ISTITUTO LOMBARDO
ACCADEMIA DI SCIENZE E LETTERE

SCIENZA E TECNOLOGIE AVANZATE

ANNO 1998/1999

ESTRATTO

GIACOMO MAURO D'ARIANO

OTTICA QUANTISTICA: APPLICAZIONI E NUOVI ESPERIMENTI FONDAMENTALI

Istituto Lombardo di Scienze e Lettere
—
MILANO
2010

GIACOMO MAURO D'ARIANO (*)

OTTICA QUANTISTICA: APPLICAZIONI E NUOVI ESPERIMENTI FONDAMENTALI

1. *Introduzione*

In questo seminario parlerò di alcuni recentissimi sviluppi che si sono avuti in Meccanica Quantistica negli ultimi dieci anni, sviluppi che sono stati resi possibili dagli enormi progressi tecnici raggiunti nell'Ottica Quantistica e Fisica Atomica sperimentali. In considerazione dell'eterogeneità del backround culturale del probabile lettore di questa memoria, il seminario corre simultaneamente su due livelli di comprensione: uno più divulgativo ed uno più tecnico, sperando in tal modo di non scontentare tutti i lettori! Presenterò alcune equazioni, invero molto semplici dal punto di vista matematico, ma il cui contenuto concettuale pregnante ha necessitato di più di mezzo secolo prima che i fisici addetti ai lavori potessero comprenderne, solo recentemente, alcune delle conseguenze più eclatanti.

Il mondo della Meccanica Quantistica è davvero "bizzarro", specialmente la Teoria della Misurazione, ove maggiormente si manifesta il dualismo onda-corpuscolo. In un mondo basato sull'incertezza del principio di indeterminazione di Heisenberg – ma comunque sottoposto a rigide leggi fisiche mai

(*) Dipartimento di Fisica 'Alessandro Volta'.

falsificate in cento anni di esperimenti! – in questo mondo, come vedremo, è possibile concepire nuovi computer *quantistici* che funzionano con un nuovo tipo di bit, i *qubit* ("quantum bit") che assumono valore 0 o 1 ed anche ogni possibile *sovrapposizione* fra i due valori. Questi futuri computer saranno in grado di eseguire calcoli che nessun calcolatore digitale *classico* come oggi lo concepiamo potrebbe mai eseguire nel tempo di vita dell'universo.

Il mondo quantistico delle bassissime energie (agli antipodi delle alte energie delle particelle elementari di Carlo Rubbia) si sta dischiudendo solamente oggi grazie al progresso tecnologico in Ottica Quantistica e in Fisica Atomica. Il *laser*, che ha letteralmente invaso le nostre case con i *compact disks* dopo solo quarant'anni dalla nascita (il primo laser a rubino fu costruito da Maiman nel 1960 agli Hughes labs), ha aperto la possibilità di generare luce molto potente e concentrata, la quale a sua volta ha permesso lo sviluppo dell'*Ottica Non Lineare*, con la quale oggi possiamo eseguire esperimenti (alquanto semplici e relativamente "economici") prima assolutamente impensabili.

La Meccanica Quantistica entra nel dominio ottico in modo perentorio, in quanto rappresenta la sorgente principale di rumore nelle comunicazioni ottiche. Si pensi infatti che l'indeterminazione quantistica di un solo fotone nell'infrarosso equivale ad un rumore termico di migliaia di gradi Kelvin. E gli ingegneri, ancora oggi riluttanti ad usare una teoria così paradossale come la Meccanica Quantistica, devono oggi farci i conti, nell'ottimizzare le comunicazioni in fibra ottica per raggiungere il limite teorico dei Terabit al secondo trasmessi in una fibra sottile come un capello. Quando il lettore lamenta la lentezza delle comunicazioni via *Internet*, dovrebbe considerare che con 1Tbit/sec è possibile trasmettere tutto il Wall Steet Journal dalla sua nascita in un solo secondo! Per ottenere trasmissioni così veloci occorre utilizzare segnali molto deboli, codificando l'informazione su singoli fotoni. E qui si

manifesta la bizzarria della *misurazione quantistica*, con gli amplificatori ottici che manifestano caratteristiche di guadagno e di rumore che dipendono "a posteriori" dal tipo di rivelazione all'uscita dell'amplificatore, ovvero se sia essa fotorivelazione diretta, omodina, o eterodina. Le proprietà dell'amplificatore non sono quindi intrinseche del dispositivo, ma, come si dice in gergo quantistico, dipendono dall' *osservabile* misurata, ovvero dal modo in cui si rivela la radiazione. È possibile comunicare con radiazione *squeezed* [1], codificando e rivelando il segnale ad una fase fissata, e relegando tutto il rumore sulla fase ortogonale, in accordo al principio di indeterminazione di Heisenberg, come per momento e posizione di una particella. Alla Northwestern con il Prof. Prem Kumar abbiamo studiato un ripetitore ottico che funziona perfettamente a 40 Gbit/s [2], e i calcoli teorici mostrano che potrebbe funzionare anche con pochi fotoni, al limite teorico, con errore di trasmissione (in gergo: *bit-error-rate*) trascurabile.

Nel presente seminario parlerò comunque di questioni meno tecnologiche e più di fondamento, o se volete, di *tecnologia futuribile*, ancora in fase di studio e di sperimentazione preliminare, come è il caso del *quantum computer*. Incentrerò il seminario su due concetti chiave della Meccanica Quantistica: l' *entanglement* e lo *stato quantistico*. Sulla base di questi concetti illustrerò quindi brevemente il *teletrasporto quantistico* (di cui è giunta notizia anche dai quotidiani e dai media), e le basi del *calcolo quantistico* e della tecnica della *tomografia quantistica*, quest'ultima introdotta e sviluppata a Pavia.

2. *L'entanglement*

È appena finito il secondo millennio, e la Meccanica Quantistica sta per compiere cento anni esatti (il 14 Dicembre dell'anno 1900 Max Planck presentò la sua prima memoria sui quanti alla Società di Fisica Tedesca a Berlino). È opinione

condivisa da molti che la maggior parte della teoria quantistica sia stata delineata nella prima metà del secolo [3]. Eppure, dopo tanti anni, la Meccanica Quantistica non cessa ancora di stupirci. Il fenomeno senza dubbio più "strano" della meccanica quantistica è quello che i fisici chiamano *entanglement*. Un esempio di *stato massimamente entangled* è lo stato di singoletto di due particelle a spin $\frac{1}{2}$ correlate in modo da dare spin totale nullo. Nel formalismo di Dirac [4] questo stato si scrive come segue:

$$|\Psi_{12}\rangle = \sqrt{\frac{1}{2}}(|\uparrow_1\rangle|\downarrow_2\rangle - |\downarrow_1\rangle|\uparrow_2\rangle). \tag{1}$$

La scrittura dello stato non è unica: se si cambia la base ovvero si sceglie una generica direzione di quantizzazione "obliqua" dello spin:

$$|\nearrow\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle\,, \tag{2}$$

$$|\swarrow\rangle = \beta^*|\uparrow\rangle - \alpha^*\beta|\downarrow\rangle\,, \qquad |\alpha|^2 + |\beta|^2 = 1\,, \tag{3}$$

si ottiene

$$|\Psi_{12}\rangle = \sqrt{\frac{1}{2}}(|\nearrow_1\rangle|\swarrow_2\rangle - |\swarrow_1\rangle|\nearrow_2\rangle)\,, \tag{4}$$

La conseguenza è che, in accordo a von Neumann[5], se si misura lo spin 1 in una qualunque direzione fissata $\nearrow$ si ottiene lo spin nei versi $\nearrow$ e $\swarrow$ con ugual probabilità 1/2. Ma, si ha anche che se la misura sullo spin 1 dà risultato $\nearrow$, allora si prevede con certezza che una misura nella stessa direzione per lo spin 2 darà verso opposto $\swarrow$. Analogamente, se sullo spin 1 si ottiene $\swarrow$, allora sullo spin 2 si ottiene certamente $\nearrow$. Tutto ciò è ovviamente in accordo alla conservazione del momento angolare totale, ma, cosa meno banale, ciò avviene istantaneamente (*superluminalmente*), e in assenza di alcun tipo di interazione tra le particelle, anche se le particelle vengono portate a distanza molto grande, nell'ipotesi che esse non interagiscano

con altre particelle circostanti. Invece, quando le direzioni di misura per i due spin anziché parallele sono ortogonali, i risultati ottenuti sulle due particelle sono perfettamente scorrelati. Infine, poiché la probabilità di rilevare lo spin in uno dei due versi opposti è comunque $\frac{1}{2}$, indipendentemente dal fatto che sia stata eseguita una misura sull'altro spin, ne consegue che pur essendo l'effetto di correlazione superluminale, esso non può essere utilizzato per trasmissione di informazione a velocità infinita. Infatti, quando si misura lo spin 2 si ottiene comunque un risultato casuale, e non c'è modo di sapere se il risultato sia dovuto ad un cambiamento della direzione di misura sullo spin 1: le correlazioni possono essere verificate *solo a posteriori* [6].

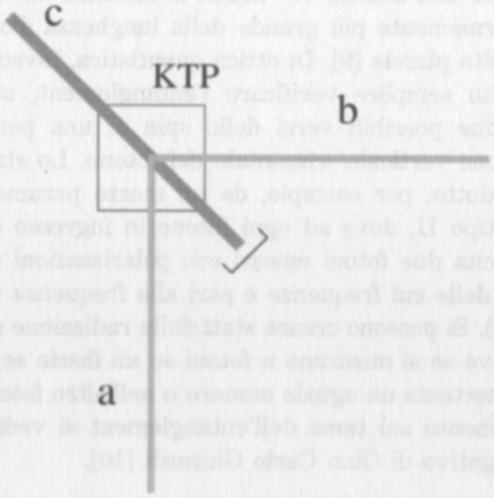

Fig. 1 – Rappresentazione schematica del processo di generazione parametrica di uno stato *entangled*. Un cristallo non lineare, ad esempio KTP, viene pompato con un intenso fascio laser c a frequenza ω_c. All'uscita si generano fasci *gemelli* a e b con frequenze più basse $\omega_a + \omega_b = \omega_c$, i quali sono in uno stato *entangled* (per maggiori dettagli si veda il testo).

Questo tipo di correlazione ha stupito Einstein che nel 1935 con Podolsky e Rosen scrisse un articolo [7] che metteva in dubbio l'obiettività e la completezza della descrizione quantistica. Esistono forse variabili nascoste che possono descrivere questa correlazione? Bell nel 1964 [8] ha dimostrato un teorema che afferma che una qualunque teoria di meccanica classica con ipotetiche variabili nascoste non è in grado di spiegare questa correlazione in particolare per direzioni di misurazione a 45° l'una rispetto all'altra (a meno di non avere teorie strane *non locali*, ovvero con interazioni che si propagano istantaneamente). È molto difficile verificare sperimentalmente questa correlazione con particelle, in quanto è difficile eliminare le interazioni fra le particelle ed il circondario. Solo molto recentemente l'entanglement è stato verificato sperimentalmente con mesoni K^o neutri a distanza del metro, distanza enormemente più grande della lunghezza d'onda di de Broglie molto piccola [9]. In ottica quantistica, invece, è veramente molto semplice verificare l'entanglement, utilizzando, anziché i due possibili versi dello spin di una particella, la polarizzazione verticale/orizzontale del fotone. Lo stato entangled è prodotto, per esempio, da un mezzo parametrico non lineare di tipo II, dove ad ogni fotone in ingresso corrispondono in uscita due fotoni emessi con polarizzazioni ortogonali (la somma delle cui frequenze è pari alla frequenza del fotone in ingresso). Si possono creare stati della radiazione detti *fasci gemelli*, dove se si misurano n fotoni su un fascio se ne troveranno con certezza un uguale numero n nell'altro fascio. Per un approfondimento sul tema dell'entanglement si veda anche il testo divulgativo di Gian Carlo Ghirardi [10].

3. *L'impossibilità di* clonare *esattamente*

Nello stato massimamente entangled $|\Psi_{12}\rangle$ nell'equazione (1) lo *stato* dello spin 2 dopo la misura sullo spin 1 è sempre "opposto" a quello corrispondente al risultato di una uguale misura sullo spin 1. Pertanto, in principio, sarebbe possibile comunicare superluminalmente se fosse possibile determinare lo stato di un singolo sistema quantistico, ovvero lo stato dello spin di una sola particella. Ma la possibilità di determinare lo stato totalmente "ignoto" a priori di una singola particella è escluso dal teorema del no-cloning, che qui illustro in versione semplificata.

L'argomento della macchina che clona gli stati [11] che qui riporto è nella versione "forte" dovuta a H. P. Yuen [12]. L'argomento afferma che una macchina che "clona" un generico stato, ovvero che ne produce n copie identiche, violerebbe l'unitarietà della meccanica quantistica. Infatti, clonare n copie di due stati nonortogonali $|\psi\rangle$ e $|\varphi\rangle$ porterebbe a una diminuzione del prodotto scalare dall'input all'output della macchina

$$|\langle\psi|\varphi\rangle| \longrightarrow |\langle\psi|\varphi\rangle|^n < |\langle\psi|\varphi\rangle| \,, \tag{5}$$

mentre, come ben noto, le trasformazioni unitarie – le uniche ammissibili in Meccanica Quantistica – conservano il prodotto scalare. (L'argomento può essere facilmente esteso includendo lo stato quantico della macchina e quello del circondario della macchina). La clonazione esatta non è quindi ammissibile per le leggi della Meccanica Quantistica. D'altra parte, l'impossibilità di determinare lo stato di un singolo sistema quantistico è "logicamente" equivalente all'impossibilità del cloning esatto [13]. Infatti, poiché in Meccanica Quantistica in linea di principio è possibile "preparare" un sistema in uno stato qualsivoglia[14], ne segue che se si potesse determinare lo stato di un singolo sistema quantistico, se ne potrebbero anche preparare n copie identiche, realizzando quindi una *cloning machine* perfetta. E, al contrario, se esistesse una *cloning machine* perfetta, si potrebbero fare infinite misure di osservabili diverse sui cloni – potenzialmente infiniti – determinando quindi lo stato del sistema originale: allo scopo si potrebbe utilizzare la Tomografia Quantistica, che vedremo più avanti. È quindi anche dimostrato che la possibilità di determinare lo stato di

un sistema singolo quantistico è anch'essa in contrasto con le leggi della Meccanica Quantistica.

Nonostante l'apparente ovvietà del teorema del *no-cloning*, ancora pochi anni fa sono apparsi in letteratura numerosi tentativi [15], ovviamente falliti, di determinare lo stato di un sistema singolo mediante misure "deboli" ripetute sullo stesso sistema. Per il teorema del *no-cloning* ciò è ovviamente impossibile, qualunque sia lo schema di misura. Infatti, se la misura è "debole" – ovvero disturba poco il sistema, che resta disponibile per una misura successiva – allora essa è anche poco "informativa". Con Yuen abbiamo mostrato che tutti gli schemi di misura possibili sono equivalenti da questo punto di vista[13]. È però possibile determinare lo stato di un sistema quantistico se si ha a disposizione un insieme (*ensemble*) contenente un gran numero di sistemi identici preparati nello stesso stato, eseguendo misure indipendenti sui diversi elementi dell'ensemble. Questo è essenzialmente il metodo della Tomografia Quantistica.

4. *Il Teletrasporto*

Il concetto di *entanglement* e il teorema del *no-cloning* sono le tessere del "puzzle" del Teletrasporto Quantistico, del quale si è anche sentito parlare sui quotidiani e sui media relativamente agli esperimenti del gruppo di Francesco De Martini a Roma La Sapienza [16], di Anton Zeilinger a Innsbruk [17], e di Jeff Kimble al Caltech [18,19].

Innanzitutto, cosa vuol dire *teletrasporto*? La definizione dell'Oxford dictionary dice testualmente: " *Paranormale* e *Fantascienza:* il trasferimento di persone (specialmente di se stesso!) o cose mediante energia psichica. In una descrizione futuristica: trasporto apparentemente istantaneo di persone o cose attraverso lo spazio mediante mezzi tecnologicamente avanzati".

Si può senz'altro affermare che il termine *Teletrasporto* è uscito dal dominio della fantascienza per entrare in quello della scienza da quando Bennet, Brassard, Crépau, Yozsa, Peres e Wotters pubblicarono nel 1993 il Physical Review Letters dal titolo: *Teletrasporto di uno stato quantistico ignoto mediante doppio canale classico e EPR*[20]. Il canale EPR è lo stato massimamente entangled che abbiamo visto nella Sezione 2, e viene così chiamato dopo il lavoro di Einstein, Podolsky, e Rosen ivi menzionato. Il problema è il seguente.

In accordo alla Meccanica Classica teletrasportare un'oggetto corrispondebbe a "spostare" fisicamente tutte le particelle di cui l'oggetto è composto. Ricostruire l'oggetto con particelle diverse da quelle originali darebbe luogo ad un'oggetto identico (cioè con le stesse proprietà fisiche), ma "distinto" dall'originale, in quanto classicamente le particelle sono *distinguibili*, ovvero, anche se identiche (per carica, massa, spin), esse mantengono sempre la loro identità, che in principio ci permette di seguirle individualmente nel loro moto. In Meccanica Quantistica, invece, particelle identiche sono anche *indistinguibili*, ovvero non è possibile seguirle individualmente nel loro moto: a tutti gli effetti, particelle identiche sono la stessa entità fisica. Il fisico teorico direbbe che particelle identiche sono l'aspetto "corpuscolare" dello stesso campo immutabile ed onnipresente. Un elettrone di questa pagina è identico ed indistinguibile da quello della pagina precedente, in quanto essi sono manifestazioni dello stesso campo: il campo di Dirac. Ovviamente i due elettroni possono avere velocità e spin diversi, ma ciò significa semplicemente che i due elettroni sono in stati fisici quantistici diversi, pur rimanendo comunque la stessa entità. Potremo quindi affermare che un oggetto non è identificabile con le molecole che lo compongono, bensì si riconosce nello stato quantistico delle sue molecole. In altri termini, l'identità dell'oggetto risiede nello stato quantistico delle particelle di cui è composto, e non si identifica con l'insieme delle particelle componenti stesse. Il teletrasporto di un oggetto

consiste appunto nel trasmettere e ricostruire a distanza, su materia ivi presente, lo stato quantistico delle particelle di cui l'oggetto è composto (ovviamente lo stato relativo al centro di massa, il quale risulterà spostato nello spazio-tempo). Quindi, in sintesi: teletrasporto significa ricostruire lo stato quantico di un oggetto in un luogo distante su materia ivi presente.

Ciò che rende non banale la realizzazione del teletrasporto è l'impossibilità in principio di conoscere lo stato quantistico di un oggetto, in accordo al teorema del *no-cloning* visto precedentemente. Come possiamo trasmettere e ricostruire a distanza lo stato se non possiamo conoscerlo? D'altra parte, abbiamo anche il secondo problema, non meno grave del precedente: se anche lo stato quantico fosse noto – come nel caso che esso fosse stato "preparato" sotto il nostro controllo – l'informazione che descrive lo stato, e che dovremmo quindi trasmettere, sarebbe infinitamente grande. Infatti, lo stato quantistico di un solo spin (ovvero di un semplice sistema a due soli livelli energetici) è descritto da un numero complesso (si veda l'equazione (3)). Pertanto, il numero di bit da trasmettere aumenta con la precisione con la quale si approssima il numero complesso, ed occorre un'informazione virtualmente infinita per trasmettere lo stato in modo esatto. Quindi, in sintesi: a) non si può conoscere lo stato quantico; b) se anche lo stato fosse noto occorrerebbe un'informazione infinita per trasmetterlo. Come quindi è possibile "teletrasportare" lo stato quantistico, ovvero trasmetterlo e ricostruirlo a distanza? E qui il risultato eclatante del lavoro [20]: non è necessario conoscere lo stato per teletrasportarlo, anzi, per non distruggerlo, si deve far in modo di non conoscerlo in alcun modo. Inoltre, per teletrasportare lo stato di uno spin bastano solo 2 bit di informazione più un canale entangled!

Ed ecco qui la soluzione del problema del teletrasporto. In Fig. 2 la lettera A rappresenta la sorgente, mentre la lettera B denota il ricevitore: nella letteratura sull'argomento essi sono chiamati rispettivamente "Alice" e "Bob". Alice deve teletrasportare uno stato $|\phi\rangle$ a Bob. Poiché Alice non deve conoscere lo stato $|\phi\rangle$, diremo che è Carol a consegnarglielo. Alice e Bob dispongono di due risorse: un canale classico (telefono, radio), ed un canale entangled costituito da una coppia di particelle in uno stato di singoletto che si dipartono da un luogo intermedio verso Alice e Bob. Alice correla la particella 1 con la particella 2 della coppia eseguendo la misura completa descritta dal set ortonormale di Bell:

$$|\Psi_{12}^{\pm}\rangle = \sqrt{\frac{1}{2}}(|\uparrow_1\rangle|\downarrow_2\rangle - |\downarrow_1\rangle|\uparrow_2\rangle)\,, \tag{6}$$

$$|\Phi_{12}^{\pm}\rangle = \sqrt{\frac{1}{2}}(|\uparrow_1\rangle|\uparrow_2\rangle - |\downarrow_1\rangle|\downarrow_2\rangle). \tag{7}$$

La misura ha quattro possibili risultati, che denoteremo con $\{\Psi^{\pm}, \Phi^{\pm}\}$. Scriviamo quindi il generico stato ignoto della particella 1 come segue:

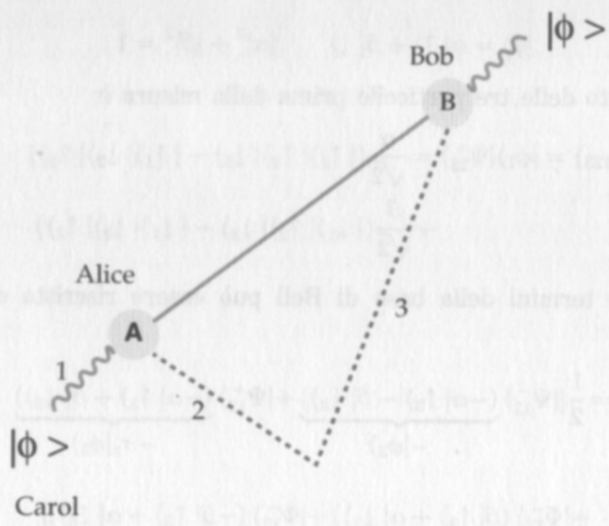

Fig. 2 – Schema del Teletrasporto Quantistico del Rif. [20]. Per la spiegazione si rimanda al testo.

$$|\phi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle \qquad |\alpha|^2 + |\beta|^2 = 1\,. \tag{8}$$

Lo stato delle tre particelle prima della misura è:

$$|\Psi_{123}\rangle = |\phi_1\rangle|\Psi^-_{23}\rangle = \frac{\alpha}{\sqrt{2}}(|\uparrow_1\rangle|\uparrow_2\rangle|\downarrow_3\rangle - |\uparrow_1\rangle|\downarrow_2\rangle|\uparrow_3\rangle) \tag{9}$$

$$+\frac{\beta}{\sqrt{2}}(|\downarrow_1\rangle|\uparrow_2\rangle|\downarrow_3\rangle - |\downarrow_1\rangle|\downarrow_2\rangle|\uparrow_3\rangle) \tag{10}$$

che in termini della base di Bell può essere riscritto come segue:

$$|\Psi_{123}\rangle = \frac{1}{2}[|\Psi^-_{12}\rangle \underbrace{(-\alpha|\uparrow_3\rangle - \beta|\downarrow_3\rangle)}_{-|\phi_3\rangle} + |\Psi^+_{12}\rangle \underbrace{(-\alpha|\uparrow_3\rangle + \beta|\downarrow_3\rangle)}_{-\sigma_z|\phi_3\rangle} \tag{11}$$

$$+|\Phi^-_{12}\rangle \underbrace{(\beta|\uparrow_3\rangle + \alpha|\downarrow_3\rangle)}_{\sigma_x|\phi_3\rangle} + |\Phi^+_{12}\rangle \underbrace{(-\beta|\uparrow_3\rangle + \alpha|\downarrow_3\rangle)}_{-i\sigma_y|\phi_3\rangle}] \tag{12}$$

Come si vede, a seconda del risultato della misura di Alice, Bob riceve uno stato diverso. Ma Alice trasmette a Bob il suo risultato sul canale classico. Se il risultato è Ψ^- Bob non fa nulla: egli ha già lo stato giusto (cambiato di segno: ma in Meccanica Quantistica lo stato è definito a meno di un fattore di fase). Se il risultato è Ψ^+ Bob fa una rotazione dello spin di 180^o gradi intorno all'asse z (descritta dalla matrice di Pauli σ_z). Se invece il risultato è Φ^- Bob fa una rotazione di 180^0 attorno all'asse x (matrice di Pauli σ_x), ed infine se il risultato è Φ^+ Bob fa una analoga rotazione attorno all'asse y (matrice σ_y). Alla fine Bob si trova sempre con la particella 3 nel corretto stato incognito $|\phi\rangle$ che precedentemente apparteneva alla particella 1. Alice ottiene uno dei quattro possibili risultati $\{\Psi^\pm, \Phi^\pm\}$ con probabilità $\frac{1}{4}$, indipendentemente dallo stato $|\phi\rangle$, del quale, pertanto, non ottiene alcuna informazione dalla misura eseguita. Si noti che poiché i risultati della misura sono quattro, i bit da trasmettere sul canale classico sono due.

Lo schema precedente è ovviamente generalizzabile in vari modi [21], per esempio a più particelle, o a bosoni anziché fermioni. Lo schema generale è però sempre lo stesso, ovvero:

1. Occorro due canali di trasmissione: uno classico ed uno quantistico massimamente entangled;
2. Alice esegue una misura che correla il canale entangled con il canale che supporta lo stato ignoto da teletrasportare;
3. Alice trasmette a Bob il risultato della misura; a seconda del risultato Bob esegue una diversa trasformazione unitaria sul suo canale;
4. Alice non ottiene nessuna informazione dalla misura eseguita.

Il segreto del funzionamento del teletrasporto stà proprio nel realizzare una misura quantistica che sia totalmente *non informativa*, e che correli il canale che supporta l'oggetto da teletrasportare con un canale entangled. Si osservi che la correlazione quantistica sul canale entangled è superluminale, ma l'informazione sul canale classico viaggia necessariamente alla velocità della luce. Occorre pertanto ritardare il canale entangled: in Fig. 2 il ritardo è rappresentato da un percorso più lungo per la particella 3 che per la particella 2, con il percorso della particella 3 circa uguale alla lunghezza del canale di trasmissione classico. Lo stato viene quindi teletrasportato alla velocità della luce, e non istantaneamente. Si noti infine che lo schema permette di teletrasportare anche uno stato che sia a sua volta entangled con un quarto sistema, e ciò è semplicemente una conseguenza della linearità della mappa: si parla in tal caso di *entanglement swapping*.

Sono stati eseguiti ben tre esperimenti di teletrasporto: tutti e tre utilizzano radiazione, ovvero teletrasportano stati della luce. Il primo esperimento in ordine cronologico è stato eseguito nei laboratori di Francesco De Martini in Roma [16], seguito quindi dall'esperimento di Anton Zeilinger in Innsbruk [17]. In entrambi gli esperimenti si teletrasporta un sistema a

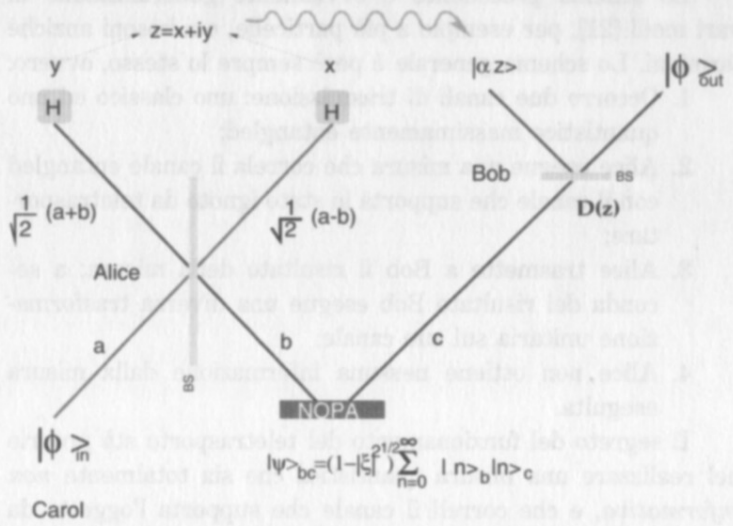

Fig. 3 – Schema dell'esperimento di Teletrasporto Quantistico di Jeff Kimble al Caltech [19]. Per la spiegazione si rimanda al testo.

due livelli codificato su due polarizzazioni ortogonali di un singolo fotone. Per entrambi gli esperimenti è dibattuto se essi realizzino veramente il teletrasporto quantistico: più precisamente bisognerebbe dire che essi verificano sperimentalmente le correlazioni quantistiche su cui si basa il teletrasporto. L'esperimento di Jeff Kimble al Caltech[18,19], l'ultimo esperimento in ordine cronologico, è invece un vero e proprio teletrasporto "attivo", e non semplicemente una verifica delle correlazioni. Per di più in questo esperimento si teletrasporta uno stato "bosonico", ovvero lo stato di un sistema ad infiniti livelli equispaziati. Si tratta anche di un esperimento relativamente più semplice da descrivere. In Fig. 3 ne è riportato lo schema sperimentale. Il NOPA (non linear optical amplifier) fornisce lo stato entangled (fasci gemelli). Alice dispone di un *beam-splitter* 50-50 (specchio semitrasparente) ove entrano le due onde a e b e ne escono le loro somma e differenza. Sulle uscite

somma e differenza Alice esegue due misure omodina separate con fasi ortogonali (questa misura equivale a misurare posizione e momento dei due oscillatori che descrivono le onde somma e differenza). Alice compone quindi i risultati x e y delle due misure nel numero complesso $z = x + iy$ che invia quindi a Bob. Si noti che ora Alice invia infiniti bit, perché teletrasporta uno stato di un sistema ad infiniti livelli, che è equivalente a teletrasportare infiniti spin. Bob fa una trasformazione unitaria detta di "spostamento" sul fascio c, spostandolo del numero complesso z: ciò viene ottenuto con con un'altro beam-splitter, nel limite di trasparenza perfetta, combinando l'onda c con radiazione laser coerente e molto intensa. In tal modo Bob riottiene lo stato $|\phi\rangle$ sull'onda c. Il teletrasporto funziona idealmente per tutti gli infiniti livelli solo per rivelatori perfetti e per guadagno infinito al NOPA, altrimenti lo stato teletrasportato risulta "distorto". Infatti, i calcoli teorici mostrano che quando il guadagno dell'amplificatore non è infinito Alice può ottenere dalla sua misura un'informazione parziale sullo stato da teletrasportare, ma lo stato teletrasportato risulta distorto. Man mano che si aumenta il guadagno dell'amplificatore la distorsione dello stato diminuisce, ma la misura di Alice produce un rumore sempre più grande, fino alla perdita totale dell'informazione. Si noti che l'impossibilità per Alice di ottenere informazione dalla misura non è altro che un'altra manifestazione del teorema del *no-cloning*. Infatti, se il teletrasporto fosse perfetto e Alice avesse allo stesso tempo una minima informazione sullo stato, si potrebbe rieseguire il teletrasporto infinite volte a catena, senza distorcere lo stato, ed aumentando a piacere l'informazione ottenuta da Alice sullo stato, fino ad ottenere un'informazione completa.

5. *Calcolatori quantistici*

Vediamo ora come l'entanglement può essere utilizzato per fare un nuovo tipo di calcolatori, i "computer quantistici". In-

nanzitutto dobbiamo amaramente constatare che la attuale tecnologia elettronica raggiungerà un punto di saturazione previsto nell'arco di 10-20 anni.

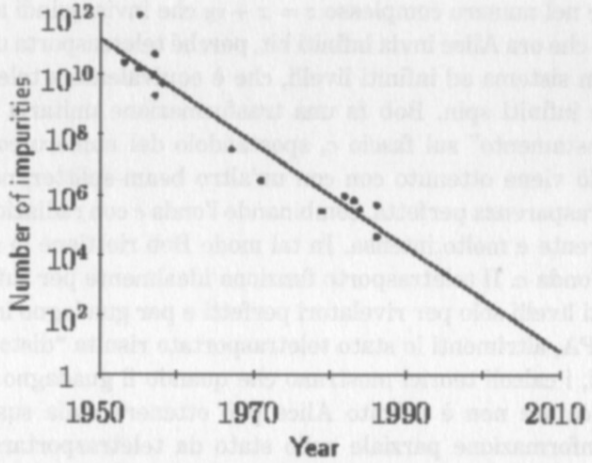

Fig. 4 – Numero di impurezze droganti per transistor in circuiti logici versus l'anno di produzione [fig. 5 da R. W. Keyes, IBM J. Res. Develop. **32**, 24 (1988), reprinted with permission of IBM T.J. Watson Research Center]

Nell'arco degli ultimi trent'anni il numero di transistor per microchip è passato da alcune migliaia alla fine degli anni '60 a miliardi o decine di miliardi con legge esponenziale (questa crescita esponenziale è detto volgarmente detta "legge di Moore"). Colin Worwick commentava alcuni anni or sono che se si avesse avuto, per confronto, un analogo progresso nell'auto avremmo automobili che costano 40 dollari, con un bagagliaio 1500m^3, che viaggiano a 2 milioni di km/h e consumano solo un litro di carburante ogni 600000 km! Purtroppo nel progresso dei computer, come già detto, si raggiungerà presto una saturazione. In Fig. 4 è riportato il numero di impurezze droganti per transistor in circuiti logici dagli anni '50 agli anni '90. Si vede che il numero di elettroni per transistor segue una legge esponenziale inversa in funzione del tempo (in realtà nell'ultima decade si è avuta addirittura una accelerazione ulteriore dovuta alla concorrenza!) Se si estrapola la retta si vede che si raggiungerà il limite dell'elettrone singolo per transistor attorno al 2010, ovvero fra pochi anni! Dopodichè o cambia la tecnologia, o inizia un nuovo medioevo di stasi tecnologica. Una memoria commerciale ha ora un dimensione minima di 0.35μm, e sta iniziando la transizione fra microtecnologia e nanotecnologia. Il prossimo obbiettivo è il cosiddetto *point one*, ovvero 0.1μm; si arriverà infine a poche decine di nanometri.

I problemi coinvolti nella miniaturizzazione elettronica spinta sono molteplici. Innanzitutto il *cross-talk:* gli elettroni cominciano a "tunnellare" fra i transistor e i fili di collegamento. Occorre poi gestire correnti molto piccole, e c'è l'enorme problema della dissipazione di calore. Ed infine, non si riesce a realizzare circuiti in tre dimensioni, nonostante l'enorme sforzo di investimento economico in questo settore.

5.1. *Il calcolo reversibile*

La dissipazione di calore nella tecnologia corrente è 1 milione di volte maggiore del limite teorico di Landaurer[22] pari a $K_B T \log 2$, necessario per cancellare 1 bit di informazione (K_B è la costante di Boltzmann, e T è la temperatura assoluta in Kelvin). In linea di principio, infatti, la dissipazione termica è necessaria per la sola cancellazione di dati. Charles Bennet dell'IBM Yorktown Heights di New York ha mostrato nel 1973[23] che è possibile il calcolo senza "erase", utilizzando "junk bits" (bits spazzatura). Per esempio, se si calcola la funzione f su diversi valori a si deve conservare i valori di input come segue:

$$f: \quad a \to (a, f(a)) \,. \tag{14}$$

I bit spazzatura $j(a)$ conservati nei calcoli intermedi possono essere eliminati semplicemente facendo andare il calcolatore alla rovescia, ricopiando il risultato e rovesciando il calcolo su un registro. Schematicamente si ha:

$$f: \quad a \to (a, j(a), f(a)) \tag{15}$$

$$\to (a, j(a), f(a), f(a)) \quad (FANOUT) \tag{16}$$

$$\to (a, f(a)) \quad (uncomputing) \tag{17}$$

È vero che molte porte logiche (gates) sono irreversibili, ma Toffoli ha mostrato che è possibile realizzare un gate universale a 3 ingressi e 3 uscite che è reversibile, e con il quale si può realizzare ogni tipo di gate!

TABELLA 1 – Tabella di verità delle diverse porte logiche.

A	B	AND	OR	XOR	NOT B
0	0	0	0	1	0
0	1	0	1	1	0
1	0	0	1	1	1
1	1	1	1	0	0

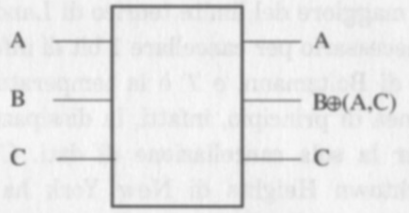

Fig. 5 – Gate universale reversibile di Toffoli con tre ingressi e tre uscite. Il gate è chiaramente reversibile, in quanto la trasformazione corrispondente è uguale alla sua inversa (il simbolo $\oplus$ denota somma modulo 2).

Il calcolo reversibile, senza dissipazione di energia, è quindi possibile, e in California hanno già realizzato un prototipo di VLS ("very large scale integration") con tecnologia CMOS e switching adiabatico dove la potenza viene derivata dal segnale di clock.

5.2. *Il calcolo parallelo quantistico*

In Meccanica Quantistica trasformazione reversibile è sinonimo di trasformazione unitaria. Utilizzando bit quantistici detti *qubit* con stati $|0\rangle$ e $|1\rangle$ (corrispondenti a spin *down* $|\downarrow\rangle$ e spin *up* $|\uparrow\rangle$) e tutte le possibili sovrapposizioni $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ il computer potrebbe avvantaggiarsi della dimensione esponenziale dello spazio di Hilbert (dimensione $q = 2^k$ per k qubits) per eseguire un *calcolo parallelo quantistico*! Le prime idee sul calcolo quantistico sono dovute a David Deutsch[24], un teorico di Oxford (alcune idee risalgono allo stesso Richard Feynman[25]). Si vede innanzitutto che esiste un gate reversibile (ovvero descritto da una trasformazione unitaria), il *controlled-NOT* (o XOR), mediante il quale con l'aggiunta dell'opera-

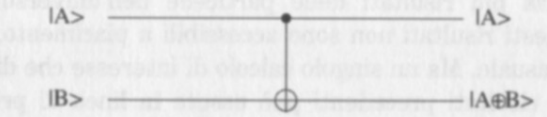

Fig. 6 – Il Controlled-NOT.

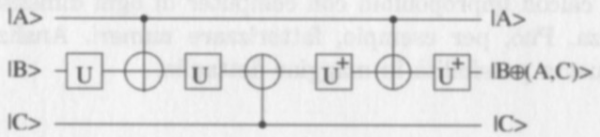

Fig. 7 – Gate di Toffoli ottenuto con gates XOR (controlled-NOT) a due bits più alcuni gates a un bit che eseguono la trasformazione $U|\downarrow\rangle = -|\uparrow\rangle$, $U|\uparrow\rangle = |\downarrow\rangle$

zione unitaria $U = \sigma_y$ (che capovolge lo spin e cambia segno alla funzione d'onda se lo spin è rivolto verso il basso) si realizza il gate di Toffoli, ottenendo di conseguenza un set universale.

Si può quindi calcolare una funzione in parallelo sullo spazio di Hilbert mediante una trasformata di Hadamard che trasforma lo stato di "reset" (con tutti i bit 0) nella sovrapposizione di tutti i possibili valori. Questa trasformazione è ovviamente unitaria. Per k qubits (dimensione $q = 2^k$ dello spazio di Hilbert) si ha

$$|0\rangle \to \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle. \tag{19}$$

Si aggiunge quindi un nuovo registro e si calcola la funzione f mediante una opportuna trasformazione unitaria U_f che dipende da f

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|0\rangle \to \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|f(a)\rangle \; . \tag{20}$$

I due registri sono ora entangled. Il computer ha in memoria tutti i risultati possibili nella sovrapposizione entangled! Si consideri che per soli $k = 140$ qubits il computer calcola e tiene in memoria più risultati delle particelle dell'universo! Purtroppo questi risultati non sono accessibili a piacimento, bensì in modo casuale. Ma un singolo calcolo di interesse che dipende da tutti i risultati precedenti può essere in linea di principio ottenuto mediante una appropriata misura quantistica sulla sovrapposizione! Il computer quantistico può eseguire in tal modo calcoli improponibili con computer di ogni dimensione o potenza. Può, per esempio, fattorizzare numeri. Analizziamo ora questa possibilità in maggior dettaglio.

5.3. *Calcolo quantistico per algoritmi complessi*

Definiamo *classe di complessità* di un algoritmo di calcolo il numero di *step* dell'algoritmo in funzione del numero di bit dell'input. Nel problema della fattorizzazione del numero N la dimensione dell'input è $\log N$, ovvero il numero di cifre di N. Il miglior algoritmo noto, una variante dell'algoritmo RSA[26], impiega un tempo di esecuzione dell'ordine di

$$O(\exp[(64/9)^{1/3}(\log N)^{1/3}(\log\log N)^{2/3}]) \; , \tag{21}$$

ovvero il tempo di calcolo cresce esponenzialmente col *size* dell'input. Facciamo un esempio per rendere l'idea. La fattorizzazione dei grandi numeri rappresenta uno dei metodi a chiave pubblica usato dai militari per comunicazioni crittografate (questo perché è molto facile costruire il prodotto di due numeri grandi a piacere, ma è difficile estrarre i fattori di un numero). Nel 1994 mediante l'algoritmo suddetto è stato fattorizzato un numero di 129 cifre, e ci sono voluti otto mesi di calcolo parallelo di 1600 workstations. Alla stessa velocità occorrerebbero 800.000 anni per un numero di 250 cifre e 10^{25} anni (molto più dell'età dell'universo!) per un numero di sole 1000 cifre. Ebbene, Peter Shor[27] ha mostrato che con un algoritmo quantistico è possibile fattorizzare in tempo polinomiale! E basterebbero pochi milioni di steps per fattorizzare un numero di 1000 cifre.

L'algoritmo RSA[26] è basato sul metodo di Riesel, che è un metodo probabilistico per trovare i fattori di un numero N dispari. Il metodo è molto semplice. Si seleziona a caso un numero $y >$ coprimo con N (cioè che ha massimo comune divisore 1 con N). Si calcola quindi il periodo r di $y \mathrm{mod} N$ (ovvero si eleva y a r e si cerca il resto della divisione per N). Se risulta $x = y^{r/2} \neq \pm 1 \mathrm{mod} N$, allora i $\gcd(N, x \pm 1)$ sono fattori non banali di N (gcd: *greatest common divisor*, denota il massimo comune divisore). Si può dimostrare che se N si fattorizza in k primi, allora la probabilità di successo è $\geq 1/2$, ed è sempre più grande per numeri grandi.

Il problema è ricondotto quindi a calcolare il periodo $y^r = 1 \mathrm{mod} N$, ovvero il periodo di una funzione. Per far questo si utilizza la trasformata di Fourier quantistica

$$DFT_q \quad |a\rangle \to \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i a c/q} |c\rangle \,, \tag{22}$$

trasformazione ovviamente unitaria, che si realizza con la semplice rete di calcolo quantistico in Fig. 8.

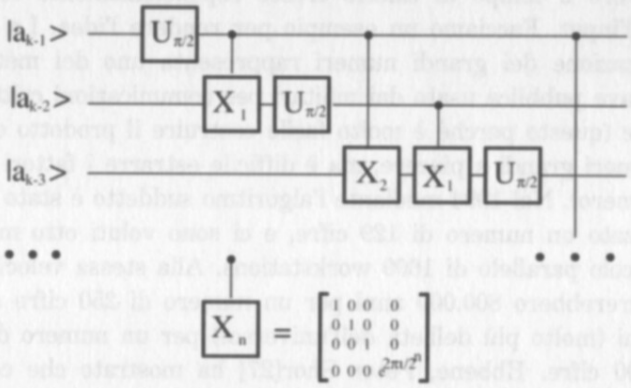

Fig. 8 – Circuito per la trasformata di Fourier quantistica basato sull'approccio della fast Fourier transform di Cöppersmith.

Si calcola la funzione f "in parallelo quantistico" mediante la trasformazione unitaria U_f nell'equazione (20), ovvero

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|0\rangle \to \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|f(a)\rangle \,. \tag{23}$$

Se ne calcola quindi la trasformata di Fourier

$$\to \frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} e^{2\pi i a c/q} |c\rangle|f(a)\rangle = \sum_{c=0}^{q-1} |c\rangle \left[\sum_{a=0}^{q-1} \frac{1}{q} e^{2\pi i a c/q} |f(a)\rangle \right] . \tag{24}$$

Se la funzione è periodica $f(a+r) = f(a)$ la somma in parentesi quadre per ogni termine entangled nell'equazione (24) *interferisce* costruttivamente solo se il numero c misurato e diviso la dimensione q dello spazio è un multiplo di $1/r$. Si ha

quindi una distribuzione di probabilità piccata sui valori 0, $1/r$, $2/r$, ..., come in Fig. 9.

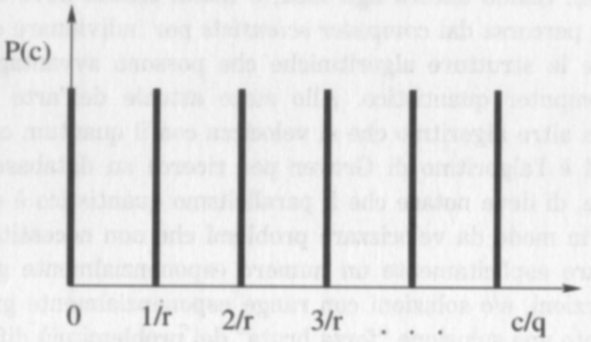

Fig. 9 – Distribuzione di probabilità del risultato della misura di c sulla trasformata di Fourier nell'equazione (24).

Per estrarre il periodo bisogna rilanciare il programma un numero di volte $\sim \log\log r/k$ per ottenere probabilità $\simeq 1$ che uno dei multipli sia coprimo di r, in modo che si possa estrarre r univocamente.

Per fattorizzare numeri occorre un numero grande di qubits $k > 2\log_2 N$. Ma per simulare un sistema quantistico di 20 spin basta un computer di soli 20 qubits (più quelli necessari per l'error correction). Ma nessun computer classico potrebbe mai eseguire una tale simulazione, in quanto occorrerebbe diagonalizzare una matrice $10^6 \times 10^6$!

Dobbiamo però cautelare facili entusiasmi sull'uso del quantum computer. Infatti, il quantum computer non è semplicemente "più veloce" del computer classico, ma permette di risolvere molto rapidamente solo problemi specifici, che si risolvono con un algoritmo particolare che può avvantaggiarsi del parallelismo quantistico. Per esempio, pur potendo eseguire il calcolo di una funzione $f \to f(a)$ in principio in una sola step (la trasformazione unitaria nell'equazione (20)), non si conosce a tutt'oggi un algoritmo quantistico che permetta di

calcolare, per esempio, la somma $\sum_a f(a)$ (come abbiamo già visto, uno solo dei risultati $f(a)$ è accessibile, e solo in modo casuale). Siamo ancora agli inizi, e molta strada deve ancora essere percorsa dai *computer scientists* per individuare e classificare le strutture algoritmiche che possono avvantaggiarsi del computer quantistico. Allo stato attuale dell'arte esiste solo un altro algoritmo che si velocizza con il quantum computer, ed è l'algoritmo di Grover per ricerca su database [28]. Inoltre, di deve notare che il parallelismo quantistico è congegnato in modo da velocizzare problemi che non necessitano di calcolare esplicitamente un numero esponenzialmente grande di soluzioni, e/o soluzioni con range esponenzialmente grande. Pertanto una soluzione "forza bruta" dei problemi più difficili – i problemi cosiddetti *NP-completi* – non può essere velocizzata. Problemi NP-completi sono quei problemi che hanno complessità esponenziale, ma la cui soluzione si verifica in tempo polinimiale. Un teorema afferma che tutti i problemi NP-completi sono equivalenti, nel senso che le rispettive soluzioni possono essere sempre connesse fra loro da un algoritmo di complessità polinomiale. Pertanto, risolvere un problema NP-completo equivale a risolverli tutti. La soluzione di un solo problema NP-completo rappresenterebbe il risultato di gran lunga più importante della storia dell'informatica, e forse fra i più importanti di tutte le scienze in genere, con impatto enorme sulla tecnologia!

H. P. Yuen [29] ha recentemente ideato un modo di utilizzare un calcolatore quantistico e la tomografia quantistica per risolvere in tempo polinomiale un problema *NP-hard* (ovvero che non ha verifica in tempo polinomiale, ma è completo, ovvero è la sua soluzione può essere connessa mediante algoritmo polinomiale a quella di un problema NP-completo). Si tratta del calcolo del *permanente* di una matrice. Il permanente $Per\mathbf{A}$ di una matrice $\mathbf{A}$ contiene gli stessi termini del determinante della matrice, ma tutti i termini sono sommati con il segno positivo

$$Per\mathbf{A} \doteq \sum_P A_{1P1} A_{1P2} \dots A_{NPN} \,. \tag{25}$$

Nell'equazione (25) la somma è calcolata su tutte le permutazioni P del secondo indice della matrice. È interessante notare come il problema del calcolo permanente, che appare a prima vista simile a quello del determinante, ha complessità esponenziale, mentre quello del determinante ha complessità polinomiale. L'algoritmo di Yuen si basa sull'idea di preparare un insieme di N sistemi identici ognuno a N livelli (il numero dei sistemi ed il numero dei livelli sono entrambi uguali a N) nello stato totalmente simmetrico

$$|\psi\rangle = \frac{1}{\sqrt{N!}} \sum_P |e_{P1}\rangle \otimes |e_{P2}\rangle \otimes \dots \otimes |e_{PN}\rangle \,, \tag{26}$$

dove $\{|e_n\rangle\}$ $n = 1 \dots N$ rappresenta una qualunque base ortonormale per il singolo sistema. Si assume ovviamente che la preparazione avvenga in modo "naturale", sfruttando una simmetria intrinseca "bosonica" della funzione d'onda (come, per esempio, in un "condensato di Bose"). Il permanente della matrice $\mathbf{A}$ è allora semplicemente il valore di aspettazione quantistico

$$Per\mathbf{A} = \langle\psi|A^{\otimes N}|\psi\rangle \,, \tag{27}$$

dell'operatore A con elementi di matrice $A_{ij} = \langle e_i|A|e_j\rangle$ uguali a quelli della matrice $\mathbf{A}$. Poiché l'operatore A non è in generale autoaggiunto, non sarà possibile eseguire una misura esatta di A. Inoltre, occorrerebbe un apparato di misura diverso per ogni matrice $\mathbf{A}$ della quale si voglia calcolare il permanente. E a questo punto viene in aiuto la Tomografia Quantistica, che è una vera tecnica di misurazione universale che permette di stimare il valore di aspettazione di un qualunque operatore (anche non autoaggiunto) dalla misura di un set (detto *quorum*) sufficientemente grande di osservabili. E l'algoritmo tomografico è polinomiale! Purtroppo, il prezzo che si paga è che l'errore statistico col quale si determina il valore di aspetta-

zione $\langle\psi|A^{\otimes N}|\psi\rangle$ mediante la Tomografia Quantistica è di per sé esponenziale in N. L'algoritmo tomografico di Yuen produce quindi solo una soluzione approssimata di un problema NP-hard, ma rimane davvero eclatante la connessione fra un problema di complessità esponenziale ed il metodo della Tomografia Quantistica!

5.4. *L'error correction quantistica*

Il grande problema che si pone nella realizzazione pratica di un calcolatore quantistico è quello della *decoerenza*, connessa alla notevole fragilità dell'entanglement, che risulta immediatamente rovinato da ogni interazione con il mondo esterno. L'effetto della decoerenza è ovviamente quello di produrre errori nel calcolo. Anche i computer tradizionali commettono errori, e per questo sono previste ed incorporate nei processori tecniche di correzione dell'errore. Ma il computer quantistico è di gran lunga più suscettibile ad errori di quello classico! Benché allo stato attuale delle nostre conoscenze sembra che non si ponga nessun limite fondamentale all'isolamento di un sistema quantistico dal circondario, non di meno un tale isolamento resta un problema tecnologico tremendamente difficile.

Perché allora non sviluppare tecniche di correzione degli errori? Le difficoltà sono molteplici: a) Benché le tecniche di correzione degli errori abbiano raggiunto un livello di sofisticazione notevole nei computer digitali, non è per nulla ovvio come tali metodi possano essere adattati alla correzione di *errori di fase*, la piaga dei sistemi quantistici; b) In un computer quantistico, come in un computer analogico, gli errori si accumulano nel tempo e alla fine si sommano a dare errori grandi; c) Per correggere un errore dobbiamo prima acquisirne l'informazione sull'accadimento, per esempio eseguendo una misura. Ma c'è il pericolo che la misura distrugga la delicata informazione quantistica codificata nel computer (la misura fatta su un qubit rompe inevitabilmente l'entanglement con gli altri qubit); d) Per proteggerla da errori si dovrà codificare l'informazione in modo ridondante. Ma il teorema del no-cloning ci dice che l'informazione codificata sullo stato quantistico non può essere copiata, cosicché non è per nulla ovvio come l'informazione possa essere memorizzata con la necessaria ridondanza.

E qui il risultato eclatante: l'*error correction quantistica* è possibile! (P. Shor 1995[30], A. Stean 1996[31], A. Ekert and C. Macchiavello[32]). L'idea base del metodo è il *dictum* "combattere l'entanglement con l'entanglement", ovvero: 1) Aggiungere qubits ed allargare lo spazio di Hilbert in modo che gli errori guidino il calcolatore su spazi ortogonali; 2) Eseguire una misura che dica in quale spazio si trova il calcolatore a seguito dell'errore; 3) Fare una trasformazione unitaria che dipende dal risultato della misura, allo scopo di correggere l'errore. Si noti che la misura diagnostica dell'errore non deve fornire nessuna informazione sui qubits usati per il calcolo. Ciò è analogo a quanto avviene nel teletrasporto, secondo lo schema generale: entanglement + misura non informativa + trasformazione unitaria che dipende dal risultato. Anche nel settore dell'error correction quantistica siamo solo agli inizi, e molta attività di ricerca è in corso sulla computazione quantistica *fault tolerant*, che rappresenta il punto chiave nella realizzazione di un quantum computer di utilità pratica.

5.5. *Candidati fisici al quantum computer*

Nella realizzazione sperimentale del quantum computer si intravedono vari possibili candidati, con il qubit codificato su due diverse polarizzazioni della luce, o su due diversi livelli elettronici o di spin nucleare. I migliori candidati sono attualmente considerati atomi/ioni raffreddati con luce laser in trap-

pole ioniche o magneto-ottiche (o atomi di Rydberg viaggianti a bassissima velocità in cavità a microonde). Negli ultimi anni si è avuta una vera e propria *escalation* di "laser cooling", attraverso prima il cooling Doppler di atomi di sodio intrappolati all'intersezione di sei fasci laser, quindi in trappole magneto-ottiche dove bobine magnetiche producono rallentamento Zeeman. Il limite Doppler è stato infine battuto con l'effetto Sisifo. Poi si è superato il "limite di rinculo", mettendo atomi di elio in uno stato "dark" in cui l'atomo non assorbe o emette fotoni, raggiungendo la temperatura di $0.18\mu K$, che corrisponde ad una velocità degli atomi di soli di 2cm/sec. Nel 1997 il Nobel per la Fisica è stato assegnato per il laser cooling a Steven Chu (Standford CA), Claude Cohen-Tannudji (College de France e Ecole Normale Supérieure di Parigi) e William Phillips (del NIST di Goithersburg MA). Il limite è poi stato successivamente battuto varie volte, e si parla ora di $30nK$ o ancora meno. Particolarmente promettenti sembrano i reticoli ottici, in cui atomi raffreddati in cavità sono ordinati in una fila unidimensionale in un potenziale periodico effettivo Stark dovuto a campi stazionari in cavità. Atomi in diversi stati sentono potenziali differenti, e possono essere spostati selettivamente ruotando la polarizzazione dell'onda stazionaria, come con una manovella (si realizzano così "collisioni fredde"). Si parla anche di utilizzare "quantum dots" e "squid" (superconducting quantum interference devices). Ma il metodo più efficace, anche se condannato a funzionare solo per pochi qubit, è la Risonanza Magnetica Nucleare (NMR), dove è possibile eseguire con semplicità varie trasformazioni unitarie sugli spin nucleari, utilizzando la tecnica degli impulsi di Rabi e il "chemical shift" su molecole in liquidi, con tempi di decoerenza lunghi rispetto al tempo del calcolo. La misura finale di magnetizzazione è simile ad una Tomografia Quantistica eseguita su molte molecole simultaneamente: ogni molecola riesegue il calcolo come un quantum computer autonomo. Gruppi impegnati nelle implementazioni sperimentali di quantum computers sono ancora una volta quello di Jeff Kimble al Caltech di Pasadena (atomi iniettati in cavità), quello di Serge Haroche all'Ecole Normale Superiéure di Parigi (cavity QED, con atomi iniettati in cavità di nobio superconduttore ad alto Q), quello di Dave Wineland al NIST di Boulder in Colorado (trappole di Paul ioniche), il gruppo di Neil Gershenfeld al MIT (NMR), quello di Ike Chuang a Standford (NMR), e quello di Herbert Walther al Max Planck di Monaco (cavity QED, trappole ioniche). Per delle semplici rassegne divulgative sui quantum computer si vedano i testi [33,34,35]. Per una serie di rassegne più avanzate si veda [36,37].

6. *Tomografia Quantistica*

Ma veniamo ora alla Tomografia Quantistica. Si tratta di un metodo per misurare lo stato di un sistema quantistico che abbiamo sviluppato a Pavia [38] (in una fase intermedia ho collaborato con Ulf Leonordth e Harry Paul al Max Planick di Berlino[39]). Il primo metodo [38] – detto Tomografia Quantistica Omodina – riguardava solo lo stato della radiazione, e permette di determinarne lo stato mediante misure omodina ripetute su un ensemble di stati di radiazione identicamente preparati (per una rassegna tecnica si veda il riferimento [40]). Esso utilizza la tecnica di rivelazione omodina a fase variabile (allo *scanning* in fase si deve il nome "Tomografia"). Si può misurare anche una qualunque osservabile della radiazione[41,42,43]. Il metodo funziona anche con un numero arbitrario di modi della radiazione[44], ed è ora in uso in molti laboratori. Michael Raymer (Oregon, Eugene) – che ha eseguito il primo esperimento pionieristico[45] ancora prima che si sviluppasse la teoria – ha recentemente utilizzato il metodo per misure di correlazione della luce emessa da un laser semiconduttore su scale di tempi del subpicosecondo [46]. Il gruppo di Costanza ha pubblicato interessanti esperimenti su Na-

ture[47]. Con Prem Kumar alla Northwestern abbiamo misurato lo stato da emissione spontanea parametrica (il twin beam)[48], e ora stiamo progettando un nuovo esperimento per verificare la riduzione di stato al cambio di osservabile[49]. Con Yanhua Shih a Baltimora stiamo progettando un esperimento per vedere lo stato GHZ [50], una delle verifiche più stringenti dell'inadeguatezza della descrizione classica della misura [51]. La tecnica della Tomografia Quantistica Omodina permette l'osservazione di *gatti di Schrödinger* della radiazione[52], e potrebbe infine ricoprire un interesse strategico nelle future tecnologie fotoniche come metodo di caratterizzazione quantica di dispositivi e di materiali ottici non lineari[53]. Recentemente la tecnica è stata generalizzata a sistemi quantistici arbitrari[54], permettendo la ricostruzione dello stato di spin di una particella, ed, in principio, dello stato di un qualsiasi sistema quantistico.

In sintesi, il metodo della Tomografia Quantistica si basa sulla possibilità di stimare la media di ensemble $\langle A\rangle$ di un qualsiasi operatore A (generalmente non osservabile) di un sistema quantistico mediante misure ripetute di un insieme esaustivo – detto *quorum* – di osservabili Q_λ, dove $\lambda\in\Lambda$ è una variabile casuale in un insieme Λ. Si estrae a caso un valore di λ e se ne misura l'osservabile corrispondente Q_λ. La media di ensemble $\langle A\rangle$ viene quindi ottenuta per mezzo di un opportuno estimatore $\mathcal{E}[A]$ (che dipende da A ed è funzione di Q_λ) che viene mediato sia sull'ensemble che sul quorum, come segue

$$\langle A\rangle = \int_\Lambda d\mu(\lambda)\langle \mathcal{E}[A](Q_\lambda)\rangle \ . \tag{28}$$

La determinazione dei possibili quorum e dell'estimatore rappresenta il compito del fisico teorico: il fisico sperimentale dovrà implementare la misurazione delle osservabili Q_λ. Esistono infinite scelte del quorum di osservabili Q_λ, con l'opportunità di utilizzare insiemi di osservabili effettivamente misurabili sperimentalmente. Una tecnica generale permette anche

di eliminare gli errori sistematici derivanti da ogni tipo di rumore nella misurazione[54], come quello dovuto alla limitata efficienza quantica dei rivelatori della radiazione. Si noti che una volta collezionato un numero sufficientemente grande di misure di diversi Q_λ, dallo stesso *file* di dati si può estrarre la media di ensemble $\langle A\rangle$ per qualunque operatore A desiderato! Il prezzo che si paga per l'universalità del metodo è che l'errore statistico nella determinazione finale risulta ovviamente più grande di quello che si otterrebbe nella misura di un'unica osservabile. Recenti tecniche "adattative" permettono di ridurre l'errore statistico al minimo, mentre tecniche basate sul metodo della massima verosimiglianza[56] permettono una riduzione considerevole dell'errore statistico, al prezzo dell'introduzione di un piccolo errore sistematico (noto), e di restringere la tecnica alla sola determinazione della matrice densità[42,43]. In tal modo si arriva ad una riduzione fino a $10^4 \div 10^5$ volte del numero di dati sperimentali necessari per ottenere un errore statistico desiderato, rendendo possibili esperimenti con efficienze molto basse di produzione degli stati dell'ensemble.

7. *Conclusioni e prospettive future*

È difficile fare delle previsioni sul futuro delle nuove tecniche di Informatica Quantistica. Anche se sono già disponibili prototipi di quantum computers basati su spettrometri NMR, è difficile immaginare la realizzazione in tempi brevi di computer quantistici che lavorino con alcune decine – o addirittura un centinaio – di qubit, in quanto allo stato attuale delle conoscenze si presume che essi debbano funzionare con reticoli ottici, ed il problema dell'isolamento dal circondario (pur considerata la possibile implementazione di tecniche di correzione degli errori) sembra a tutt'oggi quasi insormontabile. Per ora, si parla di realizzare appena due qubit in uno stato entangled!

Altrettanto difficile risulta l'implementazione di un teletrasporto quantistico di un sistema esteso o composito. Qui il problema maggiore è rappresentato dalla misurazione quantistica di Bell che deve essere condotta su tutto il sistema congiuntamente. Per esempio, non si conosce attualmente nemmeno una tecnica per teletrasportare un singolo atomo di idrogeno, ed una vera tecnica di teletrasporto dovrebbe funzionare invariabilmente in modo indipendente dal tipo di sistema (ovvero dalla sua composizione chimica). In altri settori, quali la crittografia quantistica, i progressi tecnici hanno invece già raggiunto la fase applicativa. Con le tecniche di crittografia quantistica (che non sono state illustrate in questa memoria: si veda, ad esempio, il riferimento [37]), è possibile una comunicazione crittografata sulla base di leggi fisiche – anziché su algoritmi matematici – con l'impossibilità di principio di decriptare il messaggio in un qualunque lontano futuro (si noti che l'algoritmo RSA[26] potrebbe essere violato da un futuro metodo di fattorizzazione oggi sconosciuto). Si eseguono già comunicazioni crittografiche in fibra ottica a distanze superiori a 10km (si veda l'esperimento condotto sotto il lago di Ginevra [57]) e comunicazioni in aria a distanza di alcuni km, in piena luce solare, estraendo un singolo fotone del canale di trasmissione con tecniche di selezione temporale ed di frequenza (esperimenti del gruppo di Richard Huges e di Paul Kwiat a Los Alamos: queste tecniche saranno prossimamente utilizzate per cambiare la password sui satelliti per telecomunicazioni). La tecnica di tomografia quantistica, d'altro canto, è ora completamente matura, ed è entrata nella fase di applicazione sperimentale sistematica.

Per quanto riguarda l'implementazione di nuove misure congiunte – allo scopo di realizzare misure di Bell congiunte per il teletrasporto quantistico di sistemi estesi o compositi – è in fase di studio una nuova tecnica basata sul *cloning quantistico ottimo* (si rammenta che il cloning *perfetto* è vietato dal teorema del nocloning già citato). Recentemente si è visto che

questa tecnica permette la misura congiunta ottimale in alcuni schemi di misurazione. D'altro canto, il cloning ottimo potrebbe essere anche la base per nuove tecniche di correzione quantistica degli errori.

REFERENCES

[1] R.E. Slusher, L.W. Hollberg, B. Yurke, J.C. Mertz, and J.F. Valley, Phys. Rev. Lett. **55** 2409 (1985); R.E. Slusher, and B. Yurke, J. Lightwave Tech. **8** 466 (1990).

[2] G.M. D'Ariano and P. Kumar, *A quantum-mechanical study of optical regenerators based on nonlinear-loop mirrors*, IEEE Photonics Technology Letters, **10** 699 (1998).

[3] S.S. Schweber, *QED and the Men who made it: Dyson, Feynman, Schwinger, and Tomonaga*, Princeton University Press (Princeton 1994).

[4] P.A.M. Dirac, *Principles of Quantum Mechanics, 4th Ed.*, (Oxford University Press, London, 1954).

[5] J. von Neumann, *Mathematical Foundations of Quantum Mechanics* Princeton University Press, (Princeton 1955).

[6] Nonostante l'ovvietà dell'impossibilità di comunicare superluminale mediante entanglement, questo metodo (fallace) è stato addirittura oggetto di un brevetto! Si veda: N. Herbert, *Found. Phys.* **12**, 1171 (1982). Sull'impossibilità delle comunicazioni superluminali nonostante la nonlocalità si veda anche: G.C. Ghirardi, A. Rimini and T. Weber, Lett. Nuovo Cim. **27** 263 (1980), e più recentemente D. Brus, G.M. D'Ariano, C. Macchiavello, and M.F. Sacchi, Phys. Rev., A **62**, 062302 (2000).

[7] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev., **47**, 777 (1935).

[8] S. Bell, *Speakable and unspeakable in quantum mechanics*, Cambridge University Press (Cambridge 1987); si veda anche: J.F. Clauser, M. Horne, A. Shimony, and R.A. Holt, Phys. Rev. Lett. **23** 880 (1969).

[9] A. Apostolakis *et al.*, Phys. Lett. B **422** 339 (1998).

[10] G.C. Ghirardi, *Un'Occhiata alle Carte di Dio*, il Saggiatore (Milano 1997).

[11] W.K. Wootters, W.H. Zurek, Nature **299**, 802 (1982). In questa referenza si mostra che la cloning machine viola la *linearità*. Comunque, in principio, questo non implica la violazione dell'unitarietà, la quale è l'assunzione più basilare della Meccanica Quantistica: questo è dimostrato nel Rif. [12]. Si veda anche il Rif. [13].

[12] H.P. Yuen, Phys. Lett. A**113** 405 (1986).

[13] G.M. D'Ariano and H.P. Yuen, Phys. Rev. Lett. **76** 2832 (1996).

[14] È possibile "preparare" un sistema in uno stato qualsivoglia, ovviamente senza violare le regole di "superselezione" connesse all'indistinguibilità delle particelle identiche. Ciò richiede che bosoni identici debbano sempre essere in una funzione d'onda simmetrica per permutazione delle particelle, mentre per i fermioni la funzione d'onda è antisimmetrica.

[15] O. Alter, and Y. Yamamoto, Phys. Rev. Lett. **74**, 4106 (1995); Y. Aharonov, J. Anandan, L. Vaidman, Phys. Rev. A **47**, 4616 (1993); Y. Aharonov and L. Vaidman, Phys. Lett. A **178**, 38 (1993); M. Ueda and M. Kitagawa, Phys. Rev. Lett. **68**, 3424 (1992); A. Imamoglu, Phys. Rev. A **47**, R4577 (1993); A. Royer, Phys. Rev. Lett. **73**, 913 (1994).

[16] D. Boschi, S. Branca, F. De Martini, L. Hardy and S. Popescu, Phys. Rev. Lett. **80** 1121 (1998).

[17] D. Boumeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, Nature (London) **390** 575 (1997).

[18] S.L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80** 869 (1998).

[19] A. Furasawa, J.L. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble and E.S. Polzik, Science **282** 706 (1998).

[20] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wooters, Phys. Rev. Lett. **70**, 1895 (1993).

[21] S.L. Braunstein, G.M. D'Ariano, G.J. Milburn, and M.F. Sacchi, Phys. Rev. Lett. **84** 3486 (2000).

[22] R. Landauer, IBM J. Res. Dev. **5** 183 (1961).

[23] C. Bennet, IBM J. Res. Dev. **17** 525 (1973).

[24] D. Deutsch, Proc. R. Soc. Lond. A **400** 97 (1985).

[25] R.P. Feynman, Int. J. Theor. Phys. **21** 467 (1982).

[26] R. Rivest, A. Shamir and L. Adleman, "On Digital Signatures and Public-Key Cryptosystems, *MIT Laboratory for Computer Science Technical Report*, MIT/LCS/TR-212 (January 1979).

[27] P.W. Shor, p. 124 in *Proceedings pf the 35th Annual Symposium of the Foundations of Computer Science*, ed. S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA, 1994).

[28] L.K. Grover, p. 212 in *Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC)*, (May 1996), preprint quant-ph/9605043; Phys. Rev. Lett. **79**, 325 (1997).

[29] H.P. Yuen, in *Quantum Communication, Computing, and Measurement*, Edited by P. Kumar, G. M. D'Ariano, and O. Hirota, Kluwer Academic/ Plenum Publishers (New York and London 2000), p. 249.

[30] P.W. Shor, Phys. Rev. A **52** 2493 (1995).

[31] A.M. Steane, Proc. R. Soc. Lond. A **452** 2551 (1996).

[32] A. Ekert and C. Macchiavello, Phys. Rev. Lett **77** 2585 (1996).

[33] G.J. Milburn, *Schrödinger's Machines*, Freeman & Co. (New York 1997).

[34] G.J. Milburn, *Feynmann Processors*, Perseus Books, Allen & Unwin Pty Ldt, (Sydney 1998).

[35] D. Deutsch, *The Fabric of Reality*, Penguin Books (New York 1998).

[36] M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge Univ. Press, Cambridge 2000).

[37] *Introduction to Quantum Computation and Information*, Ed. by H.-K. Lo, S. Popescu, T. Spiller, World Scientific (Singapore 1998).

[38] G.M.D'Ariano, C. Macchiavello and M.G.A. Paris, Phys. Rev. A **50** 4298 (1994).

[39] G.M. D'Ariano, U. Leonhardt and H. Paul, Phys. Rev. A **52** R1801 (1995).

[40] G.M. D'Ariano, *Measuring Quantum States*, in *Quantum Optics and Spectroscopy of Solids*, ed. by T. Hakioğlu and A. S. Shumovsky, (Kluwer Academic Publisher, Amsterdam 1997), p. 175-202.

[41] G.M. D'Ariano, *Homodyning as universal detection*, in *Quantum Communication, Computing, and Measurement*, Edited by O. Hirota, A. S. Holevo, and C. M. Caves, Plenum Publishing (New York and London 1997), p. 253.

[42] Si potrebbe pensare che la determinazione sperimentale della sola matrice densità sia sufficiente a determinare una media di ensemble qualsivoglia $\langle A \rangle$. Ma per spazi di Hilbert infinito-dimensionali, ciò non è possibile, in quanto l'errore sperimentale sugli elementi di matrice dello stato si "propaga" nella determinazione dell'errore su $\langle A \rangle$ attraverso una serie generalmente non convergente [43].

[43] G.M. D'Ariano and C. Macchiavello, Phys. Rev. A **57** 3131 (1998).

[44] G. D'Ariano, P. Kumar, M. Sacchi, Phys. Rev. A **61**, 13806 (2000).

[45] D.T. Smithey, M. Beck, M.G. Raymer, and A. Faridani, Phys. Rev. Lett. **70**, 1244 (1993).

[46] D.F. McAlister, M.G. Raymer, Phys. Rev. A. **55** R1609 (1997).

[47] G. Breitenbach, S. Schiller, and J. Mlynek, Nature **387**, 471 (1997); C. Kurtsiefer, T. Pfau, and J. Mlynek, Nature **386**, 150 (1997).

[48] M. Vasilyev, S.-K. Choi, P. Kumar, and G.M. D'Ariano, Phys. Rev. Lett. **84** 2354 (2000).

[49] G.M. D'Ariano, P. Kumar, Macchiavello, L. Maccone, and N. Sterpi, Phys. Rev. Lett. **83** 2490 (1999).

[50] G.M. D'Ariano, M. Sacchi, M. Rubin, and Y. Shih, Fortschr. Phys. **48**, 599 (2000).

[51] D.M. Greenberger, M.A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, M. Kafatos, Ed. (Kluwer, Dordrecht 1989) p. 69.

[52] G.M. D'Ariano, C. Macchiavello and L. Maccone, Phys. Rev. A **59** 1816 (1999).

[53] G.M. D'Ariano and L. Maccone, Phys. Rev. Lett. **80** 5465 (1998).

[54] G.M. D'Ariano, *Universal quantum estimation*, Phys. Lett. A **268** 151 (2000).

[55] G.M. D'Ariano and M.G.A. Paris, Phys. Rev. A **60** 518 (1999).

[56] K. Banaszek, G.M. D'Ariano, M.G.A. Paris, M. Sacchi, Phys. Rev A **61**, 010304 (2000) (rapid communication)

[57] W. Tittel, J. Brendel, H. Zbiden, and N. Gisen, Phys. Rev. Lett. **81**, 3563 (1998).