Nature Phys.*, 5 (2009) 19.
- [3] A. Broadbent, J. Fitzsimons, E. Kashefi *Universal Blind Quantum Computation* 2009 50th Annual IEEE Symposium on Foundations of Computer Science, Atlanta, GA, USA, (2009) 517.
- [4] V. Giovannetti, L. Maccone, T. Morimae, T. G. Rudolph: *Efficient Universal Blind Quantum Computation*, *Phys. Rev. Lett.*, 111 (2013) 230501.
- [5] E. Farhi, S. Gutmann: *Analog analogue of a digital quantum computation*, *Phys. Rev. A*, 57 (1998) 2403.
- [6] S. J. Devitt, W. J. Munro, K. Nemoto: *Quantum error correction for beginners.*, *Reports on Progress in Physics*, 76 (2013) 076001.
- [7] B. P. Lanyon et al.: *Measurement-Based Quantum Computation with Trapped Ions*, *Phys. Rev. Lett.*, 111 (2013) 210501.
- [8] A. Das, B. K. Chakrabarti: *Colloquium: Quantum annealing and analog quantum computation*, *Rev. Mod. Phys.*, 80 (2008) 1061.
- [9] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden: *Quantum cryptography*, *Reviews of modern physics*, 74 (2002) 145.
- [10] A. K. Ekert: *Quantum cryptography based on Bell's theorem*, *Phys. Rev. Lett.*, 67 (1991) 661.
- [11] C. H. Bennett, G. Brassard: *Quantum cryptography: Public key distribution and coin tossing*. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, New York, 175 (1984) 8.
- [12] S. Pirandola et al.: *Advances in quantum cryptography*, *Advances in optics and photonics*, 12 (2020) 1012.
- [13] S. K. Liao et al.: *Satellite-to-ground quantum key distribution*, *Nature*, 549 (2017) 43.
- [14] M. H. Devoret, A. Wallraff, J. M. Martinis *Superconducting Qubits: A Short Review* (2004) ArXiv./abs/cond-mat/0411174
- [15] M. Kjaergaard et al.: *Superconducting qubits: Current state of play*, *Annual Review of Condensed Matter Physics*, 11 (2020) 369.

- [16] H. J. Briegel et al.: *Quantum computing with neutral atoms*, *Journal of modern optics*, 47 (2000) 415.
- [17] L. Henriët et al.: *Quantum computing with neutral atoms*, *Quantum*, 4 (2020) 327.
- [18] C. D. Bruzewicz, J. Chiaverini, R. McConnell, J. M. Sage: *Trapped-ion quantum computing: Progress and challenges*, *Applied Physics Reviews*, 6 (2019) 021314.
- [19] You-Song Ding, Yi-Fei Deng, Yan-Zhen Zheng: *The rise of single-ion magnets as spin qubits*, *Magnetochemistry*, 2 (2016) 40.
- [20] L. Childress, R. Hanson: *Diamond NV centers for quantum computing and quantum networks*, *MRS bulletin*, 38 (2013) 134.
- [21] A. Gaita-Ariño, F. Luis, S. Hill, E. Coronado: *Molecular spins for quantum computation*, *Nature chemistry*, 11 (2019) 301.
- [22] J. J. Pla et al.: *A single-atom electron spin qubit in silicon*, *Nature*, 489 (2012) 541.
- [23] F. Flamini, N. Spagnolo, F. Sciarrino: *Photonic quantum information processing: a review*, *Reports on Progress in Physics*, 82 (2018) 016001.
- [24] J. Wang, F. Sciarrino, A. Laing, A., M. G. Thompson: (2020). *Integrated photonic quantum technologies* *Nature Photonics*, 14 (2020) 273;  
E. Pelucchi et al. *The potential and global outlook of integrated photonics for quantum technologies* *Nature Reviews Physics*, 4 (2022) 194.
- [25] IBM Quantum <https://quantum-computing.ibm.com/>
- [26] Amazon Web Service (AWS), Amazon Braket <https://aws.amazon.com/it/braket/>
- [27] Xanadu, Xanadu cloud, <https://www.xanadu.ai/>
- [28] L. S. Madsen et al.: *L, ., S (. ) .*, Laudenbach, F., Askarani, M.F. et al. *Quantum computational advantage with a programmable photonic processor* *Nature* 6062022 75
- [29] Y.A. Chen et al.: *An integrated space-to-ground quantum communication network over 4,600 kilometres*, *Nature*, 589 (2021) 214.
- [30] Quantum Communications Hubs, <https://www.quantumcommshub.net/>
- [31] The European Quantum Communication Infrastructure (EuroQCI) Initiative, <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>



**Taira Giordani:** ha conseguito il dottorato di ricerca nel 2020 nel Dipartimento di Fisica della Sapienza Università di Roma dove è attualmente ricercatrice. Le sue attività di ricerca riguardano protocolli di computazione quantistica basati su piattaforme fotoniche. In particolare, si occupa

di esperimenti su fotonica integrata e bulk, sfruttando diversi gradi di libertà di stati a singolo fotone.

**Alessia Suprano:** ha conseguito il dottorato di ricerca nel 2022 nel Dipartimento di Fisica della Sapienza Università di Roma dove attualmente è titolare di un assegno di ricerca. Le sue attività si focalizzano principalmente su protocolli di informazione quantistica che impiegano risorse fotoniche ad alta dimensione.

**Fabio Sciarrino:** è Professore Ordinario presso il Dipartimento di Fisica dell'Università di Roma La Sapienza e Senior Research Fellow presso la Scuola Internazionale Superiore di Studi Avanzati Sapienza, SSAS. È Principal Investigator del Quantum Information Lab, Dipartimento di Fisica. Le sue principali competenze sono l'ottica quantistica sperimentale, il calcolo e l'informazione quantistica e le basi della meccanica quantistica.



---

# Dequantizzazione Geometrica

**Giuseppe Marmo**

*Dipartimento di Fisica "E. Pancini", Università di Napoli Federico II;  
INFN - Sezione di Napoli, Via Cintia - 80126 Napoli, Italy*

**Alessandro Zampini**

*Dipartimento di Matematica ed Applicazioni "R. Caccioppoli", Università di Napoli Federico II;  
INFN - Sezione di Napoli, Via Cintia - 80126 Napoli, Italy*

---

## 1. Introduzione

Sin dalla sua introduzione all'inizio del secolo ventesimo al fine di descrivere misure osservate in sistemi fisici microscopici o in interazione con particolari campi di radiazione, la meccanica quantistica ha portato con sé l'idea che, alle scale di lunghezze o energie in cui la meccanica classica (e la teoria classica della radiazione) predice risultati in accordo con le misure, essa deve accordarsi alla descrizione classica. Questo pensiero è presente già nelle parole di Bohr [1],

“Per ottenere la necessaria connessione con la ordinaria teoria della radiazione, noi dobbiamo assumere che una relazione, analoga a quella già provata per le frequenze, valga nel limite per grandi  $n$ , per le intensità delle diverse linee dello spettro [...]”.

A tale assunzione si è fatto poi riferimento con il nome di **principio di corrispondenza**. In poche righe, Bohr evidenzia che l'esistenza di una corrispondenza tra la descrizione quantistica di un sistema e quella classica è concettualmente necessaria, che essa si possa pensare come formulata matematicamente in termini di un opportuno limite, e che questo limite si applichi

<sup>1</sup>Ovvero per nel limite per energie crescenti, identificate da valori discreti di  $n$  per i sistemi considerati.

allo spettro di specifiche quantità misurate (osservabili, nel linguaggio che usiamo oggi) e più in generale vada considerato in modo specifico per ogni singolo sistema.

Questi temi sono presenti, all'interno di uno studio più generale sui principi e sulla formulazione matematica della meccanica quantistica, in ciò che scrive Dirac nel suo famoso manuale [2], ovvero

“La meccanica classica deve essere un caso limite di quella quantistica. Noi ci aspettiamo che nozioni importanti in meccanica classica corrispondano a nozioni importanti in meccanica quantistica. Dalla comprensione della natura generale dell'analogia tra la meccanica classica e la meccanica quantistica noi possiamo allora sperare di ottenere leggi e teoremi in meccanica quantistica che appaiano come semplici generalizzazioni di ben noti risultati in meccanica classica.”

Il problema del limite classico della meccanica quantistica è stato naturalmente studiato da allora, e ha portato ad una comprensione migliore sia delle teorie quantistiche che di quelle classiche, analizzate secondo tale prospettiva (la bibliografia su questi temi è sterminata, e noi ci limitiamo a rimandare il lettore a [3], in cui l'autore analizza i principali riferimenti, ponendoli in una

prospettiva storica). Lo scopo di questa nota è presentare, all'interno di una descrizione geometrica di un sistema fisico, un insieme di domande sul problema della **dequantizzazione**, ovvero del limite classico di un sistema quantistico, ed analizzare più in dettaglio alcune di esse in relazione alle varie rappresentazioni della meccanica quantistica <sup>2</sup>.

Nella sezione 2 presentiamo una formulazione matematica sia della dinamica quantistica di un sistema fisico, che della dinamica classica di un sistema fisico, individuando i termini di stato, osservabile, evoluzione temporale e sottolineando analogie e differenze fra i due formalismi. In virtù di esse, concludiamo tale sezione (nella 2.4) enucleando alcune domande sul problema del limite classico. In questa descrizione proviamo inoltre a mostrare come lo studio della fisica teorica resti circostanziato attraverso nozioni di geometria, algebra, analisi funzionale, e che le questioni concettualmente più delicate richiedano una solida traduzione all'interno di un formalismo matematico. Coerenti con l'osservazione che la descrizione matematica della meccanica quantistica ha sviluppato differenti rappresentazioni <sup>3</sup>, nella sezione 3 descriviamo il formalismo di Poisson e quello simplettico per la meccanica classica, e la formulazione à la Weyl-Wigner per la meccanica quantistica, fondato sulla nozione di sistema di Weyl e di prodotto à la Moyal. Lungo questo cammino, nella sezione 4 descriviamo come un'opportuna procedura di limite conduca dalla descrizione dell'evoluzione quantistica in termini dell'equazione di Schrödinger alla descrizione classica in termini dell'equazione di Hamilton-Jacobi, e nella sezione 5 come l'evoluzione quantistica e quella classica possono essere formulate in termini della nozione di evoluzione unitaria su un opportuno spazio di Kähler.

<sup>2</sup>Un approccio nello spirito di questa nota è presente in [4], in cui l'autore descrive ciò che risulta parte di un programma più ampio di dequantizzazione geometrica (in particolare, per quella classe di dinamiche quantistiche a cui corrispondono dinamiche classiche il cui spazio delle fasi è uno spazio vettoriale simplettico) – programma che sorge naturalmente all'interno del formalismo, in quegli anni intensamente studiato, della quantizzazione geometrica (il lettore incontrerà una descrizione di questo formalismo nella sezione 3).

<sup>3</sup>Con il termine di rappresentazione della meccanica quantistica intendiamo qui la traduzione italiana del termine inglese *picture*.

## 2. Descrizione matematica di un sistema fisico

Ogni descrizione matematica di un sistema fisico e della sua evoluzione temporale richiede di identificare un insieme  $\mathcal{S}$  di stati, che rappresentano un'informazione massimale sul sistema, un insieme  $\mathcal{O}$  di osservabili, ovvero le quantità misurabili per il sistema, ed un accoppiamento tra essi (un *pairing*) dato da una applicazione

$$\mu : \mathcal{O} \times \mathcal{S} \rightarrow \mathcal{P}$$

in cui  $\mathcal{P}$  è l'insieme delle misure di probabilità su  $\mathbb{R}$ . Dato uno stato  $\rho \in \mathcal{S}$  e un'osservabile  $A \in \mathcal{O}$ , la quantità

$$0 \leq \mu(A, \rho)(\Delta) \leq 1$$

fornisce la probabilità che la misura di  $A$ , con il sistema nello stato  $\rho$ , dia un risultato in  $\Delta$ , un elemento nella  $\sigma$ -algebra di Borel su  $\mathbb{R}$ . Analizzare, inoltre, sistemi costituiti da un insieme di sottosistemi richiede di avere una legge di composizione in virtù della quale definire sistemi composti a partire da sistemi più elementari. Tali nozioni appaiono coerentemente descritte in termini geometrici considerando l'insieme delle osservabili  $\mathcal{O}$  come il sottospazio reale di una  $*$ -algebra unitale  $\mathcal{A}$  sul campo complesso  $\mathbb{C}$  dotata di una norma. L'uso di strutture complesse in fisica permette di descrivere fenomeni di interferenza, e sembra necessaria <sup>4</sup> nei problemi di creazione e distruzione di particelle in teorie di campo quantistiche. All'algebra normata  $\mathcal{A}$  corrisponde il suo duale  $\mathcal{A}^*$ , ovvero lo spazio dei funzionali lineari  $\rho : \mathcal{A} \rightarrow \mathbb{C}$  continui <sup>5</sup>. La norma su  $\mathcal{A}$  induce una topologia su  $\mathcal{A}^*$ : in virtù di essa, l'insieme degli stati  $\mathcal{S}$  si identifica con gli elementi positivi e normalizzati in  $\mathcal{A}^*$ . Il *pairing* tra osservabili e stati è formulato attraverso la dualità tra  $\mathcal{A}$  e  $\mathcal{A}^*$ , mentre la composizione di sistemi viene descritta in termini di prodotto tensoriale fra le corrispondenti algebre.

<sup>4</sup>Un recente esperimento sembra indicare la necessità che nella formulazione matematica di un sistema quantistico sia presente una struttura complessa. Rimandiamo il lettore a [5].

<sup>5</sup>Sono continui quei funzionali  $\rho : \mathcal{A} \rightarrow \mathbb{C}$  per cui, per ogni  $a \in \mathcal{A}$ , esiste una costante  $\alpha \in \mathbb{R}$  tale che  $|\rho(a)| \leq \alpha \|a\|$ .

Ciò che abbiamo visto nelle righe precedenti può essere considerato come una descrizione geometrica della cinematica di un sistema fisico <sup>6</sup>, ovvero di una sua descrizione indipendente dal tempo. La dinamica di un sistema fisico (ovvero l'evoluzione temporale delle sue osservabili, o alternativamente dei suoi stati) associato ad un'algebra  $\mathcal{A}$  si può formulare come l'azione di un gruppo ad un parametro  $\Phi_t$  (con  $t \in \mathbb{R}$  la variabile temporale) di opportuni automorfismi di  $\mathcal{A}$  su sé stessa, o (dualmente) sullo spazio  $\mathcal{S}$  degli stati <sup>7</sup>. Intendiamo con ciò che, per ogni  $t \in \mathbb{R}$ , la composizione di tali automorfismi dia

$$\Phi_{t+t'} = \Phi_t \circ \Phi_{t'}$$

con  $\Phi_{t=0} = \mathbb{I}$  (ovvero l'identità su  $\mathcal{A}$ ). Ogni gruppo (continuo<sup>8</sup>) ad un parametro di automorfismi in  $\mathcal{A}$  ha un generatore infinitesimo, che è una **derivazione** <sup>9</sup> in  $\mathcal{A}$ .

Sia la descrizione di una dinamica classica che quantistica di un sistema fisico rientrano in questo dominio. Qui ci limiteremo a considerare sistemi fisici con un numero finito di gradi di libertà – secondo l'espressione dei manuali classici di meccanica – intendendo con ciò che non considereremo teorie di campo. Invero non considereremo sistemi fisici limitati in interazione con un ambiente (la cui evoluzione si studia in termini di semigrupp), o sistemi la cui evoluzione temporale è descritta da equazioni differenziali implicite, come ad esempio quelle relative a Lagrangiane degeneri.

<sup>6</sup>In quale misura abbia senso una suddivisione tra cinematica e dinamica per un sistema classico è analizzato, ad esempio, in [6], a cui rimandiamo.

<sup>7</sup>Per automorfismi di  $\mathcal{A}$  intendiamo le corrispondenze  $\Phi : \mathcal{A} \rightarrow \mathcal{A}$  che sono compatibili con le strutture algebriche di  $\mathcal{A}$ , ovvero per cui  $\Phi(a + a') = \Phi(a) + \Phi(a')$ ,  $\Phi(aa') = \Phi(a)\Phi(a')$ ,  $\Phi(\alpha a) = \alpha\Phi(a)$  e  $\Phi(a^*) = (\Phi(a))^*$  per ogni  $a, a' \in \mathcal{A}$  e  $\alpha \in \mathbb{C}$ .

<sup>8</sup>Intendiamo gruppi ad un parametro  $\Phi_t$  che siano continui in norma, ovvero che soddisfino la condizione  $\lim_{t \rightarrow 0} \|\Phi_t(a) - a\| = 0$  per ogni  $a \in \mathcal{A}$ .

<sup>9</sup>Un operatore lineare  $\delta : D(\delta) \rightarrow \mathcal{A}$  da una \*-sottoalgebra  $D(\delta) \subseteq \mathcal{A}$  (il dominio di  $\delta$ ) tale che  $\delta(a^*) = \delta(a)^*$  e  $\delta(aa') = a\delta(a') + (\delta(a))a'$  è detta una \*-derivazione. È possibile provare che, se  $\Phi_t$  è un gruppo ad un parametro di automorfismi in  $\mathcal{A}$ , allora il suo generatore infinitesimo è la \*-derivazione data da  $\delta(a) = \lim_{t \rightarrow 0} (\Phi_t(a) - a)/t$  sul dominio  $\mathcal{D}(\delta)$  dato dagli elementi  $a \in \mathcal{A}$  per cui il limite esiste. Vedi anche [7, 8].

Come il lettore avrà osservato, questa descrizione richiama strutture matematiche tradizionalmente riferite ad aree differenti: quella di algebra e di suo spazio duale, quello di norma (e quindi di topologia), quello di automorfismi e gruppi, quello di misure di probabilità, di insiemi boreliani, di prodotti tensoriali e di prodotti di misure. Questa uniformità è ciò a cui ci si riferisce quando si parla di analogie tra la descrizione classica e quella quantistica per la dinamica di un sistema fisico.

Il primo scopo delle pagine seguenti in questa sezione è allora quello di delineare tali analogie, ovvero presentare il modo in cui sia una descrizione matematica della meccanica quantistica che della meccanica classica corrispondano a specifiche realizzazioni delle strutture formali presentate nell'introduzione precedente. Sarà all'interno di queste analogie che illustreremo in seguito alcuni aspetti del problema del limite classico della meccanica quantistica, inteso nel senso di analizzare il significato del passaggio tra diverse realizzazioni di una stessa struttura geometrica nell'ambito dello studio della dinamica di un sistema fisico.

## 2.1 Una descrizione geometrica della meccanica quantistica

In meccanica quantistica l'insieme  $\mathcal{O}$  delle osservabili è dato dallo spazio vettoriale (su  $\mathbb{R}$ ) degli operatori autoaggiunti  $Op(\mathcal{H})$  su uno spazio di Hilbert  $\mathcal{H}$  complesso e separabile. Facendo riferimento alla notazione bra-ket à la Dirac [2], se

$$a = a^* = a^\dagger$$

è un operatore autoaggiunto su  $\mathcal{H}$ , e ha una parte di spettro puntuale  $\sigma_p(a)$  con

$$a|e_k\rangle = \lambda_k|e_k\rangle$$

e una parte di spettro continuo  $\sigma_c(a)$  con

$$a|\varphi_\alpha\rangle = \alpha|\varphi_\alpha\rangle$$

in termini di autofunzioni proprie e generalizzate (indicate con  $|\rangle$ ), allora possiamo scrivere una risoluzione spettrale

$$1 = \sum_{\lambda_k \in \sigma_p(a)} |e_k\rangle\langle e_k| + \int_{\sigma_c(a)} d\alpha |\varphi_\alpha\rangle\langle \varphi_\alpha|$$

e, per ogni  $\Delta$  dato da un sottoinsieme (boreliano, ovvero misurabile) di  $\mathbb{R}$ , un proiettore ortogonale

$$E_a(\Delta) = \sum_{\lambda_k \in \Delta} |e_k\rangle\langle e_k| + \int_{\Delta} d\alpha |\varphi_\alpha\rangle\langle \varphi_\alpha|.$$

Ogni misura di probabilità che corrisponde a uno stato  $\rho \in \mathcal{S}$  si può scrivere allora come <sup>10</sup>

$$\mu(a, \rho) : \Delta \mapsto \text{Tr}(W_\rho E_a(\Delta))$$

dove  $W_\rho$  è un operatore densità su  $\mathcal{H}$ , ovvero un operatore positivo <sup>11</sup> per cui  $\text{Tr}(W_\rho) = 1$ . Il valor medio della distribuzione di probabilità  $\mu(a, \rho)$  è quindi dato da

$$\langle a \rangle_\rho = \text{Tr}(W_\rho a).$$

La dispersione associata alla misura di probabilità  $\mu(a, \rho)$  è in generale data da

$$\sigma_\rho^2(a) = \langle (a - \langle a \rangle_\rho)^2 \rangle_\rho.$$

È possibile dimostrare – ed è uno degli aspetti più peculiari della meccanica quantistica – che non esiste stato  $\rho$  che dia una distribuzione di probabilità con dispersione nulla per ogni osservabile. Lo spazio delle misure di probabilità risulta convesso, e i suoi elementi di bordo sono gli stati puri, che si possono identificare con gli operatori densità di rango 1, ovvero quelli che soddisfano le condizioni

$$W_\rho^2 = W_\rho = W_\rho^\dagger, \\ \text{Tr}(W_\rho) = 1$$

su  $\mathcal{H}$ ; equivalentemente, gli stati puri corrispondono agli elementi del proiettivo complesso

$$\mathbb{P}(\mathcal{H}) = \mathcal{H}_0/\mathbb{C}_0,$$

attraverso

$$\rho = \frac{|\psi\rangle\langle\psi|}{\langle\psi|\psi\rangle}$$

con  $\psi \neq 0_{\mathcal{H}}$ . Se il vettore  $\psi \in \mathcal{H}$  di norma unitaria rappresenta uno stato puro, è immediato

<sup>10</sup>Questa frase sintetizza, per gli scopi di questa nota, il teorema di Gleason, per la cui analisi in relazione alle misure di probabilità à la Born in meccanica quantistica rimandiamo il lettore al libro [9].

<sup>11</sup>Un operatore  $a$  su uno spazio di Hilbert  $\mathcal{H}$  è positivo se è autoaggiunto e ha spettro non negativo.

riconoscere una relazione di indeterminazione à la Heisenberg <sup>12</sup> data da

$$\sigma_\psi^2(a)\sigma_\psi^2(b) \geq \langle \psi | i[a, b] | \psi \rangle^2 \quad (1)$$

in termini del *commutatore* tra due operatori su  $\mathcal{H}$ , definito antisimmettizzando l'operazione di composizione  $\circ$  in  $Op(\mathcal{H})$ , ovvero

$$[a, b] = a \circ b - b \circ a \quad (2)$$

con  $a, b \in Op(\mathcal{H})$ . Tale funzione è antisimmetrica (vale cioè che  $[a, a'] = -[a', a]$ ), bilineare (ovvero  $[a + a', a''] = [a, a''] + [a', a'']$  e analogamente sul secondo membro), soddisfa le identità di Jacobi e di Leibniz (rispetto alla composizione), che si scrivono come

$$[[a, a'], a''] + [[a', a''], a] + [[a'', a], a'] = 0 \\ [a \circ a', a''] = a \circ [a', a''] + [a, a''] \circ a' \quad (3)$$

per ogni terna  $a, a', a'' \in Op(\mathcal{H})$ .

Quando due sistemi quantistici associati agli spazi di Hilbert  $\mathcal{H}_1$  e  $\mathcal{H}_2$  sono composti, lo spazio di Hilbert che corrisponde alla composizione di essi è dato dal prodotto tensoriale  $\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2$ . È l'esistenza di stati puri per  $\mathcal{H}_{12}$  che non sono separabili, ovvero che non si possono scrivere come il prodotto tensoriale di uno stato puro in  $\mathcal{H}_1$  con uno stato puro in  $\mathcal{H}_2$  che origina il problema dell'*entanglement*.

Per formalizzare in termini geometrici l'evoluzione temporale di un sistema quantistico così descritto, notiamo che l'interpretazione probabilistica à la Born della meccanica quantistica induce a considerare l'evoluzione temporale di un sistema come descritto da un gruppo ad un parametro di automorfismi **unitari** (ovvero che conservano la norma operatoriale) sullo spazio delle osservabili  $\mathcal{A} \subset Op(\mathcal{H})$  dato dagli operatori autoaggiunti eventualmente illimitati su  $\mathcal{H}$ . Il teorema di Wigner dimostra che, se  $\Phi_t$  è un

<sup>12</sup>È possibile dimostrare relazioni di indeterminazione più generali, di cui quella à la Heisenberg è un caso particolare, così come è possibile analizzare le relazioni di indeterminazione per stati non puri. Per esse rimandiamo a [10, 11, 12], limitandoci a menzionare che, se lo spazio di Hilbert  $\mathcal{H}$  ha dimensione finita, allora si può dimostrare che si ha

$$\sigma_\rho^2(a)\sigma_\rho^2(b) \geq \frac{1}{4} |\text{Tr}(W_\rho [a, b])|^2.$$

gruppo continuo ad un parametro sullo spazio degli operatori  $Op(\mathcal{H})$  che preserva la norma operatoriale (ovvero che  $\|\Phi_t(a)\| = \|a\|$ ) allora esiste un gruppo ad un parametro  $u_t \subset Op(\mathcal{H})$  di operatori unitari<sup>13</sup> per cui

$$a(t) = \Phi_t(a) = u_t^* a u_t, \quad (4)$$

e tale relazione di coniugazione non altera il dominio di  $a$  anche nel caso in cui  $a$  non sia limitato. È possibile poi provare (è parte del contenuto del teorema di Stone - von Neumann) che per ogni gruppo ad un parametro di operatori unitari su  $\mathcal{H}$  esiste un operatore autoaggiunto  $\delta = \delta^*$  (eventualmente non limitato) su  $\mathcal{H}$  per cui vale  $u_t = e^{it\delta}$ . Tale operatore  $a$  fornisce il generatore infinitesimo della dinamica quantistica, o operatore Hamiltoniano della dinamica. La versione infinitesima della relazione precedente risulta in

$$\frac{da}{dt} = i[a, \delta], \quad (5)$$

che fornisce la descrizione della dinamica quantistica alla Heisenberg. Le proprietà del commutatore in  $Op(\mathcal{H})$  chiariscono che la corrispondenza  $a \mapsto i[a, \delta]$  è una derivazione in  $Op(\mathcal{H})$  rispetto alla composizione, e che è interna, poichè è definita da un elemento  $\delta \in Op(\mathcal{H})$ . Sugli stati puri, l'evoluzione temporale in (4) si scrive come

$$\psi(t) = u_t \psi(0), \quad (6)$$

la cui versione infinitesima è data dall'equazione di Schrödinger (con  $\delta = -H/\hbar$ )

$$i\hbar \frac{d\psi}{dt} = H\psi \quad (7)$$

in termini dell'operatore Hamiltoniano  $H$  in  $\mathcal{H}$  e della costante di Planck  $\hbar = h/2\pi$ . Dall'equazione di Schrödinger segue che, nello spazio degli stati che si possono identificare di operatori densità su  $\mathcal{H}$ , l'evoluzione temporale è data dall'equazione di Landau - von Neumann

$$\frac{dW_\rho}{dt} = \frac{i}{\hbar} [W_\rho, H]. \quad (8)$$

<sup>13</sup>Ricordiamo che un operatore  $u : \mathcal{H} \rightarrow \mathcal{H}$  su uno spazio di Hilbert complesso separabile è unitario se  $uu^* = u^*u = 1$ . Un gruppo a un parametro di operatori unitari è dato da un insieme  $u_t$  (per ogni  $t \in \mathbb{R}$ ) di operatori unitari per cui  $u_t u_{t'} = u_{t+t'}$ .

Notiamo che, quando  $H$  corrisponde all'osservabile energia meccanica del sistema, si richiede che  $H$  sia limitato dal basso, ovvero che il suo spettro (che è necessariamente reale) abbia almeno un estremo limitato.

## 2.2 Una descrizione geometrica della meccanica classica

Una descrizione geometrica della meccanica classica inizia dall'identificare le osservabili come elementi di un insieme  $\mathcal{O} = \mathcal{F}(M)$  di funzioni opportunamente regolari a valori in  $\mathbb{R}$  definite su una varietà differenziale  $M$  (liscia e a dimensione finita). Tale insieme  $\mathcal{F}(M)$  è un'algebra commutativa rispetto all'usuale definizione puntuale di somma e prodotto di funzioni, ovvero

$$\begin{aligned} (f + g)(m) &= f(m) + g(m), \\ (fg)(m) &= f(m)g(m). \end{aligned}$$

Gli stati sono elementi  $\rho \in \mathcal{S}$  dell'insieme delle misure di probabilità su  $M$ . Gli stati densità sono dati da misure di probabilità  $d\mu_\rho$  assolutamente continue rispetto ad una misura di riferimento  $dm$ , ad esempio la misura di Lebesgue invariante per traslazioni nel caso in cui  $M = \mathbb{R}^{\dim M}$ , e il pairing corrispondente è dato da

$$\mu(f, \rho) : \Delta \quad \mapsto \quad \int_{f^{-1}(\Delta)} d\mu_\rho,$$

dove abbiamo denotato  $f^{-1}(\Delta) = \{m \in M : f(m) \in \Delta\}$ . Gli stati puri sono dati dalle misure di Dirac singolari  $\delta_m$ , con il pairing

$$\mu(f, \delta_m) : \Delta \quad \mapsto \quad \begin{cases} 1 & \text{if } m \in \Delta \\ 0 & \text{if } m \notin \Delta \end{cases}$$

Dato uno stato  $\rho$ , il valor medio di una osservabile è dato da<sup>14</sup>

$$\langle f \rangle_\rho = \int d\mu_\rho f.$$

<sup>14</sup>Anche questa dualità può essere analizzata più rigorosamente in termini del teorema di Riesz. Se  $\mathcal{A} = C_0(M)$  è l'insieme delle funzioni continue che si annullano all'infinito, l'azione di ogni funzionale lineare continuo positivo  $\phi \in \mathcal{A}^*$  si può rappresentare attraverso una misura regolare su  $M$ . Tale insieme, con la topologia  $w^*$  indotta da quella su  $\mathcal{A}$  risulta compatto e convesso. I punti sul bordo sono le misure singolari, ovvero gli stati puri.

Resta evidente che gli stati puri forniscono distribuzioni di probabilità con dispersione nulla per ogni osservabile. La composizione di due sistemi descritti in termini di due varietà lisce  $M_1$  e  $M_2$  risulta in un sistema descritto sulla varietà prodotto cartesiano  $M_1 \times M_2$ .

All'interno di tale descrizione, è possibile dimostrare che, se  $\mathcal{F}(M)$  denota l'algebra a valori reali delle funzioni lisce su  $M$ , allora l'insieme  $\text{Aut}(\mathcal{F}(M))$  degli automorfismi continui è equivalente all'insieme  $\text{Diff}(M)$  dei diffeomorfismi su  $M$ : se  $\Phi \in \text{Aut}(\mathcal{F}(M))$ , allora esiste un  $\phi \in \text{Diff}(M)$  per cui

$$\Phi(f) = \phi^*(f) = f \circ \phi$$

attraverso il concetto di pull-back. Ancora, il teorema di Willmore [13] prova che l'insieme delle derivazioni per  $\mathcal{F}(M)$  coincide con l'insieme  $\mathfrak{X}(M)$  dei campi vettoriali su  $M$ , e quindi può essere scritta localmente (ovvero in termini di un sistema di coordinate locali  $\{x^a\}_{a=1, \dots, \dim M}$  su  $M$ ) come

$$\mathfrak{X}(M) \ni \delta = \delta^a(x) \frac{\partial}{\partial x^a}. \quad (9)$$

L'evoluzione temporale di un'osservabile  $f \in \mathcal{F}(M)$  si può pertanto scrivere come

$$\frac{df}{dt} = \delta(f) = L_\delta(f), \quad (10)$$

in termini della derivata di Lie lungo  $\delta$ , a cui corrisponde l'evoluzione temporale sugli stati puri<sup>15</sup> data localmente come un sistema di equazioni differenziali ordinarie

$$\frac{dx^a}{dt} = \delta^a(x) \quad (11)$$

con un opportuno dato iniziale  $x^a(0) = x_0^a$ .

### 2.3 Non solo analogie

Le pagine precedenti hanno fornito al lettore un quadro delle analogie tra la descrizione quantistica e quella classica della dinamica di un sistema

<sup>15</sup>L'evoluzione temporale di uno stato  $\rho$  non puro, a cui corrisponde una misura di probabilità data in termini della derivata di Radon-Nikodym rispetto alla misura di Lebesgue come  $d\mu_\rho = \tilde{\rho} dm$  ha una forma esplicita rispetto al campo vettoriale  $\delta$  alquanto complicata, che in casi opportuni si riduce all'equazione di Liouville (nota dalla meccanica statistica, ad esempio) per  $\tilde{\rho}$ .

fisico. È invece interessante iniziare ad analizzare le differenze fra le due descrizioni. Nell'ottica del limite classico, o della dequantizzazione, di un sistema quantistico, un primo aspetto di differenza tra le due descrizioni appare evidente. Le osservabili quantistiche sono gli elementi autoaggiunti di  $Op(\mathcal{H})$ , la norma è data da

$$\|a\| = \sup_{0 \neq \psi \in \mathcal{H}} \frac{\|a(\psi)\|_{\mathcal{H}}}{\|\psi\|_{\mathcal{H}}}$$

rispetto alla norma  $\|\psi\|_{\mathcal{H}}$  in  $\mathcal{H}$ . Come noto, un operatore  $a \in Op(\mathcal{H})$  è continuo se e solo se è limitato, ed in questo caso il suo dominio  $\text{Dom}(a) = \mathcal{H}$ . In particolare, l'insieme  $B(\mathcal{H})$  degli elementi limitati in  $Op(\mathcal{H})$  è una  $\mathbb{C}^*$ -algebra non commutativa, rispetto alla definizione naturale di somma e prodotto data dalla composizione di operatori su  $\mathcal{H}$ , e la coniugazione complessa data da  $a \mapsto a^* = a^\dagger$ , in quanto risulta un'algebra di Banach e vale l'identità

$$\|aa^*\| = \|a\|^2.$$

Se, in particolare,  $\mathcal{H}$  ha dimensione finita (e quindi  $\mathcal{H} \simeq \mathbb{C}^{n=\dim \mathcal{H}}$ ) lo spazio degli operatori coincide con l'insieme delle matrici  $n \times n$  ad elementi in  $\mathbb{C}$ , e la composizione si riduce al prodotto matriciale (e questo è uno dei motivi per cui la meccanica quantistica fu anche pensata da Heisenberg, Born, Jordan, come una meccanica delle matrici, eventualmente con infinite righe e colonne).

Nella descrizione classica di un sistema fisico, le osservabili sono le funzioni (opportuno regolare: lo specifico problema rende naturale considerare ad esempio funzioni misurabili, o continue, o differenziabili) a valori reali definite su una varietà  $M$ . In particolare l'insieme  $C_0(M)$  delle funzioni a valori in  $\mathbb{C}$  continue su  $M$  e che si annullano all'infinito (ovvero lo spazio delle funzioni continue  $C(M)$  se  $M$  è compatto) risulta, rispetto alla somma e al prodotto puntuale di funzioni, e alla coniugazione complessa in  $\mathbb{C}$ , una  $\mathbb{C}^*$ -algebra *commutativa*, rispetto alla norma di Banach

$$\|f\|_\infty = \sup_{x \in M} |f(x)|.$$

Ancora, possiamo notare che gli elementi autoaggiunti in  $B(\mathcal{H})$  non esauriscono l'insieme delle

osservabili di un sistema quantistico. Un esempio ben noto è quello che si ha considerando un sistema quantistico per cui  $\mathcal{H} = \mathcal{L}^2(\mathbb{R}, dx)$  (una particella che si muove lungo una retta, nella rappresentazione à la Schrödinger), e le osservabili momento e posizione, la cui azione su opportuni domini densi in  $\mathcal{H}$  è data da

$$\begin{aligned} p &: \psi \mapsto -i\hbar \frac{d\psi}{dx}, \\ x &: \psi \mapsto x\psi \end{aligned}$$

e per essi si ha

$$[x, p] = i\hbar 1 \quad (12)$$

su un dominio che risulta essere denso in  $\mathcal{H}$ . Anche in meccanica classica esistono osservabili che sono rappresentate da funzioni che non si annullano all'infinito con  $M$  non compatto: pensiamo ancora alla velocità (nel formalismo non relativistico) di una particella vincolata a muoversi lungo una retta.

Osserviamo ancora che le equazioni della dinamica quantistica per le osservabili (5) e per gli stati (8), così come le relazioni di indeterminazione (1) fanno riferimento alla struttura di commutatore definita in (9) antisimmetrizzando<sup>16</sup> il prodotto non commutativo in  $Op(\mathcal{H})$  dato dalla composizione. La non commutatività del prodotto permette altresì di definire una funzione binaria (detta *prodotto di Jordan*), attraverso<sup>17</sup>

$$a \odot b = \frac{1}{2}(a \circ b + b \circ a). \quad (13)$$

Risulta immediato provare che il prodotto di Jordan è simmetrico, ovvero  $a \odot b = b \odot a$ , ed interno allo spazio vettoriale degli operatori autoaggiunti, in quanto

$$(a \odot b)^* = (a \odot b)$$

<sup>16</sup>È immediato verificare che, se  $(A, \cdot)$  è un'algebra associativa, il cui prodotto non è commutativo, la posizione  $[a, b] = a \cdot b - b \cdot a$  definisce un commutatore che è bilineare, antisimmetrico, e soddisfa le relazioni (10).

<sup>17</sup>Una algebra di Jordan è uno spazio vettoriale  $A$  in cui è definito un prodotto binario  $\odot : A \times A \rightarrow A$  che sia bilineare, simmetrico, non associativo in generale ma per cui valga l'identità di Jordan, data da

$$\begin{aligned} (a \odot b) \odot (a \odot a) &= a \odot (b \odot (a \odot a)) \\ \forall a, b \in A. \end{aligned}$$

se  $a = a^*$  e  $b = b^*$ . Tale prodotto risulta non associativo, e la non associatività si può esprimere in termini del commutatore, come

$$(a \odot b) \odot c - a \odot (b \odot c) = \frac{1}{4}[[a, c], b]. \quad (14)$$

Simmetrizzare, attraverso la formula (13), un prodotto di un'algebra commutativa non fornisce una nuova struttura algebrica: in tali casi, il prodotto di Jordan si riduce a quello stesso dell'algebra. Questo è il motivo per cui non si ha un prodotto di Jordan nell'algebra  $\mathcal{F}(M)$  delle funzioni su uno spazio  $M$  rispetto al prodotto puntuale, e ciò costituisce un'ulteriore differenza tra la descrizione quantistica e quella classica della dinamica di un sistema fisico.

## 2.4 Alcune domande sul problema del limite classico

Lo studio della transizione dalla descrizione quantistica alla descrizione classica per un sistema dinamico comporta alcune domande inerenti alle strutture matematiche che intervengono nelle descrizioni stesse.

Come ottenere, ad esempio, un'algebra commutativa a partire da una non commutativa? Come definire un formalismo matematico in cui l'insieme  $Op(\mathcal{H})$  abbia come limite l'insieme  $\mathcal{F}(M)$  delle funzioni opportunamente regolari su una varietà liscia, ed il prodotto non commutativo in  $Op(\mathcal{H})$  abbia come limite il prodotto commutativo e puntuale (ovvero che dipende solo dal valore che le funzioni assumono in  $m \in M$ ) in  $\mathcal{F}(M)$ ?

E ancora, ancor prima: in che senso la varietà  $M$  si può ottenere come un'opportuna dequantizzazione di un sistema fisico quantistico su  $\mathcal{H}$ , ovvero in che senso una varietà  $M$  può emergere da uno spazio di Hilbert  $\mathcal{H}$ ? Come sappiamo, tutti gli spazi di Hilbert complessi e separabili sono isomorfi se e solo se hanno la stessa dimensione, e sono isomorfi se hanno dimensione infinita, mentre esistono varietà lisce, pur con la stessa dimensione, che sono solo localmente diffeomorfe. Ciò sembra indicare che uno spazio classico  $M$ , ottenuto come dequantizzazione di un sistema quantistico, dipenda non solo da  $\mathcal{H}$  (nel senso che lo spazio degli stati puri di un sistema quantistico non origina, attraverso un

processo di limite, lo spazio degli stati puri di un sistema classico) quanto anche da una specifica classe di osservabili per il sistema quantistico e dalla loro evoluzione temporale.

Naturalmente, una ulteriore questione: rispetto a quali grandezze introdurre un concetto di limite classico (quindi non commutativo) di un sistema quantistico? Quanto tale concetto è generale, e può valere per classi di sistemi fisici? Tale limite va inteso lungo una scala di azioni (con unità di misura in  $\hbar$ ), o lungo una scala di energie (il parametro  $n$  di cui parlava Bohr), o una scala di lunghezze (la distanza tra due punti materiali, ad esempio elettroni o atomi carichi)?

Ancora: ogni sistema quantistico deve necessariamente avere un limite classico? Più in dettaglio: ogni osservabile quantistico deve necessariamente avere un osservabile classico come opportuno limite? In che modo interpretare il limite classico per sistemi quantistici il cui spazio di Hilbert  $\mathcal{H}$  ha dimensione finita, problema oggi che ha interesse teorico e sperimentale notevole, alla luce della teoria geometrica dell'informazione e della computazione? Cosa significa studiare il problema del limite classico per sistemi a molti corpi, che manifestano comportamenti molto peculiari a seconda che i singoli componenti seguano statistiche bosoniche o fermioniche? Che ruolo ha, in tali sistemi, la temperatura come scala per definire un limite classico; e più in generale: in che significato il limite classico emerge in termini dinamici, attraverso l'interazione con un ambiente?

Risulta evidente che un'analisi generale che risponda a tali domande sia più che ardua, e supera gli scopi di questa nota. Pur ritenendo interessante, e concettualmente appropriato studiare il problema del limite classico a partire da un singolo sistema quantistico o da famiglie di sistemi analoghi, ciò che ci proponiamo nelle prossime pagine è di descrivere alcune questioni legate al limite classico dal punto di vista delle strutture geometriche utilizzate per descrivere i sistemi quantistici, in questo seguendo la linea tracciata proprio da Dirac e citata nell'introduzione.

### 3. Il limite classico della meccanica quantistica nel formalismo à la Weyl-Wigner

Tra le questioni che abbiamo evidenziato nelle righe precedenti vi è quella di comprendere come sia possibile ottenere un'algebra commutativa come un opportuno limite di un'algebra non commutativa. Il formalismo à la Weyl-Wigner che descriviamo in questa sezione fornisce una risposta a tale questione. Esso risulta fondato sulla nozione di struttura simplettica, e più in generale di struttura di Poisson su uno spazio classico, e permette perciò anche di definire un limite classico per l'evoluzione temporale di un'osservabile quantistico. Questo è il motivo per cui la nostra descrizione di tale formalismo inizia proprio introducendo la nozione di varietà di Poisson e di varietà simplettica.

Nella sezione precedente abbiamo già incontrato la celebre relazione di commutazione (12) tra le osservabili momento e posizione per un sistema quantistico per cui  $\mathcal{H}$  è dato dalle funzioni a quadrato sommabile su una retta. Partendo da essa, nel suo studio [14] sulle equazioni fondamentali della meccanica quantistica (in cui esprime le cosiddette *quantum conditions*), Dirac scrive

“Consideriamo ora a cosa l'espressione  $xy - yx$  corrisponda nella teoria classica. [...] la differenza del prodotto di Heisenberg di due quantità (quantistiche) è uguale al prodotto di  $i\hbar/2\pi$  per l'espressione della loro parentesi di Poisson. In simboli,

$$xy - yx = i\hbar\{x, y\}'' . \quad (15)$$

In questa espressione Dirac osserva *in primis* che ci sono osservabili quantistiche, il cui commutatore (il prodotto di Heisenberg) è un multiplo dell'identità, e pertanto commuta con ogni altro osservabile quantistico. In virtù di ciò, in seguito, introduce una relazione tra tale commutatore e la parentesi di Poisson tra le corrispondenti osservabili classiche. In linguaggio più moderno, tale espressione suggerisce che la dequantizzazione proceda dall'identificazione di opportune algebre di Lie di operatori quantistici (vedi la

(9)-(10)), e che per esse si identifichi, in un opportuno spazio classico, che a tale algebra di Lie corrisponda un insieme di osservabili classici le cui parentesi di Poisson sono analoghe alle relazioni di commutazione quantistiche, a meno del fattore in  $\hbar$ . Questo, ancora, suggerisce che tale corrispondenza possa interpretarsi come un limite per  $\hbar \rightarrow 0$ .

Per analizzare il limite classico della struttura di commutatore, richiamiamo brevemente cosa sia una struttura di Poisson su una varietà liscia.

Una parentesi di Poisson su uno spazio  $\mathcal{F}(M)$  di funzioni opportunamente regolari su  $M$  è una struttura geometrica definita da

$$\{, \} : \mathcal{F}(M) \times \mathcal{F}(M) \rightarrow \mathcal{F}(M)$$

tale che

$$\begin{aligned} \{f, f'\} &= -\{f', f\}, \\ \{f + f', g\} &= \{f, g\} + \{f', g\}, \\ \{f, \{g, h\}\} + \{g, \{h, f\}\} + \{h, \{f, g\}\} &= 0 \\ \{f f', g\} &= f\{f', g\} + \{f, g\}f' \end{aligned} \quad (16)$$

rispetto alla somma e al prodotto puntuale in  $\mathcal{F}(M)$ . L'analogia con il commutatore in  $Op(\mathcal{H})$  è chiara, le prime tre relazioni indicano che si ha una algebra di Lie (infinito dimensionale) su  $\mathcal{F}(M)$ , e si manifesta notando ulteriormente che la corrispondenza  $f \mapsto \{f, h\}$  è una derivazione in  $\mathcal{F}(M)$  che dipende da  $h$ . Diviene allora naturale definire che una dinamica classica espressa in termini infinitesimi da un campo vettoriale  $\delta \in \mathfrak{X}(M)$  abbia una descrizione *à la Poisson* se su  $M$  esiste una parentesi di Poisson ed una funzione  $h$  (detta Hamiltoniana) per cui

$$\frac{df}{dt} = \delta(f) = \{f, h\}. \quad (17)$$

Se  $M = T^*Q$  è lo spazio delle fasi (il fibrato cotangente) corrispondente ad uno spazio delle configurazioni  $Q$ , in cui le coordinate  $\{q^a\}_{a=1, \dots, d}$  su  $Q$  rappresentano le posizioni e le coordinate  $\{p_b\}_{b=1, \dots, d}$  sulla fibra rappresentano i momenti, esiste una struttura di Poisson canonica data da

$$\{q^a, p_b\} = \delta_b^a, \quad (18)$$

e tale relazione mostra una chiara analogia con l'espressione quantistica data dal commutato-

re in (12). Per una varietà liscia  $M$  con coordinate locali  $\{x^a\}_{a=1, \dots, \dim M}$ , il tensore di Poisson risulta essere un bivettore caratterizzato da

$$\{x^a, x^b\} = \Lambda^{ab}$$

che soddisfa<sup>18</sup>

$$\Lambda^{ck} \partial_k \Lambda^{ab} + \Lambda^{ak} \partial_k \Lambda^{bc} + \Lambda^{bk} \partial_k \Lambda^{ca} = 0$$

(l'identità di Jacobi) e  $\Lambda^{ab} = -\Lambda^{ba}$ , e fornisce

$$\{f, f'\} = \Lambda^{ab} \frac{\partial f}{\partial x^a} \frac{\partial f'}{\partial x^b}.$$

Quando la matrice  $\Lambda^{ab}(x)$  è invertibile per ogni  $x \in M$ , ad essa corrisponde una struttura simplettica su  $M$ , data da una 2-forma che assume l'espressione locale

$$\omega = \omega_{ab} dx^a \wedge dx^b$$

con  $\Lambda^{ab} \omega_{bc} = -\delta_c^a$ . Tale forma risulta non degenera per costruzione, mentre l'identità di Jacobi soddisfatta dal tensore di Poisson implica che sia chiusa, ovvero  $d\omega = 0$ . Nel caso in cui  $M = T^*Q$ , la parentesi di Poisson canonica corrisponde alla nota 2-forma simplettica

$$\omega = dq^a \wedge dp_b. \quad (19)$$

Se  $(M, \omega)$  è una varietà simplettica, un campo vettoriale  $\delta \in \mathfrak{X}(M)$  (ovvero il generatore infinitesimo di una dinamica) risulta Hamiltoniano se e solo se esiste una funzione  $h$  per cui

$$i_\delta \omega = dh$$

in termini dell'operatore di contrazione. Su  $(M = T^*Q, \omega = dq^a \wedge dp_b)$  le equazioni del moto relative ad una dinamica Hamiltoniana (con Hamiltoniana  $h$ ) assumono la forma

$$\begin{aligned} \frac{dq^a}{dt} &= \{q^a, h\} = \frac{\partial h}{\partial p_a} \\ \frac{dp_a}{dt} &= \{p_a, h\} = -\frac{\partial h}{\partial q^a}. \end{aligned} \quad (20)$$

Tali equazioni descrivono l'evoluzione temporale infinitesima degli stati puri<sup>19</sup> su  $M = T^*Q$ .

<sup>18</sup>In questa nota assumiamo che il simbolo di sommatoria sia implicito se nell'espressione sono presenti indici ripetuti.

<sup>19</sup>Per circostanziare un'osservazione precedente, conside-

Riprendiamo l'analisi del problema della dequantizzazione seguendo la linea di Dirac, ed assumiamo di avere un sistema quantistico a cui corrisponde uno spazio di Hilbert  $\mathcal{H}$  ed un insieme di osservabili  $\hat{q}^a, \hat{p}_a$  con  $a = 1, \dots, N$  che soddisfano le regole di commutazione canoniche, ovvero per esse valgono

$$[\hat{q}^a, \hat{p}_b] = i\hbar\delta_b^a 1. \quad (21)$$

Quali sono le realizzazioni, più propriamente le rappresentazioni di tali operatori? È immediato osservare (Weyl lo scrive nel suo libro sulla meccanica quantistica) che, se  $N$  coppie di operatori soddisfano la (21), allora  $\mathcal{H}$  non può avere <sup>20</sup> dimensione finita; ancora, è possibile dimostrare (teorema di Wintner) che gli operatori autoaggiunti che realizzano le regole di commutazione canoniche non sono limitati su  $\mathcal{H}$ , e quindi sono definiti su domini eventualmente densi in  $\mathcal{H}$ , ma che non coincidono con  $\mathcal{H}$ . Un modo per rappresentare tali operatori evitando una analisi dei domini è quella di considerare opportuni gruppi ad un parametro di operatori unitari su  $\mathcal{H}$ , di cui essi risultino generatori infinitesimi. Nell'approccio à la Weyl, si considerano perciò (ci limitiamo al caso  $N = 1$  per non appesantire la notazione) gruppi ad un parametro  $U(s), V(t) \in \mathcal{U}(\mathcal{H})$ , con  $s, t \in \mathbb{R}$ , che siano continui nella topologia operatoriale e soddisfino le relazioni

$$U(s)V(s') = e^{iss'/\hbar}V(s')U(s). \quad (22)$$

Richiamando il teorema di Stone, si vede che se  $\hat{p}$  è il generatore infinitesimo di

$$U(s) = e^{is\hat{p}/\hbar}$$

---

riamo il caso di uno stato non puro  $\rho$ , che si può descrivere attraverso la misura  $d\mu_\rho = \tilde{\rho}dm$  rispetto alla misura *simplettica*  $dm = dq^1 \wedge \dots \wedge dq^n \wedge dp_1 \wedge \dots \wedge dp_n = \omega \wedge \dots \wedge \omega = \omega^{\wedge n}$ . La misura *simplettica* risulta invariante lungo una dinamica Hamiltoniana, ed il fattore  $\tilde{\rho} = \tilde{\rho}(q, p, t)$  si evolve secondo l'equazione di Liouville data da

$$\frac{\partial \tilde{\rho}}{\partial t} = -\{\tilde{\rho}, h\}.$$

<sup>20</sup>Se si avesse  $\dim \mathcal{H} = d$  finita, allora  $\hat{q}, \hat{p}$  sarebbero rappresentati da matrici di rango finito. Dalla ciclicità dell'operazione di Traccia, si avrebbe che  $\text{Tr}([\hat{q}^a, \hat{p}_b]) = 0 = i\hbar d$ , che è assurdo.

e  $\hat{q}$  è il generatore infinitesimo di

$$V(s') = e^{is'\hat{q}/\hbar},$$

si ha  $\hat{q} = \hat{q}^\dagger$  e  $\hat{p} = \hat{p}^\dagger$ , e tali generatori soddisfano le regole di commutazione canoniche. Il caso più noto di realizzazione di tali gruppi ad un parametro è detta **rappresentazione di Schrödinger**. Per essa, si ha  $\mathcal{H} = \mathcal{L}^2(\mathbb{R}, dx)$ , e su tale spazio si definiscono

$$\begin{aligned} U(s) &: \psi(x) \mapsto \psi(x+s), \\ V(s') &: \psi(x) \mapsto e^{-ixs'/\hbar}\psi(x) \end{aligned} \quad (23)$$

che soddisfano la (22). Per i generatori infinitesimi abbiamo

$$\begin{aligned} U(s) &= e^{is\hat{p}\hbar} : (\hat{p}\psi)(x) = -i\hbar \frac{d\psi}{dx} \\ V(s') &= e^{is'\hat{q}\hbar} : (\hat{q}\psi)(x) = x\psi(x) \end{aligned} \quad (24)$$

Il teorema di Stone - von Neumann permette anche di analizzare l'unicità di tale realizzazione. È infatti possibile dimostrare che ogni altra rappresentazione irriducibile dei gruppi a un parametro che soddisfano le regole di commutazione canoniche (22) è unitariamente equivalente a quella di Schrödinger (tale risultato rivestì anche una notevole importanza, poiché permise di dimostrare l'equivalenza tra la formulazione tra la meccanica delle matrici à la Heisenberg e quella in termini di operatori differenziali à la Schrödinger).

Dagli operatori (22) possiamo definire l'operatore unitario

$$\begin{aligned} D(s, s') &= U^\dagger(s)V(s')e^{-iss'/2\hbar} \\ \psi(x) &\mapsto e^{\frac{i}{2\hbar}(ss' - 2xs')}\psi(x-s) \end{aligned} \quad (25)$$

su  $\mathcal{H} = \mathcal{L}^2(\mathbb{R}, dx)$ . Se interpretiamo  $s, s'$  come un sistema di coordinate globali su  $\mathbb{R}^2$ , per cui scriviamo un vettore  $v = (s, s') \in \mathbb{R}^2$ , vediamo che tale operatore soddisfa

$$D(v_1)D(v_2)D^\dagger(v_1)D^\dagger(v_2) = e^{i\omega(v_1, v_2)/\hbar}, \quad (26)$$

rispetto alla struttura *simplettica canonica*  $\omega = ds \wedge ds'$ . Per tali operatori si ha

$$D(v_1 + v_2) = e^{i\omega(v_1, v_2)/2\hbar}D(v_1)D(v_2) : \quad (27)$$

essi danno una rappresentazione unitaria pro-

iettiva del gruppo delle traslazioni  $(\mathbb{R}^2, +)$  su  $\mathcal{H}$ , ed il fattore proiettivo dipende dalla struttura simplettica canonica per  $\mathbb{R}^2$ . Gli operatori  $D(v)$  si dicono operatori di *displacement*, e danno un **sistema di Weyl**.

Notiamo inoltre che l'estensione al caso  $N > 1$  finito è immediato, su  $\mathcal{H} = \mathcal{L}^2(\mathbb{R}^N, dx)$ . L'origine di tale spazio di Hilbert risulta naturale osservando ancora l'espressione (27). Essa mostra che, se  $v_1$  e  $v_2$  appartengono allo stesso sottospazio Lagrangiano di  $\mathbb{R}^2$  rispetto alla struttura simplettica  $\omega$ , gli operatori corrispondenti commutano e hanno come spettro comune proprio il sottospazio Lagrangiano  $\mathbb{R}^N$  che compare in  $\mathcal{H}$ .

Come si vede, una realizzazione irriducibile delle regole di commutazione canoniche porta ad un sistema di Weyl per lo spazio vettoriale  $\mathbb{R}^2$  che si può naturalmente identificare con lo spazio delle fasi  $T^*\mathbb{R}$  (o con  $T^*\mathbb{R}^N$  a dimensioni superiori). Questa identificazione risulta molto interessante, e permette di studiare altri aspetti della dequantizzazione di un sistema quantistico. Per illustrarli, notiamo che, attraverso gli operatori di displacement (25) per  $N > 1$ , si può definire su un dominio opportuno, la corrispondenza (solitamente detta mappa di Wigner)  $W : Op(\mathcal{H}) \rightarrow \mathcal{F}(\mathbb{R}^{2N})$  data da

$$W_A(z) = \int_{\mathbb{R}^{2N}} \frac{dw}{(2\pi\hbar)^N} e^{-i\omega(w,z)/\hbar} \text{Tr}[A D^\dagger(w)]$$

in cui abbiamo denotato con  $z = (q, p)$  le coordinate su  $T^*\mathbb{R}^N$  e con  $w$  le sue coordinate duali secondo Fourier. Tale corrispondenza  $W$  associa ad un operatore  $A$  su  $\mathcal{H}$  il suo *simbolo* à la Wigner  $W_A \in \mathcal{F}(\mathbb{R}^{2N})$ . Tale corrispondenza risulta iniettiva (con inversa detta mappa di Weyl), e quindi si può definire l'algebra (non commutativa) di Moyal come lo spazio dei simboli di Wigner (il codominio di  $W$  in  $\mathcal{F}(\mathbb{R}^{2N})$ ) attraverso

$$(W_A * W_B)(z) = W_{AB}(z), \quad (28)$$

con  $AB$  il prodotto operatoriale. Si può dimostrare che ([15, 16, 17])

$$(f * g)(x) = \frac{1}{(\pi\hbar)^{2N}} \int \int dudv f(x+u) g(x+v) e^{-2i\omega(u,v)/\hbar} \quad (29)$$

se  $f, g \in \mathcal{S}(\mathbb{R}^{2N})$ , lo spazio delle funzioni di

Schwartz in  $\mathbb{R}^{2N}$ . Ciò significa che nello spazio vettoriale  $\mathcal{S}(\mathbb{R}^{2N})$  abbiamo sia il prodotto commutativo puntuale che il prodotto di Moyal, che risulta non locale e non commutativo, in quanto traduce il prodotto operatoriale. Lo spazio delle funzioni di Schwartz è però non sufficiente per rappresentare molte osservabili di un sistema fisico: si pensi alla funzione unità, o ad esempio alle posizioni e ai momenti, che sono funzioni lineari  $q^a, p_b$ . Un'analisi più raffinata ci permette di risolvere questo problema. Attraverso le proprietà della misura, è possibile estendere il prodotto di Moyal dapprima allo spazio delle distribuzioni temperate  $\mathcal{S}'(\mathbb{R}^{2N})$  e poi a quello dei moltiplicatori, ovvero

$$\begin{aligned} \mathcal{M}_L^\hbar &= \{T \in \mathcal{S}'(\mathbb{R}^{2N}) : \\ &T * f \in \mathcal{S}(\mathbb{R}^{2N}) \forall f \in \mathcal{S}(\mathbb{R}^{2N})\} \\ \mathcal{M}_R^\hbar &= \{T \in \mathcal{S}'(\mathbb{R}^{2N}) : \\ &f * T \in \mathcal{S}(\mathbb{R}^{2N}) \forall f \in \mathcal{S}(\mathbb{R}^{2N})\}; \end{aligned}$$

l'intersezione  $\mathcal{M}^\hbar = \mathcal{M}_L^\hbar \cap \mathcal{M}_R^\hbar$  risulta una  $*$ -algebra con unità che contiene i polinomi, le onde piane, le distribuzioni delta di Dirac e le sue derivate. Come si vede, il prodotto di Moyal dipende da  $\hbar$ , così come quindi l'algebra  $\mathcal{M}^\hbar$ . La condizione

$$\lim_{\hbar \rightarrow 0} \mathcal{M}^\hbar = \mathcal{O}_M$$

definisce l'insieme di ciò che possiamo chiamare osservabili classiche su  $M = \mathbb{R}^{2N}$ , e che coincide con lo spazio delle funzioni lisce a crescita polinomiale con tutte le loro derivate in  $\mathbb{R}^{2N}$ . Su di esse, il prodotto di Moyal si scrive come una serie asintotica in  $\hbar$ . Per  $N = 1$ , tale espressione risulta data da

$$\begin{aligned} f * g &\sim fg + \frac{i\hbar}{2}\{f, g\} \\ &+ \sum_{k=2}^{\infty} \left(\frac{i\hbar}{2}\right)^k \frac{1}{k!} D_k(f, g) \\ \text{se } \hbar &\rightarrow 0 \end{aligned} \quad (30)$$

in cui  $D_k$  è un operatore bidifferenziale di ordine

$k$  che si può scrivere come

$$D_k(f, g) = \frac{\partial^k f}{\partial q^k} \frac{\partial^k g}{\partial p^k} - \binom{k}{1} \frac{\partial^k f}{\partial^{k-1} q \partial p} \frac{\partial^k g}{\partial^{k-1} p \partial q} + \dots + (-1)^k \frac{\partial^k f}{\partial p^k} \frac{\partial^k g}{\partial q^k}. \quad (31)$$

L'espressione (30) indica che il prodotto di Moyal deforma quello puntuale, e si riduce ad esso nel limite in cui  $\hbar \rightarrow 0$ : in questo senso, il formalismo che stiamo descrivendo permette di descrivere l'algebra delle osservabili quantistiche e l'algebra delle osservabili classiche sullo stesso spazio vettoriale, con il prodotto operatoriale che si scrive come un prodotto non commutativo e non locale. Nel limite per  $\hbar \rightarrow 0$ , la struttura algebrica del sistema quantistico che consideriamo si riduce a quella classica. In essa si osserva che primo termine di deformazione è dato dalla parentesi di Poisson associata alla struttura simplettica  $\omega$  su  $\mathbb{R}^{2N}$ ; i termini  $D_k(f, g)$  risultano simmetrici in  $f \leftrightarrow g$  per  $k$  pari, antisimmetrici per  $k$  dispari. Ne segue che antisimmetrizzare il prodotto conduce al commutatore à la Moyal,

$$[f, g]_{\hbar} = f * g - g * f = i\hbar \{f, g\} + \sum_{s=1}^{\infty} \frac{2}{(2s+1)!} \left(\frac{i\hbar}{2}\right)^{2s+1} D_{2s+1}(f, g): \quad (32)$$

tale commutatore deforma la parentesi di Poisson su  $\mathbb{R}^{2N}$ , e si ha

$$\{f, g\} = \lim_{\hbar \rightarrow 0} \frac{1}{i\hbar} (f * g - g * f). \quad (33)$$

In questo senso, osserviamo che la struttura di Poisson si ottiene all'interno del formalismo à la Moyal come un opportuno limite del commutatore, e questo pone la frase di Dirac (15) in un contesto matematicamente meno formale. In particolare, per le funzioni coordinate si ha

$$\begin{aligned} [q^a, q^b]_{\hbar} &= 0, \\ [p^a, p^b]_{\hbar} &= 0, \\ [q^a, p^b]_{\hbar} &= i\hbar \delta^{ab}, \end{aligned}$$

e per le funzioni che sono polinomi in  $q, p$  di

grado non superiore a 2 si ha proprio la (15)

$$[f, g]_{\hbar} = i\hbar \{f, g\}. \quad (34)$$

È interessante osservare che il formalismo à la Weyl-Wigner che stiamo descrivendo permette di analizzare anche il limite classico della dinamica, (ovvero dell'evoluzione temporale) di un sistema quantistico. L'evoluzione temporale quantistica viene descritta da un gruppo  $u_t = e^{it\hat{H}/\hbar}$  di operatori unitari su  $\mathcal{H}$ , con generatore autoaggiunto  $\hat{H} = \hat{H}^\dagger$ . All'evoluzione temporale di un'osservabile autoaggiunto  $\hat{a} \in Op(\mathcal{H})$  dato da (4)  $\hat{a} = u^\dagger(t)\hat{a}u_t$  corrisponde, attraverso la mappa di Weyl, l'evoluzione temporale del suo simbolo, dato da

$$a(t) = u_t^\dagger * a * u_t \quad (35)$$

con  $u_t = \exp^{-itH/\hbar}$  in cui l'esponenziazione è rispetto al prodotto di Moyal. La versione infinitesima di tale relazione si scrive come

$$\frac{da}{dt} = \frac{i}{\hbar} [a, H]_{\hbar} \quad (36)$$

che, nel limite per  $\hbar \rightarrow 0$ , mostra che l'evoluzione temporale quantistica si riduce ad una evoluzione temporale Hamiltoniana su  $T^*\mathbb{R}^N$  con una opportuna funzione Hamiltoniana  $H$  che è il limite per  $\hbar \rightarrow 0$  del simbolo di Weyl dell'operatore Hamiltoniano quantistico  $\hat{H}$ .

A conclusione di questa sezione, osserviamo che se si simmetrizza il prodotto di Moyal si ottiene un prodotto di Jordan, che scriviamo come

$$\begin{aligned} f \odot g &= \frac{1}{2}(f * g + g * f) \\ &= fg - \frac{\hbar^2}{8} D_2(f, g) + o(\hbar^4). \end{aligned} \quad (37)$$

Diversamente da ciò che accade per l'espressione antisimmetrica in (32), è possibile dimostrare che nessun troncamento ad un ordine finito in  $\hbar$  della serie asintotica (37) risulta in un prodotto di Jordan, che quindi non si può ottenere come una opportuna approssimazione di quello à la Moyal [18].

### 3. Sulla quantizzazione di una dinamica classica attraverso il formalismo à la Weyl-Wigner

Il formalismo à la Weyl-Wigner, che noi abbiamo presentato nell'ottica della dequantizzazione di una dinamica quantistica, è stato analizzato anche nell'ottica della quantizzazione di una dinamica classica. Ne descriviamo brevemente alcuni aspetti, a complemento della descrizione precedente, per mostrare come il problema del limite classico sia legato a quello della quantizzazione.

In particolare, osserviamo che la rappresentazione di Schrödinger di un sistema di Weyl per lo spazio simplettico  $(\mathbb{R}^2, \omega = dq \wedge dp)$  fornisce un esempio di immersione di uno spazio delle configurazioni classico  $Q = \mathbb{R}$  in uno spazio di Hilbert  $\mathcal{H} = \mathcal{L}^2(Q = \mathbb{R}, dx)$ , in virtù del fatto che ogni elemento  $x \in \mathbb{R}$  fornisce un elemento di una base, in senso generalizzato, di  $\mathcal{H}$  per cui si ha una risoluzione dell'identità<sup>21</sup>

$$1 = \int_{\mathbb{R}} dx |x\rangle\langle x| \quad (38)$$

da cui uno scrive

$$|\psi\rangle = \int_{\mathbb{R}} dx |x\rangle\psi(x) \quad (39)$$

con  $\langle x|\psi\rangle = \psi(x)$ . Gli stati puri si possono descrivere in termini di funzioni d'onda normalizzate  $\psi(x)$  a cui corrispondono densità di probabilità date dal prodotto  $\psi^*(x)\psi(x) = \langle x|\psi\rangle\langle\psi|x\rangle$ . In tale realizzazione, gli osservabili momento corrispondono a operatori di derivazione, e l'evoluzione si può scrivere in termini di una equazione d'onda  $i\hbar\dot{\psi} = \hat{H}\psi$  in termini di un operatore differenziale  $\hat{H}$  il cui simbolo di Weyl coincide con una funzione Hamiltoniana classica di una data dinamica.

Il formalismo à la Weyl-Wigner-Moyal è stato studiato all'interno del problema più generale della quantizzazione per deformazione di una varietà simplettica  $(M, \omega)$  (vedi [19, 20, 21]), e ancor più in generale della quantizzazione per deformazione di una varietà di Poisson  $(M, \Lambda)$  [22].

<sup>21</sup>Notiamo che tale risoluzione, con parte discreta o continua vale, seguendo Dirac, una volta scelto  $Q$  come spettro comune di un insieme massimale di osservabili che commutano su  $\mathcal{H}$ .

All'interno di tale formalismo è noto che differenti realizzazioni della mappa di Weyl forniscono diverse corrispondenze tra operatori e simboli, e che queste corrispondenze danno una formulazione del problema dell'ordinamento nella quantizzazione<sup>22</sup>. Una classe di esempi interessanti viene da una immediata generalizzazione della definizione di sistema di Weyl per il gruppo abeliano  $(V = \mathbb{R}^{2N}, +)$ . Rispetto alla definizione posta in (26), si possono considerare sistemi di Weyl definiti come rappresentazioni unitarie proiettive di  $(\mathbb{R}^{2N}, +)$  per cui

$$D_S(v_1 + v_2) = e^{i\phi(v_1, v_2)/\hbar} D_S(v_1) D_S(v_2) \quad (40)$$

in cui il fattore di fase  $\phi : V \times V \rightarrow \mathbb{R}$  è un bilineare<sup>23</sup> che non è necessariamente antisimmetrico, e che scriviamo come

$$\phi(v_1, v_2) = \omega(v_1, v_2) + S(v_1, v_2) \quad (41)$$

con  $S(v_1, v_2) = S(v_2, v_1)$ . È possibile dimostrare (vedi [23]) che, rispetto al caso di un fattore proiettivo puramente simplettico dato da (26) (che corrisponde al caso  $S = 0$ ), si ha

$$D_S(v) = D(v) e^{iS(v, v)/4\hbar},$$

e che ad esso corrisponde una ben definita mappa di Weyl-Wigner che permette un corrispondenza fra operatori su  $\mathcal{H}$  e simboli in  $\mathcal{F}(\mathbb{R}^{2N})$ . Rispetto all'ordinamento, si vede che se  $T^*Q = \mathbb{R}^2$  con  $\omega = dq \wedge dp$ , la scelta  $S = 0$  fornisce una quantizzazione

$$f = qp \quad \mapsto \quad \hat{f} = \frac{1}{2}(\hat{q}\hat{p} + \hat{p}\hat{q})$$

in termini degli operatori canonici nella rappresentazione (24) à la Schrödinger. Il fattore di fase

<sup>22</sup>Ci stiamo riferendo al cosiddetto problema dei diversi ordinamenti nella quantizzazione. La funzione classica  $qp$  su  $\mathbb{R}^2$  corrisponde in principio al limite per  $\hbar \rightarrow 0$  delle diverse (tra molte altre) espressioni operatoriali  $\alpha\hat{q}\hat{p} + (1 - \alpha)\hat{p}\hat{q}$ , con  $\alpha \in \mathbb{R}$ .

<sup>23</sup>La richiesta che  $D_S : V \rightarrow \mathcal{U}(\mathcal{H})$  sia una rappresentazione proiettiva implica che il fattore di fase debba soddisfare una condizione di cociclo data da

$$\phi(v_1, v_2 + v_3) + \phi(v_2, v_3) = \phi(v_1, v_2) + \phi(v_1 + v_2, v_3)$$

$$\forall v_1, v_2, v_3 \in V.$$

Tale condizione è soddisfatta da funzioni  $\phi$  bilineari.

$S = 2dq \otimes dp$  fornisce una quantizzazione

$$f = qp \quad \mapsto \hat{f} = \hat{p}\hat{q}$$

ed un prodotto à la Moyal dato da

$$f *_S g = \sum_{k=0}^{\infty} \frac{(-i\hbar)^k}{k!} \frac{\partial^k f}{\partial q^k} \frac{\partial^k g}{\partial p^k}, \quad (42)$$

mentre il fattore  $S = -2dq \otimes dp$  dà

$$f = qp \quad \mapsto \hat{f} = \hat{q}\hat{p}.$$

ed un prodotto di Moyal

$$f *_S g = \sum_{k=0}^{\infty} \frac{(i\hbar)^k}{k!} \frac{\partial^k f}{\partial p^k} \frac{\partial^k g}{\partial q^k}. \quad (43)$$

Questi casi forniscono degli esempi di risultati più generali che si possono provare (vedi [20]). Per i prodotti à la Moyal ottenuti da sistemi di Weyl del tipo (40), e che sono detti *pesati*, si ha ancora

$$\{f, g\} = \lim_{\hbar \rightarrow 0} -\frac{i}{\hbar} (f *_S g - g *_S f),$$

rispetto alla parentesi di Poisson relativa alla struttura simplettica  $\omega$ . Ancora una volta, inoltre, nessun troncamento della serie asintotica del prodotto simmetrizzato ad un ordine finito in  $\hbar$  fornisce una struttura di Jordan. Tutti i prodotti deformati ottenuti a partire da sistemi di Weyl del tipo (40) con un fattore proiettivo (41) con lo stesso termine antisimmetrico legato alla struttura simplettica  $\omega$  risultano equivalenti, nel senso che esiste una trasformazione invertibile  $T_S : \mathcal{F}(\mathbb{R}^{2N}) \rightarrow \mathcal{F}(\mathbb{R}^{2N})$  – che dipende dal bilineare simmetrico  $S$  – per cui

$$T_S(f *_S g) = (T_S f) *_S (T_S g).$$

Questo risultato indica ancor più chiaramente che, sebbene il prodotto di Moyal, in quanto associativo e non commutativo, dia origine ad un commutatore e ad un prodotto di Jordan, nel limite classico formulato secondo  $\hbar \rightarrow 0$  queste due strutture hanno comportamenti profondamente diversi.

Il problema della quantizzazione e del limite classico è stato parallelamente analizzato all'interno della formulazione tomografica della meccanica quantistica (vedi [24]), ed anche nella pro-

spettiva dello studio della dinamica quantistica scritta in termini di stati coerenti generalizzati [25]. Un esempio interessante in tal senso è dato considerando (vedi [26]) una varietà liscia  $M$  ed una forma di volume che scriviamo come  $d\mu_M$ . Nello spazio di Hilbert  $\mathcal{H} = \mathcal{L}^2(M, d\mu_M)$  consideriamo un insieme ortonormale  $\{\phi_n\}_{n \in \mathbb{N}}$  per cui  $0 < k(m) = \sum_n |\phi_n(m)|^2 < \infty$ . Indicando i vettori  $\phi_n \sim |n\rangle$ , definiamo

$$|m\rangle = \frac{1}{\sqrt{k(m)}} \sum_n \phi_n^*(m) |n\rangle;$$

tali vettori  $|m\rangle$  risultano normalizzati, ovvero  $\langle m|m\rangle = 1$ , ma non ortogonali fra di loro, e forniscono una risoluzione dell'identità (in questo senso generalizzando la nozione di stati coerenti)

$$\int_M d\mu_M k(m) |m\rangle \langle m| = 1$$

su  $\mathcal{H}$ . Attraverso questo sistema di stati coerenti generalizzati, che forniscono ancora una immersione di  $M$  in  $\mathcal{H}$ , possiamo trasformare un operatore  $A \in Op(\mathcal{H})$  in un simbolo  $f_A \in \mathcal{F}(M)$  dato da

$$f_A(m) = \langle m|A|m\rangle; \quad (44)$$

questa corrispondenza si può invertire attraverso una quantizzazione data da

$$\mathcal{F}(M) \ni f \quad \mapsto \quad A_f = \int_M d\mu_M k(m) f(m) |m\rangle \langle m|. \quad (45)$$

Attraverso la scelta  $M = \mathbb{R}^2$  (con coordinate  $(q, p)$  che identificano  $\mathbb{R}^2 \simeq \mathbb{C}$  secondo  $z = q + ip$ ) con il volume  $d\mu_M = dq \wedge dp / 2\pi\hbar$  e

$$\phi_n(z) = e^{-|z|^2/2\hbar} \frac{z^n}{\sqrt{\hbar n!}}$$

possiamo definire

$$|z\rangle = \sum_n \frac{e^{-|z|^2/2\hbar}}{\sqrt{\hbar n!}} z^n |n\rangle$$

ed abbiamo gli stati coerenti nella rappresentazione à la Fock dello spazio di Hilbert  $\mathcal{H}$ . Per essi si ha

$$\int_{\mathbb{C}} d^2z \frac{1}{\hbar\pi} |z\rangle \langle z| = 1, \\ \langle z|z'\rangle = e^{-|z-z'|^2/2\hbar} e^{i\omega(z, z')/\hbar}$$

rispetto alla struttura simplettica standard su  $\mathbb{R}^2$ . La mappa di quantizzazione

$$f(z, z^*) \mapsto \int_{\mathbb{R}^2} \frac{dz \wedge dz^*}{\hbar\pi} f(z, z^*) |z\rangle \langle z|$$

dà operatori simmetrici se  $f = f^*$ , limitati se  $f$  è limitata, autoaggiunti (attraverso l'estensione di Friedrichs) se  $f$  è reale e semi-limitata. Alle funzioni coordinate  $z, z^*$  corrispondono gli operatori di *distruzione* e di *creazione* nello spazio di Fock, dati come

$$\begin{aligned} A_z &= \hat{a} & \hat{a}|n\rangle &= \sqrt{\hbar n}|n-1\rangle, \\ A_{z^*} &= \hat{a}^\dagger & \hat{a}^\dagger|n\rangle &= \sqrt{\hbar(n+1)}|n+1\rangle \end{aligned}$$

con la regola di commutazione  $[\hat{a}, \hat{a}^\dagger] = \hbar 1$ .

## 4. Dall'equazione di Schrödinger alla equazione di Hamilton-Jacobi

Uno degli aspetti più interessanti in cui la descrizione classica differisce da quella quantistica sorge immediatamente dal confronto tra l'equazione di Schrödinger (7) e le equazioni del moto classico (11). Lo spazio  $\mathcal{H}$  è uno spazio vettoriale lineare e complesso, le equazioni dell'evoluzione quantistica sono lineari; la dinamica classica è non lineare su uno spazio di supporto  $M$  che non è necessariamente uno spazio lineare. Anche negli esempi, notevoli per le applicazioni fisiche, di dinamiche classiche in cui  $M \simeq \mathbb{R}^d$ , le equazioni del moto sono in generale non lineari <sup>24</sup>. Sin dalla introduzione della meccanica quantistica, l'assunzione che le funzioni d'onda  $\psi$  siano ampiezze di probabilità, ed elementi di uno spazio vettoriale complesso  $\mathcal{H}$ , è stata invocata come un elemento costitutivo in quanto in grado di descrivere matematicamente i fenomeni di inter-

<sup>24</sup>Tra gli esempi, consideriamo il caso in cui la varietà  $M$  coincide con  $TQ$ , il fibrato tangente di uno spazio delle configurazioni  $Q = \mathbb{R}^n$  i cui punti  $q$  rappresentano le posizioni e le cui coordinate di fibra rappresentano le velocità  $v$ . Una dinamica  $\delta \in \mathfrak{X}(TQ)$  ha una formulazione Newtoniana se l'evoluzione descritta da  $\delta$  risulta in

$$\dot{q}^a = v^a, \quad \dot{v}^a = F^a.$$

Se la forza  $F$  è una funzione lineare di posizione e velocità (come – inter alias – nel caso dell'oscillatore armonico, con  $F^a = -\omega^2 q^a$  o della particella libera, con  $F^a = 0$ ), allora la dinamica è lineare.

ferenza e diffrazione osservati sperimentalmente, insieme all'assunto ulteriore che le densità di probabilità corrispondono ai quadrati delle ampiezze, e che tali ampiezze si possono linearmente sovrapporre.

Il problema di comprendere come sia possibile ottenere una descrizione non lineare a partire da una lineare era stato affrontato storicamente già da Schrödinger stesso. Caratterizzando gli stati coerenti presentati nella sezione precedente come quelli su cui le relazioni di indeterminazione assumono il valore minimo possibile, aveva osservato che tale insieme non è una sottovarietà lineare in  $\mathcal{H}$  e che purtuttavia risulta stabile rispetto all'evoluzione quantistica di una opportuna classe di sistemi. Questo aspetto risulta anche in meccanica classica, in cui si possono esibire esempi notevoli di sistemi lineari la cui riduzione rispetto a sottovarietà non lineari fornisce sistemi integrabili nel senso di Arnold - Liouville <sup>25</sup>.

Invero, una prima naturale osservazione sulla questione della linearità della descrizione quantistica viene richiamando ciò che Dirac scrisse a tal proposito

“...la sovrapposizione in meccanica quantistica ha una natura essenzialmente diversa da quella che si verifica nelle teorie classiche, come si può vedere considerando che il principio di sovrapposizione quantistico richiede indeterminazione nei risultati al fine di avere una interpretazione fisica coerente coi risultati sperimentali.”

Nelle teorie quantistiche, quindi, l'aspetto strutturalmente cruciale sembra essere una regola di sovrapposizione per gli stati, non necessariamente legata ad una struttura lineare, e che tale sovrapposizione sia coerente con le relazioni di indeterminazione, che sembrano legate (vedi la (1)) alla non commutatività della composizione fra osservabili. Questa osservazione è legata anche al fatto che lo spazio degli stati puri è, come abbiamo visto, il proiettivo complesso  $\mathbb{P}(\mathcal{H}) = \mathcal{H}_0/\mathcal{C}_0$  (eventualmente a dimensione infinita), e che tale spazio quoziente risulta

<sup>25</sup>Per essi, rimandiamo il lettore allo studio dei sistemi di Calogero - Moser dal punto di vista della meccanica quantistica, come in [27, 28]

in una varietà (eventualmente a dimensione infinita), non uno spazio lineare. In quest'ottica sembra quindi naturale studiare se in tale spazio degli stati puri esista una nozione di sovrapposizione compatibile con l'evoluzione quantistica, evolvendo un'analisi iniziata in [29], e parimenti analizzare, all'interno del formalismo classico, dinamiche non lineari nel cui spazio delle soluzioni esista una regola di sovrapposizione, per cui da due soluzioni se ne ottiene una terza, come ad esempio nell'equazione di Riccati e più in generale nei cosiddetti sistemi di Lie-Scheffers [30].

Queste considerazioni si rivelano invero legate più ad uno studio dei fondamenti di una descrizione geometrica della meccanica quantistica e delle relazioni fra la meccanica quantistica e della meccanica classica, che al problema del limite classico di una dinamica quantistica. Per riprendere la nostra analisi sul limite classico di un sistema quantistico, osserviamo che l'equazione di Schrödinger è il punto di partenza di un interessante percorso di dequantizzazione. Questo percorso evidenzia una relazione tra la linearità delle equazioni della dinamica quantistica e la non linearità delle equazioni di una dinamica classica.

Questo cammino inizia considerando una varietà  $Q$  liscia e orientabile, su cui è definito un tensore metrico che scriviamo come

$$g = g_{ab}dq^a \otimes dq^b$$

rispetto ad un sistema di coordinate locali  $\{q^a\}_{a=1, \dots, N=\dim Q}$ . Se  $f \in \mathcal{F}(Q)$  è una funzione opportunamente regolare, il gradiente  $\nabla f \in \mathfrak{X}(Q)$  è il campo vettoriale che soddisfa la condizione

$$g^{-1}(df, \alpha) = i_{\nabla f} \alpha \quad (46)$$

per ogni 1-forma  $\alpha$  su  $Q$ , e l'operatore di Laplace-Beltrami è dato da

$$\Delta \phi = \operatorname{div}(\nabla \phi),$$

in cui la divergenza di un campo vettoriale  $X$  su  $Q$  è definita da  $L_X \tau = (\operatorname{div} X) \tau$  rispetto ad una forma di volume <sup>26</sup>  $\tau$  su  $Q$ . Consideriamo

<sup>26</sup>Sebbene la divergenza di un campo vettoriale  $X$  possa essere definita per ogni dato volume  $\tau$  che dia una orien-

il sistema quantistico descritto dall'evoluzione temporale della funzione d'onda  $\psi = \psi(q, t) \in \mathcal{H} = \mathcal{L}^2(Q, \tau)$  secondo l'equazione di Schrödinger relativa ad una particella di massa  $m$  in  $Q$  soggetta ad un potenziale  $V(q)$  è data da<sup>27</sup>

$$i\hbar \frac{\partial \psi}{\partial t} = \hat{H} \psi = -\frac{\hbar^2}{2m} \Delta \psi + V(q) \psi. \quad (47)$$

Visto che  $\psi$  assume valori in  $\mathbb{C}$ , possiamo scriverla in termini di un'ampiezza e di una fase,

$$\psi(q, t) = A(q, t) e^{iS(q, t)/\hbar} \quad (48)$$

in cui  $A, S$  sono funzioni a valori reali. L'equazione di Schrödinger dà origine a

$$\begin{aligned} \frac{\partial A}{\partial t} + \frac{1}{m} \nabla A \cdot \nabla S + \frac{1}{2m} A \Delta S &= 0, \\ A \left( \frac{\partial S}{\partial t} + \frac{1}{2m} \nabla S \cdot \nabla S + V(q) \right) &= \frac{\hbar^2}{2m} \Delta A \end{aligned} \quad (49)$$

in cui intendiamo, come prodotto scalare di due gradienti, l'espressione

$$\nabla f \cdot \nabla g = g(\nabla f, \nabla g) = g^{-1}(df, dg). \quad (50)$$

La prima relazione in (49) fornisce una equazione di continuità per la densità di probabilità  $\rho = A^2$  ed il vettore corrente  $\nabla S/m$ , che si può scrivere come

$$\frac{\partial \rho}{\partial t} + \frac{1}{m} \operatorname{div}(\rho \nabla S) = 0 \quad (51)$$

e che dipende dall'autoaggiuntezza dell'operatore Hamiltoniano  $\hat{H}$  in (47), o equivalentemente dall'unitarietà della dinamica quantistica.

Nella regione in cui  $A(q, t) \neq 0$ , la seconda equazione in (49) si può scrivere come

$$\frac{\partial S}{\partial t} + \frac{1}{2m} \nabla S \cdot \nabla S + V(q) - \frac{\hbar^2}{2m} \frac{\Delta A}{A} = 0. \quad (52)$$

Essa è l'equazione di Hamilton-Jacobi [31, 32] rispetto alla struttura simplettica canonica su  $T^*Q$  con Hamiltoniana classica

$$H = \frac{1}{2m} g^{ab} p_a p_b + V(q) - \frac{\hbar^2}{2m} \frac{\Delta A}{A} \quad (53)$$

tazione a  $Q$ , si considera, se su  $Q$  si ha una metrica  $g$ , la forma di volume  $\tau = \sqrt{\det[g_{ab}]} dq^1 \wedge \dots \wedge dq^N$ .

<sup>27</sup>Osserviamo che il potenziale  $V(q)$  deve essere tale che l'operatore Hamiltoniano  $\hat{H}$  sia limitato dal basso.

in cui l'energia potenziale ha un termine di origine quantistica, variabile nel tempo  $t$ , che dipende da  $\hbar$ . Vediamo quindi che l'equazione di Schrödinger, che è una equazione alle derivate parziali lineare per la funzione d'onda  $\psi$  a valori complessi, si può scrivere in termini di ampiezza e fase come una coppia di equazioni alle derivate parziali non lineari. Una di esse è una equazione di continuità per la densità di probabilità; l'altra è una equazione di Hamilton-Jacobi per la funzione di fase  $S$ , ovvero

$$H(q, \frac{\partial S}{\partial q}, t) + \frac{\partial S}{\partial t} = 0$$

con Hamiltoniana (53). Il primo passo dell'approssimazione JWKB consiste nel trascurare, rispetto al termine  $V(q)$ , il termine potenziale che dipende da  $\hbar$  e  $A$ , ovvero disaccoppiare, nelle regioni in cui  $A \neq 0$ , l'equazione per la fase dall'equazione per l'ampiezza della funzione d'onda. L'equazione che ne risulta è naturalmente

$$\frac{\partial S}{\partial t} + \frac{1}{2m} \nabla S \cdot \nabla S + V(q) = 0, \quad (54)$$

che scriviamo, per l'Hamiltoniana

$$H = \frac{1}{2m} g^{ab} p_a p_b + V(q) \quad (55)$$

indipendente dal tempo, come

$$H(q, \frac{\partial W}{\partial q}) = E \quad (56)$$

per  $S = W - Et$ . Un integrale completo dell'equazione di Hamilton-Jacobi nella forma (56), ovvero una funzione  $W(q, x)$  che dipende in modo essenziale da un numero di parametri  $x$  pari alla dimensione di  $Q$  per cui

$$\det \left| \frac{\partial^2 W}{\partial q^a \partial x^a} \right| \neq 0, \quad (57)$$

permette di definire una trasformazione canonica su  $T^*Q$  data da  $(q, p) \mapsto (x, k)$  con

$$p_a = \frac{\partial W}{\partial q^a}, \quad k_a = \frac{\partial W}{\partial x^a},$$

che riduce il sistema all'equilibrio, ovvero riduce le equazioni del moto a  $\dot{x}^a = 0$  e  $\dot{k}_a = 0$ . Al medesimo ordine di approssimazione, è possibile dimostrare (vedi anche [33]), che la soluzione

per l'ampiezza  $A$  dall'equazione di continuità in (49) è proprio

$$\rho = \det \left| \frac{\partial^2 W}{\partial q^a \partial x^a} \right| \neq 0, \quad (58)$$

e che pertanto possiamo scrivere una soluzione semiclassica all'ordine più basso in uno sviluppo in  $\hbar$  come

$$\psi = \sqrt{\rho} e^{it(W-Et)/\hbar}. \quad (59)$$

È interessante osservare che, se  $\psi = Ae^{iS/\hbar}$  e  $\tilde{\psi} = \tilde{A}e^{i\tilde{S}/\hbar}$  sono una coppia di soluzioni della dinamica nell'approssimazione che stiamo considerando (ovvero la condizione che permette di trascurare in (53) è soddisfatta per entrambe le ampiezze, indipendentemente) si ha che in generale tale condizione di approssimazione non vale per la somma  $\psi + \tilde{\psi}$ . Inoltre si vede che, pur nei casi in cui la condizione di approssimazione sia valida per la somma  $\psi + \tilde{\psi}$ , tale somma non è necessariamente una soluzione dell'equazione di Hamilton-Jacobi associata: la linearità dell'equazione della dinamica quantistica non si conserva nel limite semiclassico che dà una dinamica classica Hamiltoniana descritta nella formulazione di Hamilton-Jacobi.

## 4.1 Equazioni d'onda e formalismo à la Hamilton-Jacobi

Le relazioni tra l'equazione di Schrödinger ed il formalismo à la Hamilton-Jacobi che abbiamo succintamente descritto permette alcune ulteriori interessanti osservazioni, sia nell'ottica del limite classico che della quantizzazione di una dinamica classica.

Abbiamo visto che la teoria di Hamilton-Jacobi venne ideata in [34] come metodo di soluzione delle equazioni del moto nella formulazione Hamiltoniana. Se la funzione  $W = W(q, x)$  è un integrale completo della (56), allora si considerano le equazioni differenziali ordinarie su  $Q$  date da

$$\frac{dq^a}{dt} = \frac{\partial H}{\partial p_a} \Big|_{p_a = \frac{\partial W}{\partial q^a}} : \quad (60)$$

le relazioni

$$p_a = \frac{\partial W}{\partial q^a} \Big|_{q^a = q^a(t)}, \quad (61)$$

in cui le funzioni  $q^a(t)$  risolvono (60), danno un insieme di curve integrali per le equazioni di Hamilton relative alla Hamiltoniana  $H$  in (55) con dati iniziali

$$(q^a(0), p_a(0)) = \frac{\partial W}{\partial q^a}(q(0), x). \quad (62)$$

Un integrale completo  $W$  fornisce pertanto una famiglia di equazioni differenziali ordinarie (che corrispondono ai diversi valori assunti dalle variabili  $x$ ) su  $Q$  le cui soluzioni sono sufficienti, attraverso la (61), a dare soluzioni delle equazioni di Hamilton su  $T^*Q$ .

Relazioni simili appaiono nell'analisi geometrica di equazioni ondulatorie  $D\psi = 0$  date dall'azione di operatori differenziali iperbolici che agiscono su una funzione d'onda  $\psi$  definita su uno spazio delle configurazioni  $Q$ . Se  $\psi$  ha valori complessi, la fase  $S$  di tale funzione d'onda soddisfa la cosiddetta equazione caratteristica, che nell'equazione d'onda data dall'operatore di D'Alembert descrive la propagazione per fronti d'onda. Essa risulta del tipo di Hamilton-Jacobi per una funzione Hamiltoniana su  $T^*Q$  in cui alle componenti del gradiente  $\nabla S$  corrispondono le componenti dei momenti canonici. La proiezione su  $Q$  delle equazioni di Hamilton associate, come in (60), fornisce le equazioni delle bicaratteristiche dell'operatore d'onda  $D$ . Nel linguaggio dell'ottica, esse descrivono l'evoluzione dei raggi del sistema. Il metodo JWKB consiste, in tale prospettiva, a considerare lo studio semiclassico della dinamica quantistica come l'analogo dello studio dell'ottica geometrica come approssimazione per l'ottica ondulatoria. Il confronto in (52) tra  $V(q)$  ed il termine in  $\hbar\Delta A/2mA$  si interpreta in modo analogo al confronto tra la lunghezza d'onda di un'onda elettromagnetica e la scala di variazione dell'indice di rifrazione del mezzo in cui si propaga.

Ancora: all'interno del formalismo che stiamo descrivendo, ad una equazione d'onda  $D\psi = 0$  in cui  $D$  è un operatore differenziale di ordine  $n$  su  $Q$ , corrisponde una funzione  $H$  (la (55)) a valori *reali* su  $T^*Q$ , dato da un polinomio di grado  $n$  nelle coordinate momento  $p$ . Tale corrispondenza può essere letta come un ulteriore modo di formalizzare una corrispondenza tra operatori differenziali che agiscono su una funzione d'onda, ed il proprio simbolo. Non è questo il

modo più generale per associare ad un operatore differenziale su  $Q$  un simbolo, ovvero una funzione definita su uno spazio a dimensione doppia di quella di  $Q$ . Una analisi più ampia è in [26, 32, 35].

Ai fini di questa nota, ci interessa sottolineare che l'equazione di Schrödinger, scritta come in (48), ha una approssimazione semiclassica non lineare, descritta attraverso l'equazione di Hamilton-Jacobi e una equazione di continuità che è conseguenza dell'unitarietà dell'evoluzione quantistica. Che una teoria lineare (ovvero la meccanica quantistica) abbia una approssimazione non lineare (ovvero la meccanica classica), mentre le equazioni lineari appaiono in molti problemi in fisica come approssimazioni (teorie effettive) di equazioni non lineari, indica che lo studio della meccanica quantistica obbliga ad un cambio di prospettiva nella lettura delle relazioni tra linearità e non linearità: un processo di unificazione sembra far emergere teorie più generali e lineari, rispetto ad un processo di riduzione [27, 6]. In quest'ottica, il problema della quantizzazione di un sistema classico appare come un problema in cui una dinamica non lineare debba essere opportunamente linearizzata e resa unitaria: all'interno delle descrizione à la Schrödinger in termini di operatori differenziali, ciò significa passare dalle soluzioni di una equazione di Hamilton-Jacobi per una funzione di fase ad una descrizione in termini anche di una ampiezza conservata con una opportuna equazione di trasporto. Tale problema risulta naturalmente non univoco, come si vede considerando che la stessa funzione su  $T^*Q$  è il simbolo di operatori differenziali diversi.

## 5. La dinamica quantistica come evoluzione unitaria su uno spazio di Kähler

Come abbiamo visto nelle sezioni precedenti, la meccanica quantistica è stata fondata su strutture algebriche lineari. In questa sezione vogliamo descrivere come l'evoluzione quantistica si possa descrivere attraverso il formalismo della geometria differenziale [27, 36, 37], e come all'interno di questo formalismo l'equazione di Schrödinger (presentata in (4)-(5)) si possa scrivere come un

equazione differenziale ordinaria del primo ordine, ovvero come un campo vettoriale su una opportuna varietà  $M$ , in modo analogo alla descrizione classica di una evoluzione temporale. La struttura geometrica<sup>28</sup> che permette ciò è un tensore di Kähler su  $M$ . Tale tensore permette di definire sia una struttura simplettica che una struttura metrica Riemanniana (che vengono dette compatibili), e l'equazione di Schrödinger risulta unitaria, ovvero Hamiltoniana e di Killing rispetto alla metrica. Lo scopo di questa sezione è descrivere il modo attraverso cui una dinamica si possa scrivere attraverso un campo vettoriale, su uno spazio eventualmente a dimensione infinita, e che questo fornisce un quadro per lo studio del limite classico.

Il primo passo di questa analisi è mostrare come l'equazione di Schrödinger su uno spazio di Hilbert a dimensione finita si possa scrivere in termini di un campo vettoriale su uno spazio vettoriale reale. Tale campo vettoriale risulta unitario, nel senso che mostreremo.

Iniziamo pertanto considerando uno spazio di Hilbert  $\mathcal{H} \simeq \mathbb{C}^N$  a dimensione finita, in cui denotiamo il prodotto scalare come  $\langle z|z' \rangle$  e assumiamo che tale prodotto scalare sia  $\mathbb{C}$ -lineare nel secondo argomento e  $\mathbb{C}$ -antilineare nel primo. Se  $\{e_a\}_{1,\dots,N}$  è una base Hermitiana per  $\mathcal{H}$ , le componenti di  $z$  rispetto ad essa sono date da

$$\langle e_a|z \rangle = q_a + ip_a,$$

con  $(q^a, p_a) \in \mathbb{R}$ . Possiamo allora identificare  $\mathcal{H} = \mathbb{C}^N \simeq \mathbb{R}^{2N} \simeq \mathcal{H}_{\mathbb{R}}$  con un sistema globale di coordinate dato da  $(q, p)$ . Visto che  $\mathbb{R}^{2N}$  è uno spazio vettoriale, abbiamo  $T\mathbb{R}^{2N} \simeq \mathbb{R}^{2N} \times \mathbb{R}^{2N}$  e possiamo scrivere il prodotto scalare Hermitiano in forma reale come

$$\begin{aligned} \left\langle \frac{\partial}{\partial q_a}, \frac{\partial}{\partial q_b} \right\rangle &= \left\langle \frac{\partial}{\partial p_a}, \frac{\partial}{\partial p_b} \right\rangle = \delta_{ab}, \\ \left\langle \frac{\partial}{\partial q_a}, \frac{\partial}{\partial p_b} \right\rangle &= -\left\langle \frac{\partial}{\partial p_a}, \frac{\partial}{\partial q_b} \right\rangle = i\delta_{ab}, \end{aligned} \quad (63)$$

<sup>28</sup>Una interessante introduzione alla nozione di struttura di Kähler e alla sua analisi nella descrizione di sistemi fisici è in [38], a cui rimandiamo il lettore interessato.

ovvero come tensore

$$\begin{aligned} \mathbf{h} &= (dq_a \otimes dq_a + dp_a \otimes dp_a) \\ &+ i (dq_a \otimes dp_a - dp_a \otimes dq_a) \\ &= \mathbf{g} + i\omega \end{aligned} \quad (64)$$

su  $\mathbb{R}^{2N}$ . La parte reale  $\mathbf{g}$  fornisce una metrica Euclidea, la parte immaginaria  $\omega$  la forma simplettica canonica. Il tensore (1-1) dato da

$$\mathbf{J} = \frac{\partial}{\partial p_a} \otimes dq_a - \frac{\partial}{\partial q_a} \otimes dp_a, \quad (65)$$

soddisfa  $\mathbf{J}^2 = -1$ , e dà una struttura complessa su  $\mathcal{H}_{\mathbb{R}}$  compatibile sia con la struttura metrica che con quella simplettica, poiché si ha

$$\begin{aligned} \mathbf{g}(\mathbf{J}u, v) &= \omega(u, v), \\ \mathbf{g}(\mathbf{J}u, \mathbf{J}v) &= \mathbf{g}(u, v), \\ \omega(\mathbf{J}u, \mathbf{J}v) &= \omega(u, v) \end{aligned} \quad (66)$$

per ogni coppia di campi vettoriali  $u, v$  su  $\mathcal{H}_{\mathbb{R}}$ . Lo spazio  $(\mathcal{H}_{\mathbb{R}}, \mathbf{J}, \mathbf{g}, \omega)$  è pertanto una varietà di Kähler (vedi [?]), in cui  $\mathbf{J}$  ha torsione nulla (è una condizione di integrabilità globale) e struttura simplettica  $\omega$ . Se invece si adottano coordinate  $z_a = q_a + ip_a$  e  $\bar{z}_a = q_a - ip_a$  si ha

$$\begin{aligned} \mathbf{g} &= \frac{1}{2} (dz_a \otimes d\bar{z}_a + d\bar{z}_a \otimes dz_a), \\ \omega &= \frac{i}{2} dz_a \wedge d\bar{z}_a, \\ \mathbf{J} &= i \left( \frac{\partial}{\partial z_a} \otimes dz_a - \frac{\partial}{\partial \bar{z}_a} \otimes d\bar{z}_a \right). \end{aligned} \quad (67)$$

Le trasformazioni unitarie su  $\mathcal{H}$ , ovvero quelle lineari per cui la struttura Hermitiana  $\mathbf{h}$  è invariante, risultano date equivalentemente da una delle intersezioni

$$\begin{aligned} \mathbf{U}(N) &= \mathbf{O}(2N, \mathbb{R}) \cap \mathbf{Sp}(2N, \mathbb{R}) \\ &= \mathbf{GL}(N, \mathbb{C}) \cap \mathbf{O}(2N, \mathbb{R}) \\ &= \mathbf{Sp}(2N, \mathbb{R}) \cap \mathbf{GL}(N, \mathbb{C}), \end{aligned} \quad (68)$$

in cui il gruppo ortogonale è quello che lascia invariata la metrica  $\mathbf{g}$ , quello simplettico è quello che lascia invariata la forma simplettica  $\omega$ . Un generico campo vettoriale lineare su  $\mathbb{R}^{2N}$  si scrive come

$$X_W = W_{ab} x_b \partial_a$$

(indicato con  $\{x_a\}_{a=1,\dots,2N} = (q, p)$  le coordinate

globali su  $\mathbb{R}^{2N}$ ) rispetto ad una matrice  $W$  ad elementi in  $\mathbb{R}$ . Esso genera un gruppo ad un parametro di trasformazioni unitarie se e solo se vale uno tra gli insiemi di condizioni equivalenti dati da<sup>29</sup>

- $L_{X_W}J = 0$ , e  $L_{X_W}g = 0$ ;
- $L_{X_W}J = 0$ , e  $L_{X_W}\omega = 0$ ;
- $L_{X_W}g = 0$ , e  $L_{X_W}\omega = 0$ .

che corrispondono alle intersezioni in (68). Queste condizioni sono realizzate se e solo se la matrice  $W \in \mathbb{M}^{2N,2N}(\mathbb{R})$  si scrive come

$$W = \begin{pmatrix} A & B \\ -B & A \end{pmatrix} \quad \text{con} \quad A = -A^T, B = B^T. \quad (69)$$

I corrispondenti campi vettoriali lineari  $X_W$  sono detti Hermitiani: essi sono sia Hamiltoniani rispetto alla forma simplettica  $\omega$  che di Killing rispetto alla metrica  $g$ . Ciò implica anche che  $J$  risulti invariante lungo il flusso che generano. La corrispondente funzione Hamiltoniana, ovvero la  $f_W$  su  $\mathbb{R}^{2N}$  per cui  $i_{X_W}\omega = df_W$  risulta quadratica, ovvero

$$\begin{aligned} & f_W(q, p) \\ &= \frac{1}{2} \begin{pmatrix} q_a & p_a \end{pmatrix} \begin{pmatrix} B_{ab} & -A_{ab} \\ A_{ab} & B_{ab} \end{pmatrix} \begin{pmatrix} q_b \\ p_b \end{pmatrix} \\ &= \frac{1}{2} \bar{z}_a (H_{ab}) z_b = \frac{1}{2} \langle z | H | z \rangle \\ &= f_H(z, \bar{z}) \end{aligned} \quad (70)$$

con  $H \in \mathbb{M}^{N,N}(\mathbb{C})$  data da  $H = B + iA = H^\dagger$ . La dinamica unitaria data da  $X_W$  (o equivalentemente da  $X_H$ ) si può scrivere come

$$\begin{aligned} i\hbar \frac{dz_a}{dt} &= H_{ab} z_b, \\ -i\hbar \frac{d\bar{z}_a}{dt} &= \bar{H}_{ab} \bar{z}_b, \end{aligned} \quad (71)$$

pertanto possiamo identificare il settore olomorfo di  $\mathbb{C}^{2N}$  con  $\mathbb{R}^{2N}$  e osservare che una dinamica quantistica (ovvero una equazione à la Schrödinger) sullo spazio vettoriale di Kähler  $(\mathcal{H}, h = g + i\omega)$  è data da tutti e soli i campi vettoriali lineari Hermitiani su  $(\mathcal{H}_{\mathbb{R}}, J, g, \omega)$ .

<sup>29</sup>L'operatore  $L_{X_W}$  indica la derivata di Lie di un tensore lungo il campo  $L_{X_W}$ , ovvero la derivata di un tensore lungo le curve integrali di  $X_W$ .

La dinamica di Schrödinger (71) si può anche scrivere in termini della parentesi di Poisson

$$\Lambda = \frac{\partial}{\partial q_a} \wedge \frac{\partial}{\partial p_b} = -2i \frac{\partial}{\partial z_a} \wedge \frac{\partial}{\partial \bar{z}_a}, \quad (72)$$

corrispondente alla struttura simplettica  $\omega$ . Si ha infatti

$$\begin{aligned} \dot{q}_a &= \frac{1}{\hbar} \{q_a, f_W\}, \\ \dot{p}_a &= \frac{1}{\hbar} \{p_a, f_W\} \end{aligned} \quad (73)$$

su  $\mathcal{H}$  rispetto a coordinate reali  $(q, p)$  e una matrice  $W$  che soddisfa (69) e

$$\begin{aligned} \dot{z}_a &= \frac{1}{\hbar} \{z_a, f_H\}, \\ \dot{\bar{z}} &= \frac{1}{\hbar} \{\bar{z}_a, f_H\} \end{aligned} \quad (74)$$

rispetto a coordinate olomorfe, con  $H = H^\dagger$ . Così come il tensore di Poisson permette di associare ad ogni funzione  $f$  su  $\mathcal{H}$  un campo vettoriale Hamiltoniano  $X_f$ , anche la struttura metrica, scritta in forma controvariante,

$$\begin{aligned} G &= \frac{\partial}{\partial q_a} \otimes \frac{\partial}{\partial q_a} + \frac{\partial}{\partial p_a} \otimes \frac{\partial}{\partial p_a} \\ &= 2 \left( \frac{\partial}{\partial z_a} \otimes \frac{\partial}{\partial \bar{z}_a} + \frac{\partial}{\partial \bar{z}_a} \otimes \frac{\partial}{\partial z_a} \right) \end{aligned} \quad (75)$$

permette di associare ad ogni funzione  $f$  (come in (46)) un campo *gradiente*  $\nabla f$  su  $\mathcal{H}$ , ed il prodotto scalare tra essi si può scrivere come una parentesi simmetrica (come in (50)) che denotiamo come

$$(f, f') = G(df, df'). \quad (76)$$

Consideriamo ora la corrispondenza, che amplia la (70) data da

$$A \mapsto f_A(z, \bar{z}) = \frac{1}{2} \langle z | A | z \rangle. \quad (77)$$

Essa risulta una biiezione tra l'insieme  $\mathbb{M}^{N,N}(\mathbb{C})$  e l'insieme delle funzioni quadratiche nelle coordinate lineari  $z, \bar{z}$ . Visto che sia il tensore di Poisson che il tensore metrico (72)-(75) sono omogenei di grado  $(-2)$ , è immediato verificare che

$$\begin{aligned} \{f_A, f_B\} &= f_{-i[A,B]} = -i f_{[A,B]}, \\ (f_A, f_B) &= f_{AB+BA} \end{aligned} \quad (78)$$

da cui si ha

$$f_{AB} = \frac{1}{2}(f_A, f_B) + \frac{i}{2}\{f_A, f_B\}. \quad (79)$$

Questa relazione mostra che lo spazio vettoriale delle funzioni quadratiche su  $\mathcal{H}$  non è un'algebra rispetto al prodotto puntuale, ma la corrispondenza (77) induce in essa una struttura di prodotto non commutativo (bilineare) che rappresenta il prodotto non commutativo in  $Op(\mathcal{H})$ , in analogia al prodotto alla Moyal descritto precedentemente. Al commutatore in  $Op(\mathcal{H})$  corrisponde ancora una volta una struttura di Poisson, al prodotto di Jordan corrisponde una struttura metrica compatibile (nel senso di Kähler, vedi la (66)) e pertanto equivalentemente una struttura complessa  $J$ . L'evoluzione quantistica, che è lineare e unitaria, preserva i tensori  $g, \omega, J$ .

La domanda naturale diviene ora se sia possibile descrivere questa dinamica sullo spazio degli stati puri del sistema, ovvero sul proiettivo complesso dato dal quoziente  $\mathbb{P}(\mathcal{H}) = \mathcal{H}_0/\mathbb{C}_0$ , che non è più uno spazio lineare, ma una varietà. Invero, è possibile dimostrare che tale quoziente si può realizzare come base di un fibrato principale, le cui fibre sono le distribuzioni integrali generate dai campi vettoriali  $\Delta$  e  $\Gamma$ , dove

$$\Delta = q_a \frac{\partial}{\partial q_a} + p_a \frac{\partial}{\partial p_a}$$

è il generatore infinitesimo del gruppo delle dilatazioni (il campo di Eulero) e codifica la presenza di una struttura lineare su  $\mathbb{R}^{2N}$ , mentre  $\Gamma = J(\Delta)$  è il generatore infinitesimo dell'azione del fattore di fase da  $\mathbb{C}$  come rotazione in  $\mathbb{R}^{2N}$  intorno ad un punto fisso dato dallo zero. Tale quoziente risulta ancora una varietà di Kähler. A partire<sup>30</sup> dai tensori  $\Lambda$  e  $G$  su  $\mathcal{H}$  si osserva che i tensori

$$\begin{aligned} \tilde{\Lambda} &= \langle z|z \rangle \Lambda, \\ \tilde{G} &= \langle z|z \rangle G \end{aligned}$$

non forniscono una struttura di Kähler su  $\mathcal{H}$ , ma sono proiettabili sul quoziente  $\mathbb{P}(\mathcal{H})$ , dove invero forniscono l'inverso di una struttura simplettica

<sup>30</sup>Un'analisi più completa di questa procedura di riduzione è in [39, 40, 41]. Accanto ad essa, si dimostra la struttura di Kähler si può indurre attraverso le proprietà di una momentum map sul proiettivo complesso poiché esso risulta un'orbita dall'azione simplettica del gruppo unitario.

ca  $\tilde{\omega}$  e un tensore metrico  $\tilde{g}$  globalmente compatibili<sup>31</sup>, ovvero una struttura di Kähler. Una funzione  $f : \mathbb{P}(\mathbb{C}^N) \rightarrow \mathbb{R}$  si dice Kähleriana se il corrispondente campo vettoriale Hamiltoniano  $X_f$  rispetto a  $\tilde{\omega}$  è anche di Killing rispetto alla metrica  $\tilde{g}$  di Fubini-Study, una funzione  $f : \mathbb{P}(\mathbb{C}^N) \rightarrow \mathbb{C}$  si dice Kähleriana se sono Kähleriane sia la sua parte reale che la sua parte immaginaria. In particolare,  $f$  risulta Kähleriana se e solo se<sup>32</sup> esiste una matrice  $A \in \mathbb{M}^{N,N}(\mathbb{C})$  per cui

$$f = e_A = \frac{\langle z|A|z \rangle}{\langle z|z \rangle}. \quad (80)$$

In particolare, il campo vettoriale unitario dato da  $X_H$  in (74) in  $\mathcal{H}$  risulta anche esso proiettabile su  $\mathbb{P}(\mathcal{H})$ , ovvero risulta una derivazione dell'algebra delle funzioni su  $\mathbb{P}(\mathcal{H})$ . Non solo: esso risulta unitario rispetto alla struttura di Kähler introdotta in precedenza, e la sua Hamiltoniana risulta la funzione  $e_H/2$ . Le funzioni di Kähler forniscono un ulteriore esempio di rappresentazione dell'algebra non commutativa delle matrici, con un prodotto non commutativo dato da

$$\begin{aligned} e_{AB} &= e_A * e_B \\ &= e_A e_B + \frac{1}{2}[(e_A, e_B)_{\tilde{g}} + i\{e_A, e_B\}_{\tilde{\omega}}] \end{aligned}$$

che risulta ancora una deformazione di quello puntuale lungo il tensore metrico  $\tilde{g}$  e la struttura simplettica  $\tilde{\omega}$ .

Questa descrizione si può estendere al caso in cui  $\dim \mathcal{H} = \infty$ , come analizzato in dettaglio in [42, 43, 44], se l'algebra non commutativa delle matrici su  $\mathbb{C}$  viene sostituita dall'algebra  $B(\mathcal{H})$  degli operatori limitati su  $\mathcal{H}$ . In particolare, si può vedere che la struttura di commutatore sullo spazio degli operatori è legato alla struttura di Poisson rispetto a  $\tilde{\omega}$  sullo spazio degli stati puri. L'evoluzione temporale (generata da un operatore Hamiltoniano  $H$ ) dell'osservabile  $A \in B(\mathcal{H})$  risulta nell'evoluzione temporale del suo valor medio, ovvero della funzione Kähleriana  $e_A$ . Tale evoluzione è sia simplettica che di Killing sul

<sup>31</sup>In particolare, il tensore metrico che ne risulta coincide con quello di Fubini-Study.

<sup>32</sup>Notiamo infatti che  $\mathbb{P}(\mathbb{C}^N)$  non è uno spazio vettoriale, e pertanto non esiste una definizione consistente di funzioni lineari, o quadratiche.

proiettivo complesso, e si scrive come

$$\frac{de_A}{dt} = -\frac{i}{\hbar} e_{[A,H]} = -\frac{i}{\hbar} \{e_A, e_H\}_{\tilde{\omega}}. \quad (81)$$

Questa relazione generalizza il teorema di Ehrenfest, e descrive l'evoluzione quantistica in termini di valori medi delle osservabili su uno spazio di Kähler.

Prima di concludere questa sezione, osserviamo che la struttura metrica  $\tilde{g}$  permette di descrivere le relazioni di indeterminazione, che nel limite classico non sono presenti, così ritrovando una analogia con l'analisi condotta all'interno del formalismo à la Weyl-Wigner. Anche la struttura complessa, la cui presenza in una geometria di Kähler è equivalente a quella di una metrica compatibile con la forma simplettica, subisce lo stesso destino.

## Conclusioni

In questa nota abbiamo provato a descrivere alcune questioni legate al problema della dequantizzazione di un sistema quantistico. Abbiamo presentato il formalismo à la Weyl-Wigner all'interno del problema di circoscrivere la forma del principio di corrispondenza à la Dirac; abbiamo descritto la cosiddetta approssimazione semiclassica (o di iconale) a partire dall'equazione di Schrödinger al fine di analizzare come si ottenga una classica non lineare a partire da una descrizione quantistica lineare del moto di un sistema. Al termine, abbiamo descritto la geometria dello spazio degli stati puri di un sistema quantistico, evidenziando che la dinamica quantistica risulta naturalmente unitaria rispetto ad una struttura di Kähler su uno spazio non lineare dato dal proiettivo complesso di uno spazio di Hilbert complesso e separabile a dimensioni infinite.

Chiudiamo questa nota con altre due questioni, che meritano una ulteriore futura analisi. La prima riguarda la possibilità di studiare come un prodotto commutativo sorga come contrazione di un prodotto non commutativo, evolvendo una idea descritta in [45], la cui origine poggia sull'analisi di un esperimento di diffusione da doppia fenditura di un sistema in cui la posizione di una lastra di conduttore permette di definire un opportuno parametro che fornisce una scala

per quantificare la classicità (ovvero) la non classicità di un insieme di misure. La seconda riguarda il problema di sviluppare una nozione di integrabilità (nel senso di Arnold - Liouville), per una dinamica quantistica, visto che nel caso classico una dinamica lineare e unitaria è sempre completamente integrabile.



- [1] N. Bohr, *On the quantum theory of line spectra*, D. Kgl. Danske Vidensk. Selsk. Skrifter, Naturvidensk. og Mathem. 8 (1918), ripubblicato come parte di un testo dal medesimo titolo da Dover, NY 2005;
- [2] P.A.M. Dirac, *The principles of quantum mechanics*, 4th edition 1958, Pergamon Oxford.
- [3] M.C. Gutzwiller, Resource Letter ICQM-1: The interplay between classical and quantum mechanics, *Am. Jour. Physics* 66 (1998) 304-324.
- [4] G.G. Emch, *Geometric dequantization and the correspondence problem*, *Int. J. Theor. Phys.* 22 (1983) 397-420;
- [5] Z. Li, Y. Mao, M. Weilenmann, A. Tavakoli, H. Chen, L. Feng, S. Yang, M.O. Renou, D. Trillo, T. Le, N. Gisin, A. Acín, M. Navascués, Z. Wang, J. Fan, *Testing real quantum theory in an optical quantum network*, *Phys. Rev. Lett.* 128 (2022) 040402.
- [6] G. Marmo, E.J. Saletan, A. Simoni, B. Vitale, *Dynamical system: a differential geometric approach to symmetry and reduction*, John Wiley New York 1985;
- [7] O. Bratteli, D.W. Robinson, *Operator algebras and quantum statistical mechanics I*, Springer Berlin Heidelberg 1987;
- [8] O. Bratteli, *Derivations, dissipations and group actions on C\*-algebras*, *Lect. Notes in Math.* 1229, Springer Berlin Heidelberg 1986;
- [9] K. Landsman, *Foundations of quantum theory*, Springer Open 2017;
- [10] E. Schrödinger, *Zum heisenbergschen Unschärfepprinzip*, *Ber. Kgl. Akad. Wiss.* 296 (1930) 296-303.
- [11] H.P. Robertson, *A general formulation of the uncertainty principle and its classical interpretation*, *Phys. Rev.* 35 (1930) 667;
- [12] H.P. Robertson, *An indeterminacy relation for several observables and its classical interpretation*, *Phys. Rev.* 46 (1934) 794-801;
- [13] G. Rudolph, M. Schmidt, *Differential Geometry and Mathematical Physics. Part I: Manifolds, Lie groups and Hamiltonian systems*, Springer 2013;
- [14] P.A.M. Dirac, *The fundamental equations of quantum mechanics*, *Proc. Royal Soc. London. Series A.* 109 (1925) 642-653;
- [15] V. Gayral, J.M. Gracia-Bondía, B. Iochum, T. Schücker, J.C. Varilly, *Moyal planes are spectral triples*, *Comm. Math. Phys.* 246 (2004) 569;

- [16] J. M. Gracia-Bondía, J. C. Varilly, *Algebras of distributions suitable for phase space quantum mechanics I*, J. Math. Phys. 29 (1988) 869-879;
- [17] J. C. Varilly, J. M. Gracia-Bondía, *Algebras of distributions suitable for phase space quantum mechanics II – Topologies on the Moyal algebra*, J. Math. Phys. 29 (1988) 880-887;
- [18] G. Marmo, G. Sclarici, A. Simoni, F. Ventriglia, *The quantum-classical transition: the fate of the complex structure*, Int. J. Geom. Meth. Mod. Phys. 2 (2005) 127-145;
- [19] F. Bayen, M. Flato, C. Fronsdal, A. Lichnerowicz, D. Sternheimer, *Deformation theory and quantization – I Deformations of symplectic structures*, Ann. Phys. 111 (1978) 61-110;
- [20] M. Bertelson, M. Cahen, S. Gutt, *Equivalence of star products*, Class. Quantum Grav. 14 (1997) 93-107;
- [21] M. Schlichenmaier, *Berezin-Toeplitz quantization for compact Kähler manifolds, a review of results*, Adv. Math. Phys. 927180 (2010) Hindawi;
- [22] M. Kontsevich, *Deformation quantization of Poisson manifolds*, Lett. Math. Phys. 66 (2003) 157-613;
- [23] A. Zampini, *Applications of the Weyl-Wigner formalism to noncommutative geometry*, Ph.D. thesis 2005. Una copia è su arXiv:hep-th/0505271.
- [24] A. Ibort, V.I. Man'ko, G. Marmo, A. Simoni, F. Ventriglia, *An introduction to the tomographic picture of quantum mechanics*, Phys. Scr. 79 (2009) 065013.
- [25] A. Perelomov, *Generalised coherent states and their applications*, Text Monograph in Physics, 1986, Springer Berlin;
- [26] J.F. Cariñena, E. Martinez, G. Marmo, X. Gràcia, M.C. Muñoz-Lecanda, *A quantum route to Hamilton-Jacobi equation: comments and remarks*, Banach Centre Pub. 110 (2016) 41-56;
- [27] J.F. Cariñena, L.A. Ibort, G. Marmo, G. Morandi, *Geometry from Dynamics, classical and quantum*, Springer Dordrecht 2015;
- [28] P. Etingof, *Lectures on Calogero - Moser systems*, <https://math.mit.edu/~etingof/zlecnew.pdf>;
- [29] V.I. Man'ko, G. Marmo, E.C.G. Sudarshan, F. Zaccaria, *Interference and entanglement: an intrinsic approach*, J.Phys. A: Math. Gen. 35 (2002) 7137-7157;
- [30] J.F. Cariñena, J. Grabowski, G. Marmo, *Lie-Scheffers systems: a geometric approach*, Bibliopolis 2000, Napoli.
- [31] G. Marmo, G. Morandi, N. Mukunda, *A geometrical approach to the Hamilton-Jacobi form of dynamics and its generalisations*, Riv. Nuovo Cimento 13 (1990) 1-74;
- [32] G. Marmo, G. Morandi, N. Mukunda, *The Hamilton-Jacobi theory and the analogy between classical and quantum mechanics*, J. Geom. Mech. 1 (2009) 317-355;
- [33] G. Esposito, G. Marmo, E.C.G. Sudarshan, *From classical to quantum mechanics*, Cambridge Univ. Press 2004, Cambridge;
- [34] C.G. Jacobi, *Jacobi's lecture on dynamics*, ed. A. Clebsch (2nd. rev. ed.) Hindustan Book Ag 1884/2009;
- [35] F. Lizzi, G. Marmo, G. Sparano, A.M. Vinogradov, *Eikonal type equations for geometrical singularities of solutions in field theory*, J. Geom. Phys. 14 (1994) 211-235;
- [36] A. Ashtekar, T.A. Schilling, *Geometrical formulation of quantum mechanics*, in *On Einstein's Path*, 23-65; Springer Verlag 1999.
- [37] E. Ercolessi, G. Morandi, G. Marmo, *From the equations of motion to the canonical commutation relations*, Riv. Nuovo Cimento 033 08-09 (2010) 401-590.
- [38] V. Guillemin, S. Sternberg, *Symplectic techniques in physics*, Cambridge Univ. Press 1984, New York;
- [39] J. Grabowski, M. Kuś, G. Marmo, *Geometry of quantum systems: density states and entanglement*, J Phys. A: Math. Gen. 38 (2005) 10217;
- [40] J. Grabowski, M. Kuś, G. Marmo, *Symmetries, group actions and entanglement*, Open Sys. and Information Dyn. 13 (2006) 343-362.
- [41] G. Marmo, A. Zampini, *Kähler geometry on complex projective spaces by reduction and unfolding*, Rend. Mat. Appl. 7 (2018) 329-345;
- [42] R. Cirelli, P. Lanzavecchia, *Hamiltonian vector fields in quantum mechanics*, Nuovo Cimento, 79B (1984) 271-283.
- [43] R. Cirelli, A. Manià, L. Pizzocchero, *Quantum mechanics as an infinite dimensional Hamiltonian system with uncertainty structures – I*, J. Math. Phys. 31 (1990) 2891-2897;
- [44] R. Cirelli, A. Manià, L. Pizzocchero, *Quantum mechanics as an infinite dimensional Hamiltonian system with uncertainty structures – II*, J. Math. Phys. 31 (1990) 2898-2903;
- [45] A. Ibort, V.I. Man'ko, G. Marmo, C. Stornaiolo, A. Simoni, F. Ventriglia, *The quantum-to-classical transition: contractions of associative products*, Phys. Scripta 91 (2016) 045201;



**Giuseppe Marmo:** è Professore Emerito di fisica teorica, modelli e metodi matematici della Fisica presso l'Università di Napoli "Federico II". Ha dato notevoli contributi alla fisica matematica tra i quali la teoria dei monopoli non-abeliani, il problema inverso nel calcolo delle variazioni e nella teoria classica e quantistica dei sistemi bi-Hamiltoniani.

**Alessandro Zampini:** è Professore di Geometria presso l'Università di Napoli "Federico II". Si è interessato del formalismo simplettico all'interno del problema della quantizzazione di un sistema dinamico classico e del limite classico di un sistema dinamico quantistico.

Numero XXII Anno 2023

Viaggio nella Scienza

# Ithaca



---

Euclid e l'energia oscura

---

