Bollettino
Unione Matematica Italiana

Sezione A – La Matematica nella Società e nella Cultura

Mario Rasetti

Il calcolo quantistico: una sfida per la matematica del 2000

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **3-A**—*La Matematica nella Società e nella Cultura* (2000), n.2, p. 201–222.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2000_8_3A_2_201_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2000.

Bollettino U. M. I.
La Matematica nella Società e nella Cultura
Serie VIII, Vol III-A, Agosto 2000, 201-222

Il calcolo quantistico: una sfida per la matematica del 2000

MARIO RASETTI

Sommario. – *Il calcolo quantistico cerca la risposta, ad un secolo esatto di distanza, al decimo problema di Hilbert. Nuovo paradigma nella teoria del calcolo, esso costituisce una sfida senza precedenti per la fisica, ma anche una prospettiva importante per la matematica: lo stimolo a superare i vincoli posti dalla teoria della complessità algoritmica e affrontare problemi, che spaziano dalla teoria dei numeri alla logica formale, che si ritenevano inattaccabili.*

Credo si possa sostenere con ragione che la complessa vicenda concettuale che ci porta oggi a parlare di *computazione quantistica* ebbe origine esattamente un secolo fa, nell'agosto 1900, quando in una conferenza divenuta famosa, tenuta a Parigi al secondo Congresso Internazionale dei Matematici, David Hilbert fece un elenco dei 23 problemi che egli riteneva costituissero la sfida cui i matematici avrebbero dovuto far fronte nel secolo che stava per iniziare. Negli anni a seguire, alcuni di questi problemi furono risolti rapidamente, altri no e potrebbero forse non essere mai completati; uno, il X (definito semplicemente come l'*entscheidungsproblem*), ha segnato la nascita di un capitolo nuovo della Matematica: la teoria della complessità algoritmica. Hilbert, nella sua incrollabile fede di matematico («*Wir müssen wissen. Wir werden wissen*»; dobbiamo conoscere, conosceremo) riteneva che quello speciale sistema formale assiomatico che è la matematica debba essere *consistente* (privo di contraddizioni), *completo* (in quanto rappresenta la verità) e *decidibile* (nel senso che deve

esistere una procedura meccanica, un «programma», per stabilire se i suoi predicati sono veri o falsi).

Il lungo percorso che seguì l'enunciazione del X problema passa in primo luogo attraverso il teorema con cui nel 1931 il logico austriaco Kurt Gödel dimostrò come se si fa l'ipotesi che un sistema assiomatico che includa l'aritmetica elementare sia consistente (requisito questo minimale: sarebbe imbarazzante parlare di una struttura formale in cui si possono dimostrare proposizioni false!), allora esso è necessariamente incompleto. Solo successivamente esso approdò alla teoria formale della computazione.

Benché nella storia della matematica la nozione di *computazione* entri naturalmente molto presto, con la stessa definizione di numero, così come per il numero, tuttavia, il suo *status* non è senza tempo: essa è solo lentamente giunta alla forma astratta con cui la conosciamo oggi. Di fatto una cogente e completa analisi del concetto e della struttura della computazione ha avuto inizio solo nel 1936, con il pionieristico lavoro di Alan Turing. Fu infatti Turing, il matematico inglese noto per il sostanziale contributo che il suo genio diede – durante la seconda guerra mondiale – alla vittoria degli alleati sui nazisti, mediante la costruzione della macchina, denominata *Enigma*, che fu capace di decodificare sistematicamente i codici segreti tedeschi, a porre le basi per una risposta soddisfacentemente rigorosa alla domanda su che cosa sia computazione.

Con la sua analisi Turing, diede un colpo fatale al sogno di Hilbert mostrando come non esista alcuna procedura meccanica – e quindi nessuna teoria assiomatica formale – che possa risolvere la questione se un dato programma possa terminare o meno (l'*halting problem*).

In questo contesto nasceva la teoria della computazione, il cui fondamento era la tesi di Church-Turing, secondo la quale qualsiasi modello «ragionevole» di computazione può essere simulato in maniera efficiente (vale a dire in un modo il cui tempo di operazione sia limitato da una funzione polinomiale del tempo di funzionamento della macchina da calcolo simulata) da una macchina di Turing probabilistica (una macchina cioè che opera algoritmi probabilistici). Ragionevole sta qui a ricordarci che in ogni macchina da calcolo si

deve fare una scelta in merito alla precisione: non è sensato immaginare un modello di computer che manipoli in tempi finiti gli infiniti decimali di un numero irrazionale! In quanto alla *Macchina di Turing*, essa è un oggetto ideale al quale si può concettualmente ricondurre – almeno in linea di principio – ogni calcolatore, per complesso che esso sia: la macchina consiste di un *nastro* (una terminologia che oggi ce ne permette una visualizzazione molto concreta pensando ad esempio ad un registratore magnetico), sul quale e dal quale un apparato (la «*testa*» del registratore) può sia scrivere sia leggere simboli e sequenze di simboli (ad esempio di un «alfabeto» binario). Elemento essenziale nella analisi di Turing è il fatto che la testa legga (o scriva) le sequenze di simboli uno alla volta e che essa possa stare in un numero limitato di stati interni, definiti a loro volta da numeri binari. Il nastro, inoltre, si immagina suddiviso in una sequenza (in linea di principio anche illimitata) di celle, in ciascuna delle quali o non è scritto nulla o è scritto uno dei simboli dell'alfabeto (0 o 1); dunque quando la testa legge o scrive, lo fa sul contenuto di una singola cella, quella su cui essa è posizionata.

Il comportamento della macchina è definito da un rigoroso insieme di regole logiche, che si possono rappresentare come un vero e proprio programma di computer. Tale programma consiste di una sequenza numerabile di passi, ognuno dei quali a sua volta consiste di una fra sette istruzioni fondamentali.

Tutto questo faceva della macchina di Turing (o del modello, ad essa polinomialmente equivalente, proposto circa trent'anni dopo da John von Neumann, detto *automa cellulare*) il prototipo concettuale di «calcolatore»: un sistema in cui la manipolazione di informazione (calcolo) non è che l'evoluzione dinamica di un sistema altamente organizzato (sia esso un oggetto fisico prodotto dalla tecnologia, come un computer, o naturale, quale un complesso di particelle o un cervello) nei cui stati si possa codificare (e dai cui stati si possa decodificare) informazione.

Oltre al programma, la macchina deve naturalmente poter ricevere i dati di *input*, sui quali operare. Sia il programma che i dati sono scritti nel medesimo alfabeto che è proprio della macchina. I dati di ingresso saranno semplicemente la sequenza di 0 e 1 che li rap-

presenta come numeri binari, mentre il programma può essere codificato in maniera convenzionale nello stesso linguaggio, purchè distinguibile senza ambiguità.

Turing dimostrò come un pur così semplice schema concettuale sia sufficiente non soltanto a riprodurre la struttura di qualsiasi processo di computazione (di una funzione «ricorsiva» computabile), ma anche a costruire una *macchina universale*, capace di simulare l'azione di qualsiasi programma in qualsiasi macchina di Turing. È in questa forma di autoreferenzialità illimitata che sta la vera grandezza del modello di computazione di Turing.

La moderna teoria della complessità computazionale, che ha origine nelle idee seminali di Turing e Church, di cui si può dire sia la naturale estensione, consiste nell'interrogarsi sulle risorse (energetiche, spaziali ed anche temporali), necessariamente finite in ogni computer reale che implementi fisicamente quel sistema formale astratto che è una Macchina di Turing Universale, di cui occorre disporre per portare a termine una data procedura di calcolo.

La fisica non pare avere molto a che fare con tutto questo ed i teorici della computazione e della complessità non la includono fra gli elementi rilevanti ai fini dei loro ragionamenti fino a che, nel 1985, inaspettatamente, il fisico matematico inglese David Deutsch non mette la cosa in discussione. Deutsch argomenta che il principio di Turing-Church può essere riformulato assumendone come base l'ipotesi che esso equivalga a chiedere che qualsiasi sistema fisico realizzabile con risorse finite possa essere perfettamente simulato da un modello finito di macchina da calcolo che operi con mezzi finiti. Questo nuovo punto di vista non è indolore. Già nel 1982 Richard Feynman aveva messo in evidenza un problema, la cui serietà è oggi ben presente ai fisici teorici della materia condensata: sembra impossibile simulare un generico sistema fisico quantistico con una macchina di Turing probabilistica senza doversi assoggettare ad un rallentamento esponenziale dei tempi di calcolo. Questo, insieme con l'osservazione che nella costruzione del modello «macchina di Turing» di computazione si fa implicitamente l'ipotesi che tutte le variabili fisiche che definiscono lo stato della macchina siano simultaneamente osservabili, comporta che il paradigma fisico su cui l'inte-

ra teoria tradizionale della computazione è basata sia di fatto quello della fisica classica.

Fu a partire da considerazioni di questa natura che nacque, all'inizio degli anni '90 ad opera di fisici ed informatici prestigiosi, quali appunto David Deutsch per primo, ma poi da Charlie Bennett a Umesh Vazirani, da Seth Lloyd a Andrew Steane, per citarne solo alcuni, la definizione concettuale di una nuova classe di modelli di macchina da calcolo, che sono la generalizzazione quantistica della macchina di Turing. Per queste nuove «macchine» non si ha più contraddizione fra i principi base della computazione e la teoria quantistica della materia. Alla base del modello che le caratterizza sta infatti l'idea che un sistema quantistico isolato idoneo possa costituire il supporto fisico per uno schema formale di computazione totalmente innovativo: la computazione quantistica. La *Macchina di Turing Quantistica* è simile strutturalmente a quella classica (si può ancora pensare ad un nastro, una testa, un puntatore sulle singole celle), ma ora gli stati di questi vari componenti sono stati quantistici (tecnicamente, elementi di uno spazio di Hilbert) e la loro evoluzione temporale – che costituisce il processo di calcolo – è regolata dalle leggi dinamiche della fisica quantistica; le equazioni di Schrödinger e di Heisenberg.

Un elemento importante nella costruzione, che indica una sorta di maggiore «naturalezza» di una struttura fisica di riferimento quantistica rispetto ad una classica per quanto riguarda il calcolo, è la nozione di *reversibilità*, che implica il fatto che ogni computazione possa essere fattorizzata in una serie di operazioni elementari – come è necessario che avvenga per poter eseguire qualsiasi calcolo e poter pensare a macchine *multi-purpose* e non necessariamente dedicate – ciascuna delle quali si possa ripercorrere all'indietro riportandosi al passo precedente. Questa infatti è assicurata automaticamente nel caso quantistico, mentre deve essere implementata in quello classico. Tecnicamente, ciò è dovuto al fatto che nella fisica quantistica l'evoluzione temporale di un sistema isolato è necessariamente descritta in maniera unitaria, vale a dire in modo tale che l'evoluzione *all'indietro nel tempo*, rappresentata dal coniugato hermitiano U^* dell'operatore $U(t)$ che descrive la dinamica «in avanti», è di fatto

controllata da questo stesso operatore, che esegue il passaggio del sistema dallo stato attuale a quello futuro, nel quale si cambi il segno della variabile tempo, $U(-t)$, cioè dal suo inverso, poiché $U(-t) = U(t)^{-1}$. Unitarietà è proprio la proprietà che $U^* = U^{-1}$.

Sul piano pragmatico, forse un po' schematicamente, si può dire che le motivazioni per studiare la teoria della informazione e della computazione quantistica provengono da quattro direzioni diverse, eppure fra di loro complementari: la fisica, sia per la forte tensione conoscitiva che le è propria sia per gli strumenti di base di cui essa dispone; la tecnologia, per il suo continuo tendere verso l'innovazione; le scienze cognitive e la matematica, per le nuove prospettive culturali, potenzialmente enormi, che esse vi potranno esprimere.

Per quanto riguarda la fisica, la motivazione principale sta nel fatto che essa considera il «modo» quantistico di descrivere la natura più fondamentale – e dunque concettualmente più robusto e universale – di quello classico. La meccanica quantistica ci confronta tuttavia con uno schema fatto di paradigmi ben diversi dal suo corrispondente classico: variabili dinamiche associate ad operatori che agiscono in uno spazio degli stati (uno spazio di Hilbert) in cui i vettori possono avere infinite componenti complesse, le funzioni d'onda, solo con una sequenza di difficili reinterpretazioni del concetto stesso di misura e del significato delle proprietà spettrali di tali operatori si possono mettere in relazione con le analoghe variabili classiche. Tutto questo fa tuttavia sì che ci sia molto di più in gioco: la fisica moderna ci insegna che la «quantizzazione» di un sistema classico con N gradi di libertà genera un sistema quantistico il cui spazio degli stati (che è uno spazio proiettivo complesso $\mathbb{CP}_N$, $(N-1)$-dimensionale) ha un volume che cresce esponenzialmente con N e dunque si presta ad una complessità combinatoria di strutture dinamiche possibili enormemente maggiore. È comprensibile che si sia pensato che se si potesse mai costruire un computer quantistico secondo il modello di Deutsch (o il suo equivalente a circuiti di *gates* booleani) esso avrebbe incredibilmente più potenza e più memoria di uno classico.

D'altra parte, per quanto riguarda la tecnologia, gli enormi recenti progressi nelle tecniche di microfabbricazione e nello sviluppo

di materiali per la microelettronica hanno ormai portato ad un livello tale la miniaturizzazione dei componenti circuitali dei calcolatori che gli effetti quantistici non possono più non essere tenuti in considerazione se si vuole garantire un corretto funzionamento dei microchips, anche quando questi vengono utilizzati per effettuare calcolo secondo i paradigmi classici. Se si riportassero su di un grafico le dimensioni medie, ad esempio il «diametro», del sistema fisico necessario per immagazzinare una unità di informazione (un *bit*) in funzione degli anni, a iniziare dai parecchi centimetri delle valvole termoioniche che costituivano il primo computer elettronico (l'ENIAC, costruito alla Moore School of Electrical Engineering dell'Università di Pennsylvania alla fine della II^{a} guerra mondiale, o il suo immediato successore, l'EDVAC, disegnato da John von Neumann all'Institute for Advanced Study di Princeton a cavallo fra gli anni '40 e '50), passando attraverso i millimetri dei transistor prima e le frazioni di millimetro dei microchips poi, fra gli anni sessanta e ottanta, per arrivare alle poche decine di micron delle moderne componenti circuitali, si potrebbe vedere che questi dati sono ben interpolati da una retta che interseca la linea orizzontale delle dimensioni di un singolo atomo (qualche Ångström) proprio intorno all'anno 2000!

Motivazioni più sottili e spettacolari sul piano conoscitivo, seppure al momento attuale fortemente speculative, possono poi essere ricercate nella congettura che meccanismi complessi della materia biologica, dal *protein folding* alle funzioni del cervello umano, siano di fatto essi stessi necessariamente da rappresentare come una sorta di computer quantistico.

Quanto alla matematica, le proprietà che rendono le varie operazioni di *manipolazione quantistica della informazione* (immagazzinamento, trasferimento, acquisizione, modificazione, lettura) così radicalmente differenti dalle loro analoghe classiche, sono naturalmente proprio quelle proprietà quantistiche che non hanno un corrispondente classico. Innanzi tutto, l'informazione classica, come si è detto, è abitualmente codificata in sequenze di caratteri (che possono essere anche infinite) $\mathbf{x} \equiv \{x_1, \ldots, x_n\}$; tipicamente – nello schema Booleano – *bit* x_i che assumono i valori 0 o 1 e che sono ben defi-

niti, vale a dire sono completamente misurabili, ad ogni passo del processo di calcolo (o ad ogni istante t). Al contrario l'informazione quantistica è immagazzinata in stati quantistici, $|\psi\rangle$ (nella notazione con cui i fisici abitualmente denotano i vettori nello spazio degli stati). La struttura dello spazio di tali stati, che è quello che i matematici chiamano uno spazio di Hilbert, è tale che essi risultano essere genericamente la sovrapposizione complessa di tutte le sequenze possibili di bit, ciascuna con una sua probabilità di essere individuata da una operazione di misura:

$$|\psi\rangle = \sum_{\mathbf{x}} \alpha_{\mathbf{x}} |\mathbf{x}\rangle,$$

dove $\alpha_{\mathbf{x}}$ è l'«ampiezza di probabilità» (complessa) dello stato $|\mathbf{x}\rangle = |x_1, \ldots, x_n\rangle$, vale a dire $|\alpha_{\mathbf{x}}|^2$ è la probabilità di trovare il sistema nello stato $|\mathbf{x}\rangle$ al tempo t e ad ogni istante $\sum_{\mathbf{x}} |\alpha_{\mathbf{x}}|^2 = 1$. Nella somma $\sum_{\mathbf{x}}$, $\mathbf{x}$ varia su tutte le possibili «stringhe» booleane di caratteri. La evoluzione quantistica si rappresenta scrivendo che $|\psi\rangle_{t=T} = U(T)\,|\psi\rangle_{t=0}$, dove T è il tempo di calcolo e $U(t)$ l'operatore unitario (come si è detto tale che il suo coniugato $U^* = U^{-1}$, $\forall t$) che descrive l'evoluzione temporale del sistema. L'unitarietà ci garantisce altresì che nel corso delle trasformazioni che il sistema stesso subisce nel tempo le probabilità vengano al più ridistribuite, perché ad ogni istante continua a valere il fatto che $\sum_{\mathbf{x}} |\alpha_{\mathbf{x}}|^2 = 1$: se dunque si riesce a controllare l'evoluzione nel modo appropriato si può far sì che lo stato finale che si ottiene dopo aver codificato l'*input* nello stato iniziale ($|\psi\rangle_{in} \equiv |\psi\rangle_{t=0}$) contenga in sé proprio l'*output* del calcolo che si vuole eseguire ($|\psi\rangle_{\text{out}} \equiv |\psi\rangle_{t=T}$).

Gli ingredienti che la fisica quantistica ci fornisce, necessari per perseguire questo obiettivo, sono dunque:

i) la *sovrapponibilità degli stati*: un computer quantistico può stare in qualsiasi combinazione (complessa e normalizzata) di tutti i possibili stati di uno classico. I coefficienti di tali combinazioni sono numeri complessi, caratterizzati in quanto tali da un modulo (come si è visto uguale alla radice quadrata della

probabilità di trovare il sistema in quel particolare stato) e da una fase $\phi_{\mathbf{x}}$: $\alpha_{\mathbf{x}} = |\alpha_{\mathbf{x}}| e^{i\phi_x}$;

ii) l'*interferenza*: essenziale ai fini del calcolo, perché è grazie ad essa che gli stati coesistenti si possono fare interferire, *costruttivamente* (quelli «buoni», che cioè codificano la soluzione al calcolo che si intende effettuare), o *distruttivamente* (quelli «cattivi», che codificano una soluzione errata), manipolando le loro fasi relative. Occorre osservare che l'interferenza è proprietà generica delle onde e dunque non è esclusivamente quantistica, come sono invece tutte le altre in questo elenco;

iii) l'«*entanglement*» (intreccio): è una delle proprietà caratteristiche della natura quantistica di un sistema fisico a più componenti. Essa comporta che si possano costruire stati quantistici composti ben definiti i quali non corrispondono a stati ben definiti delle loro parti costituenti. L'entanglement è forse la più enigmatica ed elusiva delle proprietà caratteristiche della meccanica quantistica, legata alla struttura di prodotto tensore dello spazio di Hilbert degli stati di un sistema a tante componenti. Dal punto di vista dell'informazione quantistica e in particolare del calcolo, l'entanglement è risorsa molto più importante che non la pura e semplice sovrapponibilità degli stati: l'entanglement, infatti, è quel tipo particolare di sovrapposizione degli stati, che può appunto aver luogo quando nello spazio di Hilbert si abbia una struttura di prodotto, vale a dire quando il sistema sia costituito di tanti sottosistemi, il cui risultato sono stati che non possono essere espressi a loro volta come un prodotto. Fra i sistemi «entangled» un ruolo molto importante l'hanno gli stati detti EPR (da Einstein, Podolski e Rosen): esempio significativo ne è quello dei due elettroni emessi in direzioni opposte da un nucleo di momento angolare zero; un osservatore che misuri lo spin di uno degli elettroni fa sì non solo che questo «*collassi*» (come la teoria della misura quantistica prevede) nello stato che corrisponde all'esito della misura, ma che l'altro elettrone, per effetto di questa stessa misura, vada necessariamente a porsi nello stato di spin opposto di quello osservato. L'osservatore, dunque, ricava informazioni

anche sull'elettrone che si trova fuori della sua portata. Questa proprietà è nota come la *non località* della meccanica quantistica;

iv) l'*indeterminazione*: è proprietà anch'essa caratteristica, ma essenzialmente negativa, che fa sì – fra le altre cose – che uno stato quantistico non noto non possa essere *clonato* (vale a dire ricostruito in un luogo diverso) senza essere irreversibilmente disturbato dal processo (che è di fatto una misura). Fortunatamente, l'informazione quantistica pur non potendosi clonare si può tuttavia trasferire per *teletrasporto* sfruttando un vettore intermediario classico, grazie ancora proprio all'entanglement. Il principio di indeterminazione, dovuto a Werner Heisenberg, ci dice che le osservabili, vale a dire le variabili dinamiche che possono essere fisicamente osservate, misurate, hanno, a coppie (dette coniugate), la strana proprietà che non è possibile conoscere il loro valore esatto nello stesso stato per entrambe: dobbiamo accettare che la misura sia affetta da un errore (attenzione, intrinseco, non dovuto agli strumenti di osservazione), e gli errori per le due osservabili sono legati uno all'altro. È ben nota la formula $\Delta x \Delta p \geqslant \frac{1}{2}\hbar$ che lega l'incertezza nella misura della posizione (Δx) a quella nella quantità di moto (Δp); h è la costante di Plank; $\hbar = h/2\pi$.

Mentre nei computer classici l'informazione viene codificata nei bit, in quelli quantistici essa può venire codificata negli stati interni (microscopici) della materia. Da questa considerazione è nato l'analogo quantistico del bit: il *qu-bit*, che può essere fisicamente realizzato in molti modi differenti: negli stati di polarizzazione dei fotoni; negli stati di *spin* degli elettroni o dei nuclei in un atomo, come nella risonanza magnetica nucleare; nella localizzazione dei protoni in molecole biologiche complesse con legami idrogeno, come il DNA. Recentemente molta attenzione è stata dedicata alla possibilità di realizzare non solo singoli qu-bit, ma anche i gates da essi composti, in maniere che permettano di scalarne con relativa facilità il numero da poche unità ad un numero che consenta al computer quantistico di competere veramente con quello classico: nanostrutture a stato

solido, i cosiddetti *quantum dots*, o sistemi quantistici mesoscopici, quali le *giunzioni Josephson*. Non tratteremo tuttavia qui il pur affascinante problema della realizzazione fisica, limitandoci invece agli aspetti di base concettuali del calcolo quantistico.

Naturalmente anche la stessa nozione di informazione acquista nel contesto quantistico un contenuto diverso dal caso classico. L'informazione quantistica si può pensare immagazzinata in un insieme di qu-bit arbitrariamente sovrapposti e la sua differenza più spettacolare rispetto alla informazione classica sta nel fatto che soltanto quando il processo di misura abbia avuto luogo uno specifico stato di output verrà effettivamente conosciuto, con la probabilità che gli compete.

Un'altra differenza basilare è inoltre nel fatto che i computer classici sono seriali, in quanto eseguono ogni algoritmo venga loro assegnato passo dopo passo, completando sempre un passo prima di iniziare il successivo: lo stato complessivo della macchina esegue durante il calcolo un ben preciso percorso dallo stato di input a quello di output. Un computer quantistico universale (oggi nella scienza dei calcolatori si dice *multi-purpose*) ha invece un numero infinito di stati computazionali (in quanto le fasi ϕ_x sono variabili continue seppure compatte, definite (mod 2π)) e il processo di calcolo si può pensare come una infinità di percorsi in ciascuno dei quali tutti gli stati evolvono in parallelo. Sono le fasi di questi stati lungo i vari percorsi che interferendo danno luogo ad un unico ben definito output.

Questa descrizione mette in evidenza allo stesso tempo la potenza e le difficoltà del calcolo quantistico: da un lato il calcolo quantistico è intrinsecamente parallelo, con tutti i vantaggi che questo comporta, dall'altro occorre saper esercitare un controllo rigorosissimo sulle fasi per evitare la possibilità di errori. Quest'ultimo requisito è la fonte delle maggiori difficoltà nel realizzarne l'implementazione fisica: l'esistenza della *decoerenza* dovuta alla inevitabile interazione del sistema con l'ambiente circostante (i sistemi reali non sono mai perfettamente isolati) è il vero nemico da battere. Un importante risultato è però che, così come nella computazione classica, anche in quella quantistica si possono definire *codici di correzione di errore* che, ricorrendo ad una codifica ridondante, individuano e correggo-

no specifiche classi di errori. Il costo che tali codici comportano in termini di complessità li rende naturalmente meno interessanti. Tuttavia, poiché in un computer quantistico la più rilevante fonte di errore sta nella impossibilità di un completo isolamento del sistema dall'ambiente, che inevitabilmente genera decoerenza, sono state concepite anche strategie molto promettenti che consistono nel codificare l'informazione in stati quantistici particolari, i quali, in virtù della loro simmetria dinamica, sono difficilmente corruttibili dai processi caratteristici della decoerenza (scambio di quanti con il mondo circostante, che comportano la transizione di uno o più qubits a una configurazione «sbagliata»), i cosiddetti *codici che evitano l'errore*.

In sintesi, una macchina di Turing quantistica può computare tutte le funzioni ricorsive computabili da una macchina di Turing classica e, come per quest'ultima, ad ogni suo protocollo di calcolo di una funzione può essere associato il protocollo di un appropriato circuito Booleano, ma essa ha proprietà caratteristiche che non hanno analogo classico: l'intriseco parallelismo, la reversibilità, il numero esponenziale di stati disponibili in sovrapposizione.

Tutte queste proprietà si riflettono sulla problematica della *complessità algoritmica* del calcolo. Un algoritmo è una procedura generale per risolvere, di solito attraverso una sequenza di passi, un dato problema o una classe di problemi. Si dice che un dato algoritmo genera la soluzione ad un problema se, applicato ad uno specifico insieme di valori dei parametri del problema, esso genera una soluzion valida per quella data specificazione. Uno degli obiettivi della teoria della computazione è proprio di riuscire a trovare gli algoritmi più efficienti per risolvere problemi assegnati. Qui il punto importante è la definizione di «efficienza», che coinvolge le risorse computazionali necessarie per operare un dato algoritmo. È convenzione ormai universalmente accettata nella *computer science* il fatto che il «più efficiente» significhi il «più veloce». Ciò permette di quantificare l'efficienza algoritmica in termini di una sola variabile, la quantità dei dati di input necessari per specificare un problema (espressa mediante il numero n di bit: se N è il numero di dati, $n =$

$\log_2 N$), e di introdurre una funzione che misura la complessità dell'algoritmo, definendola semplicemente come la modalità con cui cresce il numero dei passi algoritmici (a sua volta espresso in bit) necessari per risolvere il problema per tutte le specificazioni possibili di tale variabile.

Differenti algoritmi danno luogo a diverse funzioni di complessità, la cui classificazione, proprio a seguito dello sviluppo della computazione quantistica, sta radicalmente cambiando. Un *problema decisionale* $\mathcal{P}$, vale a dire un problema le cui risposte possibili possono essere soltanto SI o NO (sono dunque processi decisionali i processi di calcolo di funzioni ricorsive), può appartenere – in una prima, incompleta classificazione – a una delle classi seguenti:

- **P** (classe di *complessità polinomiale*); la classe dei *linguaggi* (cioè dell'insieme degli input di un dato problema decisionale che portano alla risposta SI) per i quali il numero di passi di calcolo necessari per arrivare alla risposta SI cresce con legge polinomiale in funzione della lunghezza dell'input. Una sottoclasse importante di **P**, indicata con **BPP** è quella dei problemi che possono essere risolti in tempo polinomiale da macchine di Turing *probabilistiche* con probabilità di errore che è inferiore a 1/3 per tutti gli input. **BPP** sta appunto per «bounded (error) probability polynomial»;

- **NP** (classe di complessità *polinomiale non-deterministica*); che denota l'insieme di quei problemi decisionali per cui è possibile verificare in tempo polinomiale se una soluzione ipotizzata sia effettivamente una soluzione, ma per i quali non si è stati in grado di trovare un algoritmo che li risolva in un numero di passi che cresca solo con legge polinomiale in funzione della lunghezza dell'input. Non-deterministico è un algoritmo che permette più di una scelta nei vari passi della sua esecuzione;

- **NP-c** (**NP**-*completa*); la sottoclasse dei problemi $\mathcal{P} \in$ **NP** tali che ogni altro problema in **NP** può essere ricondotto con un numero di passi algoritmici polinomiale in n ad uno di essi;

- **EXP** (classe di complessità *esponenziale*); i problemi così ardui che la crescita del «tempo» di calcolo è funzione esponenziale della lunghezza dell'input. Questi problemi si ritengono insolubili.

Con l'avvento del calcolo quantistico queste definizioni sono state estese alle operazioni delle macchine di Turing o dei circuiti quantistici. Particolarmente interessante, per la natura intrinsecamente probabilistica del modo di operare di una macchina che obbedisca alle leggi della fisica quantistica, è la classe **BQPP** («bounded (error) quantum probabilistic polynomial»), definita formalmente come **BPP**, ma riferita a un computer quantistico. Il più importante problema aperto è di stabilire se $\mathbf{NP} \subseteq \mathbf{BQPP}$, cioè se un computer quantistico possa risolvere problemi che stanno in **NP-c** in tempo polinomiale.

Molti problemi «naturali» stanno in **NP-c**. Il più famoso è quello noto come *k-SAT*, con $k \in \mathbb{N}$ maggiore o uguale a 3, così definito:

indichiamo con $\mathcal{B} \equiv \{x_1, \ldots, x_N; \overline{x}_1, \ldots, \overline{x}_N\}$ un insieme di $2N$ variabili booleane ($\overline{x}_j$ denota qui il complemento di x_j: vale a dire se $x_j = 0$, $\overline{x}_j = 1$ e viceversa). $\mathcal{B}$ è detto l'insieme dei *letterali*. Si chiama *forma normale congiuntiva* la generalissima formula booleana data dalla *congiunzione* (AND, $\vee$) di un insieme di *clausole* $\{C_l\}_{l=1}^{M}$, a loro volta definite da una *disgiunzione* (OR, $\wedge$) di letterali:

$$\mathbf{F}_{\mathbf{X}[x]} = \bigwedge_{l=1}^{M} C_l; \qquad C_l = \bigvee_{j=1}^{2N} X_{l,j} x_j, \qquad x_{j+N} \equiv \overline{x}_j,\ j = 1, \ldots, N\,.$$

La formula è caratterizzata dalla matrice $\mathbf{X}$, di elementi $X_{l,j}$. Per il problema $k - SAT$, $\mathbf{X}$ deve soddisfare le proprietà seguenti:

i) $X_{l,j} \in \{0, 1\}$,

ii) $\sum_{j=1}^{2N} X_{l,j} = k,\ \forall l,\ l = 1, \ldots, M.$

Il problema consiste nell'individuare gli elementi $[x] \in \mathcal{B}$ che *soddisfano* la forma $\mathbf{F}_{\mathbf{X}[x]}$, vale a dire la rendono uguale ad 1 (*vera*) per una assegnata $\mathbf{X}$.

Altri problemi di grande importanza pratica, ad esempio nella realizzazione di reti di computer o di sistemi di comunicazione complessi, ma anche nella comprensione di molte questioni importanti della fisica e della biologia, sono invece **NP-hard** (cioè polinomialmente riconducibili a **NP**). Qui un esempio notissimo

è il cosiddetto «problema del commesso viaggiatore», che si formula molto semplicemente così:

assegnati un insieme $\mathcal{C} = \{c_j\}_{j=1}^{N}$ di punti (i vertici di un grafo o le città di una regione) e una distanza $d(c_k, c_j) \in \mathbb{Z}_+$ per ogni coppia $c_k, c_j \in \mathcal{C}$, quale permutazione π di $\mathcal{C}$, $\{c_{\pi(j)}\}_{j=1}^{N}$, rende minima la lunghezza di un percorso chiuso che tocchi tutti i punti (tutte le città) una e una sola volta (tranne naturalmente quello di partenza cui l'ultimo passo deve ricondurre)?

Sino ad ora il più interessante, rispetto alla comprensione delle potenzialità del calcolo quantistico, è il problema della scomposizione di un numero intero N nei suoi fattori primi. Un numero N richiede $n = \log_2 N$ bit di memoria binaria per essere dato come input a un computer. A tutt'oggi non è stato individuato alcun algoritmo di fattorizzazione classico la cui complessità sia migliore di

$$\exp[(\log_2 N)^{1/3}(\log_2 \log_2 N)^{2/3}],$$

vale a dire che non appartenga essenzialmente alla classe di complessità **EXP** (il tempo di calcolo è di fatto $\sim n^{2/3} \exp(n^{1/3})$). Ad esemplificare la rilevanza del problema ricordiamo che proprio per questa ragione si basa sulla fattorizzazione di un numero intero molto grande, prodotto di due numeri primi a loro volta grandi, il sistema crittografico «a *chiave pubblica*» detto RSA (dai nomi degli inventori, Rivest, Shamir e Adleman); il più diffuso fra i sistemi di codifica e decodifica crittografica e quello ritenuto più sicuro, addirittura inviolabile.

Nel 1994 – proprio agli inizi della avventura del calcolo quantistico – Peter Shor costruì un algoritmo quantistico per il problema della fattorizzazione la cui complessità è dell'ordine di $(\log_2 N)^{1/4} = n^{1/4}$, cioè appartiene alla classe (quantistica) **P**: un risultato che avrebbe dato pieno impulso ad una disciplina ritenuta sino a quel momento poco più che uno straordinario esercizio intellettuale. A tutt'oggi questo algoritmo rimane l'esempio più interessante di applicazione con successo dei concetti del calcolo quantistico, in quanto mostra in modo esplicito come quantisticamente si possa effettivamente avere un guadagno esponenziale nel numero di passi di im-

plementazione di un algoritmo. È dunque istruttivo darne una rapida discussione.

Innanzi tutto, occorrerà avere a disposizione un registro di memoria la cui dimensione M (espressa in bit m, $M = 2^m$) sia dell'ordine del doppio di quella di N: $N^2 \leqslant M \leqslant 2N^2$ $(2n \leqslant m \leqslant 2n+1)$. Inoltre è necessario un parametro intero random q, $1 < q < N$, coprimo con N (vale a dire il massimo comune divisore fra q e N è 1). È un risultato classico della teoria dei numeri che se

$$r \doteq \min \{p \,|\, q^p \equiv 1 \pmod N\},$$

è il periodo della funzione

$$f\colon x \mapsto q^x \pmod N,$$

e soddisfa alle condizioni

$$r \equiv 0 \pmod 2 \text{ (vale a dire } r \text{ pari)}, \qquad q^{(1/2)r} \not\equiv \pm 1 \pmod N,$$

allora ciascuno dei due numeri $q^{(1/2)r} \pm 1$ ha almeno un divisore primo in comune con N ([1]). Poiché la probabilità di trovare una coppia q ed r con le proprietà richieste è $\geqslant 1 - \frac{1}{2^{p-1}}$, essendo p il numero di fattori primi di N, troveremo un q «buono» con probabilità prossima quanto desiderato ad uno (vale a dire $\geqslant 1 - N^{-t}$, per qualsiasi prefissato t) con un numero di tentativi che per $p = 2$ è $\mathcal{O}(\log_2 N)$. Poiché inoltre trovare il massimo comune divisore fra due numeri (ad esempio con l'antico algoritmo di Euclide) non richiede che risorse

([1]) Un semplice esercizio esemplifica bene questo teorema. Si voglia fattorizzare $N = 15$. Si sceglie in modo casuale un q con le caratteristiche indicate, diciamo $q = 2$. Per un numero di valori interi di x dell'ordine di N^2 (qui basta molto meno) si calcola la funzione f:

x	0	1	2	3	4	5	7	8	9	10	…
q^x	1	2	4	8	16	32	64	128	256	512	…
$f(x) = q^x \pmod N$	1	2	4	8	1	2	4	8	1	2	…

Si vede, osservando l'ultima riga, che $f(x)$ è periodica con periodo $r = 4$. Il teorema dice che i due numeri $q^{r/2} - 1 = 3$ e $q^{r/2} + 1 = 5$ hanno un fattore primo in comune con N. Naturalmente il fatto che in questo esempio i due numeri siano esattamente e solo i fattori primi di N è dovuto soltanto alla semplicità dell'esempio considerato.

di tempo polinomiali, sappiamo dunque di poter individuare i fattori primi di N in modo efficiente (appunto con un numero di passi polinomiale in n) se riusciremo a trovare con la stessa efficienza r.

Queste sono le premesse del problema, di cui sappiamo anche che non si è stati in grado di costruire un algoritmo classico per il calcolo di r se non con la complessità quasi esponenziale indicata sopra. È qui che entra in tutta la sua eleganza e potenza l'algoritmo di Shor. Esso mira proprio a calcolare r, dato N e fissati M e q. Dal punto di vista degli stati quantistici, l'algoritmo richiede uno spazio di Hilbert con struttura di prodotto tensore di due spazi fattore, $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, ciascuno in grado di contenere stati-registro $|x\rangle$ «etichettati» da un intero $x \in \mathbb{N}$, $0 \leqslant x \leqslant M - 1$. Il primo dei due registri sarà quello di lavoro, l'altro svolgerà funzioni di «scratchpad» (blocco per gli appunti, vale a dire servirà per operazioni transitorie, di servizio e, fatto di estrema importanza, il suo contenuto verrà reversibilmente cancellato ogni qual volta esso sarà stato utilizzato). Useremo la notazione $|x_1\rangle|x_2\rangle$ per gli stati-prodotto in $\mathcal{H}$, invece della più corretta, ma più pesante, scrittura $|x_1\rangle \otimes |x_2\rangle$.

Lo schema di Shor di calcolo quantistico del periodo r consiste nel ripetere più volte la sequenza di operazioni che ora descriveremo, la quale consiste fondamentalmente di quattro passi strettamente quantistici, seguiti da due classici:

i) partendo dallo stato iniziale $|0\rangle\ |0\rangle$, si costruisce lo stato (in sovrapposizione)

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle|0\rangle.$$

È interessante osservare che cosa accade qui nel primo registro. $\mathcal{H}_1$ si può a sua volta pensare come uno spazio prodotto tensore di m spazi di Hilbert uguali di dimensione 2, $\mathcal{H}_1 = \mathcal{H}_0 \otimes \cdots \otimes \mathcal{H}_0$ (m fattori), $\mathcal{H}_0 \sim \mathbb{C}^2$. In questo modo, poiché ciascun $\mathcal{H}_0$ è sotteso da una base di vettori, $\{|0\rangle, |1\rangle\}$, etichettati dai due valori possibili, 0 e 1, del bit classico (ma, attenzione, gli stati di $\mathcal{H}_0$ possono essere sovrapposizioni di $|0\rangle$ e $|1\rangle$!), e poiché si può rappresentare un generico numero intero x in forma binaria, $x = \sum_{k=0}^{m-1} a_k 2^k$, con $a_k = 0, 1$, è

possibile dunque scrivere $|x\rangle = |a_{m-1}\rangle\cdots|a_0\rangle$ con ciascun $|a_k\rangle$ un vettore di base della k-esima copia di $\mathcal{H}_0$ in $\mathcal{H}$. Ne segue che in $\mathcal{H}_1$

$$\frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle$$

$$= \frac{1}{\sqrt{M}}\sum_{a_0=0,1}\cdots\sum_{a_{m-1}=0,1}|a_{m-1}\rangle\cdots|a_0\rangle = \left[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right]^{\otimes m},$$

(si è usata la notazione $|\psi\rangle^{\otimes m}$ per indicare il prodotto tensore $|\psi\rangle\otimes\cdots\otimes|\psi\rangle$ con m fattori). In altre parole,

$$\frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle = \underbrace{\mathcal{U}\otimes\cdots\otimes\mathcal{U}}_{m\text{ times}}\ \underbrace{|0\rangle\cdots|0\rangle}_{m\text{ vectors}} \equiv (\mathcal{U}|0\rangle)^{\otimes m},$$

dove l'operatore unitario $\mathcal{U}$ opera in $\mathcal{H}_0$ (di cui, si ricordi, in $\mathcal{H}$ ci sono m copie) nel modo seguente:

$$\mathcal{U}\colon |0\rangle\mapsto\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\quad |1\rangle\mapsto\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle);\quad \mathcal{U}^{-1}=\mathcal{U}.$$

ii) Si effettua il calcolo di $f(x) = q^x \pmod N$ sulla x etichetta del primo registro e si usa il risultato come etichetta del secondo registro, ottenendo:

$$\frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle|f(x)\rangle.$$

Due osservazioni sono importanti a questo punto. La prima è che il calcolo di qualsiasi funzione ricorsiva Booleana che, come $f(x)\colon \mathbb{Z}_2^m\to\mathbb{Z}_2^m$ ($\mathbb{Z}_2$ denota il corpo dei numeri interi (mod 2)) si può ricondurre ad una *permutazione*, è equivalente ad una sequenza – la cui lunghezza misura la complessità del calcolo – di poche operazioni fondamentali (*gates*), fatte poche (due, tre) alla volta. La seconda osservazione è che nel caso quantistico la azione di ogni gate si può associare ad un operatore unitario e dunque il passo illustrato sopra si implementa, grazie all'intrinseco parallelismo quantistico, attraver-

so una unica operazione dell'operatore unitario $\mathcal{U}_f$ tale che $\mathcal{U}_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$:

$$\mathcal{U}_f\left(\frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle|0\rangle\right) = \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle|f(x)\rangle.$$

Pur essendo la computabilità in tempo polinomiale di una generica permutazione tipicamente esponenziale, nel caso in esame la lunghezza, cioè il numero di operazioni di singolo gate necessarie e dunque il numero di operazioni unitarie elementari di cui $\mathcal{U}_f$ è il prodotto, è polinomiale (quadratico) in m.

iii) Si effettua la trasformata di Fourier (quantistica) sul primo sottospazio:

$$\mathcal{F}_{\mathcal{Q}}\colon\ |x\rangle \mapsto \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}\exp\left(i2\pi\frac{x\cdot y}{M}\right)|y\rangle.$$

Anche per questa operazione, quantisticamente sono sufficienti $\mathcal{O}(m^2)$ gates elementari, rappresentati da due tipi di operatori soltanto, realizzati da matrici 2×2 (che operano localmente in un singolo $\mathcal{H}_0$) e 4×4 (che operano su due sottospazi adiacenti, $\mathcal{H}_0^{(j)}\otimes\mathcal{H}_0^{(j+1)}$). Abbiamo dunque a disposizione ora lo stato *entangled*:

$$\frac{1}{M}\sum_{x=0}^{M-1}\sum_{y=0}^{M-1}\exp\left(i2\pi\frac{x\cdot y}{M}\right)|y\rangle|q^x(\mathrm{mod}\ N)\rangle.$$

iv) L'ultimo passo quantistico consiste nella «misura» del sistema, cioè della sua osservazione rispetto alla base naturale. Questo, come ci insegna la meccanica quantistica, dà come risultato uno specifico stato $|y\rangle|q^l(\mathrm{mod}\ N)\rangle$ con probabilità

$$P_l(y) = Pr(|y\rangle|q^l(\mathrm{mod}\ N)\rangle) = \left|\frac{1}{N}\sum_{x\,:\,q^x\equiv q^l(\mathrm{mod}\ N)}\exp\left(i2\pi\frac{x\cdot y}{M}\right)\right|^2.$$

I due passi successivi di una singola «passata» della sequenza sono classici e possono essere eseguiti con un computer classico:

I) innanzi tutto occorre trovare la migliore approssimazione di $\frac{y}{M}$ con denominatore r' tale che $r' < N < \sqrt{M}$:

$$\left| \frac{y}{M} - \frac{d'}{r'} \right| < \frac{1}{2M} .$$

Cerchiamo di capire la ragione di questa scelta. Se

$$\exists s \in \mathbb{Z}, \qquad -\frac{r}{2} \leqslant s \leqslant \frac{r}{2}, \qquad \text{tale che } r \cdot y \equiv s \pmod{M},$$

allora esiste un d tale che

$$-\frac{r}{2} \leqslant r \cdot y - dM \leqslant \frac{r}{2},$$

e dunque

$$\left| \frac{y}{M} - \frac{d}{r} \right| < \frac{1}{2M},$$

vale a dire l'r' trovato sopra di fatto divide r. Possiamo dire che y in questo caso è «buono». Noi siamo ovviamente interessati a $r' = r$ (y «molto buono»). Stimando la somma di esponenziali in $P_l(y)$ si vede d'altronde facilmente che la probabilità di trovare un y buono è $\geqslant \frac{1}{3r^2}$. Ma ci sono $r\phi(r)$ stati della forma $|y\rangle |q^l (\mathrm{mod}\ N)\rangle$ con y molto buono (dove $\phi(r)$ è la funzione di Eulero), quindi con probabilità $\mathcal{O}(r^2 \ln r)$, cioè facendo un numero al più polinomiale di tentativi, possiamo avere r' coincidente con r.

Proviamo infine r' nel suo ruolo, vale a dire:

II) se r' è pari, calcoliamo il massimo comune denominatore fra $q^{(1/2)r'} \pm 1$ ed N.

Se r' è dispari, oppure r' è pari ma non abbiamo trovato un divisore proprio di N, si ripete la procedura con lo stesso valore di q, un numero di volte $\mathcal{O}(\log_2 \log_2 N)$. In caso di mancata soluzione, si cambia q e si inizia una nuova passata.

Esistono altri bellissimi algoritmi quantistici, anche se nessuno forse così efficace come quello di Shor. Fra i più importanti è quello

relativo al problema di scelta fra N oggetti. È questo un problema che classicamente richiede un numero di tentativi proporzionale ad N. All'algoritmo quantistico, dovuto a Lov Grover, è invece sufficiente un numero di passi $\propto \sqrt{N}$: non si cambia la classe di complessità (**P**), ma i vantaggi pratici possono essere enormi.

Un'altra questione importante nel progetto (almeno concettuale) di un computer quantistico riguarda le architetture. Una soluzione interessante, che potrebbe anche gettare una nuova luce sulla interpretazione di altri affascinanti problemi complessi, quali il funzionamento del sistema nervoso o del cervello umano, particolarmente importante per l'implementazione di algoritmi quantistici, consiste di uno o più *quantum chips* (registri) controllati da un computer classico: a quest'ultimo e alle sue componenti (reti elettroniche o neuronali) oltre al compito di controllare i chip quantistici verrebbe assegnata anche quella parte del lavoro di calcolo che non richieda il massiccio parallelismo che è proprio e caratteristico delle componenti quantistiche. La difficoltà principale può sembrare qui legata al fatto che la misura quantistica produce tipicamente risultati non deterministici. Tuttavia non è così: la meccanica quantistica ci insegna infatti che ci sono situazioni in cui è possibile distinguere bene fra l'aleatorietà di origine quantistica e quella classica semplicemente analizzando le distribuzioni di probabilità e utilizzando quel potente strumento concettuale che sono le cosiddette diseguaglianze di Bell. Queste, un ingrediente standard della teoria dei quanti, in questo contesto giocano il ruolo di prima istanza di una situazione tipo teoria dei giochi in cui i giocatori quantistici dimostrabilmente si comportano in modo molto più efficiente di quelli classici. La vera difficoltà invece, come già detto, è di natura fisica: quella di eliminare le numerose fonti di decoerenza, sia isolando il sistema dall'ambiente circostante, sia imparando a preparare gli stati ed a manipolare l'informazione che essi contengono senza uscire dall'ambito di codici che evitano l'errore.

BIBLIOGRAFIA

Testi sulla teoria della computazione e della informazione quantistica:

[1] D. AHARONOV, *Quantum Computation*, in *Annual Reviews of Computational Physics*, vol. VI, a cura di D. Stauffer, World Scientific Publ. Co., 1998.

[2] HOI-KWONG LO - S. POPESCU - T. SPILLER (curatori), *Introduction to Quantum Computation and Information*, World Scientific Publ. Co., 1999.

[3] I. L. CHUANG - M. NIELSEN, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

Un buon testo di riferimento per la meccanica quantistica:

[4] A. PERES, *Quantum Theory: Concepts and Methods*, Kluwer Academic Press, 1993.

Mario Rasetti, Dipartimento di Fisica e Unità INFM
Politecnico di Torino, I-10129 Torino