*L&PS – Logic & Philosophy of Science*
*Vol. X, No. 1, 2012, pp. 31-51*

# La logica computazionale quantistica dei sistemi aperti

Giuseppe Sergioli
Dipartimento di Pedagogia, Psicologia e Filosofia,
Università di Cagliari, Via Is Mirrionis 1, I-09123 Cagliari
giuseppe.sergioli@gmail.com

**1** Introduzione
**2** L'approccio unitario alla computazione quantistica
**3** Dall'universo reversibile a quello irreversibile
**4** L'universalità in computazione quantistica: due approcci differenti
**5** Un nuovo strumento per trattare l'irreversibilità
**6** Conclusione

SOMMARIO. Esistono fenomeni fisici come la decoerenza, il rumore, la misura effettuata nel mezzo del processo computazionale, che difficilmente possono essere interpretati attraverso il paradigma quantistico standard. In un processo computazionale, una qualsiasi interazione del sistema con l'ambiente causa un'inevitabile perdita di informazione che rende il processo stesso irreversibile. Per tener conto di situazioni di questo tipo, la computazione quantistica ha recentemente adottato un nuovo approccio che si spinge oltre a quello standard. Lo scopo di questo articolo è quello di riassumere in maniera descrittiva (evitando di entrare in dettagli tecnici) i caratteri principali di questo nuovo approccio e analizzarne qualche possibile applicazione.

ABSTRACT. There are physical phenomena that can be hardly interpreted by standard quantum paradigm: decoherence, noise, measurements in the middle of a computation – basically, any computational process that involves an interaction with the environment – call into play an unavoidable loss of information that renders the process itself irreversible. To conveniently describe such situations, alongside with the kind of processes that


Published by L&PS – Logic and Philosophy of Science
http://www2.units.it/~episteme/ – ISSN: 1826-1043

are dealt with by the standard approach, a new, more comprehensive perspective has been recently developed in quantum computation. The aim of this paper is to survey and to describe (without come into technical details) some original applications of this new approach.

KEYWORDS: Computazione quantistica, reversibilità, universalità, logica computazionale quantistica.

## 1. Introduzione

La teoria della *computazione quantistica* [3, 5, 22] si pone l'obiettivo di offrire un modello formale di calcolatore in cui l'evoluzione da uno stato al successivo sia determinata dalla teoria quantistica. Come verrà mostrato in dettaglio nel paragrafo 2, la teoria della computazione quantistica fu inizialmente pensata in termini esclusivamente reversibili: vennero considerate solo situazioni in cui uno stato iniziale evolvesse verso uno stato finale in modo tale che fosse sempre possibile considerare l'evoluzione inversa, quella cioè che conduceva dallo stato finale a quello iniziale. Vedremo in seguito come questo tipo di situazioni siano in realtà piuttosto "ideali" e rappresentino solo il caso in cui un sistema fisico sia completamente isolato dall'ambiente esterno. In realtà, per quanto accurate possano essere le precauzioni prese dallo sperimentatore per schermare il sistema che sta osservando, è ben noto come l'idea di ottenere un sistema perfettamente chiuso (cioè completamente isolato) sia in realtà di difficilissima realizzazione (ancor di più in ambito microscopico). Per questo motivo può risultare utile generalizzare la teoria della computazione quantistica ad un generico sistema aperto, in modo da tenere in considerazione anche le interazioni sistema-ambiente. Ogni interazione del sistema con l'ambiente – tra cui ad esempio la misura di una qualsivoglia osservabile fisica – consiste in un'operazione che, in ambito microscopico, modifica in maniera irreversibile lo stato del sistema. In questo articolo verrà presentata una panoramica molto generale relativa a un nuovo approccio alla computazione quantistica, in cui l'evoluzione dello stato del sistema possa essere sia reversibile che irreversibile. Verrà introdotto anche il tema dell'universalità in computazione quantistica e, in conclusione, verranno indicati possibili nuovi sviluppi di ricerca in cui l'approccio di

natura irreversibile suggerisce nuove soluzioni relativamente all'individuazione di nuovi insiemi di operazioni universali in computazione quantistica.

L'articolo è organizzato nel seguente modo: nel paragrafo 2, dopo una breve introduzione storica, verranno descritte le principali caratteristiche dell'approccio standard alla computazione quantistica, che vede operatori unitari (che rappresentano trasformazioni reversibili) agire su vettori unitari; nel paragrafo 3 verrà invece trattato il passaggio dall'approccio unitario a quello più generale, in cui operazioni quantistiche (che rappresentano trasformazioni sia reversibili che irreversibili) agiscono su operatori di densità; verranno quindi analizzate nel dettaglio le caratteristiche del nuovo approccio e le implicazioni che ne conseguono. In particolare verranno discusse le sue conseguenze sulla nuova logica che sostiene questo nuovo approccio formale alla computazione quantistica. Nel paragrafo 4 verranno introdotte la definizione di universalità approssimata e di insieme di operazioni approssimativamente universale. Infine, nel paragrafo 5, verrà presentato un nuovo strumento formale per trattare alcune particolari trasformazioni fisiche irreversibili nel contesto quantistico computazionale.

## 2. L'approccio unitario alla computazione quantistica

All'inizio del ventesimo secolo la meccanica quantistica e la teoria della computazione erano due teorie studiate in maniera del tutto separata [21, 8, 1, 27, 26].

Già precedentemente all'avvento dei computer, la comunità scientifica era solita interrogarsi su questioni del tipo: "che cosa intendiamo per problema?", "Quali problemi sappiamo risolvere?", "Con quante e quali macchine?", "Se non fosse possibile risolvere un certo problema con una certa macchina, potrebbe essere possibile risolverlo con un'altra?" e molte altre ancora. Questo tipo di interrogativi diede vita, nella prima metà del secolo scorso, a quella che venne denominata *teoria della calcolabilità* (o della *computabilità*).

La teoria della calcolabilità intendeva quindi comprendere quali fossero le funzioni che potevano essere calcolate tramite un determinato procedimento automatico (*algoritmo*) a prescindere dalla quantità di risorse richieste. Per offrire una risposta a tali esigenze teoriche, lo sforzo iniziale fu quello di offrire una definizione formale e rigorosa all'idea intuitiva di funzione calcolabile, in modo da distinguere la categoria dei problemi teoricamente risolvibili da quella dei

problemi non risolvibili. Passo successivo fu quello di definire rigorosamente il concetto di algoritmo, in modo che i programmi potessero essere concretamente pensati in termini di funzioni che, a partire da un certo input, restituissero un determinato risultato.

Non è difficile identificare in Alan Turing il pioniere della teoria della calcolabilità. Fu lui a introdurre una macchina ideale – chiamata appunto, *macchina di Turing* – che, eseguendo delle semplici istruzioni (algoritmo) inizialmente impostate (da un programma) fosse in grado di calcolare in maniera deterministica qualsiasi funzione intuitivamente computabile (tesi di Church-Turing). La macchina di Turing, però, pur offrendo lo spunto per nuovi straordinari contributi scientifici dal punto di vista teorico, rimaneva comunque una macchina ideale che non offriva allo stesso modo grandi prospettive in termini di efficienza e concreta utilizzabilità. Inoltre, la nascita dei primi computers, la rapidissima miniaturizzazione delle componenti hardware degli stessi e la continua ricerca di dispositivi sempre più efficienti, condussero a una nuova idea di computazione in cui vennero considerati per la prima volta anche fenomeni di natura microscopica (quindi regolati dalla teoria quantistica) e in cui l'efficienza implementativa assunse un ruolo di primaria importanza.

Il primo studioso a immaginare un'applicazione del paradigma quantistico alla teoria della calcolabilità fu Richard Feynman. L'idea di base era quella secondo cui, mentre la macchina di Turing è rigorosamente deterministica e sequenziale, al contrario la meccanica quantistica presenta in maniera essenziale la nozione di *stato sovrapposto* che – come verrà meglio mostrato in seguito – si basa sui concetti di probabilità e parallelismo. Inoltre, mentre l'alfabeto utilizzato dalla macchina di Turing si limita a un numero di simboli estremamente ristretto, questa limitazione non viene mantenuta nella teoria quantistica. In sostanza, mentre l'informazione espressa da un bit classico era limitata a soli due valori (lo *zero* e l'*uno*), il bit quantistico risulta infinitamente più informativo e questo fece pensare a come un possibile calcolatore quantistico potesse essere assai più efficiente di qualsiasi macchina di Turing. Nel 1982 Feynman dimostrò [13] che nessuna macchina di Turing è in grado di simulare certi fenomeni fisici senza subire un rallentamento esponenziale delle prestazioni. Di contro, un calcolatore quantistico sarebbe in grado di effettuare tali simulazioni con un' efficienza enormemente superiore. Nel 1985 David Deutsch formalizzò il primo modello teorico di macchina di Turing quantistica universale [10] e da lì ebbe inizio una nuova disciplina che ha avuto notevoli sviluppi negli ultimi anni e che

prende il nome di *computazione quantistica*, di cui adesso verranno presentate le caratteristiche essenziali che la differenziano in maniera evidente dal modello classico.

In meccanica quantistica a ogni stato di un arbitrario sistema fisico è associato un vettore unitario (cioè di lunghezza 1) in uno spazio di Hilbert di dimensione adeguata. Allo stesso modo, in computazione quantistica l'unità di informazione è rappresentata da un vettore unitario in uno spazio di Hilbert basato sui numeri complessi. Tale vettore unitario è il corrispettivo quantistico del bit classico e per questo prende il nome di *quantum-bit* o, più sinteticamente, *qubit*. Dal punto di vista logico, mentre i valori di verità che assume un bit classico possono essere solo il "vero" o il "falso", il bit quantistico rappresenta un'informazione più ricca che è formalmente espressa da una *sovrapposizione* tra lo stato vero e lo stato falso: in sostanza un bit quantistico può rappresentare un'informazione vera, falsa o qualsiasi possibile "via di mezzo" tra il vero e il falso. L'espressione "via di mezzo" va però intesa in termini probabilistici: vi è quindi una certa probabilità di *rilevare* – dopo un processo di misura – il sistema (o l'informazione) che si sta descrivendo nello stato "vero" oppure nello stato "falso" e tale probabilità è espressa formalmente dalla nota regola di Born. Ogni stato sovrapposto corrisponde quindi a uno stato "incerto" .

Il qubit è un vettore unitario: dal punto di vista formale l'unitarietà del vettore corrisponde alla *massimalità* dell'informazione che questo rappresenta: la quantità d'informazione si definisce massimale se non può essere ulteriormente incrementata – in modo non contraddittorio – attraverso successive osservazioni. È, in sostanza, l'informazione più completa possibile sullo stato del sistema fisico che si sta descrivendo, che in questo caso si dirà essere uno *stato puro*. La lunghezza del vettore corrisponde quindi alla quantità di informazione che il vettore stesso porta con sé: l'informazione massimale sarà per questo rappresentata da un vettore di lunghezza unitaria. Può essere utile notare come uno stato sovrapposto, quindi *incerto*, possa rappresentare comunque una quantità di informazione massimale e sia quindi ancora uno stato *puro*. Risulta conveniente offrire una rappresentazione geometrica del qubit tramite la sfera di Bloch-Poincaré: è una sfera di raggio unitario, sicché vi è una naturale biiezione tra ciascun punto sulla superficie della sfera e ciascun vettore di lunghezza unitaria (Fig. 1).

Quanto appena detto riguarda esclusivamente la descrizione formale di un singolo sistema fisico. È facile immaginare come in realtà sia necessario offrire

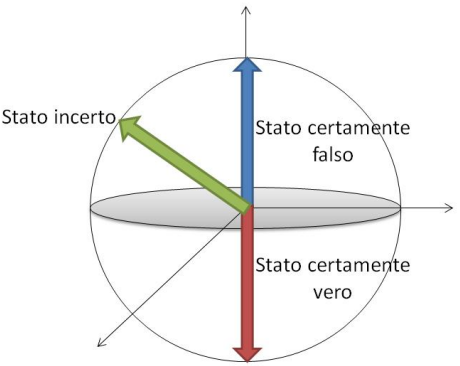


FIGURA 1: *Sfera di Bloch-Poincaré*

una rappresentazione formale anche di più sistemi fisici che interagiscono tra loro. Lo strumento formale che permette tale rappresentazione è il prodotto tensoriale. Due (o più) sistemi fisici che interagiscono sono quindi formalmente rappresentati dal prodotto tensoriale tra i due (o più) vettori unitari nello spazio di Hilbert dei numeri complessi, ciascuno dei quali è la rappresentazione formale del sistema fisico a cui ci si riferisce. Tale prodotto tensoriale di più vettori unitari sarà ancora un vettore unitario che viene chiamato *registro quantistico* o *quregister* e la sua dimensione dipende direttamente dal numero di sistemi fisici interagenti che il registro rappresenta. Chiaramente un registro quantistico di dimensione arbitraria non può essere rappresentato tramite la sfera di Bloch-Poincaré, ma quanto precedentemente detto circa la corrispondenza tra unitarietà del vettore e massimalità dell'informazione resta valido.

Fino ad ora si è offerta una descrizione dello stato del sistema, ma non della sua evoluzione. Così come in ambito classico le porte logiche sono quelle che determinano l'evoluzione del bit classico, lo stesso avviene nell'ambito computazionale quantistico: l'evoluzione dei qubits è regolata dalle porte logico-quantistiche (quantum gates) che formalmente sono rappresentate da operatori unitari. Quando si è definita l'unità di informazione quantistica, si è mostrato come l'espressione "unitarietà del vettore" fosse sinonimo di "massimalità dell'informazione". Adesso invece unitarietà è sinonimo di reversibilità. Per definizione, infatti, affinché un operatore sia unitario deve esistere il suo operatore inverso: applicando un operatore unitario su un sistema fisico, questo passa

da uno stato iniziale a uno stato finale; l'operatore inverso è quell'operatore che, applicato allo stato finale, lo riporta nuovamente allo stato iniziale. È proprio in questo senso che unitarietà dell'operatore e reversibilità della trasformazione sono due concetti così strettamente correlati.

Le porte logico-quantistiche riproducono il comportamento delle porte classiche ma inoltre lo generalizzano ad un contesto molto più ampio. Si consideri per esempio la negazione: dal punto di vista classico, la negazione del falso (cioè di un'informazione falsa) offrirà il vero come output (cioè un'informazione vera) e viceversa. In ambito quantistico questo comportamento viene perfettamente riprodotto, ma, a differenza del caso classico, una porta logico-quantistica potrà essere applicata anche a sovrapposizioni di vero e falso, mantenendo il proprio connotato di reversibilità. Come già accennato in precedenza, una sovrapposizione di vero e falso corrisponde a un terzo stato (differente sia dal "vero" che dal "falso" ) su cui è possibile soltanto dire che, dopo un eventuale processo di misura, si avrà una certa probabilità che il sistema *collassi* nello stato "vero" e un'altra probabilità che collassi nello stato "falso". L'azione della negazione quantistica su di un siffatto stato agirà invertendo tali probabilità. Applicando però nuovamente l'operatore negazione al vettore appena ottenuto, questo invertirà nuovamente le probabilità del vero e del falso, restituendo alla fine lo stesso vettore che si aveva all'inizio. L'esempio appena analizzato costituisce un caso particolare. La negazione è infatti un operatore quantistico che corrisponde al suo inverso: l'operazione che consiste nell' applicare due volte la negazione può quindi essere interpretata come la sequenza che consiste nell'applicare la negazione e successivamente l'operazione inversa, giungendo quindi allo stesso stato di partenza (in altre parole anche in computazione quantistica vale il principio secondo cui due negazioni affermano). L'esempio poc'anzi citato può essere visto come un caso particolarmente semplice di reversibilità dell'operatore quantistico.

È interessante notare come la negazione quantistica sia un esempio di porta che viene detta *semiclassica*, poiché, se si rimanesse confinati esclusivamente agli stati "vero" e "falso" (cioè ai vettori che costituiscono la base computazionale), riprodurrebbe esattamente il comportamento di una porta classica; però, a differenza di queste ultime, la negazione quantistica è applicabile anche a stati sovrapposti ed è in questo senso che le porte logico-quantistiche sono utilizzabili in un contesto molto più ampio rispetto a quelle classiche. Inoltre, mentre le porte logico-quantistiche conservano sempre il loro connotato di reversibilità,

la logica classica è invece naturalmente irreversibile. Basti pensare alla congiunzione: se il risultato del valore di verità di una congiunzione è "falso", non c'è modo di sapere con certezza il valore di verità dei due congiunti o, in altri termini, non è possibile applicare un'operazione inversa alla congiunzione per tornare univocamente dallo stato finale a quello iniziale. La congiunzione quantistica (che è un altro esempio di porta semiclassica) invece lo consente, anche se a costo di un aumento della dimensione dello spazio vettoriale su cui agisce.

Esistono però porte logico-quantistiche che non riproducono neanche in parte il comportamento di alcuna porta classica e che per questo vengono dette *genuinamente quantistiche*. Si tratta di porte che, applicate al "vero" o al "falso", danno in uscita uno stato sovrapposto, comportamento che non è assimilabile in nessun modo ad alcun fenomeno classico. Un esempio è la porta "radice della negazione", così chiamata poiché, se applicata una volta allo stato (ad esempio) "vero", darà in uscita una sovrapposizione tra vero e falso, ma se a tale sovrapposizione si applica nuovamente lo stesso operatore allora in uscita si otterrà lo stato "falso". La radice della negazione si comporta quindi come una sorta di *semi-negazione*. Questa semi-negazione non è solamente un'astrazione matematica ma è la rappresentazione di numerosi fenomeni fisici: uno specchio semi-riflettente che si fa attraversare da metà dei fotoni incidenti ma riflette tutti gli altri costituirebbe un perfetta rappresentazione fisica della radice della negazione. L'intero comportamento dell'interferometro di Mach-Zehnder può essere spiegato mediante il coinvolgimento della radice della negazione [23].

Ritornando quindi alla rappresentazione geometrica offerta in precedenza, così come ogni bit quantistico corrisponde a un vettore di lunghezza unitaria all'interno di una sfera di raggio pari a 1, analogamente l'azione di una porta logico-quantistica corrisponde semplicemente a una rotazione che, essendo un'isometria, preserva l'unitarietà del vettore finale e corrisponde sempre a un'operazione reversibile. Lo stesso discorso può facilmente essere generalizzato a una dimensione arbitrariamente grande: l'operatore, per essere applicato a un vettore, dove naturalmente avere la sua stessa dimensione.

## 3. Dall'universo reversibile a quello irreversibile

Nel paragrafo precedente si è detto come l'unità di informazione sia espressa da un vettore unitario che rappresenta un'informazione massimale. Non è però

difficile convincersi di come sia piuttosto implausibile che un osservatore riesca ad avere un'informazione massimale sul sistema fisico osservato: se infatti le dimensioni di un sistema fisico non sono estremamente ridotte e se il sistema fisico non è perfettamente schermato dall'esterno, allora avere un'informazione massimale sulle possibili interazioni tra tutte le varie componenti del sistema e sulle molteplici interazioni tra sistema e ambiente è un compito davvero molto arduo [6]. Nasce quindi l'esigenza di un modello formale più generale, in cui sia possibile considerare dei sistemi su cui l'osservatore abbia solo un certo "grado di conoscenza".

L'oggetto matematico capace di descrivere l'unità di informazione in termini di conoscenza non esclusivamente massimale è l'operatore di densità. Dal punto di vista strettamente matematico, un operatore di densità è un operatore autoaggiunto, non negativo con traccia 1. Dal punto di vista computazionale l'operatore di densità viene chiamato *qumix*, cioè stato quantistico misto, proprio in contrapposizione con la definizione di stato puro offerta nel paragrafo precedente. Rimanendo confinati, per semplicità, alla descrizione di un solo sistema, è possibile mostrare come ogni operatore di densità sia rappresentabile nello spazio vettoriale degli operatori che agiscono su spazi di Hilbert, tramite combinazione lineare delle matrici di Pauli e della matrice identità; proprio i coefficienti di tale combinazione lineare rappresentano il "grado di conoscenza" dell'informazione che l'operatore di densità porta con sé e esattamente: la somma dei quadrati dei coefficienti della combinazione lineare prima citata è un numero compreso tra 0 e 1. Si può vedere che tale valore gioca per gli operatori di densità ruolo analogo a quello della lunghezza nel contesto dei vettori, ragion per cui può essere interpretato come "grado di conoscenza".

In particolare, nel caso in cui questa lunghezza sia pari a 1 allora si è nuovamente in presenza di un'informazione massimale: in questo caso l'informazione potrà essere espressa tanto da un vettore unitario quanto da un operatore di densità che, in questo caso particolare, sarebbe un operatore di proiezione che proietta proprio su quel vettore unitario. Insomma, in questo caso limite l'operatore di densità e il vettore unitario corrisponderebbero perfettamente e avrebbero lo stesso significato fisico. In tutti gli altri casi, però, l'operatore di densità esprime un grado di conoscenza sempre minore e viene graficamente rappresentato da un vettore di lunghezza minore di 1, fino al caso degenere in cui finisce per rappresentare la totale ignoranza sul sistema. Per riepilogare, un operatore di densità può essere visto:

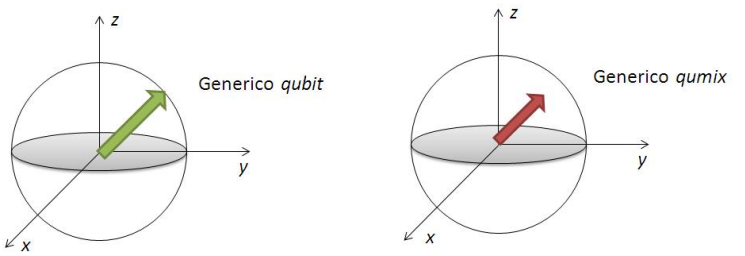


FIGURA 2: *Qubit and qumix*

- dal punto di vista geometrico come un punto (interno o sulla superficie) della sfera di Bloch-Poincaré (Fig. 2);
- dal punto di vista algebrico come un vettore di lunghezza minore o uguale all'unità;
- dal punto di vista epistemico come un'informazione generalmente non massimale.

Da questa prima descrizione dovrebbe quindi apparire già evidente come gli operatori di densità *generalizzino* effettivamente i qubit, nel senso che ogni qubit può essere espresso tramite un operatore di densità (in particolare come un operatore di proiezione), mentre tutti quegli operatori di densità che rappresentano informazioni non massimali non possono in nessun modo essere espressi come qubit.

Così come gli operatori unitari agiscono sui vettori unitari descrivendone l'evoluzione, analogamente è possibile introdurre una nuova entità matematica che sia capace di determinare l'evoluzione di un qualsiasi operatore di densità e che nello stesso tempo possa generalizzare il comportamento di un qualsiasi operatore unitario. Tale entità matematica è rappresentata dalle *operazioni quantistiche*: un'operazione quantistica è una mappa da operatori di densità a operatori di densità che gode di particolari proprietà (è una mappa lineare, completamente positiva che preserva la traccia [18]). Ma una caratteristica fondamentale è quella secondo la quale il comportamento di ogni operatore unitario può essere replicato da un'opportuna operazione quantistica: in sostanza, è possibile applicare una operazione quantistica che rappresenti l'evoluzione di un operatore unitario ad una quantità di informazione che non sia unitaria.

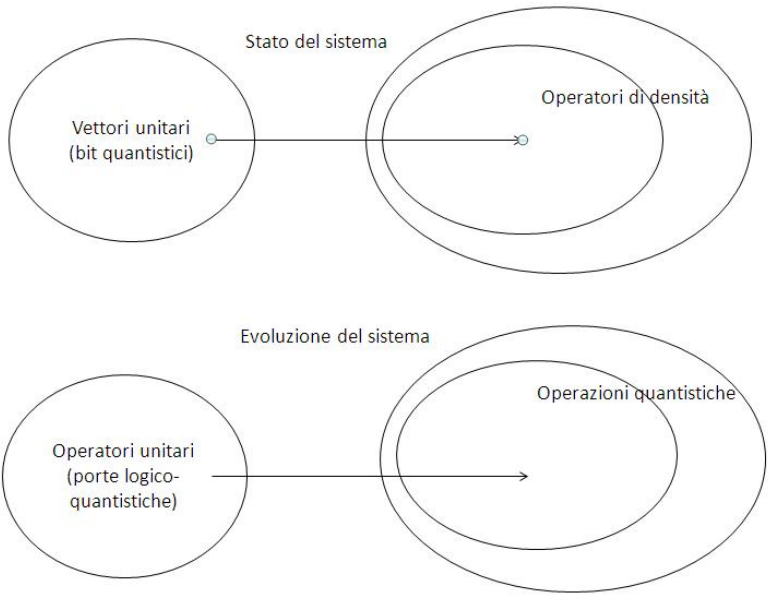


FIGURA 3: *Stato ed evoluzione del sistema*

Rimane il fatto che, se il comportamento di ogni operatore unitario è replicabile da un'operazione quantistica (in questo caso si parlerà di *operazioni quantistiche unitarie*), di contro esistono operazioni quantistiche che non possono essere rappresentate da alcun operatore unitario (in questo caso si parlerà di *operazioni quantistiche non unitarie*). Se un'operazione quantistica corrisponde ad un operatore unitario vuol dire che il significato fisico di entrambi è, ancora una volta, quello di una trasformazione reversibile, ma nel caso in cui l'operazione quantistica non corrisponda ad alcun operatore unitario allora vuol dire che tale operazione quantistica corrisponde fisicamente ad una trasformazione irreversibile.

Si è quindi passati da un contesto in cui si valutava l'evoluzione esclusivamente reversibile di quantità di informazione esclusivamente massimali ad un contesto molto più generale in cui si valuta l'evoluzione sia reversibile che irreversibile di quantità di informazione sia massimali sia non massimali. Nella figura 4 a seguire viene riassunto graficamente quanto detto nel presente paragrafo.

Informazione quantistica

| | QUBIT | QUMIX |
|---|---|---|
| Geometricamente | Punto sulla superficie della sfera | Punto sulla superficie o interno alla sfera |
| Algebricamente | Vettore unitario | Operatore di densità |
| Epistemicamente | Informazione massimale | Informazione generalmente non massimale |
| Evoluzione | Reversibile | Generalmente irreversibile |

FIGURA 4: *Schema riassuntivo sull'informazione quantistica*

## 4. L'universalità in computazione quantistica: due approcci differenti

È ben noto come in logica classica le leggi di interdefinibilità dei connettivi consentano di esprimere alcuni connettivi tramite l'esclusivo utilizzo di altri. Ad esempio, all'interno del contesto classico, la negazione e la congiunzione consentono di rappresentare, tramite opportuni principi di equivalenza, il comportamento degli altri connettivi classici. In questo caso si dirà che la negazione e la congiunzione costituiscono un insieme di connettivi *funzionalmente* universale. In ambito computazionale, la tematica dell'universalità ha sempre rappresentato un problema fondamentale [11, 10, 25, 2].

Trovare un insieme di porte logiche universale di cardinalità più ridotta possibile, permetterebbe di contare sull'esclusivo utilizzo di porte appartenenti a tale insieme per "replicare" il comportamento di ciascuna altra porta logica. Insomma, con l'esclusivo impiego di un numero ridotto di porte logiche sarebbe possibile "costruire" un circuito qualsiasi. Dal punto di vista classico, ad esempio, è noto come la porta di Toffoli sia capace, da sola, di riprodurre il comportamento di ciascuna altra porta di un circuito classico. Quindi la sola porta di Toffoli è funzionalmente universale in ambito computazionale classico.

In computazione quantistica, in virtù di quanto ampiamente discusso nei paragrafi precedenti, gli operatori sono delle isometrie che, dal punto di vista geometrico, corrispondono a rotazioni. Per questo l'insieme degli operatori quantistici (e quindi anche delle operazioni quantistiche) è più che numerabile (poichè

l'isieme delle possibili rotazioni è più che numerabile) e non è quindi possibile in computazione quantistica – sia nel suo approccio unitario sia in quello non unitario – trovare un insieme finito di operatori (o operazioni quantistiche) che possa risultare funzionalmente universale. In virtù del fatto, sottolineato nel paragrafo 3, che l'approccio non unitario generalizza quello unitario, d'ora in avanti il tema dell'universalità verrà affrontato rimanendo confinati all'approccio più generale che prevede operazioni quantistiche che agiscono su operatori di densità.

Shi e Aharonov hanno mostrato [2, 25] come esistano due operazioni quantistiche unitarie capaci di replicare in maniera "approssimata" il comportamento di qualsiasi altra operazione quantistica. In questo caso si parlerà di *universalità approssimata*: un insieme di operazioni quantistiche viene detto approssimativamente universale se, scelta una qualsiasi altra operazione quantistica, è sempre possibile "costruire" un circuito (in cui siano presenti solo le operazioni quantistiche dell'insieme approssimativamente universale) che replichi in maniera arbitrariamente approssimata (cioè a meno di una costante arbitraria) l'azione dell'operazione scelta su un arbitrario operatore di densità. L'insieme di operazioni quantistiche approssimativamente universale introdotte da Shi e Aharonov è costituito dalle operazioni quantistiche di *Toffoli* e di *Hadamard*[1]. L'operatore di Toffoli è ternario e si comporta mantenendo inalterati i primi due qubits e cambiando il terzo solo quando i primi due siano entrambi *veri*. La funzione corrispondente all'operatore di Toffoli risulta già universale in computazione classica ed è particolarmente importante in computazione quantistica in quanto offre la possibilità di ottenere una congiunzione quantistica reversibile (la congiunzione si ottiene grazie all'operatore di Toffoli, dove i primi due qubits corrispondono ai due congiunti e il terzo è un qubit-*ancilla* fissato, in input, sempre nello stato *falso*). L'operatore di Hadamard è genuinamente quantistico e viene anche chiamato "*radice dell'identità* ", per un motivo simile a quello descritto precedentemente per la radice della negazione. Applicando infatti la radice dell'identità a un vettore della base computazionale si ottiene in uscita un vettore sovrapposto, ma applicando a tale vettore sovrapposto nuovamente la radice dell'identità, si otterrà nuovamente il vettore di partenza. La radice dell'identità si comporta quindi come una *semi-identità*.

[1] Per operazione quantistica di Toffoli – o Hadamard – si intende l'*operazione quantistica* che corrisponde all'*operatore quantistico* di Toffoli – o Hadamard – rispettivamente.

Dal punto di vista intuitivo, il fatto che l'insieme di operazioni quantistiche approssimativamente universali sia costituito proprio da Toffoli e Hadamard, potrebbe risultare fortemente emblematico e niente affatto "casuale" : l'operatore di Toffoli infatti contiene tutti i fondamentali ingredienti di "classicità", essendo già da solo classicamente universale; di contro l'operatore di Hadamard, essendo genuinamente quantistico, racchiude uno stretto connotato quantistico. Ecco che l'insieme costituito da queste due porte può apparire come la sintesi più completa e essenziale tra universo computazionale classico e quantistico, rendendo così molto intuitiva l'idea che proprio queste due porte costituiscano un insieme approssimativamente universale in computazione quantistica.

Un volta individuati in Toffoli e Hadamard due operatori particolarmente significativi in computazione quantistica, passaggio naturale è risultato quello di cercare di ottenere una struttura logico-algebrica basata appunto su questi due operatori [15, 9], una struttura algebrica quindi in cui le operazioni consentite riproducano proprio il comportamento degli operatori Toffoli ed Hadamard.

Essendo costruita *ad hoc* sui due operatori, tale struttura è stata nominata "*algebra computazionale quantistica di Shi-Aharonov*". Si tratta di una struttura il cui universo è costituito dall'insieme di tutti gli operatori di densità (di arbitraria dimensione) e le cui uniche operazioni sono le operazioni quantistiche di Hadamard e Toffoli, oltre a tre elementi privilegiati: gli operatori di densità che rappresentano rispettivamente il *vero*, il *falso* e il *perfettamente indeterminato* (che corrisponde a uno stato la cui probabilità del "vero" corrisponde esattamente alla probabilità del "falso" ). In tale struttura è definibile una relazione basata esclusivamente sulla probabilità degli operatori di densità del dominio e degli operatori di densità evoluti in seguito all'applicazione dell'operazione quantistica di Hadamard. Si dimostra come tale relazione sia un preordine il quale induce in modo canonico una relazione d'equivalenza che risulta essere una congruenza sull'algebra. Quozientando il dominio della struttura algebrica precedentemente introdotta rispetto a tale relazione[2], si ottiene [15, 9] un'algebra isomorfa alla più semplice *algebra quantistica computazionale*, il cui universo è dato dalle coppie di numeri reali che designano i punti all'interno di un

[2] Dato che la struttura algebrica è basata fondamentalmente sulla probabilità degli operatori di densità del dominio e degli operatori di densità evoluti in seguito all'applicazione dell'operazione quantistica di Hadamard, il quoziente permette di considerare come equivalenti tutti gli operatori di densità *equiprobabili* nei due sensi appena indicati.

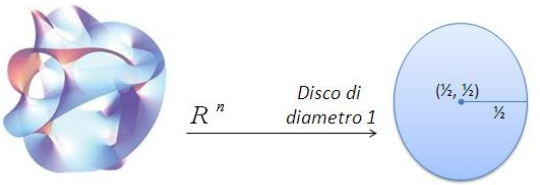


FIGURA 5: *Da* $\mathbb{R}^n$ *al disco*

disco di diametro unitario e centrato sul punto $(\frac{1}{2}, \frac{1}{2})$ e le cui operazioni sono le operazioni quantistiche di Toffoli e Hadamard, il cui dominio d'azione si riduce ai punti del disco sopra indicato (Fig. 5). I punti di questo disco sono ricavabili da considerazioni di carattere matematico riferite ad alcune proprietà della probabilità di un arbitrario operatore di densità.

Il significato intuitivo di tale risultato consiste in una notevolmente semplificazione dell'attività di ricerca delle proprietà logico-algebriche dell'insieme approssimativamente universale di Toffoli e Hadamard: il risultato descritto consente infatti di confinare la ricerca di tali proprietà a una struttura molto più semplice (che ha come universo il disco unitario) e di estendere successivamente ciascun risultato al ben piú ampio dominio degli operatori di densità di dimensione arbitraria.

Si noti infine come tale risultato si sia ottenuto non utilizzando il contesto unitario, bensì il più generale contesto delle operazioni quantistiche (che costituiscono le operazioni della struttura algebrica considerata) applicate a operatori di densità (che costituiscono il dominio della stessa struttura algebrica).

Le due operazioni che formano l'insieme approssimativamente universale che è stato introdotto sopra, derivano comunque da operatori unitari. Ma, in base alle considerazioni del paragrafo precedente, è possibile includere anche operazioni quantistiche che non derivino unicamente da operatori unitari e che magari corrispondano a funzioni di natura irreversibile.

## 5. Un nuovo strumento per trattare l'irreversibilità

Nel § 3 si è visto come da ogni operatore unitario sia possibile ottenere la corrispettiva operazione quantistica unitaria, che rappresenta ancora una volta una

evoluzione reversibile dell'operatore di densità a cui è applicata. Si è però notato come questo sia solo un caso particolare: esistono operazioni quantistiche che non risultano provenire da alcun operatore unitario e che quindi rappresentano un'evoluzione irreversibile. In questo paragrafo introdurremo una classe speciale di operazioni quantistiche, chiamate *operazioni quantistiche polinomiali*, che sono in grado di rappresentare, propriamente o approssimativamente, il comportamento di alcune particolari trasformazioni irreversibili di largo uso sia puramente teorico sia più applicativo [4, 3, 19, 9].

Una operazione quantistica polinomiale è definita in termini esclusivamente probabilistici: si dirà che un'operazione quantistica è polinomiale se e solo se esiste un polinomio a coefficienti reali e ad $n$ variabili tale che per ogni $n$-pla di operatori di densità si ha che la probabilità dell'operazione quantistica applicata al prodotto tensoriale tra tutti gli $n$ operatori di densità è uguale al valore che il polinomio assume quando a ciascuna delle $n$ variabili è assegnata come interpretazione il valore di probabilità di ciascuno degli $n$ operatori di densità. Dal punto di vista intuitivo, una operazione quantistica polinomiale può essere immaginata come quell'operazione che rappresenterebbe una evoluzione di tipo polinomiale di un determinato sistema quantistico. L'importanza di considerare evoluzioni polinomiali è dovuta al fatto che, se il polinomio non è una funzione iniettiva, questo rappresenta un'evoluzione di tipo irreversibile, in quanto partendo da stati iniziali differenti si può giungere allo stesso stato finale. L'introduzione delle operazioni quantistiche polinomiali risulta essenziale per quel teorema [24] in cui si mostra come esista sempre una operazione quantistica polinomiale in grado di rappresentare probabilisticamente una qualunque funzione polinomiale che rispetti le seguenti condizioni:

- i coefficienti del polinomio sono compresi tra i valori 0 e 1;
- la restrizione della funzione per valori compresi tra 0 e 1 assume a sua volta valori compresi tra 0 e 1.

Successivamente, in una versione ulteriormente affinata del teorema [12] si mostra come esista sempre un'operazione quantistica polinomiale in grado di rappresentare in maniera approssimata, cioè *a meno di una costante*, il comportamento di una qualsiasi funzione continua (e quindi non necessariamente polinomiale) che rispetti le due stesse condizioni elencate sopra. A corredo di questo risultato vi è un ulteriore teorema di convergenza che mostra come il valore della costante che sancisce l'accuratezza dell'approssimazione possa essere arbitrariamente piccolo. Il prezzo che però bisognerà pagare sarà il sempre più elevato

grado di complessità dell'operazione quantistica approssimante. Dal punto di vista strettamente intuitivo, il teorema appena introdotto consente di affermare che: se un sistema fisico evolve secondo una funzione polinomiale (reversibile o irreversibile) che soddisfa determinati requisiti, allora è sempre possibile costruire un circuito quantistico che rappresenti (a limite in maniera approssimata) l'evoluzione di tale sistema.

L'attenzione verso la rappresentazione operazionale in chiave quantistica di determinate funzioni irreversibili, è suggerita dall'esigenza di offrire una rappresentazione fisica di alcune particolari funzioni note come *norme triangolari* o, più brevemente, *t*-norme. Le *t*-norme sono funzioni in due variabili nell'intervallo reale $[0,1]$ che soddisfano i requisiti di commutatività, associatività, monotonia; inoltre 1 deve fungere da elemento neutro e 0 da annichilatore. Queste funzioni hanno trovato presto largo uso in ambiti di ricerca anche molto vari: dalla fisica delle particelle alla statistica, dalla teoria dei giochi fino alla teoria del pensiero critico [7, 14, 16, 20]. Le *t*-norme sono utilizzate per interpretare il connettivo di congiunzione nell'ambito delle logiche fuzzy [17, 28], i cui valori di verità non sono soltanto il *vero* (indicato, in maniera usuale, col numero 1) o il *falso* (indicato con lo 0), ma tutti i possibili valori "intermedi" tra essi compresi. La logica fuzzy ha trovato numerose applicazioni in ambito elettronico: i *sistemi di controllo fuzzy* costituiscono infatti una alternativa ai sistemi digitali ed hanno consentito la realizzazione di strumenti di uso quotidiano (quali lavatrici, macchine fotografiche, condizionatori) contando su un'elettronica in cui il segnale è rappresentato da un numero appartenente all'intervallo continuo compreso tra il valore 0 ed il valore 1. Tale idea, in realtà, richiama immediatamente il significato di bit quantistico introdotto all'inizio di questo lavoro.

Tre *t*-norme di particolare importanza sono le seguenti:

- la *t*-norma Prodotto (che corrisponde proprio al prodotto algebrico);
- la *t*-norma di Łukasiewicz;
- la *t*-norma di Gödel (che corrisponde al *minimo*).

L'importanza è legata al fatto che, tramite l'utilizzo esclusivo di queste tre *t*-norme è possibile esprimere, in un senso appropriato, qualsiasi altra *t*-norma continua. Inoltre, è importante notare come la rispettiva definizione in termini funzionali di ciascuna di queste tre, corrisponda a una evoluzione di tipo strettamente irrervesibile. Ecco che esprimere queste tre *t*-norme in termini di operazioni quantistiche sancisce la stesura di un forte legame tra gli studi in ambito quantistico computazionale e il vasto ambito relativo alle logiche polivalenti.

La prima versione del teorema che è stato sopra descritto permette in maniera quasi immediata di rappresentare la *t*-norma prodotto come operazione quantistica polinomiale. Essendo infatti il prodotto algebrico già di per sé un polinomio (che rispetta i vincoli preposti), è direttamente possibile ottenere l'operazione quantistica che ne rappresenti il comportamento. Per far questo è dunque sufficiente ricorrere alla prima versione del teorema che permette di ottenere una rappresentazione *esatta* (e non approssimata) della *t*-norma Prodotto come operazione quantistica polinomiale.

Discorso differente va fatto per le altre due *t*-norme che, pur essendo funzioni continue, non corrispondono ad alcuna espressione polinomiale. Ecco che, per rientrare nelle condizioni richieste dalla seconda versione del teorema, è risultato necessario ricorrere a un passo preliminare: tramite strumenti analitici è stato possibile approssimare tali *t*-norme ad altre funzioni che però rispettassero le condizioni richieste dal teorema. Si sono così ottenute due operazioni quantistiche in grado di riprodurre in maniera approssimata, ma arbitrariamente accurata, il comportamento sia della *t*-norma di Łukasiewicz che della *t*-norma di Gödel.

## 6. Conclusione

L'obiettivo di questo lavoro è stato quello di presentare in maniera generale ma dettagliata, volutamente senza il coinvolgimento di dettagli formali, le caratteristiche peculiari di una struttura che permette innanzitutto di rappresentare sistemi fisici aperti (consentendo così di tener conto delle svariate interazioni tra sistema fisico e ambiente circostante) e anche la loro evoluzione, eventualmente di natura irreversibile. Questi risultati possono rappresentare un punto di incontro tra sistemi fisici reali e teoria computazionale quantistica la quale, seppur altamente predittiva, appariva praticamente descrittiva solo di sistemi fisici estremamente schermati da qualsiasi tipo di interazione esterna e le cui evoluzioni fossero strettamente di natura reversibile. Cioè, in sostanza, sistemi fisici ideali.

I risultati descritti nell'ultimo paragrafo, infine, aprono a nuove interessanti prospettive di ricerca nell'individuazione di insiemi di operazioni quantistiche approssimativamente universali: sarebbe infatti interessante individuare un insieme approssimativamente universale costituito (totalmente o in parte) da ope-

razioni quantistiche non unitarie. Tale possibilità, oltre a rappresentare una sostanziale novità dal punto di vista teorico, offrirebbe l'opportunità di disporre di un modello teorico pensato appositamente in risposta all'esigenza di tener conto delle inevitabili interazioni del sistema con l'ambiente e, per questo, risulterebbe più adeguato dal punto di vista dell'implementazione ed offrirebbe nuovi stimolanti prospettive dal punto di vista applicativo.

RINGRAZIAMENTI. Il presente lavoro di ricerca è stato finanziato dalla Regione Autonoma della Sardegna, POR Sardegna FSE-M.S. 2007-2013 L.R. 7/2007. Desidero ringraziare Roberto Giuntini e Francesco Paoli per i numerosi e preziosi suggerimenti, utili sia per il conseguimento dei risultati riassunti nel presente articolo sia per la stesura dello stesso.

## Riferimenti bibliografici

[1] P. Adrien, M. Dirac. *The principles of Quantum Mechanics*. Oxford University Press, 1981.

[2] D. Aharonov. "A simple proof that Toffoli and Hadamard are quantum universal". [arXiv:quant-ph/0301040v1], 2003.

[3] E. Beltrametti, G. Cassinelli. *The logic of quantum mechanics*. Encyclopedia of Mathematics and its Applications, Vol. 15. Addison-Wesley, Reading, Massachusetts, 1981.

[4] J. Berchtold, A. Bowyer. "Robust arithmetic for multivariate Bernstein-form polynomials". *Computer Aided Design*, 32, pp. 681–689, 2000.

[5] S. L. Braunstein. *Quantum computing: where do we want to go tomorrow?*. Wiley-VCH, 1999.

[6] H. P. Breuer, F. Petruccione. *The Theory of Open Quantum Systems*. Oxford University Press, 2002.

[7] D. Butnariu, E. P. Klement. "Triangular Norm-Based Measures and Games with Fuzzy Coalitions". Kluwer Academic Publishers, Dordrecht, 1993.

[8] C. Cohen-Tannoudji, B. Diu, F. Laloe. *Quantum Mechanics*. Wiley-Interscience, 2006.

[9] M. L. Dalla Chiara, R. Giuntini, H. Freytes, A. Ledda, G. Sergioli. "The algebraic structure of an approximately universal system of quantum computational gates". *Foundations of Physics*, 39, 6, 2009.

[10] D. Deutsch. "Quantum theory, the Church-Turing principle and the universal quantum computer". *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 400 (1818), pp. 97–117, 1985.

[11] D. Deutsch, A. Barenco, A. Ekert. *Universality in Quantum Computation. Proc. Royal Society London A*, 449, pp. 669–677, 1980.

[12] H. Freytes, G. Sergioli, A. Aricò. "Representing continuous t-norms in quantum computation with mixed states". *Journal of Physics A: mathematical and theoretical* 43, 465–306, 2010.

[13] R. Feynman. "Simulating physics with computers". *International Journal of Theoretical Physics*, 21(6), pp. 467–488, 1982.

[14] J. Fodor, M. Roubens. "Fuzzy Preference Modeling and Multicriteria Decision Support". Kluwer Academic Publishers, Dordrecht, 1994.

[15] R. Giuntini, F. Paoli, A. Ledda, G. Sergioli. "Some generalizations of fuzzy structures in quantum computational logic". *International Journal of General Systems*, 40, 1, pp. 61–83, 2009.

[16] M. Grabisch, H. T. Nguyen, E.A. Walker. *Fundamentals of Uncertainty Calculi with Applications to Fuzzy Inference*. Dordrecht, Kluwer, 1995.

[17] P. Hájek. *Metamathematics of Fuzzy Logic*. Kluwer, Dordrecht,, 1998.

[18] A. Y. Kitaev, A. H. Shen, M. N. Vylayi. *Classical and Quantum Computation*. AMS Bookstore, 2002.

[19] A. Ledda, G. Sergioli. "Towards quantum computational logics". *International Journal of Theoretical Physics*, 49 (12), pp. 3158–3165, 2010.

[20] K. Menger. “Statistical metrics”. *Proceedings of the National Academy of Sciences*, 37, pp. 57-60, 1942.

[21] A. Messiah. *Quantum Mechanics*. Courier Dover Publications, 1999.

[22] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[23] J. G. Rarity, P. R. Tapster, E. Jakeman, T. Larchuk, R. A. Campos, M. C. Teich, B. E. A. Saleh. “Two-photon interference in a Mach-Zehnder interferometer”. *Physical Review Letters*, 65, pp. 1348–1351, 1990.

[24] G. Sergioli, A. Ledda, H. Freytes. “Continuous functions as quantum operations: a probabilistic approximation”. *Logic & Philosophy of Science*, 3, 4, pp. 1–17, 2010.

[25] Y. Shi. “Both Toffoli and controlled-not need little help to do universal quantum computation”. [arXiv:quant-ph/0205115v2], 2002.

[26] T. Toffoli. “Reversible computing”. In *Automata, Languages and Programming* a cura di J. W. de Bakker e J. van Leeuwen, Springer, pp. 632-644, 1980.

[27] A. M. Turing. “Computability and $\lambda$-definability”. *The Journal of Symbolic Logic*, 2, 4, pp. 153–163, 1937.

[28] L. Zadeh “Fuzzy sets”. *Information and Control*, 8, pp. 338–353, 1965.