

1

FISICA DELLA COMPUTAZIONE E MODELLI ALTERNATIVI DI COMPUTER

I – PORTE LOGICHE UNIVERSALI

La logica standard del computer è costruita su un numero di limitato di porte logiche. Le più comuni sono le porte: AND, OR e NOT. La porta NOT è indicata con una barra sul bit di input e cambia il valore del bit originale. Ciò vuol dire che $\text{NOT}(A) \equiv \bar{A}$ è uguale a 1 se $A = 0$ e a 1 se $A = 1$.

Le tabelle delle verità associate alle porte AND e OR sono riportate in Tab. ???. Tradizionalmente l'operazione logica AND su due bit A e B viene indicata alternativamente come $A \text{ AND } B$ oppure con il simbolo \wedge , ovvero $A \text{ AND } B \equiv A \wedge B$. Il risultato della porta AND può essere espresso anche in termini di operazioni decimali (più comuni). In particolare, $A \text{ AND } B = A \cdot B$ dove $A \cdot B$ è l'usuale moltiplicazione decimale. Infatti, se gli input A e B sono binari (assumono solo i valori 0 e 1), $A \cdot B = 1$ solo se entrambi A e B sono uguali a 1 mentre sarà 0 in tutti gli altri casi.

L'operazione logica OR viene indicata come $A \text{ OR } B$ oppure con il simbolo \vee , ovvero $A \text{ OR } B \equiv A \vee B$.

L'insiemi di AND e NOT oppure di OR e NOT sono insiemi universali. Questo significa che, ad esempio, usando porte solo combinazioni di porte AND e NOT è possibile implementare una qualsiasi funzione booleana [[Feynman Lectures Computation, Functional completeness](#)].

Ci sono anche delle singole porte logiche universali che cominate opportunamente permettono di implementare una qualsiasi funzione booleana. Queste sono le porte NAND e NOR. La porta NAND o *negative-AND* è costituita da una porta AND seguita da una porta NOT quindi $A \text{ NAND } B = \overline{A \wedge B}$. In maniera analoga la porta NOR o *negative-OR* è costituita da una porta OR seguita da una porta NOT quindi $A \text{ NOR } B = \overline{A \vee B}$. Le tabelle delle verità associate alle porte AND e OR sono riportate in Tab. ?? e Tab. ??.

A	B	$A \text{ AND } B$	$A \text{ NAND } B$
0	0	0	1
1	0	0	1
0	1	0	1
1	1	1	0

A	B	$A \text{ OR } B$	$A \text{ NOR } B$
0	0	0	1
1	0	1	0
0	1	1	0
1	1	1	0

Table 1: Tabella delle verità per le porte AND, NAND, OR e NOR.

Per utilizzo futuro, introduciamo anche la porta *exclusive OR* o XOR la cui tabella delle verità è mostrata Tab. 2. Anche l'operatore XOR può essere associato ad un'operazione decimale indicata con il simbolo \oplus : $A \text{ XOR } B \equiv A \oplus B$. L'operatore \oplus denota la somma modulo 2; ovvero, $A \text{ XOR } B \equiv A \oplus B = A + B \text{ (mod 2)}$. Infatti,

essendo A e B binari la loro somma è 0 se $A = B = 0$, è 1 se $A = 0$ e $B = 1$ o $A = 1$ e $B = 0$. Nel caso $A = B = 1$, la loro somma decimale è 2 ma visto che l'operazione è modulo 2, $A + B \pmod{2} = 0$.

A	B	A XOR B
0	0	0
1	0	1
0	1	1
1	1	0

Table 2: Tabella delle verità della porta XOR.

1.1.1 Porte logiche reversibili

Pur formando dei set universali, le porte AND, OR, NAND e NOR sono però *irreversibili*. Questo perchè ricevono due bit di input ma generano un solo bit di output. Dunque parte dell'informazione iniziale viene persa.

A livello concettuale è interessante introdurre delle porte logiche che siano *reversibili*. Questo vuol dire che se combiniamo in sequenza una porta logica reversibile con la sua inversa, riotteniamo l'informazione originale (ad esempio, la stringa di bit di input). Le porte reversibili devono avere necessariamente un uguale numero di input e output.

Esiste una porta logica che è allo stesso tempo reversibile e universale. Venne proposta nel 1982 da Fredkin e Toffoli [Fredkin-Toffoli]. La sua tabella delle verità è riportata in Tab. 3 e mostrata in figura 1. La porta di Fredkin può essere interpretata come uno *switch* controllato di bit. Il bit di controllo è A ; se questo è acceso i bit B e C vengono scambiati altrimenti vengono lasciati identici.

In altre parole, il bit di output $O_1 = A$ per ogni combinazione di input. Se $A = 0$, $O_2 = B$ e $O_3 = C$. Se invece $A = 1$, $O_2 = C$ e $O_3 = B$.

Per dimostrare l'universalità della porta di Fredkin è sufficiente dimostrare che una delle porte universali NAND o NOR può essere costruita con una combinazione di porte di Fredkin. Dalla tabella 3, si può notare che se il bit C è fissato a 1, l'output O_2 è equivalente a una porta OR applicata sui bit A e B . Ovvero, se $C = 1$, $O_2 = A \vee B$. In maniera analoga, notiamo che se fissiamo i bit $B = 0$ e $C = 1$, l'output O_3 è la negazione dell'input A ; se $B = 0$ e $C = 1$, $O_3 = \bar{A}$.

Visto che fissando i bit di input è possibile ottenere una porta OR e una porta NOT da una porta di Fredkin, è sufficiente combinarne due per ottenere una porta NOR. Il modo è mostrato in Figura 2. Gli input sono A e B mentre nella prima porta il bit C è fissato a 1. Il secondo output della prima porta fi Fredkin diventa il bit di controllo della seconda porta dove i bit di input B e C sono fissati a 0 e 1, rispettivamente.

A	B	C	Out1	Out2	Out3
0	0	1	0	0	1
1	0	1	1	1	0
0	1	1	0	1	1
1	1	1	1	1	1
0	0	0	0	0	0
1	0	0	1	0	0
0	1	0	0	1	0
1	1	0	1	0	1

Table 3: Tabella delle verità per la porta di Fredkin.

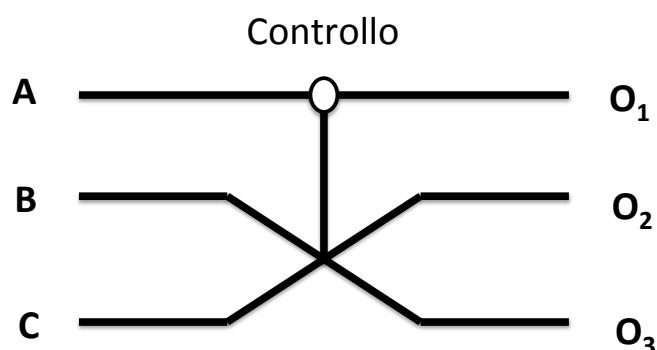


Figure 1: La porta di Fredkin schematizzata come uno switch controllato.

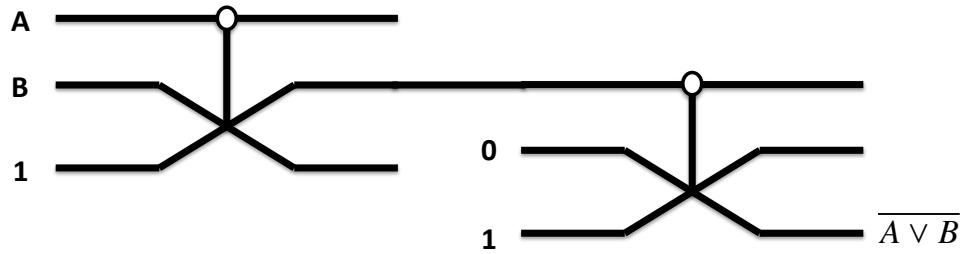


Figure 2: La composizione di due porte di Fredkin può generare una porta NOR.

II – OPERAZIONI BIT-A-BIT

Se invece di singoli bit abbiamo delle stringhe di bit, possiamo comunque manipolarle, sommare o moltiplicarle. Queste operazioni saranno utili in seguito quando parleremo degli algoritmi quantistici. Prima però è importante ricordare come si associa ad un intero una stringa di bit.

Consideriamo uno spazio logico generato da n bit. A una stringa di n bit possiamo associare un intero compreso fra 0 e $N - 1$ (associati rispettivamente alle stringhe 000...00 e 111...11) con $N = 2^n$. Al crescere di n lo spazio logico cresce esponenzialmente come 2^n . In genere, è possibile passare da un intero alla una stringa di n bit (con n opportuno) nel seguente modo. All'intero x associamo la stringa di bit $x_1x_2\dots x_n$ con $x_i = 0, 1$ e $i = 0, 1, \dots, n$ tale che $x = x_12^{n-1} + x_22^{n-2} + \dots + x_n2^0$ [nielsen-chuang_book]. Con questa notazione, tradizionalmente usata in informatica, possiamo codificare $N = 2^n$ interi ma questi saranno compresi fra 0 e $N - 1 = 2^n - 1$.

Ad esempio, per rappresentare in forma binaria il numero $x = 3$ abbiamo bisogno di 3 bit (la dimensione dello spazio totale sarà 8 e potremo codificare gli interi $0 \leq x \leq 7$). Possiamo scrivere $x = 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 3$ da cui otteniamo che la stringa associata a è $x = 011$. La stringa $x = 101$ sarà associata all'intero $x = 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 5$.

1.2.1 Prodotto interno bit-per-bit

Date due stringhe a n bit, $x = x_1, x_2, \dots, x_n$ e $z = z_1, z_2, \dots, z_n$, indichiamo con $x \cdot z$ il prodotto interno (o scalare) bit-per-bit, modulo 2. Questo equivale a

$$x \cdot z \equiv x_1z_1 + x_2z_2 + \dots + x_nz_n \pmod{2} \quad (1.2.1)$$

Il prodotto $x \cdot z$ è binario e può assumere i valori 0 o 1. È anche chiamato prodotto AND *bitwise* perché si ottiene prendendo le operazioni AND fra i singoli bit.

Si noti che in fisica e matematica l'operazione AND *bitwise* ricorda il prodotto scalare fra due vettori.

1.2.2 Somma bit-per-bit: *bitwise XOR*

Date due stringhe a n bit, $x = x_1, x_2, \dots, x_n$ e $z = z_1, z_2, \dots, z_n$, indichiamo con $x \oplus z$ la somma bit-per-bit, modulo 2. Il risultato questa volta è una stringa il cui i -esimo bit ha il valore $x_i + z_i \pmod{2} = x_i \text{ XOR } z_i$. Ovvero

$$\begin{aligned} x \oplus z &\equiv x_1 + z_1 \pmod{2}, x_2 + z_2 \pmod{2}, \dots, x_n + z_n \pmod{2} \\ &= x_1 \text{ XOR } z_1 \pmod{2}, x_2 \text{ XOR } z_2 \pmod{2}, \dots, x_n \text{ XOR } z_n. \end{aligned} \quad (1.2.2)$$

Anche questo caso, c'è un'analogia con la fisica e matematica dato che l'operazione XOR *bitwise* ricorda la somma fra due vettori.

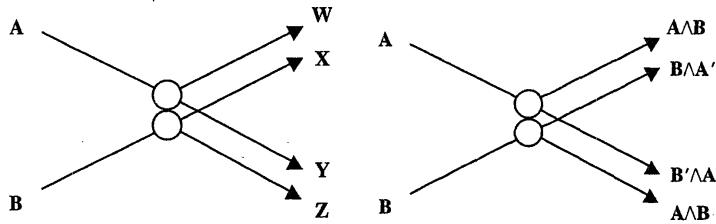


Figure 3: La porta elementare della porta di collisione del computer a palle di biliardo. A sinistra è mostrato lo schema fisico mentre a destra è mostrata la relazione logica fra input e output. L'immagine è presa da [FeynmanLecturesComputation] e il l'apice indica la negazione: $A' = \bar{A}$.

III – COMPUTER E BILIARDO

Lo studio delle porte logiche elementari, universali e reversibili ci permette di descrivere un'implementazione singolare di un computer [FeynmanLecturesComputation]. Gli stessi Fredkin e Toffoli proposero un computer costruibile con palle da biliardo [Fredkin-Toffoli]. Sebbene l'idea sia puramente teorica ci permette di comprendere che il calcolo o la manipolazione dei dati e dell'informazione può essere svolta con strumenti differenti da quelli a cui siamo abituati.

Dalla nostra discussione precedente, è chiaro che qualsiasi sistema in cui si possano implementare delle porte logiche universali può essere usato per costruire un computer altrettanto universale.

Una porta logica di un computer a palle di biliardo è mostrata in Figura 4. Due palle da biliardo sulla sinistra e costituiscono gli input logici. La presenza di una palla da biliardo è associata all'input 1 mentre la sua assenza è associata all'input 0. Le palle da biliardo possono proseguire il loro moto in linea retta o urtarsi nel centro.

Supponiamo che gli urti delle palle da biliardo siano elastici (l'energia è sempre conservata) e idealmente precisi. Una descrizione dettagliata del processo fisico implicherebbe l'introduzione del concetto di quantità di moto (o momento) e della sua conservazione. Qui ci limiteremo ad usare l'intuizione e le osservazioni della vita quotidiana.

Se non ci sono palle, $A = 0$ e $B = 0$ e la dinamica è banale dato che tutti gli output saranno nulli $W = 0$, $X = 0$, $Y = 0$ and $Z = 0$. Se c'è una palla inizialmente in A e nessuna in B (a livello logico diremo che $A = 1$ e $B = 0$), questa proseguirà il suo moto uscendo nel punto Y . Negli altri punti W , X , Z non ci saranno palle. In termini, logici per $A = 1$ e $B = 0$ abbiamo $W = 0$, $X = 0$, $Y = 1$ e $Z = 0$. In maniera analoga, se $A = 0$ e $B = 1$ otteniamo $W = 0$, $X = 1$, $Y = 0$ e $Z = 0$. In fine, se $A = 1$ e $B = 1$, le due palle urteranno e usciranno dai canali W e Z mentre gli altri saranno vuoti. In termini di logica abbiamo che per $A = 1$ e $B = 1$, $W = 1$, $X = 0$, $Y = 0$ and $Z = 1$. Concludiamo che se vogliamo che la porta agisca come un AND basterà osservare l'output in W o Z . Gli output in X equivalgono alla porta $B \wedge \bar{A}$ mentre quelli in Y a $\bar{B} \wedge A$. I risultati sono riportati in tabella 4.

A	B	$W = A \wedge B$	$X = B \wedge \bar{A}$	$Y = \bar{B} \wedge A$	$Z = A \wedge B$
0	0	0	0	0	0
1	0	0	0	1	0
0	1	0	1	0	0
1	1	1	0	0	1

Table 4: Tabella delle verità per la porta fondamentale di un computer a palle di biliardo.

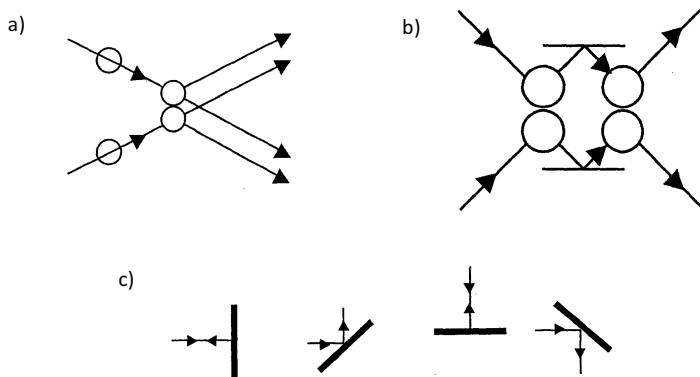


Figure 4: Le porte logiche a) *collision gate*, b) *crossover gate* e c) quattro *redirection gates*.

La porta logica discussa deve essere affiancata da altre operazioni mostrate in Fig. 4. Sono la *collision gate*, una *crossover gate* e quattro *redirection gates* [FeynmanLecturesComputation]. Nella prima due palle da biliardo sono piazzate (e in quiete) al centro e vengono urtate da quelle che definiscono gli input logici. A due palle da biliardo entranti corrispondono quattro uscenti. A livello logico questa porta non è rilevante ma diventa fondamentale a livello fisico per ridirezionare le palle da biliardo. L'operazione di reindirizzamento è completata dalle quattro *redirection gates* mostrate in Fig. 4.

Con questi elementi possiamo costruire porte logiche sempre più complicate. Ad esempio, in Fig. 4 b) è mostrata una *crossover gate* che scambia gli input. Più precisamente, lo stato 10 viene trasformato in 01 (leggendo gli input dall'alto verso il basso) e viceversa. Naturalmente, gli input simmetrici 00 o 11 rimangono gli stessi.

Le porte logiche ottenute fino ad ora sono sufficienti per avere un computer universale. Tuttavia possiamo fare un passo ulteriore e mostrare che è possibile implementare anche la porta di Fredkin e quindi un computer universale e reversibile. In questo caso, l'implementazione è molto più complicata ed è mostrata in figura 5.

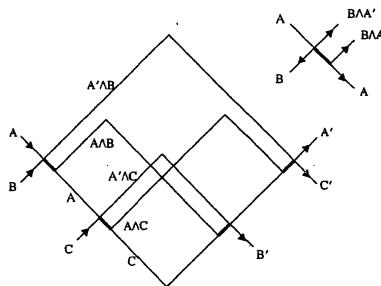


Figure 5: Implementazione della porta di Fredkin sul un computer a palle di biliardo [FeynmanLecturesComputation].

IV – COMPUTER CON DNA

Fino a questo punto abbiamo visto come, in linea di principio, sia possibile costruire un computer utilizzando un processo fisico inusuale (l’urto fra palle da biliardo). Questo suggerisce che altri sistemi possano essere usati per costruire dei computer e per fare calcolo.

In questa contesto, una delle scoperte più recenti è che anche i sistemi biologici possono svolgere calcoli. Riflettendo sulle radici stesse della biologia molecolare questo dovrebbe sembrare più naturale anche se comunque stupefacente.

La biologia e l’evoluzione degli esseri viventi è basata sulla conservazione e la trasmissione del patrimonio genetico. La conservazione e la trasmissione di informazione sono alla base del funzionamento dei computer e, in termini più astratti, delle macchine di Turing.

Le idee e la discussione che segue sono frutto della ricerca di Leonard M. Adleman [Adleman1994, Adleman1998]. Adleman è un informatico noto per il codice crittografico a chiave pubblica più usato al mondo. Infatti l’algoritmo sistema RSA prende il nome dai suoi inventori: Ron Rivest, Adi Shamir e Leonard Adleman.

1.4.1 Breve compendio di biologia molecolare

Tutta l’informazione genetica è immagazzinata nel DNA (*Deoxyribonucleic acid* o acido desossiribonucleico). Il DNA si presenta come una doppia elica (Fig. 6). Le eliche del DNA rappresentano solo lo scheletro mentre l’informazione è immagazzinata in quattro basi azotate: Adenina (A), Citosina (C), Timina (T) e Guanina (G). La sequenza di queste basi azotate rappresenta l’informazione genetica delle diverse specie e individui. Ad esempio, l’informazione sul colore degli occhi potrebbe essere codificata nella sequenza ACCTGAA....TTGC. A livello informatico quindi l’informazione codificata nel DNA usa quattro stati; invece degli usuali bit 0 e 1 potremmo associare le basi azotate a dei numeri interi A=0, B=1, C=2 e D=3¹.

¹ Se volessimo codificare la stessa informazione in termini binari dovremmo usare due bit. Ad esempio, potremmo porre A=00, B=10, C=01 e D=11.

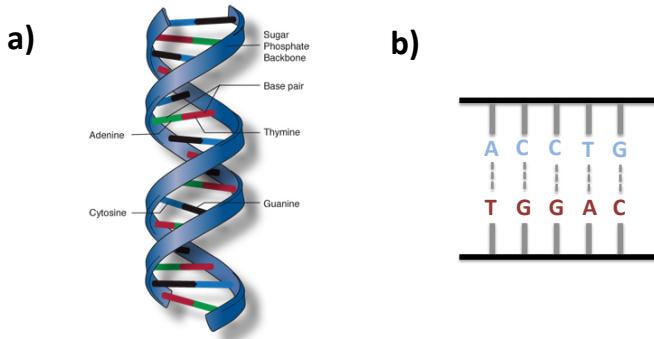


Figure 6: a) Rappresentazione tridimensionale della doppia elica del DNA. b) Schematizzazione della doppia elica del DNA. Lo scheletro è rappresentato dal segmento nero. Ad esso sono collegate le basi azotate. La sequenza rossa della seconda elica è la complementare di quella blu.

Questa sequenza si trova su una delle eliche mentre sull'altra elica si trova la sequenza detta complementare. Data una sequenza di basi azotate, la sua sequenza complementare si ottiene scambiano $A \leftrightarrow T$ e $C \leftrightarrow G$ come mostrato in figura 6².

La principale caratteristica del DNA è che si può duplicare. Questo avviene tramite un enzima che si chiama DNA polimerasi. Il processo è il seguente. Quando la doppia elica si apre, la DNA polimerasi passa un'elica leggendo le basi azotate. Quando la DNA polimerasi incontra una sequenza di attivazione (detto *primer*), inizia a duplicare la sequenza di basi azotate leggendole e scrivendo la sequenza complementare.

Altri enzimi importanti sono la DNA-ligasi che prende due sezioni del DNA e le unisce in un'unica catena e la DNA-nucleasi che legge il DNA e quando trova una sequenza di attivazione taglia la molecola in due parti.

Noi non discuteremo nel dettaglio l'uso pratico di questi enzimi ma basta sapere che è possibile tagliare e collegare dei tratti di DNA.

1.4.2 Problema del cammino Hamiltoniano

Dalla descrizione di come funziona la DNA polimerasi si può notare (è quello che fece Adleman) un'incredibile somiglianza con la macchina di Turing. Questa è la schematizzazione più semplice di modello matematico di computazione.

Questa è costituita da una *testa* e da due nastri. La *testa* può far scorrere i nastri, leggere da uno e copiare sull'altro. Si sa che la macchina di Turing è universale e quindi può essere programmata per compiere qualsiasi operazione logica.

Nello schema biologico che stiamo discutendo la *testa* è costituita dalla DNA polimerasi mentre i nastri sono le eliche di DNA. Da questa analogia è naturale

² Il motivo fisico-chimico o biologico per questo è che basi complementari possono sviluppare legami chimici. Quindi quando si trovano affacciate nelle due semi-eliche di DNA questi legami tendono a stabilizzare la struttura.

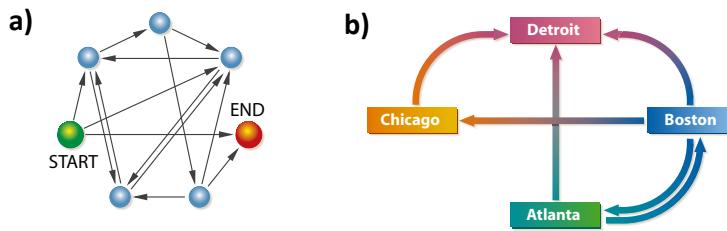


Figure 7: (Sinistra) Rappresentazione tridimensionale della doppia elica del DNA. (Destra) Schematizzazione della doppia elica del DNA. Lo scheletro è rappresentato dal segmento nero. Ad esso sono collegate le basi azotate. La sequenza rossa della seconda elica è la complementare di quella blu.

aspettarsi che il DNA (come una macchina di Turing) possa essere un computer biologico universale.

Appurato e capito questo Adleman decise però di implementare e risolvere con il DNA un problema computazionale difficile. Scelse il Problema del Cammino Hamiltoniano (PCH) originalmente proposto da William Rowan Hamilton nel diciannovesimo secolo. Il problema si può impostare nel seguente modo [si veda la figura 7 a)]:

Date una serie di città e dei voli unidirezionali che le connettono, e date una città di partenza P e una di arrivo A, è possibile trovare un cammino che parta da P e arrivi ad A passi una e una sola volta per ogni città ?

Per capire meglio, possiamo fare un esempio. In figura 7 b) è mostrata la rete di quattro città con sei voli. Supponiamo che le città di partenza e di arrivo siano, rispettivamente, Atlanta e Detroit. Vediamo subito che è possibile volare direttamente fra le due città. Ma per risolvere il PCH dobbiamo passare per le altre città una e una sola volta. Nell'esempio in figura 7 b) si vede immediatamente che una soluzione esiste ed è il percorso o cammino Atlanta-Boston-Chicago-Detroit. In modo analogo si può facilmente controllare che se la città di partenza è Detroit (per qualsiasi città di arrivo) non esiste nessun cammino Hamiltoniano.

Nell'esempio discusso è facile dare una risposta sull'esistenza di un cammino Hamiltoniano. Quando però il numero di città e di collegamenti cresce, non esiste nessun algoritmo efficiente capace di risolvere il PCH; nella pratica gli algoritmi si limitano a sondare tutto lo spazio dei possibili camini fino a trovarne uno Hamiltoniano. Al crescere del numero di città, questa procedura in genere richiede delle risorse che crescono esponenzialmente. Addirittura è stato dimostrato che il PCH è un problema computazionalmente difficile ed cade nella categoria dei problemi NP-C (*nondeterministic polynomial time complete*).

Vediamo ora come è possibile risolvere il PCH con il DNA. Prima di tutto è bene definire alcuni concetti che useremo. Con il termine grafo intendiamo l'insieme delle città (dette più in generale *nodi* o *vertici*) e dei voli aerei che le congiungono.

CITY	DNA NAME	COMPLEMENT
ATLANTA	ACTTGCA	TGAACGTC
BOSTON	TCGGACTG	AGCCTGAC
CHICAGO	GGCTATGT	CCGATACA
DETROIT	CCGAGCAA	GGCTCGTT
FLIGHT	DNA FLIGHT NUMBER	
ATLANTA - BOSTON	GCAGTCGG	
ATLANTA - DETROIT	GCAGCCGA	
BOSTON - CHICAGO	ACTGGGCT	
BOSTON - DETROIT	ACTGCCGA	
BOSTON - ATLANTA	ACTGACTT	
CHICAGO - DETROIT	ATGTCCGA	

Figure 8

Un esempio di grafo è mostrato in figura 7 a). Fatta questa precisazione, un algoritmo per risolvere il PCH può essere il seguente.

Algoritmo:

Dato un grafo a n vertici

1. Genera un insieme di cammini casuali sul grafo.
2. Per ogni cammino dell'insieme
 - a) Controlla se il cammino parte e finisce con i vertici (ovvero città) giusti. Se non lo fa rimuovi dall'insieme.
 - b) Controlla se il cammino passa per n vertici. Se non lo fa rimuovi dall'insieme.
 - c) Per ogni vertice, controlla se il cammino passa per quel vertice. Se non lo fa rimuovi dall'insieme.
 - d) Se l'insieme non è vuoto, c'è un cammino Hamiltoniano. Se l'insieme è vuoto, non c'è un cammino Hamiltoniano.

Questo algoritmo non è sicuramente il più efficiente ma ha il vantaggio di essere facilmente implementabile con il DNA. Come è possibile implementarlo con il DNA?

Prima di tutto è necessario codificare l'informazione nelle basi azotate. In particolare, ogni città sarà identificata da una stringa di otto basi azotate come mostrato in Fig. 8. Ad esempio, possiamo associare la città di Atlanta alla stringa ACTT-GCGA. Possiamo considerare le prime quattro basi azotate ACTT come il "nome" della città (per quanto questo possa avere significato) e le quattro finali GCGA come il "cognome" della città . Un'altra importante osservazione è che esisterà anche il complemento TGAA-CGTC che contiene esattamente la stessa informazione. Questo è generato e presente in tutte le soluzioni di DNA.

I voli aerei saranno codificati da un'altra stringa di otto basi azotate. Le prime quattro contengono il "cognome" della città di partenza e le ultime quattro il "nome" della città di arrivo. Ad esempio, il volo Atlanta-Boston sarà codificato

dalla stringa GCGA ("cognome" di Atlanta) e TCGG ("nome" di Boston); ovvero GCGA-TCGG.

Possiamo ora capire come il nostro algoritmo compie il primo passo e genera i diversi cammini. Quello che dobbiamo fare è costruire le stringhe associate alle città e ai voli e poi, tramite un processo chimico, farle reagire. In questo modo abbiamo implementato il punto 1 dell'algoritmo (*Genera un insieme di cammini casuali sul grafo*).

Punto 2.a)

Per implementare il punto 2.a) e selezionare i cammini che iniziano per Atlanta e finiscono per Detroit, si può usare la DNA polimerasi e la *polymerase chain reaction* (PCR). Questa tecnica permette di duplicare una parte di DNA compresa fra una sequenza di "inizio" e una sequenza di "fine" assegnate da noi. Nel nostro caso, la sequenza di inizio è identificata da GCAG (per Atlanta) e quella finale da GGCT (per Detroit). La sequenza iniziale impone la DNA polimerasi di iniziare a copiare il DNA fino a che non trova la sequenza di fine. In questo modo, duplichiamo solo i cammini che iniziano per Atlanta e finiscono per Detroit. Quelli che non soddisfano le condizioni sull'inizio e la fine della catena non verranno duplicati e diventeranno quindi irrilevanti nell'esperimento. Si noti comunque che in questo modo duplichiamo anche cammini non Hamiltoniani (ed esempio, le sequenze Atlanta-Detroit o Atlanta-Boston-Detroit).

Punto 2.b)

Nel punto 2.b) dell'algoritmo è necessario selezionare solo i cammini che passano per n vertici. Questo può essere fatto sfruttando il fatto che il peso della stringa di DNA dipende dal numero di vertici che la compongono. Se il DNA è posto in una placca di gel e gli si applica della corrente elettrica, le molecole di DNA caricate si sposteranno (DNA elettroforesi). La velocità di spostamento dipende dal peso e quindi dal numero di vertici che compongono il cammino. Quindi, se vogliamo selezionare solo quelli con n vertici, basta usare la tecnica del DNA elettroforesi, in modo da separare i cammini con diversi nodi e recuperare dal gel solo quelli desiderati. Questi verranno poi duplicati con altre tecniche in modo da avere campioni con un numero di molecole di DNA elevato.

Punto 2.c)

Per controllare se i cammini passano per tutti i vertici (punto 2.c) si è necessaria una procedura leggermente più complessa. Supponiamo di voler selezionare solo i cammini che passano per la città di Boston. In questo caso, usiamo delle microsfere di ferro a cui viene attaccata il complemento del nome della città di Boston (AGCC). Stimolando la separazione della doppia elica di DNA, le stringhe che contengono il nome Boston si attaccheranno alla stringa AGCC e quindi alla microsfera di ferro. A questo punto, usando un magnete o campo elettrico, è possibile

attrarre e spostare le microsfere con i cammini selezionati. In questo modo, possiamo separarli dagli altri. Ripetendo questa procedura per tutte le città intermedie siamo in grado di selezionare solo i cammini che passano per tutte le città .

Punto 2.d)

L'ultimo punto consta semplicemente nel controllo se l'insieme dei cammini selezionati è vuoto o no. Questo può essere facilitato, ad esempio, usando la PCR che aumenta il numero di eventuali stringhe di DNA presenti nella provetta. Se la provetta non è vuota, siamo sicuri che esiste un cammino Hamiltoniano. Si noti però che a questo livello non abbiamo informazione diretta sul cammino che risolve il PCH. Per averla dovremmo sapere la sequenza delle basi azotate ma questo richiede procedure più complicate a livello di laboratorio. In altre parole, abbiamo risolto il problema decisionale ma trovato il cammino Hamiltoniano.

V — PROBLEMI NEL SIMULARE SISTEMI QUANTISTICI E COMPUTER QUANTISTICI (FEYNMANN)

[FeynmanLecturesComputation]

2

APPARATO MATEMATICO

I – PREREQUISITI MATEMATICI

I due ingredienti essenziali per lo studio dell'informazione quantistica sono i numeri complessi e gli spazi vettoriali complessi in due dimensioni.

2.1.1 Numeri complessi

Unità immaginaria

L'equazione

$$x^2 + 1 = 0$$

non è risolubile nel campo reale perché $x^2 \geq 0$ per ogni $x \in \mathbb{R}$. Se introduciamo l'*unità immaginaria*, ovvero il numero i tale che $i^2 = -1$, otteniamo invece le due soluzioni $x_{1,2} = \pm i$.

L'algebra non cambia

Siamo ora in grado di calcolare la radice quadrata di un qualunque numero reale negativo e possiamo risolvere tutte le equazioni di secondo grado estendendo la validità delle regole usuali dell'algebra nel campo reale al campo complesso \mathbb{C} . Ogni numero complesso $z \in \mathbb{C}$ può essere scritto come $z = a + ib$, con $a \in \mathbb{R}$ *parte reale* e $b \in \mathbb{R}$ *parte immaginaria*. Se $z = a + ib$ e $w = c + id$, abbiamo

$$\begin{aligned} z + w &= (a + ib) + (c + id) = (a + c) + i(b + d) \\ z \cdot w &= (a + ib) \cdot (c + id) = (ac - bd) + i(ad + bc). \end{aligned}$$

Il *complesso coniugato* di $z = a + ib$ è $z^* = a - ib$. Per ogni $z \in \mathbb{C}$, $z \cdot z^* = a^2 + b^2$ è reale e non negativo. Inoltre, $\sqrt{a^2 + b^2} = |z|$ è detto *modulo* di z .

Due rappresentazioni equivalenti

Possiamo rappresentare un numero complesso $z = a + ib$ come una coppia (a, b) sul piano complesso (vedi figura 9). L'asse delle ascisse è utilizzato per la parte reale e l'asse delle ordinate per la parte immaginaria. Si ha $a = |z|\cos\theta$ e $b = |z|\sin\theta$ con $b/a = \tan\theta$ e dove θ è la *fase*. Se $z = 0$, la fase è indefinita.

Questo capitolo è basato sulle note di Alessandro Verri.

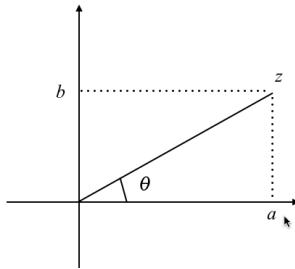


Figure 9: Vedi testo.

Per $|z| = 1$, $z = \cos \theta + i \sin \theta$. Più in generale, $\forall z \in \mathbb{C}$ possiamo scrivere $z = \rho e^{i\theta}$ con $\rho = |z|$ e

$$\cos \theta + i \sin \theta = e^{i\theta}.$$

In questa notazione, detta *olare*, è evidente che il prodotto di due numeri complessi è un numero complesso che ha per modulo il prodotto dei moduli e per fase la somma delle fasi. In particolare, i numeri con lo stesso modulo ρ nel piano complesso giacciono sulla circonferenza con centro nell'origine e raggio ρ .

2.1.2 Spazi vettoriali in 2D

Vettori nel piano

Rappresentiamo i vettori nel piano come frecce che hanno la base in un punto fissato, l'origine, e la punta in un punto qualunque del piano. I vettori si indicano in diverse maniere; le più comuni sono in grassetto \mathbf{v} o con una freccia \vec{v} .

Un vettore è caratterizzato da tre quantità : modulo, direzione e verso. Il modulo rappresenta la lunghezza del vettore. La direzione è rappresentata dalla retta su cui giace il vettore (e da tutte quelle parallele ad essa). In fine, il verso specifica in che direzione punta il vettore (dato che ogni retta ha due direzioni). Consideriamo per esempio, il vettore spostamento che descrive lo spostamento da Genova a Milano. In questo caso, il modulo sarà 150 km, il verso sarà dato dalla retta congiungente Genova e Milano e il verso sarà da Genova (presa come origine) a Milano.

Possiamo definire alcune operazioni di base fra e con vettori. Se abbiamo due vettori \mathbf{u} e \mathbf{v} possiamo definire la somma che sarà un vettore $\mathbf{w} = \mathbf{u} + \mathbf{v}$ ottenuto mediante la regola *regola del parallelogramma* (vedi figura 10).

Dato un numero $\alpha \in \mathbb{R}$, per ogni vettore \mathbf{v} , possiamo definire il vettore $\alpha\mathbf{v}$ è la freccia ottenuta moltiplicando \mathbf{v} per $|\alpha|$ e invertendone il verso se $\alpha < 0$. Questa operazione è detta *moltiplicazione per scalare* e permette di definire anche il vettore opposto. Se $\alpha = -1$, otteniamo il vettore $-\mathbf{v}$ che stesso modulo, stessa direzione ma verso opposto a \mathbf{v} . Sommando $\mathbf{v} + (-\mathbf{v}) = \mathbf{o}$ otteniamo il vettore nullo \mathbf{o} .

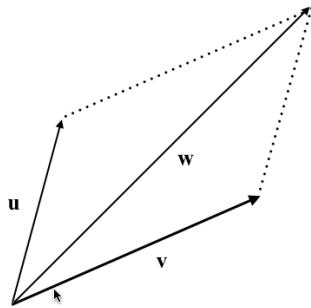


Figure 10: Vedi testo.

L'insieme di tutti i vettori del piano è allora uno spazio vettoriale reale V chiuso rispetto all'operazione di combinazione lineare: ovvero, $\forall \mathbf{u} \in V$ e $\forall \alpha \in \mathbb{R}$, si ha che il vettore $\alpha\mathbf{u} \in V$. Se α è reale sono complessi, V è uno spazio vettoriale complesso: gli spazi vettoriali complessi e reali godono delle stesse proprietà. Nel seguito assumeremo sempre di trattare il caso di spazi vettoriali complessi. Due vettori \mathbf{v}_0 e \mathbf{v}_1 che non sono uno multiplo dell'altro generano lo spazio V . Pertanto, $\forall \mathbf{v} \in V$, esistono $\alpha, \beta \in \mathbb{C}$ tali che $\mathbf{v} = \alpha\mathbf{v}_0 + \beta\mathbf{v}_1$. La coppia \mathbf{v}_0 e \mathbf{v}_1 è una base per V . Il vettore nullo è indicato ancora con $\mathbf{0}$.

Prodotto scalare e componenti

Nel caso quantistico gli spazi vettoriali complessi ammettono la definizione di un prodotto scalare. Il prodotto scalare è una funzione $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{C}$ che soddisfa le seguenti tre proprietà:

1. $\forall \mathbf{u} \in V$, $\langle \mathbf{u}, \mathbf{u} \rangle$ è un numero reale non negativo, con $\langle \mathbf{u}, \mathbf{u} \rangle = 0$ se e solo se $\mathbf{u} = \mathbf{0}$;
2. $\forall \mathbf{u}, \mathbf{v} \in V$, $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle^*$;
3. $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V$, $\forall \alpha, \beta \in \mathbb{C}$, $\langle \mathbf{w}, \alpha\mathbf{u} + \beta\mathbf{v} \rangle = \alpha \langle \mathbf{w}, \mathbf{u} \rangle + \beta \langle \mathbf{w}, \mathbf{v} \rangle$.

Due vettori per i quali il prodotto scalare è nullo sono *ortogonali*. La lunghezza o norma di un vettore $\mathbf{u} \in V$ è $\sqrt{\langle \mathbf{u}, \mathbf{u} \rangle}$. Nel seguito, considereremo sempre basi costituite da coppie di vettori ortogonali e a norma unitaria, ovvero basi *ortonormali*. Fissata una base ortonormale, \mathbf{v}_0 e \mathbf{v}_1 per esempio, ogni $\mathbf{u} \in V$ può essere espresso in componenti come $\mathbf{u} = u_0\mathbf{v}_0 + u_1\mathbf{v}_1$ con

$$u_0 = \langle \mathbf{u}, \mathbf{v}_0 \rangle \quad \text{e} \quad u_1 = \langle \mathbf{u}, \mathbf{v}_1 \rangle.$$

Inoltre, si ha $\langle \mathbf{u}, \mathbf{u} \rangle = \langle u_0\mathbf{v}_0 + u_1\mathbf{v}_1, u_0\mathbf{v}_0 + u_1\mathbf{v}_1 \rangle = u_0^2 + u_1^2$.

Una notazione particolarmente utile è quella per componenti (o matriciale). Ogni vettore è associato ad una matrice 2×1 che ha per elementi le sue componenti ordinate in colonna. Per reinterpretare le definizioni di sopra in questo

contesto, dobbiamo prima fissare la base $\{\mathbf{v}_0, \mathbf{v}_1\}$. Nella rappresentazione per componenti o matriciale questi saranno descritti da

$$\begin{aligned}\mathbf{v}_0 &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ \mathbf{v}_1 &= \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \end{aligned}\quad (2.1.1)$$

In questa notazione, denotiamo con \mathbf{w}^\dagger il vettore trasposto e complesso coniugato del vettore \mathbf{w} , il prodotto scalare di due vettori \mathbf{w} e $\mathbf{u} \in V$ può essere riscritto come il prodotto righe per colonne

$$\langle \mathbf{w}, \mathbf{u} \rangle = \mathbf{w}^\dagger \mathbf{u} = [w_0^*, w_1^*]^\top \begin{bmatrix} u_0 \\ u_1 \end{bmatrix} = w_0^* u_0 + w_1^* u_1.$$

Si noti quindi che, coerentemente,

$$\langle \mathbf{v}_0, \mathbf{v}_0 \rangle = \mathbf{v}_0^\dagger \mathbf{v}_0 = [1, 0]^\top \begin{bmatrix} 1 \\ 0 \end{bmatrix} = 1,$$

e, analogamente, $\langle \mathbf{v}_1, \mathbf{v}_1 \rangle = 1$, $\langle \mathbf{v}_0, \mathbf{v}_1 \rangle = \langle \mathbf{v}_1, \mathbf{v}_0 \rangle = 0$ come ci si aspetta per una base ortonormale. Il vettore generico $\mathbf{u} = u_0 \mathbf{v}_0 + u_1 \mathbf{v}_1$ si sarà

$$\mathbf{u} = u_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + u_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} u_0 \\ u_1 \end{bmatrix}.$$

Osserviamo che cambiando la base, le componenti di un vettore cambiano ma il vettore non cambia. Vediamo ora la notazione comunemente usata in meccanica quantistica.

Vettori ket e bra

In meccanica quantistica si preferisce indicare un vettore \mathbf{u} con $|\mathbf{u}\rangle$, detto *ket*, e il suo trasposto coniugato con $\langle \mathbf{u}|$, detto *bra*. In questa notazione il prodotto scalare di due vettori $|\mathbf{u}\rangle$ e $|\mathbf{w}\rangle$ si forma allora con il *braket* (*bracketing* significa mettere in parentesi)

$$\langle \mathbf{u} | \mathbf{v} \rangle := \langle \mathbf{u}, \mathbf{v} \rangle.$$

L'identificativo del vettore, in questa nuova notazione, può essere più facilmente utilizzato per codificare lo stato che si vuole rappresentare.

2.1.3 Somma diretta

Definizioni

Se V e W sono spazi vettoriali, definiamo la *somma diretta* di V e W come

$$V \oplus W := \{(|\mathbf{v}\rangle, |\mathbf{w}\rangle) \text{ tali che } |\mathbf{v}\rangle \in V \text{ e } |\mathbf{w}\rangle \in W\}.$$

L'insieme $V \oplus W$ è uno spazio vettoriale rispetto alla somma definita come

$$|\mathbf{u}\rangle + |\mathbf{u}'\rangle := (|\mathbf{v}\rangle + |\mathbf{v}'\rangle) \oplus (|\mathbf{w}\rangle + |\mathbf{w}'\rangle)$$

per ogni $|\mathbf{u}\rangle = |\mathbf{v}\rangle \oplus |\mathbf{w}\rangle$ e $|\mathbf{u}'\rangle = |\mathbf{v}'\rangle \oplus |\mathbf{w}'\rangle \in V \oplus W$: infatti, i vettori della somma diretta $V \oplus W$ si combinano sommando i vettori di V e W separatamente.

Se V e W ammettono prodotto scalare, $V \oplus W$ ammette il prodotto scalare definito come

$$\langle \mathbf{u} | \mathbf{u}' \rangle = (\langle \mathbf{v} | \oplus \langle \mathbf{w} |)(|\mathbf{v}'\rangle \oplus |\mathbf{w}'\rangle) := \langle \mathbf{v} | \mathbf{v}' \rangle + \langle \mathbf{w} | \mathbf{w}' \rangle,$$

ovvero il prodotto scalare di vettori di $V \oplus W$ si ottiene sommando i prodotti scalari di vettori di V e W .

Se $\{|\mathbf{v}_0\rangle, |\mathbf{v}_1\rangle\}$ e $\{|\mathbf{w}_0\rangle, |\mathbf{w}_1\rangle\}$ sono basi per V e W , $\{(|\mathbf{v}_0\rangle, |\mathbf{v}_1\rangle), (|\mathbf{w}_0\rangle, |\mathbf{w}_1\rangle)\}$ è base per $V \oplus W$.

Proprietà ed esempi

Nella somma diretta la corrispondenza tra gli $|\mathbf{u}\rangle \in V \oplus W$ e le coppie ordinate $(|\mathbf{v}\rangle, |\mathbf{w}\rangle)$ con $|\mathbf{v}\rangle \in V$ e $|\mathbf{w}\rangle \in W$ è biunivoca.

Tutto quanto detto, inoltre, rimane vero per la somma diretta di un qualunque numero di spazi vettoriali di qualunque dimensione. Abbiamo allora che

$$\dim(V \oplus W) = \dim(V) + \dim(W).$$

Pertanto, la somma diretta di n copie di uno spazio V ha dimensione $n \dim(V)$.

Se gli assi coordinati X , Y e Z sono visti come spazi vettoriali 1D, il piano $X \oplus Y$ è lo spazio vettoriale 2D somma diretta di X e Y , mentre lo spazio $X \oplus Y \oplus Z$ è lo spazio vettoriale 3D somma diretta di X , Y e Z .

II – PRODOTTO TENSORE

Definizioni

Consideriamo ora due spazi vettoriali V e W con basi, rispettivamente, $A = \{|\alpha_1\rangle_V, |\alpha_2\rangle_V, \dots, |\alpha_n\rangle_V\}$ e $B = \{|\beta_1\rangle_W, |\beta_2\rangle_W, \dots, |\beta_m\rangle_W\}$. Da questa scrittura deduciamo che $\dim(V) = n$ e $\dim(W) = m$. Il *prodotto tensore* dei due spazi viene indicato con $V \otimes W$ ha dimensione $\dim(V \otimes W) = n m$, con una base costituita da $n m$ elementi della forma $|\alpha_i\rangle_V \otimes |\beta_j\rangle_W \equiv |\alpha_i \beta_j\rangle$ [Rieffel2011]. Le notazioni $|\alpha_i\rangle_V \otimes |\beta_j\rangle_W$ e $|\alpha_i \beta_j\rangle$ sono equivalenti. La prima è più precisa e tiene conto del fatto che gli stati $|\alpha_i\rangle_V$ e $|\beta_j\rangle_W$ appartengono rispettivamente allo spazio vettoriale V e W . La seconda è più concisa e quindi più usata.

Il prodotto tensoriale soddisfa le seguenti proprietà

$$1. \forall |\mathbf{v}\rangle, |\mathbf{v}'\rangle \in V, |\mathbf{w}\rangle \in W \quad (|\mathbf{v}\rangle + |\mathbf{v}'\rangle) \otimes |\mathbf{w}\rangle = |\mathbf{v}\rangle \otimes |\mathbf{w}\rangle + |\mathbf{v}'\rangle \otimes |\mathbf{w}\rangle;$$

$$2. \forall |\mathbf{v}\rangle \in V, |\mathbf{w}\rangle, |\mathbf{w}'\rangle \in W \quad |\mathbf{v}\rangle \otimes (|\mathbf{w}\rangle + |\mathbf{w}'\rangle) = |\mathbf{v}\rangle \otimes |\mathbf{w}\rangle + |\mathbf{v}\rangle \otimes |\mathbf{w}'\rangle;$$

$$3. \forall |\mathbf{v}\rangle \in V, |\mathbf{w}\rangle \in W, \alpha \in \mathbb{C} \quad (\alpha|\mathbf{v}\rangle) \otimes |\mathbf{w}\rangle = |\mathbf{v}\rangle \otimes (\alpha|\mathbf{w}\rangle) = \alpha(|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle).$$

Se V e W ammettono prodotto scalare, $V \otimes W$ ammette il prodotto scalare definito come

$$\langle \mathbf{u}|\mathbf{u}'\rangle = (\langle \mathbf{v}| \otimes \langle \mathbf{w}|)(|\mathbf{v}'\rangle \otimes |\mathbf{w}'\rangle) := \langle \mathbf{v}|\mathbf{v}'\rangle \langle \mathbf{w}|\mathbf{w}'\rangle,$$

ovvero come il prodotto dei prodotti scalari definiti su V e W .

Proprietà ed esempi

Consideriamo qualche esempio. Se, nella base canonica di V e W abbiamo che $|\mathbf{v}\rangle = a|\alpha_1\rangle_V + b|\alpha_2\rangle_V \in V$ e $|\mathbf{w}\rangle = c|\beta_1\rangle_W + d|\beta_2\rangle_W \in W$, il prodotto tensoriale $|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle$ è

$$\begin{aligned} (a|\alpha_1\rangle_V + b|\alpha_2\rangle_V) \otimes (c|\beta_1\rangle_W + d|\beta_2\rangle_W) &= \\ ac|\alpha_1\rangle_V \otimes |\beta_1\rangle_W + ad|\alpha_1\rangle_V \otimes |\beta_2\rangle_W \\ + bc|\alpha_2\rangle_V \otimes |\beta_1\rangle_W + bd|\alpha_2\rangle_V \otimes |\beta_2\rangle_W. \end{aligned} \tag{2.2.1}$$

Per la norma di $|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle$ abbiamo

$$(\langle \mathbf{v}| \otimes \langle \mathbf{w}|)(|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle) = |ac|^2 + |ad|^2 + |bc|^2 + |bd|^2 = (|a|^2 + |b|^2)(|c|^2 + |d|^2).$$

Se, invece, $|\mathbf{v}'\rangle = f|\alpha_1\rangle_V \in V$ e $|\mathbf{w}'\rangle = g|\beta_2\rangle_W \in W$, abbiamo semplicemente

$$f|\alpha_1\rangle_V \otimes g|\beta_2\rangle_W = fg|\alpha_1\rangle_V \otimes |\beta_2\rangle_W.$$

Per il prodotto scalare di $|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle$ con $|\mathbf{v}'\rangle \otimes |\mathbf{w}'\rangle$, invece, otteniamo

$$(\langle \mathbf{v}| \otimes \langle \mathbf{w}|)(|\mathbf{v}'\rangle \otimes |\mathbf{w}'\rangle) = (a^*f + b^* \cdot 0)(c^* \cdot 0 + d^*g) = a^*fd^*g.$$

Osserviamo che se $\langle \mathbf{v}|\mathbf{v}\rangle = 1$ e $\langle \mathbf{w}|\mathbf{w}\rangle = 1$ allora

$$(\langle \mathbf{v}| \otimes \langle \mathbf{w}|)(|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle) = \langle \mathbf{v}|\mathbf{v}\rangle \langle \mathbf{w}|\mathbf{w}\rangle = 1.$$

Tutto quanto detto rimane vero per il prodotto tensoriale di un qualunque numero di spazi vettoriali di qualunque dimensione. In particolare, quindi,

$$\dim(V \otimes W) = \dim(V) \times \dim(W).$$

Se si considera il prodotto tensoriale Π_{\otimes}^n di n copie dello stesso spazio vettoriale V si ha

$$\dim(\Pi_{\otimes}^n V) = \dim(V)^n.$$

In meccanica quantistica, lo stato combinato di n sistemi quantistici a 2 stati è un vettore in uno spazio vettoriale $2^n D$, prodotto tensoriale di n spazi. Nel caso classico, invece, lo stato combinato di n sistemi, ciascuno descritto da un punto in uno spazio vettoriale $2D$, è descritto da un punto in uno spazio $2nD$, somma diretta degli n spazi.

III – OPERATORI

Gli operatori lineari in generale sono tali che agendo su un vettore dello spazio lineare danno un altro vettore dello stesso spazio: $O : V \rightarrow V$. Usando la notazione *bra-ket* possiamo scrivere $O|v\rangle = |w\rangle$.

Molto spesso è utile dare una rappresentazione matriciale dell'operatore. A questo proposito, sceglieremo una base dello spazio vettoriale (supposto di dimensione n) $\{|\alpha_1\rangle, |\alpha_2\rangle, \dots, |\alpha_n\rangle\}$. L'elemento $i - j$ della matrice associata all'operatore sarà $O_{ij} = \langle \alpha_i | O | \alpha_j \rangle$.

$$O = \begin{bmatrix} & |\alpha_1\rangle & |\alpha_2\rangle & |\alpha_3\rangle & \cdots & |\alpha_n\rangle \\ \langle \alpha_1 | & O_{11} & O_{12} & O_{13} & \cdots & O_{1n} \\ \langle \alpha_2 | & O_{21} & O_{22} & O_{23} & \cdots & O_{2n} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \langle \alpha_n | & O_{n1} & O_{n2} & O_{n3} & \cdots & O_{nn} \end{bmatrix}. \quad (2.3.1)$$

Nella scrittura (2.3.1) è implicito un altro modo di scrivere un operatore. Abbiamo detto che il prodotto fra un *bra* e un *ket* rappresenta il prodotto scalare $\langle w|v \rangle$ ed è un numero complesso. Che significato ha invece la composizione fra un *ket* e un *bra* tipo $|w\rangle\langle v|$? Consideriamo prima il caso più semplice in cui $|w\rangle\langle v|$ viene applicato allo stato $|v\rangle$. Otteniamo $|w\rangle\langle v|v\rangle = |w\rangle(\langle v|v\rangle) = |w\rangle$. Quindi $|w\rangle\langle v|$ si comporta come un *operatore* che trasforma $|v\rangle$ in $|w\rangle$.

Più in generale, se lo applichiamo ad uno stato generico $|q\rangle$ otterremo

$$|w\rangle\langle v|q\rangle = |w\rangle(\langle v|q\rangle) = a|w\rangle \quad (2.3.2)$$

dove $a = \langle w|q\rangle$ è un numero complesso.

Le notazioni usate sono consistenti. Ad esempio, l'operatore O scritto in termini matriciali in Eq. (2.3.1) può essere scritto con i *bra* e *ket* della base $\{|\alpha_1\rangle, |\alpha_2\rangle, \dots, |\alpha_n\rangle\}$ come

$$O = \sum_{ij} O_{ij} |\alpha_i\rangle\langle \alpha_j|. \quad (2.3.3)$$

Infatti, prendendo l'elemento di matrice $k - p$ otteniamo

$$\langle \alpha_k | O | \alpha_p \rangle = \sum_{ij} O_{ij} \langle \alpha_k | \alpha_i \rangle \langle \alpha_j | \alpha_p \rangle = \sum_{ij} O_{ij} \delta_{ki} \delta_{jp} = O_{kp} \quad (2.3.4)$$

dove abbiamo usato il fatto che la base $\{|\alpha_1\rangle, |\alpha_2\rangle, \dots, |\alpha_n\rangle\}$ è ortonormale; quindi $\langle \alpha_k | \alpha_i \rangle = \delta_{ki}$ è zero se $k \neq i$ e 1 se $k = i$ (δ_{ki} è chiamata delta di Kronecker).

Nell'Eq. (2.3.3) O è scritto come un operatore. Se la sua struttura è nota nella base $\{\alpha_i\}$, possiamo scriverlo in un'altra base $\{\beta_i\}$ semplicemente prendendo gli elementi di matrice nella nuova base. Ad esempio, l'elemento di matrice $k - p$ nella nuova base sarà

$$\langle \beta_k | O | \beta_p \rangle = \sum_{ij} O_{ij} \langle \beta_k | \alpha_i \rangle \langle \alpha_j | \beta_p \rangle \quad (2.3.5)$$

dove $\langle \beta_k | \alpha_i \rangle$ e $\langle \alpha_j | \beta_p \rangle$ sono i prodotti scalari fra stati delle due basi.

IV – AUTOVALORI E AUTOVETTORI

Sia O un operatore lineare definito su uno spazio V . Usando la notazione *braket* per denotare i vettori dello spazio V , diremo che se $O|v\rangle = \lambda|v\rangle$ per un vettore $|v\rangle$ (non nullo), diremo che v è un *autovettore* di O e λ è l'*autovalore* corrispondente.

Fra gli operatori lineari, in meccanica quantistica hanno un ruolo particolare gli operatori *hermitiani* tali che $O^\dagger = O$ dove con il simbolo \dagger denotiamo l'*aggiunto dell'operatore*. Semplificando, possiamo pensare ad un operatore O rappresentato in una base scelta come una matrice quadrata. In questo caso, l'operatore aggiunto non è altro che l'operazione di "trasposta coniugata".

Gli operatori hermitiani hanno sempre autovalori reali. Per vedere questo partiamo dall'equazione agli autovalori $O|v\rangle = \lambda|v\rangle$ e ne facciamo il complesso-coniugato (aggiunto). In questo caso, i *ket* vengono trasformati in *bra* e otteniamo $\langle v|O^\dagger = \lambda^* \langle v|$ (dove λ^* è il complesso coniugato di λ). Usando questo risultato e ricordandoci che i *ket* sono normalizzati ($\langle v|v\rangle = 1$), possiamo scrivere

$$\lambda = \lambda \langle v|v\rangle = \langle v|\lambda|v\rangle = \langle v|(O|v)\rangle = (\langle v|O^\dagger)|v\rangle = \lambda^* \langle v|v\rangle = \lambda^*. \quad (2.4.1)$$

concludiamo che $\lambda = \lambda^*$ e che λ deve essere reale.

Un'altra importante proprietà degli autovettori degli operatori hermitiani è che, se associati ad autovalori diversi, sono ortogonali. Consideriamo due autovettori $|\phi_i\rangle$ e $|\phi_j\rangle$ associati a autovalori differenti tali che $\lambda_i \neq \lambda_j$ se $i \neq j$ ¹. Le equazioni rispettive sono

$$O|\phi_i\rangle = \lambda_i |\phi_i\rangle \quad (2.4.2)$$

e $O|\phi_j\rangle = \lambda_j |\phi_j\rangle$. Prendendo il complesso coniugato di quest'ultima equazione e ricordandoci che $O^\dagger = O$ e che λ_j deve essere reale, arriviamo alla seguente equazione

$$\langle \phi_j | O^\dagger = \langle \phi_j | O = \lambda_j \langle \phi_j |. \quad (2.4.3)$$

Calcoliamo ora l'elemento di matrice $\langle \phi_j | O | \phi_i \rangle$. Usando l'Eq. (2.4.2) possiamo scrivere che

$$\langle \phi_j | O | \phi_i \rangle = \lambda_i \langle \phi_j | \phi_i \rangle. \quad (2.4.4)$$

Usando invece l'equazione coniugata (2.4.3), otteniamo

$$\langle \phi_j | O | \phi_i \rangle = \lambda_j \langle \phi_j | \phi_i \rangle. \quad (2.4.5)$$

Naturalmente i due risultati devo essere uguali quindi arriviamo a scrivere

$$\lambda_i \langle \phi_j | \phi_i \rangle = \lambda_j \langle \phi_j | \phi_i \rangle. \quad (2.4.6)$$

¹ Gli autovettori $|\phi_i\rangle$ e $|\phi_j\rangle$ associati a autovalori differenti $\lambda_i \neq \lambda_j$ vengono detti *non-degeneri*. Mentre se $|\phi_i\rangle$ e $|\phi_j\rangle$ sono associati allo stesso autovalore $\lambda_i = \lambda_j$ vengono detti *degeneri*.

Visto che $\lambda_i \neq \lambda_j$, l'unica modo per soddisfare questa equazione è che entrambi i membri si annullino. Questo è possibile solo se $\langle \phi_j | \phi_i \rangle = 0$. Abbiamo quindi dimostrato che *gli autovettori di un operatore hermitiano associati ad autovalori diversi sono ortogonali*.

In meccanica quantistica il concetto di operatore hermitiano, di autovalore e autovettore sono particolarmente importanti quando associati alle misura. Come vedremo gli operatori hermitiano sono associati ad osservabili fisici (ad esempio, la polarizzazione della luce) e gli autovalori sono il risultato di una misura sul sistema.

Possiamo aggiungere un'altra osservazione. Se un operatore è diagonale nella base scelta allora

$$O = \sum_i O_{ii} |\alpha_i\rangle\langle\alpha_i|. \quad (2.4.7)$$

e O_{ii} saranno i suoi autovalori.

V – ESERCIZI

2.5.1 Esercizio 1

1. Si consideri la base ortonormale $B_1 = \{|0\rangle, |1\rangle\}$. In tale base, scrivere l'operatore $P_1 = |0\rangle\langle 1|$. Nella stessa base, scrivere l'operatore $P_2 = |1\rangle\langle 0|$.
2. Scrivere l'operatore $X = P_1 + P_2$. Come agisce X sugli stati della base? Ovvero, cosa otteniamo se calcoliamo $X|0\rangle$ e $X|1\rangle$? Come agisce X sullo stato $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$?
3. Si consideri l'insieme dei ket $B_2 = \{|+\rangle, |-\rangle\}$ con $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Tale insieme è una base ortonormale?
4. Calcolare $X|+\rangle$ e $X|-\rangle$.
5. Nella base B_2 , scrivere l'operatore X .

2.5.2 Esercizio 2

1. Ripetere il calcolo dell'esercizio 2.5.1, per gli operatori $P_1 = |1\rangle\langle 1|$, $P_1 = |0\rangle\langle 0|$ e $Z = P_1 - P_2$.

2.5.3 Esercizio 3

1. Usando i risultati dell'esercizio 2.5.1 per P_1 e P_2 , si scriva l'operatore $Y = -iP_1 + iP_2$ (dove i è l'unità immaginaria).
2. Per Y si ripetano i calcoli dell'esercizio 2.5.1 (nota: attenzione ai punti 4 e 5).

3 | INTRODUZIONE AI FENOMENI QUANTISTICI

I – DUE ESPERIMENTI

La meccanica quantistica è nata dall'impossibilità di spiegare alcuni fenomeni fisici. Noi discuteremo due esperimenti "prototipo" che evidenziano l'incompletezza della meccanica classica.

3.1.1 Esperimento doppia fenditura

Esperimento con palline

Secondo il Richard Feynmann [[Feynman Lectures Vol3](#)], l'esperimento della doppia fenditura racchiude tutta la meccanica quantistica.

Consideriamo inizialmente un cannone che spara delle palline in gomma 11 verso un muro con due aperture (fenditure). La direzione è molto imprecisa quindi le palline possono passare sia attraverso la fenditura 1 che la 2 e, nel passare attraverso le fenditure (piccole), possono essere deviate come mostrato in figura 11.

Le palline che passano attraverso le fenditure vanno a finire su uno schermo distante dove rimangono attaccate (oppure possiamo pensare che lascino un'impronta). Ci chiediamo qual'è la distribuzione delle palline sullo schermo ovvero con che probabilità le palline colpiscono un certo punto sullo schermo¹. Sperimentalmente si vede che la distribuzione è quella mostrata in fig. 11 c).

A questo punto chiudiamo la fenditura 2 in modo tale che le palline possano passare solo attraverso la 1. La distribuzione è P_1 mostrata in 11 c). Come ci si aspetterebbe la distribuzione è spostata lateralmente. In maniera analoga, chiudiamo la fenditura 2, la distribuzione cambia e viene spostata in senso opposto.

Questo capitolo è basato sulle note di Alessandro Verri.

¹ La distributione sarà proporzionale al numero di palline in una regione o all'intensità del colore lasciato sullo schermo dopo l'impatto

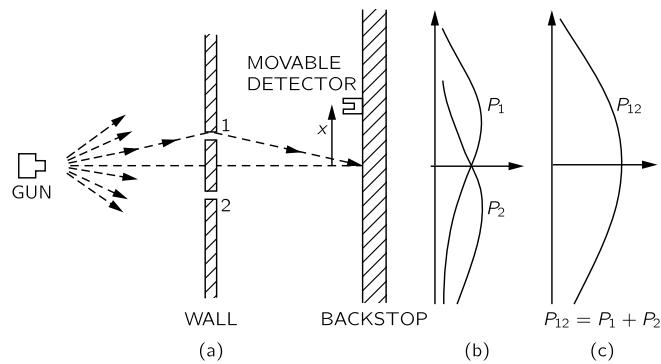


Figure 11: Esperimento con le palline.

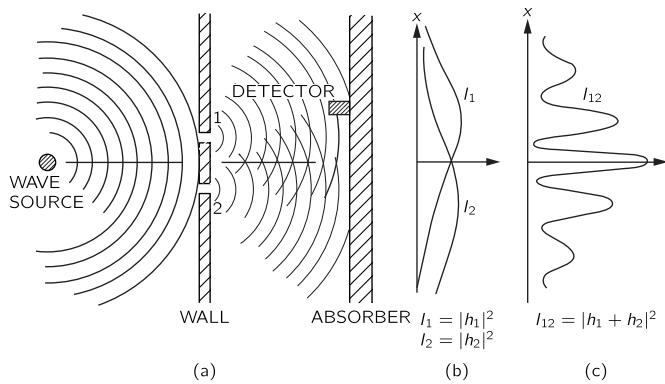


Figure 12: Esperimento con le onde.

Esperimento con onde

Consideriamo ora un esperimento simile con delle onde d'acqua (Fig. 12). Le onde sono emesse da una sorgente e incidono su un muro con due fessure. Le onde continuano a propagarsi fino ad arrivare ad un secondo muro dove un dispositivo misura l'ampiezza.

Il risultato di questo semplice esperimento è mostrato in figura (Fig. 12) c)

Esperimento con elettroni

Consideriamo per finire il caso in cui siano degli elettroni ad incidere sulla parete con le due fessure. Come prima gli elettroni potranno passare attraverso la prima o la seconda fessura e arrivano su uno schermo distante dove vengono misurati da un dispositivo apposito. Il dispositivo emette un "click" ogni volta che misura la presenza di un elettrone.

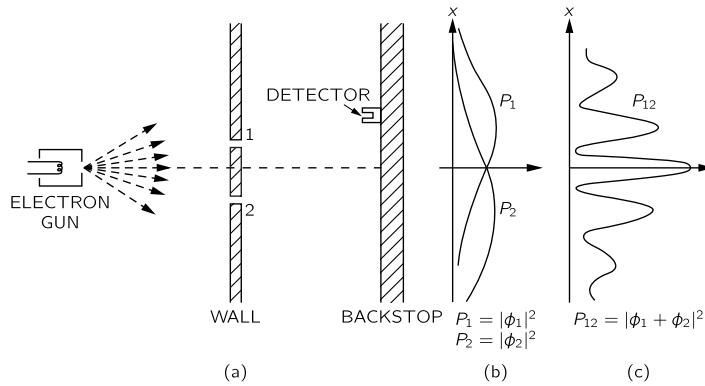


Figure 13: Esperimento con elettroni.

Quindi possiamo immaginare di ridurre il numero di elettroni emessi fino a poterli separare. Questo è il limite in cui la macchina emette un solo elettrone alla volta. Visto che gli elettroni sono emessi uno alla volta il misuratore emetterà dei "click" separati nel tempo. Gli elettroni sono particelle elementari quindi questi "click" separati non ci stupiscono.

Ma se gli elettroni sono particelle elementari, dovrebbero avere un comportamento simile alle palline e passare attraverso la fenditura 1 o attraverso la fenditura 2. Come per le palline queste situazioni sono esclusive. Con questa analogia, ci aspetteremo che con un numero sufficiente di misure la distribuzione di probabilità dell'arrivo degli elettroni sia simile a quella delle palline mostrata in Fig. 11 c).

Sorprendentemente, la distribuzione di arrivo degli elettroni (Fig. 13 c)) mostra fenomeni di interferenza ed è simile a quella delle onde (Fig. 12 c)). Siamo arrivati ad una conclusione paradossale, sebbene gli elettroni siano particelle (dato che arrivano separati) hanno una distribuzione tipica delle onde. Questo è la base del cosiddetto dualismo onda-particella nella meccanica quantistica: *gli elettroni (e le altre particelle) si comportano sia come corpuscoli che come onde*.

C'è un'altra importante osservazione. Le onde in Fig. 12 sono oggetti non-locali. Non si può dire se passano attraverso la fenditura 1 o la fenditura 2 perché passano contemporaneamente in entrambe. Per quanto possa sembrare sorprendente, questo è anche quello che succede agli elettroni: *gli elettroni passano contemporaneamente attraverso entrambe le fenditure*. Questo è uno dei risultati sorprendenti della meccanica quantistica.

3.1.2 Luce attraverso tre polarizzatori

Esiste un altro esperimento concettualmente semplice che però manifesta macroscopicamente gli effetti della meccanica quantistica.

La luce è composta da particelle dette fotoni. Un fascio di luce è in genere composto ma molti fotoni; la presenza di molti fotoni fa sì che la luce ad alta

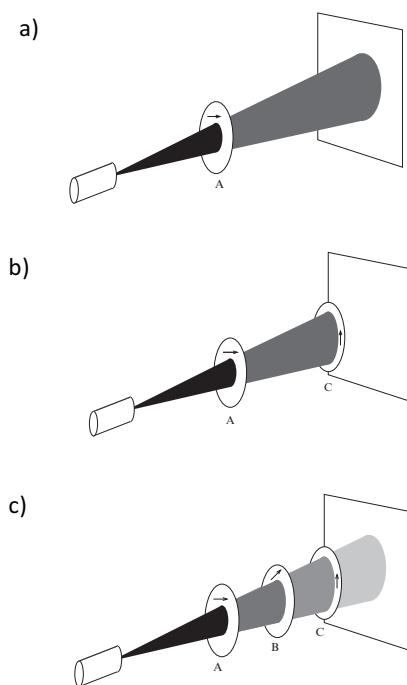


Figure 14: Esperimento dei polarizzatori. Una sorgente emette singoli fotoni che vanno ad incidere su uno schermo. a) Un polarizzatore A è riduce l'intensità del fascio selezionando solo i fotoni con polarizzazione orizzontale. b) Un secondo polarizzatore verticale C blocca completamente il fascio; nessun fotone arriva sullo schermo. c) L'inserimento di un polarizzatore a 45° B fra A e C fa in modo che i fotoni arrivino nuovamente sullo schermo.

intensità che si comporti come un mezzo continuo. Possiamo quindi osservare interferenza fra fasci di luce esattamente come le onde in acqua (Fig. 12). Se però diminuiamo l'intensità del fascio è possibile contare i fotoni, emetterli e manipolarli singolarmente.

Ogni fotone è caratterizzato dalla sua polarizzazione². La polarizzazione del fotone può essere misurata in laboratorio. Esistono ad esempio dei filtri polarizzanti che lasciano passare la luce che è polarizzata solo lungo una direzione precisa.

Supponiamo ora di avere un dispositivo che emette singoli fotoni con una polarizzazione che non conosciamo. Questi fotoni vengono assorbiti su uno schermo (Fig. 16). Inizialmente tutti i fotoni emessi arriveranno sullo schermo e noi osserveremo un'immagine la cui intensità è proporzionale al numero di fotoni emessi.

A questo punto, inseriamo fra la sorgente di fotoni e lo schermo un filtro polarizzatore nella direzione \rightarrow [Fig. 16 a)]. Vedremo che il numero di fotoni che arrivano allo schermo diminuisce (ovvero, l'intensità del fascio incidente sullo schermo diminuisce). Questo è spiegabile perché il filtro lascia passare solo i fo-

² I fisici sono soliti dire che la polarizzazione è un ulteriore grado di libertà del fotone.

toni polarizzati \rightarrow . Quelli polarizzati \uparrow vengono bloccati quindi non arrivano allo schermo.

Inseriamo una altro polarizzatore verticale \uparrow dopo il polarizzatore orizzontale come in Fig. 16 a)]. In questa configurazione, sullo schermo non arriva nessun fotone. Anche questo fatto è spiegabile con la fisica classica. Il primo polarizzatore lascia passare i fotoni con polarizzazione orizzontale ma blocca quelli con polarizzazione verticale. Quindi nel fascio che arriva al secondo polarizzatore verticale arrivano solo fotoni orizzontali che vengono assorbiti. È quindi naturale che nessun fotone arrivi sullo schermo.

L'ultimo passaggio è quello di mettere un terzo polarizzatore con polarizzazione a 45° fra i due precedenti [punto B in Fig. 16 c)]. L'intuizione ci direbbe che, secondo l'interpretazione appena discussa un polarizzatore intermedio non dovrebbe cambiare niente visto che i fotoni verrebbero comunque assorbiti dal polarizzatore orizzontale e verticale. La realtà è diversa. Sperimentalmente, si vede che se si inserisce un polarizzatore intermedio a 45° , alcuni fotoni riescono ad arrivare sullo schermo.[Fig. 16 c)].

Questo fatto controidintuitivo, è spiegabile solo con la meccanica quantistica e necessita del concetto di misura quantistica che sarà introdotto nella sezione 3.3.

II – IL SINGOLO QUBIT

Il comportamento di un sistema quantistico obbedisce a principi che non sono quelli della fisica classica. Discutiamo i concetti di stato di un sistema e di misura partendo dall'interpretazione di un esperimento di ottica che coinvolge un qubit, il componente fondamentale dell'informazione quantistica. L'esperimento rivela l'inadeguatezza della fisica classica nel trattare sistemi fisici su scala atomica.

3.2.1 Stati quantistici

Sistemi grandi e piccoli

Per la fisica classica l'evoluzione nel tempo di un sistema - quale per esempio un pianeta, un circuito elettrico o un liquido contenuto in un recipiente - è deterministica. Ottenuto lo stato iniziale da una serie di misure opportune sul sistema, compito della fisica classica è predire lo stato del sistema nei tempi successivi, ovvero il risultato di nuove misure sul sistema stesso. Questa visione, che ha consentito di ottenere descrizioni accurate nel caso di sistemi macroscopici, non è in accordo con gli esperimenti nel caso di sistemi piccoli. A partire dalla scala atomica, infatti, la natura appare intrinsecamente non deterministica. La meccanica quantistica, la teoria fisica che ha superato le contraddizioni della fisica classica ed è in accordo con tutti gli esperimenti osservati a oggi, può solo predire la probabilità con la quale una data misura produca un particolare risultato. Al crescere delle dimensioni del sistema l'indeterminazione propria della meccanica quantistica diventa rapidamente trascurabile e la vecchia fisica classica fornisce modelli in ottimo accordo con i fenomeni osservati.

Principio di sovrapposizione degli stati e qubit

Sia per l'informazione sia per la computazione quantistica è sufficiente limitarsi al caso di sistemi fisici a due stati quali la polarizzazione verticale e orizzontale di un fotone, lo stato fondamentale e uno stato eccitato di un elettrone in un atomo, o lo spin *up* e *down* di un elettrone lungo un asse fissato nello spazio.

Un sistema fisico a due stati è descritto da uno stato quantistico $|\mathbf{a}\rangle = a_0 |\mathbf{v}_0\rangle + a_1 |\mathbf{v}_1\rangle$, ovvero da una combinazione lineare di due stati, $|\mathbf{v}_0\rangle$ e $|\mathbf{v}_1\rangle$, che costituiscono una base ortonormale di uno spazio vettoriale complesso V . Le ampiezze a_0 e a_1 soddisfano il vincolo $|a_0|^2 + |a_1|^2 = 1$, per cui il vettore che rappresenta uno stato ha norma unitaria. Lo spazio V è detto spazio degli stati. Il fatto che uno stato quantistico sia una combinazione lineare a coefficienti complessi di stati è un postulato della meccanica quantistica noto come *principio di sovrapposizione degli stati*. Un sistema quantistico con due stati può essere pensato e utilizzato come un *quantum bit* o *qubit*. La dizione sistemi fisici a due stati non deve trarre in inganno: gli stati possibili in cui si può trovare un sistema fisico a due stati, infatti, sono infiniti!

III – MISURA

La misura di uno stato quantistico, il suo effetto e la sua interpretazione sono tutt'oggi argomenti di discussione e ricerca fra i fisici. Evitando di entrare nei dettagli, noi ci limiteremo all'interpretazione dominante da libro di testo detta "interpretazione di Copenhagen". Sebbene sembri chiaro che questa versione (o interpretazione) della meccanica quantistica sia incompleta, si è dimostrata estremamente efficace come strumento predittivo.

Se il nostro sistema quantistico è descritto dallo stato $|\mathbf{a}\rangle = a_0 |\mathbf{v}_0\rangle + a_1 |\mathbf{v}_1\rangle$ nella base $\{|\mathbf{v}_0\rangle, |\mathbf{v}_1\rangle\}$ e con $|a_0|^2 + |a_1|^2 = 1$, il postulato della misura ci dice che una misura detta *proiettiva* darà come risultato il valore associato allo stato $|\mathbf{v}_0\rangle$ con probabilità $|a_0|^2$ e il valore associato allo stato $|\mathbf{v}_1\rangle$ con probabilità $|a_1|^2$.

Ad esempio, supponiamo che i due stati del sistema siano il grado di polarizzazione (ad esempio, del fotone), $|\mathbf{v}_0\rangle \equiv |\uparrow\rangle$ e $|\mathbf{v}_1\rangle \equiv |\rightarrow\rangle$, e lo stato del sistema è descritto da $|\mathbf{a}\rangle = \sqrt{0.75} |\uparrow\rangle + \sqrt{0.25} |\rightarrow\rangle$. Una misura della polarizzazione ci darà polarizzazione verticale con probabilità 75% e polarizzazione orizzontale con probabilità del 25%.

È importante notare che questo implica che, per un sistema a due stati, ci sono solo due risultati possibili al contrario di quanti non accade nella fisica classica. Inoltre, la misura proiettiva *distrugge la sovrapposizione* degli stati.

Il secondo punto del postulato della misura dice che dopo la misura il sistema collappa nello stato associato al valore ottenuto. Riferendoci all'esempio precedente, se dalla prima misura abbiamo ottenuto il valore della polarizzazione verticale (che capita il 75% delle volte), istantaneamente il sistema sarà proiettato nello stato $|\uparrow\rangle$. Viceversa, se abbiamo ottenuto polarizzazione orizzontale, il sistema verrà proiettato e si troverà nello stato $|\rightarrow\rangle$. A questo punto possiamo fare un'interessante e importante osservazione. Se dopo la prima misura il sis-

tema è collassato nello stato $|\uparrow\rangle$, una qualsiasi misura successiva *nella stessa base* darà sempre lo stesso risultato. Infatti, il nuovo stato dopo la misura sarà $|v_0\rangle = |\uparrow\rangle$ e una misura successiva darà il valore "polarizzazione verticale" con il 100% di probabilità e il sistema collasserà nuovamente nello stato $|\uparrow\rangle$.

Ciò che abbiamo discusso fino ad ora può essere reso più preciso e formale. In particolare, la base in cui si fa la misura gioca un ruolo determinante. Per chiarire questo ruolo, è necessario discutere il significato degli autovalori di un operatore Hermittiano (sez. 2.4).

Un osservabile fisico (ad esempio, la polarizzazione) può essere associato ad un operatore Hermittiano. Come visto nella sezione 2.4, gli operatori Hermittiano possono essere diagonalizzati e possiamo ottenere i loro autovalori e autovettori. Se vogliamo misurare l'osservabile A, il postulato della misura ci dice che *i risultati della misura possono essere solo gli autovalori e il sistema collasserà nell'autostato di dell'operatore A*.

Possiamo rifrasare e spiegare questa frase con l'esempio della misura della polarizzazione. L'operatore polarizzazione P può essere diagonalizzato. I suoi autostati saranno $|\uparrow\rangle$ associato, ad esempio, all'autovalore +1 e $|\rightarrow\rangle$ associato all'autovalore -1. Se il sistema è in uno stato $|v_0\rangle$ per sapere quali possono essere i risultati della misura di polarizzazione dobbiamo scrivere lo stato come combinazione lineare degli autostati di P $\{|\uparrow\rangle, |\rightarrow\rangle\}$.

Nell'esempio precedente $|a\rangle = \sqrt{0.75}|\uparrow\rangle + \sqrt{0.25}|\rightarrow\rangle$. Una misura di P ci darà il valore +1 (autovalore di P) con probabilità 75% e il sistema collasserà nello stato $|\uparrow\rangle$. Nel rimanente 25% dei casi il risultato sarà -1 (autovalore di P) e il sistema collasserà nello stato $|\rightarrow\rangle$.

Il punto fondamentale di questa discussione è che la base, gli autovalori e il risultato della misura dipende dall'osservabile che vogliamo misurare. Ad esempio, sempre partendo dallo stato $|a\rangle$ se decidessimo di misurare una polarizzazione diversa (ad esempio, 45°), i risultati sarebbero completamente diversi. Questa osservazione sarà di fondamentale importanza quanto affronteremo i protocolli dell'informazione quantistica.

Riassumendo le regole dal postulato delle misura sono

1. Se vogliamo misurare un osservabile Φ , dobbiamo conoscerne i suoi autovalori $\{\phi_i\}$ e autovettori $\{|\phi_i\rangle\}$; cioè gli stati tali che $\Phi|\phi_i\rangle = \phi_i|\phi_i\rangle$. Gli autovettori saranno la base su cui decomporre lo stato del nostro sistema. Ovvero dobbiamo scrivere $|a\rangle = \sum_i a_i |\phi_i\rangle$ con $a_i = \langle \phi_i | a \rangle$.
2. La misura avrà come risultato l'autovalore ϕ_i con probabilità $|a_i|^2$.
3. Successivamente alla misura, il sistema si troverà nello stato $|\phi_i\rangle$ associato all'autovalore misurato.

IV – INTERPRETAZIONE QUANTISTICA DELL'ESPERIMENTO CON LA LUCE
POLARIZZATA

Con le informazioni acquisite riguardo alla meccanica quantistica ora siamo in grado di spiegare esperimento con la luce polarizzata discusso nella sezione 3.1.2.

In meccanica quantistica, ogni polarizzatore misura lo stato di polarizzazione di un fotone lungo una di due direzioni ortogonali. Lo stato quantistico di un fotone che incontra il polarizzatore orizzontale è la sovrapposizione di uno stato di polarizzazione orizzontale $|\rightarrow\rangle$ e di uno verticale $|\uparrow\rangle$, ovvero

$$|\mathbf{a}\rangle = a_0 |\rightarrow\rangle + a_1 |\uparrow\rangle,$$

dove $|\rightarrow\rangle$ e $|\uparrow\rangle$ costituiscono la base associata alla misura di polarizzazione orizzontale (o verticale) e a_0 e a_1 le rispettive ampiezze. Un fotone, quindi, attraversa il polarizzatore orizzontale e, al termine della misura, si trova nello stato $|\rightarrow\rangle$ con probabilità $p = |a_0|^2$. Nel caso di una comune lampadina, ovvero di un fascio non polarizzato, solo una frazione di fotoni attraversa il polarizzatore orizzontale e l'intensità del fascio conseguentemente si riduce. Supponiamo ad esempio che $a_0 = a_1 = 1/\sqrt{2}$ e quindi che $|a_0|^2 = |a_1|^2 = 1/2$. Avremmo che la probabilità di avere un fotone polarizzato \rightarrow che può passare il polarizzatore è 50%. Intuitivamente l'intensità del fascio sarà proporzionale al numero di fotoni, quindi dopo il polarizzatore in A dovremmo avere un fascio con intensità dimezzata. La meccanica quantistica, pertanto, è in grado di spiegare il risultato osservato sia nel caso di fascio costituito da un singolo fotone (il fotone non cede energia se attraversa un polarizzatore) sia in quello di grandi quantità di fotoni.

Se aggiungiamo un polarizzatore verticale e ripetiamo l'esperimento, osserviamo che il fascio è completamente assorbito. L'interpretazione quantistica non riserva sorprese. Il secondo polarizzatore, infatti, misura lo stato di polarizzazione nella direzione verticale. Anche questa volta, $|\mathbf{b}\rangle$, lo stato quantistico di un fotone prima della seconda misura è una sovrapposizione degli stati di polarizzazione orizzontale e verticale,

$$|\mathbf{b}\rangle = b_0 |\rightarrow\rangle + b_1 |\uparrow\rangle,$$

dove b_0 e b_1 sono le nuove ampiezze. Poiché un fotone che incontra il polarizzatore verticale in questo apparato ha attraversato il polarizzatore orizzontale, sappiamo però che, prima della seconda misura, il fotone si trova nello stato $|\rightarrow\rangle$ e che, quindi, l'ampiezza b_1 è nulla. Conseguentemente, il fotone è certamente assorbito dal polarizzatore verticale.

Le profonde implicazioni del principio di sovrapposizione degli stati emergono con forza quando si aggiunge un polarizzatore nella direzione di 45° (indicato con \nearrow). Lo stato quantistico generico $|\mathbf{c}\rangle$ di un fotone, in questo caso, si scrive come la sovrapposizione di uno stato di polarizzazione a 135° ,

$$|\nwarrow\rangle = \frac{|\uparrow\rangle - |\rightarrow\rangle}{\sqrt{2}} \quad (3.4.1)$$

e di uno a 45° ,

$$|\nearrow\rangle = \frac{|\uparrow\rangle + |\rightarrow\rangle}{\sqrt{2}}, \quad (3.4.2)$$

dove $|\nwarrow\rangle$ e $|\nearrow\rangle$ sono la base associata ai due stati obliqui e

$$|c\rangle = c_+ |\nwarrow\rangle + c_- |\nearrow\rangle.$$

Un fotone che incontra il polarizzatore obliquo, poiché ha attraversato il polarizzatore orizzontale, si trova nello stato $|\rightarrow\rangle$. Siccome

$$|\rightarrow\rangle = \frac{|\nwarrow\rangle - |\nearrow\rangle}{\sqrt{2}},$$

abbiamo che $p_{\nearrow} = |\langle \rightarrow | \nearrow \rangle|^2 = p_{\nwarrow} = |\langle \rightarrow | \nwarrow \rangle|^2 = 1/2$. Solo le misure che danno come risultato \nearrow sono associate a fotoni che passano il polarizzatore B; di conseguenza otteniamo che solo il 50% dei fotoni emerge dal polarizzatore B con polarizzazione \nearrow . Rispetto all'intensità del fascio iniziale avremo una fascio con intensità di $0.5 \times 0.5 = 0.25$.

Questo ragionamento si ripete per i fotoni che (con polarizzazione \nearrow) arrivano sul polarizzatore C. Dall'equazione (3.4.2) sappiamo come lo stato $|\nearrow\rangle$ si decomponga nella base $\{|\rightarrow\rangle, |\uparrow\rangle\}$. Quindi, per il fotone che arriva in C c'è una probabilità $p = |\langle \nearrow | \uparrow \rangle|^2 = 1/2$ che la misura dia il risultato \uparrow . Di conseguenza, il 50% dei fotoni che arrivano in C passa l'ultimo polarizzatore e arriva allo schermo. L'intensità finale del fascio (rispetto a quello iniziale) è del 12.5%. Il punto importante di questa discussione è che la meccanica quantistica permette di prevedere che, con l'inserimento del polarizzatore intermedio in B, i fotoni arrivino sullo schermo.

Concludiamo con un'importante osservazione. Quando diciamo che un fotone è in uno stato quantistico $|w\rangle$ dato dalla sovrapposizione di due stati $|\rightarrow\rangle$ e $|\uparrow\rangle$, con $|w\rangle = \alpha |\rightarrow\rangle + \beta |\uparrow\rangle$, per esempio, non intendiamo che il fotone è nello stato $|\rightarrow\rangle$ con probabilità $|\alpha|^2$ e nello stato $|\uparrow\rangle$ con probabilità $|\beta|^2$. Secondo la meccanica quantistica il fotone è in uno stato che è in una delle infinite possibili combinazioni lineari di $|\rightarrow\rangle$ e $|\uparrow\rangle$. Non ha senso chiedersi in che stato sia il fotone se non effettuando una misura, il risultato della quale sarà sempre e solo uno di due possibili. Questo fatto non ha corrispettivi classici ed è difficile sia da comprendere sia da accettare. Se non ci riusciamo siamo in buona compagnia. La lista degli scienziati che hanno sollevato dubbi sui fondamenti della meccanica quantistica comprende Albert Einstein, che pure ha ricevuto il premio Nobel per aver spiegato l'effetto fotoelettrico basandosi proprio sulla natura quantistica della luce. A oggi la meccanica quantistica si è mostrata in grado di prevedere i risultati sperimentali con un'accuratezza sbalorditiva e ha resistito a tutti i tentativi di metterne in discussione i fondamenti.

3.4.1 Fase globale e relativa

In precedenza abbiamo parlato indifferentemente di stati quantistici e di vettori di stato. Gli stati quantistici e i vettori di stato, tuttavia, non sono in corrispondenza

biunivoca. Consideriamo i vettori $|u\rangle$ e $e^{i\phi}|u\rangle$ che hanno lo stesso modulo ma differiscono per una fase globale ϕ . Il calcolo delle probabilità dei risultati di una qualunque misura fornisce sempre gli stessi valori.

Per semplificare la discussione, consideriamo un sistema a due livelli. Supponiamo che lo stato del sistema sia $|u\rangle = \sum_{i=1,2} \alpha_i |\phi_i\rangle$ dove $\{|\phi_i\rangle\}$ formano una base ortonormale dello spazio vettoriale. Lo stato con una fase globale si scriverà $e^{i\phi}|u\rangle = \sum_{i=1,2} e^{i\phi}\alpha_i |\phi_i\rangle$.

Supponiamo di voler misurare un osservabile O_1 che sia diagonale nella base $\{|\phi_i\rangle\}$ con relativi autovalori $\{\lambda_i\}$. Dato che $|e^{i\phi}\alpha_i|^2 = |\alpha_i|^2$, la teoria della misura ci dice che dalla misura otterremo l'autovalore λ_i con probabilità $|\alpha_i|^2$ indipendentemente dalla fase globale.

Questo risultato è generale. Supponiamo infatti di voler misurare un osservabile O_2 che è diagonale nella base $\{|\psi_i\rangle\}$ con relativi autovalori $\{\Lambda_i\}$. In questo caso dovremmo scrivere lo stato nella nuova base $|u\rangle = \sum_{i=1,2} \beta_i |\psi_i\rangle$ con diversi coefficienti ma con struttura identica. Lo stato con una fase globale si scriverà $e^{i\phi}|u\rangle = \sum_{i=1,2} e^{i\phi}\beta_i |\psi_i\rangle$. Anche in questo caso la misura darà l'autovalore Λ_i con probabilità $|\beta_i|^2$ indipendentemente dalla fase globale.

È importante evidenziare però che le differenze di fase fra stati sono osservabili e misurabili. Consideriamo, ad esempio, lo stato $|u\rangle = \alpha|0\rangle + \beta e^{i\phi}|1\rangle$ dove fra gli stati $|0\rangle$ e $|1\rangle$ c'è una differenza di fase $e^{i\phi}$. In questo caso, è possibile trovare degli osservabili e delle misure che distinguono fra lo stato $|u\rangle$ e lo stato $|v\rangle = \alpha|0\rangle + \beta|1\rangle$.

Come esempio possiamo prendere il caso in cui $\alpha = \beta = 1/\sqrt{2}$, $e^{i\phi} = -1$ e, quindi, $|u\rangle = |-\rangle = \alpha|0\rangle - \beta|1\rangle$ e $|v\rangle = |+\rangle = \alpha|0\rangle + \beta|1\rangle$. Questi stati sono autostati dell'operatore $X = |+\rangle\langle+| - |-\rangle\langle-|$ (si veda l'esercizio 1 capitolo 2). Una misura di $|u\rangle = |-\rangle$ darà con certezza il risultato -1 e una misura di $|v\rangle = |+\rangle$ darà con certezza il risultato 1 . Gli stati sono quindi distinguibili tramite una misura dell'operatore X .

Questa dimostrazione può essere estesa al caso più generale ma tralasciamo questa ulteriore complicazione.

V – STATI A MOLTI QUBIT

Siamo ora in grado di capire come descrivere un sistema di n qubit. Per ogni qubit usiamo uno spazio a due dimensioni e utilizziamo per semplicità la base canonica. Quindi il qubit i -esimo sarà associato allo spazio vettoriale V_i con base $\{|0\rangle_i, |1\rangle_i\}$. Lo spazio vettoriale di n qubit sarà dato dal prodotto tensore $V_0 \oplus V_1 \oplus \dots \oplus V_{n-1}$ (si noti che abbiamo numerato i qubit da 0 a $n-1$) che avrà dimensione 2^n .

Come discusso nella sezione 2.2, la base del prodotto tensore sarà composta dagli stati $\{|\alpha_i\rangle_0 \oplus |\beta_j\rangle_1 \oplus \dots \oplus |\gamma_k\rangle_{n-1}\} \equiv |\alpha_i\beta_j\dots\gamma_k\rangle$ dove α_i, β_j e γ_k possono assumere valore 0 o 1. Esplicitamente possiamo scriverli come

$$|0\rangle_0 \oplus |0\rangle_1 \oplus \dots \oplus |0\rangle_{n-1} = |00\dots0\rangle \quad (3.5.1)$$

$$|1\rangle_0 \oplus |0\rangle_1 \oplus \dots \oplus |0\rangle_{n-1} = |10\dots0\rangle$$

$$|0\rangle_0 \oplus |1\rangle_1 \oplus \dots \oplus |0\rangle_{n-1} = |01\dots0\rangle$$

$$\vdots \quad \vdots$$

$$(3.5.2)$$

$$|1\rangle_0 \oplus |1\rangle_1 \oplus \dots \oplus |0\rangle_{n-1} = |11\dots0\rangle$$

$$\vdots \quad \vdots$$

$$(3.5.3)$$

$$|1\rangle_0 \oplus |1\rangle_1 \oplus \dots \oplus |1\rangle_{n-1} = |11\dots1\rangle$$

Come si può vedere gli stati che compongono la base del sistema a n qubit rappresentano una base logica delle stringhe a n bit.

I ket della base canonica saranno scritti come vettori a 2^n componenti in cui tutti gli elementi sono nulli tranne uno. Ad esempio,

$$|00\dots0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, |10\dots0\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \dots, |11\dots1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \quad (3.5.4)$$

VI – STATI A DUE QUBIT E ENTANGLEMENT

L'informazione quantistica è legata allo studio dell'*entanglement*, fenomeno squisitamente quantistico che emerge nell'analisi dello stato e delle misure effettuate su qubit multipli. Lo spazio degli stati, in questo caso, è dato dal prodotto tensoriale degli spazi di ogni qubit.

3.6.1 Stati a due qubit separabili

Consideriamo un sistema a due qubit che è descritto dal prodotto tensore di due spazi vettoriali $V \otimes W$. I generici stati dei spazi vettoriali distinti sono $|\mathbf{v}\rangle_V = \alpha|\mathbf{0}\rangle_V + \beta|\mathbf{1}\rangle_V \in V$ e $|\mathbf{w}\rangle_W = \gamma|\mathbf{0}\rangle_W + \delta|\mathbf{1}\rangle_W \in W$. Lo stato congiunto sarà

$$\begin{aligned} |\mathbf{v}\rangle_V \otimes |\mathbf{w}\rangle_W &= (\alpha|\mathbf{0}\rangle_V + \beta|\mathbf{1}\rangle_V) \otimes (\gamma|\mathbf{0}\rangle_W + \delta|\mathbf{1}\rangle_W) \\ &= \alpha\gamma|\mathbf{00}\rangle + \alpha\delta|\mathbf{01}\rangle + \beta\gamma|\mathbf{10}\rangle + \beta\delta|\mathbf{11}\rangle \end{aligned} \quad (3.6.1)$$

dove nell'ultimo passaggio abbiamo tralasciato di scrivere l'indice dello spazio vettoriale sottointendendo che nel ket $|\mathbf{ij}\rangle$ il primo valore i si riferisce allo stato V e il secondo j allo spazio W .

Gli stati che si possono scrivere come il prodotto tensore $|\mathbf{v}\rangle_V \otimes |\mathbf{w}\rangle_W$ vengono detti *fattorizzabili*. In termini un pò imprecisi, si potrebbe dire che gli stati del sistema V e W sono "separabili" o e non si influenzano a vicenda durante un processo di misura.

Andiamo a vedere cosa succede quando facciamo una misura sul primo qubit. Per questo è conveniente scrivere lo stato come

$$|\mathbf{v}\rangle_V \otimes |\mathbf{w}\rangle_W = \alpha|\mathbf{0}\rangle_V \otimes (\gamma|\mathbf{0}\rangle_W + \delta|\mathbf{1}\rangle_W) + \beta|\mathbf{1}\rangle_V \otimes (\gamma|\mathbf{0}\rangle_W + \delta|\mathbf{1}\rangle_W) \quad (3.6.2)$$

Usando le regole della misura potremmo dire che dalla misura del primo qubit darà l'autovalore λ_0 con probabilità $|\alpha|^2$ e l'autovalore λ_1 con probabilità $|\beta|^2$. Successivamente, lo stato del qubit V si troverà nello stato $|\mathbf{0}\rangle_V$ o $|\mathbf{1}\rangle_V$, rispettivamente. È interessante vedere cosa succede allo stato del sistema W a causa della misura in V . Osservando lo stato composto come scritto in Eq. (3.6.2), se il sistema V collassa nello stato $|\mathbf{0}\rangle_V$ lo stato di W si troverà in $\gamma|\mathbf{0}\rangle_W + \delta|\mathbf{1}\rangle_W$. Se il sistema V collassa nello stato $|\mathbf{1}\rangle_V$ lo stato di W si troverà in $\gamma|\mathbf{0}\rangle_W + \delta|\mathbf{1}\rangle_W$. Ne consegue che la misura su V non influenza lo stato del sistema W perchè lo stato di W sarà lo stesso indipendentemente dal risultato della misura in V .

3.6.2 Stati *entangled* (fortemente correlati)

Esaminiamo ora le profonde conseguenze legate al fatto che in meccanica quantistica lo stato di un sistema che consiste di n qubit è descritto dal prodotto tensoriale di spazi vettoriali.

Gli elementi dello spazio vettoriale $V \otimes W$ non sono tutti ottenibili come prodotto tensoriale di due elementi $|\mathbf{v}\rangle \in V$ e $|\mathbf{w}\rangle \in W$. Per capirne il motivo, fissata la base

$|0\rangle$ e $|1\rangle$, cerchiamo due vettori $|\mathbf{v}\rangle = \alpha|0\rangle_V + \beta|1\rangle_V \in V$ e $|\mathbf{w}\rangle = \gamma|0\rangle_W + \delta|1\rangle_W \in W$, tali che $|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle \in V \otimes W$ si scriva come

$$|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle \stackrel{?}{=} \frac{\sqrt{2}}{2} |0\rangle_V \otimes |1\rangle_W + \frac{\sqrt{2}}{2} |1\rangle_V \otimes |0\rangle_W. \quad (3.6.3)$$

Il punto di domanda sopra il simbolo di uguale in questa equazione vuol dire che stiamo cercando di scrivere il membro di destra come prodotto tensore di due stati fattorizzabili $|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle$. Come vedremo questo non è possibile.

L'equazione (3.6.3) è da confrontare con la generica espressione che si otterrebbe combinando con il prodotto tensore $|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle$ che qui riscriviamo [rispetto all'Eq. (3.6.1)] esplicitando la dipendenza rispetto a V e W

$$|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle = \alpha\gamma|0\rangle_V \otimes |0\rangle_W + \alpha\delta|0\rangle_V \otimes |1\rangle_W + \beta\gamma|1\rangle_V \otimes |0\rangle_W + \beta\delta|1\rangle_V \otimes |1\rangle_W. \quad (3.6.4)$$

Dall'uguaglianza delle due espressioni ricaviamo i vincoli

$$\alpha\gamma = \beta\delta = 0, \quad \alpha\delta = \beta\gamma = \frac{\sqrt{2}}{2}$$

che sono chiaramente inconsistenti. Uno stato quantistico di un sistema di 2 qubit come questo si dice *entangled*.

Una delle proprietà più importanti dei sistemi entangled è come si comportano quando li si misura. Contrariamente al caso di stati fattorizzabili, in questo caso, la misura sul sistema V influenzà anche il sistema W . Per vederlo nel dettaglio, partendo dallo stato (3.6.3) pensiamo di misurare il sistema V . In questo caso, la probabilità di misurare λ_0 e λ_1 è uguale e vale 0.5. Con le stesse probabilità il sistema collasserà negli stati $|0\rangle_V$ e $|1\rangle_V$. Ma questa volta lo stato $|0\rangle_V$ è *correlato* (o associato) allo stato $|1\rangle_W$ visto che sono combinati nel ket $|0\rangle_V \otimes |1\rangle_W$. Di conseguenza, se il sistema V collassa nello stato $|0\rangle_V$ indurrà un collasso del sistema W nello stato $|1\rangle_W$ e lo stato del sistema globale dopo il collasso sarà $|0\rangle_V \otimes |1\rangle_W$. Allo stesso modo, un collasso del sistema V nello stato $|1\rangle_V$ indurrà un collasso del sistema W nello stato $|0\rangle_W$. Le misure su V e W sono quindi fortemente correlate: una misura in uno dei due sistemi influenza e vincola lo stato dell'altro. Questo fatto è ancora più sorprendente se si pensa che gli stati V e W possono essere separati spazialmente anche di chilometri quindi si può escludere una qualsiasi interazione o influenze diretta di V su W .

Gli stati *entangled* hanno un ruolo privilegiato nell'informazione quantistica dato che sono alla base di alcune delle più importanti applicazioni come il teletrasporto quantistico, il *dense coding* e la crittografia quantistica. Fra gli stati *entangled* alcuni sono particolarmente noti e utilizzati. Vengono detti stati di Bell dal nome di John

Bell che ne studiò a fondo le proprietà e il loro significato. Lo stato in Eq. (3.6.3) fa parte della cosiddetta *base di Bell* che è costituita da quattro stato ortogonali

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_V \otimes |0\rangle_W + |1\rangle_V \otimes |1\rangle_W) \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_V \otimes |0\rangle_W - |1\rangle_V \otimes |1\rangle_W) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_V \otimes |1\rangle_W + |1\rangle_V \otimes |0\rangle_W) \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_V \otimes |1\rangle_W - |1\rangle_V \otimes |0\rangle_W). \end{aligned} \quad (3.6.5)$$

Per le applicazioni in quantum information è importante notare che gli stati di Bell costituiscono una base ortonormale dello spazio a due qubit. Per descrivere lo stato di un sistema a due qubit possiamo alternativamente usare la base canonica $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ o la base di Bell $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$.

L'ortogonalità della base di Bell ci dice inoltre che è possibile distinguerli tramite una misura. In termini più precisi è possibile costruire un osservabile

$$A = \lambda_0 |\Phi^+\rangle\langle\Phi^+| + \lambda_1 |\Phi^-\rangle\langle\Phi^-| + \lambda_2 |\Psi^+\rangle\langle\Psi^+| + \lambda_4 |\Psi^-\rangle\langle\Psi^-| \quad (3.6.6)$$

che sia diagonale nella base di Bell. Quindi se il sistema si trova in uno stato di Bell, una misura dell'operatore A darà con certezza l'autovalore corrispondente.

VII – TRASFORMAZIONI UNITARIE

L'elaborazione dell'informazione quantistica consiste di una sequenza opportuna di trasformazioni dello stato quantistico di un sistema di n qubit. In meccanica quantistica le sole trasformazioni ammissibili sono unitarie. Sia $|a\rangle = a_0|x_0\rangle + a_1|x_1\rangle$ uno stato quantistico, con $\{|x_0\rangle, |x_1\rangle\}$ una qualunque base e $|a_0|^2 + |a_1|^2 = 1$. Una trasformazione *unitaria* U è

- lineare, ovvero, $U|a\rangle = U(a_0|x_0\rangle + a_1|x_1\rangle) = a_0U|x_0\rangle + a_1U|x_1\rangle$ e
- invertibile con l'inversa uguale alla trasposta coniugata, ovvero $U^{-1}|a\rangle = U^\dagger|a\rangle$.

Quest'ultima proprietà garantisce che le trasformazioni unitarie lasciano invariati i prodotti scalari, e quindi anche la norma dei vettori su cui agiscono e le probabilità associate alle misure. Infatti, prendiamo due stati $|a\rangle$ and $|b\rangle$ con prodotto scalare $\langle b|a\rangle$. Se questi evolvono secondo un operatore unitario U avremo $|a'\rangle = U|a\rangle$ and $|b'\rangle = U|b\rangle$, il prodotto scalare degli stati evoluti sarà $\langle b'|a'\rangle = \langle b|U^\dagger U|a\rangle = \langle b|a\rangle$. Quindi, come ci aspettavamo, il prodotto scalare è preservato.

La composizione di trasformazioni unitarie è una trasformazione unitaria. Identificato un insieme di trasformazioni unitarie di base, questa proprietà di gruppo apre alla possibilità di combinare le trasformazioni di base per l'implementazione

di algoritmi, alla stregua di quanto avviene con le porte logiche nei circuiti combinatori. Un'importante differenza tra il caso classico e quello quantistico è legato all'invertibilità del calcolo. Le elaborazioni *classiche* sono *dissipative*: dall'uscita di un *AND*, per esempio, non è possibile risalire ai valori all'ingresso della porta. Le elaborazioni *quantistiche*, invece, sono *reversibili*: l'effetto di una trasformazione unitaria può essere annullato applicando la trasformazione inversa, per cui a partire da uno stato quantistico trasformato è sempre possibile ricostruire lo stato originale.

3.7.1 Porte quantistiche

Trasformazioni di Pauli

Con l'espressione porte quantistiche non si intendono dispositivi ma trasformazioni unitarie che possono essere implementate nella pratica. Partiamo con quattro trasformazioni unitarie che agiscono sul singolo qubit. Trattandosi di trasformazioni lineari è sufficiente definire la loro azione su una base. Nel nostro caso sceglieremo la base canonica $\{|0\rangle, |1\rangle\}$ e definiamo, oltre all'*identità* Id , le tre *trasformazioni di Pauli* (detti anche operatori di Pauli) X , Y e Z :

$$\begin{aligned} \text{Id} |0\rangle &:= |0\rangle, & \text{Id} |1\rangle &:= |1\rangle; \\ X |0\rangle &:= |1\rangle, & X |1\rangle &:= |0\rangle; \\ Y |0\rangle &:= -i |1\rangle, & Y |1\rangle &:= i |0\rangle; \\ Z |0\rangle &:= -|0\rangle, & Z |1\rangle &:= |1\rangle. \end{aligned} \quad (3.7.1)$$

Analizzando l'effetto degli operatori, si nota che nella base canonica, X corrisponde al *NOT* tra bit classici. Infatti, la sua azione è $|0\rangle \leftrightarrow |1\rangle$. L'operatore Z genera un cambio della fase relativa dato che $|0\rangle \leftrightarrow |0\rangle$ e $|1\rangle \leftrightarrow |1\rangle$. Infine, l'operatore Y può essere visto come una combinazione dei due precedenti dato che $Y = -iXZ$.

È interessante scrivere gli operatori di Pauli in forma matriciale nella base canonica. Per fare questo, ricordiamo che l'elemento matriciale di un operatore U in posizione $i-j$ è ottenuto dal prodotto scalare $U_{i,j} = \langle i|U|j\rangle$. Ad esempio, l'elemento $X_{0,1} = \langle 0|U|1\rangle$. Usando queste definizioni e l'eq. (3.7.1), si ottiene (nella base $\{|1\rangle, |0\rangle\}$)

$$\begin{aligned} \text{Id} &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ X &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ Y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\ Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \end{aligned} \quad (3.7.2)$$

Un generico operatore unitario U agente su un singolo qubit può essere scritto sempre come combinazioni di X , Y e Z . Si può dimostrare³ che U si può scrivere come

$$U = \cos \frac{\alpha}{2} \text{Id} + i \sin \frac{\alpha}{2} (n_x X + n_y Y + n_z Z) \quad (3.7.3)$$

dove α e gli n_i ($i = x, y, z$) sono i parametri che caratterizzano l'operatore.

Trasformazione di Hadamard

Utilizzando sempre la base canonica, la trasformazione di Hadamard H , che opera sempre su un singolo qubit, corrisponde al cambio di base che abbiamo incontrato in occasione dell'esperimento dei tre polarizzatori:

$$\begin{aligned} H|0\rangle &= |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \text{ e} \\ H|1\rangle &= |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}. \end{aligned} \quad (3.7.4)$$

Nel prossimo esempio sarà chiaro che l'espressione di una trasformazione in una base, anche nel caso della base canonica, è sufficiente a definire la trasformazione senza ambiguità ma può essere fuorviante.

In forma matriciale (nella base canonica $\{|1\rangle, |0\rangle\}$) l'operatore di Hadamard si scrive come

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \quad (3.7.5)$$

Controlled-NOT

Consideriamo ora, il *controlled-NOT*, *CNOT*, una trasformazione che agisce su 2 qubit, A e B. Nella base canonica l'azione del *CNOT* è:

$$\begin{aligned} \text{CNOT}|0\rangle_A \otimes |0\rangle_B &:= |0\rangle_A \otimes |0\rangle_B \\ \text{CNOT}|0\rangle_A \otimes |1\rangle_B &:= |0\rangle_A \otimes |1\rangle_B \\ \text{CNOT}|1\rangle_A \otimes |0\rangle_B &:= |1\rangle_A \otimes |1\rangle_B \\ \text{CNOT}|1\rangle_A \otimes |1\rangle_B &:= |1\rangle_A \otimes |0\rangle_B \end{aligned}$$

Se pensiamo $|0\rangle$ e $|1\rangle$ come bit classici il CNOT nega il bit B se il bit A vale 1, altrimenti non fa nulla. Osserviamo che questa interpretazione del CNOT dipende

³ Non faremo una dimostrazione formale ma daremo un'idea del fatto che sia così parlando di rotazioni sulla sfera di Bloch nella sezione 3.8.

dalla scelta della base. Nella base $\{|+\rangle, |-\rangle\}$ è il primo qubit che passa da $|+\rangle$ a $|-\rangle$ se il secondo è $|-\rangle$, infatti:

$$\begin{aligned} \text{CNOT}|+\rangle_A \otimes |+\rangle_B &= \frac{1}{2} \text{CNOT}(|0\rangle_A + |1\rangle_A) \otimes (|0\rangle_B + |1\rangle_B) \\ &= \frac{1}{2} (|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B + |0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B) \\ &= \frac{1}{2} (|0\rangle_A + |1\rangle_A) \otimes (|0\rangle_B + |1\rangle_B) \\ &= |+\rangle_A \otimes |+\rangle_B \end{aligned}$$

$$\begin{aligned} \text{CNOT}|+\rangle_A \otimes |-\rangle_B &= \frac{1}{2} \text{CNOT}(|0\rangle_A + |1\rangle_A) \otimes (|0\rangle_B - |1\rangle_B) \\ &= \frac{1}{2} (|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B - |0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) \\ &= \frac{1}{2} (|0\rangle_A - |1\rangle_A) \otimes (|0\rangle_B - |1\rangle_B) \\ &= |-\rangle_A \otimes |-\rangle_B \end{aligned}$$

$$\begin{aligned} \text{CNOT}|-\rangle_A \otimes |+\rangle_B &= \frac{1}{2} \text{CNOT}(|0\rangle_A - |1\rangle_A) \otimes (|0\rangle_B + |1\rangle_B) \\ &= \frac{1}{2} (|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B + |0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) \\ &= \frac{1}{2} (|0\rangle_A - |1\rangle_A) \otimes (|0\rangle_B + |1\rangle_B) \\ &= |-\rangle_A \otimes |+\rangle_B \end{aligned}$$

$$\begin{aligned} \text{CNOT}|-\rangle_A \otimes |-\rangle_B &= \frac{1}{2} \text{CNOT}(|0\rangle_A - |1\rangle_A) \otimes (|0\rangle_B - |1\rangle_B) \\ &= \frac{1}{2} (|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B - |0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B) \\ &= \frac{1}{2} (|0\rangle_A + |1\rangle_A) \otimes (|0\rangle_B - |1\rangle_B) \\ &= |+\rangle_A \otimes |-\rangle_B \end{aligned}$$

L'importanza dell'operatore CNOT risiede nel fatto che può generare entanglement fra due qubit. Prendiamo, per esempio, due qubit nello stato

$$|v\rangle_V \otimes |w\rangle_W = \frac{|0\rangle_V + |1\rangle_V}{\sqrt{2}} \otimes |0\rangle_W = \frac{1}{\sqrt{2}} (|00\rangle + |10\rangle) \quad (3.7.6)$$

Secondo la definizione data in Sezione 3.6.1 questo stato è separabile visto che si può pensare come la composizione di uno stato $|v\rangle_V = \frac{|0\rangle_V + |1\rangle_V}{\sqrt{2}}$ e di uno stato $|w\rangle_W = |0\rangle_W$. Applichiamo ora l'operatore CNOT allo stato e otteniamo

$$|v\rangle_V \otimes |w\rangle_W \rightarrow \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = |\Phi^+\rangle. \quad (3.7.7)$$

Lo stato fattorizzabile è stato trasformato in uno stato entangled di Bell. La porta CNOT che quindi genera l'entanglement fra i sistemi V e W. Questo è possibile perché la porta CNOT agisce sempre sullo stato composto $V \otimes W$ (usa il primo qubit come controllo e agisce sul secondo).

È possibile dimostrare [[nielsen-chuang_book](#)] che la porta CNOT è sufficiente a generare tutti gli stati entangled anche in un sistema a n qubit. È quindi un operatore o porta logica fondamentale.

VIII – RAPPRESENTAZIONE DI UN QUBIT: SFERA DI BLOCH

Esiste un modo semplice e intuitivo di rappresentare lo stato di un qubit. Come detto un generico stato quantistico a due livelli o qubit è scritto come $|\psi\rangle = a_0 |\mathbf{0}\rangle + a_1 |\mathbf{1}\rangle$ con il vincolo uteriore di normalizzazione dello stato: $|a_0|^2 + |a_1|^2 = 1$. Le funzioni trigonometriche $\cos \theta$ e $\sin \theta$ naturalmente soddisfano la condizione di normalizzazione. Quindi in generale possiamo scrivere $|a_0|^2 = \cos^2 \theta$ e $|a_1|^2 = \sin^2 \theta$ per un opportuno θ .

Dobbiamo ricordare però che i coefficienti a_0 e a_1 sono complessi. Dato che solo la fase relativa fra gli stati è osservabile, possiamo assumere, ad esempio, che $a_0 = \cos \theta$ sia reale mentre $a_1 = \sin \theta e^{-i\phi}$ (dove $e^{-i\phi}$ rappresenta la fase relativa fra i due stati). In questo modo, lo stato del qubit è univocamente determinato dai due anelli $\{\theta, \phi\}$.

C'è un modo geometrico per rappresentare gli stati dei qubit. Consideriamo lo stato generico

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |\mathbf{1}\rangle + \sin\left(\frac{\theta}{2}\right) e^{i\phi} |\mathbf{0}\rangle \quad (3.8.1)$$

e il relativo stato *bra*

$$\langle\psi| = \cos\left(\frac{\theta}{2}\right) \langle\mathbf{1}| + \sin\left(\frac{\theta}{2}\right) e^{-i\phi} \langle\mathbf{0}| \quad (3.8.2)$$

(si noti che il termine di fase è stato coniugato: $e^{-i\phi} \leftrightarrow e^{i\phi}$).

Calcoliamo i valori medi dei operatori di Pauli X, Y e Z con lo stato $|\psi\rangle$. Abbiamo

$$\begin{aligned} x &= \langle\psi|X|\psi\rangle = \cos \phi \sin \theta \\ y &= \langle\psi|Y|\psi\rangle = \sin \phi \sin \theta \\ z &= \langle\psi|Z|\psi\rangle = \cos \theta \end{aligned}$$

Queste non sono solo altre che le coordinate in uno spazio tridimensionale di un punto che si muove su una sfera (si veda la figura 15). Se consideriamo il vettore che congiunge l'origine degli assi con il punto di coordinate $\{x, y, z\}$, l'angolo θ è quello formato dal vettore e dall'asse z mentre l'angolo ϕ è quello formato dal vettore sul piano $y - z$ (si veda la figura 15).

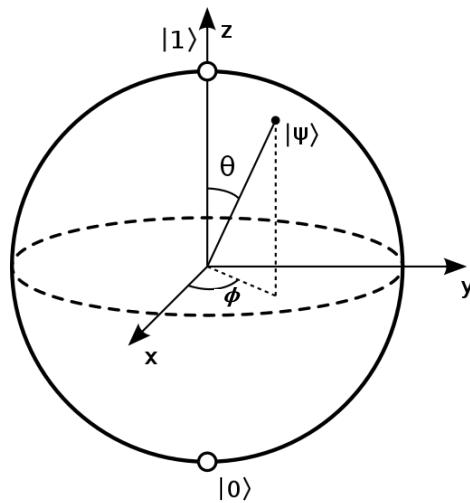


Figure 15: La sfera di Bloch per rappresentare lo stato $|\psi\rangle$ di un qubit.

Possiamo aggiungere un'importante osservazione. Gli operatori unitari permettono di manipolare e trasformare gli stati dei qubit. Per una qualsiasi trasformazione unitaria possiamo scrivere che $|\psi_f\rangle = U|\psi\rangle$; ovvero che lo stato iniziale $|\psi\rangle$ viene trasformato nello stato finale $|\psi_f\rangle$. Ma anche lo stato finale potrà essere rappresentato sulla sfera di Bloch e associato a nuovi angoli $\{\theta_f, \phi_f\}$. A livello matematico e geometrico, due stati su una sfera sono trasformabili l'uno nell'altro mediante una rotazione. Concludiamo che ogni operatore unitario può essere visto come una rotazione sulla sfera di Bloch.

Facciamo un esempio e consideriamo l'operatore X di Pauli (che è anche un operatore unitario). Dalla tabella 3.7.1 sappiamo che $X|0\rangle = |1\rangle$ (e $X|1\rangle = |0\rangle$). Se lo stato iniziale è $|\psi\rangle = |1\rangle$, dall'Eq. (3.8.3) abbiamo che $\{x, y, z\} = \{0, 0, 1\}$. Dopo l'applicazione di X lo stato finale sarà $|\psi_f\rangle = |0\rangle$ e quindi avremo $\{x_f, y_f, z_f\} = \{0, 0, -1\}$.

Più in generale possiamo scrivere l'operatore U in Eq. (3.7.3) con $n_x = n_z = 0$ e $\alpha \rightarrow -\alpha$ come

$$U = \cos\left(\frac{\alpha}{2}\right) \text{Id} - i \sin\left(\frac{\alpha}{2}\right) Y. \quad (3.8.3)$$

Se applichiamo U allo stato iniziale $|\psi\rangle = |1\rangle$ otteniamo

$$|\psi_f\rangle = U|\psi\rangle = \cos\left(\frac{\alpha}{2}\right)|1\rangle + \sin\left(\frac{\alpha}{2}\right)|0\rangle. \quad (3.8.4)$$

Passando alla rappresentazione sulla sfera di Bloch lo stato iniziale sarà $\{x, y, z\} = \{0, 0, 1\}$ mentre, usando le definizioni in Eq. (3.8.3), lo stato finale sarà $\{x_f, y_f, z_f\} = \{\sin \alpha, 0, \cos \alpha\}$. Quindi, geometricamente lo stato finale può essere visto come la rotazione dello stato iniziale di un angolo α attorno all'asse Y (si veda la Figura 15 con $\phi = 0$ e $\theta = \alpha$). Osservazioni e conti analoghi possono essere fatti per gli operatori X e Z che sono legati, rispettivamente, alle rotazioni attorno agli assi X e Z .

Per finire, usando la rappresentazione sulla sfera di Bloch si può intuire che solo due operatori della base di Pauli sono sufficienti per ottenere tutte le trasformazioni unitarie su un sistema a due livelli. Una trasformazione unitaria deve permettere di trasformare un qualsiasi stato iniziale in un qualsiasi stato finale. Se ad esempio partiamo dallo stato iniziale $\{x, y, z\} = \{0, 0, 1\}$ possiamo fare una rotazione intorno all'asse X di un angolo θ mediante l'operatore X seguita da una rotazione intorno all'asse Z di un angolo ϕ mediante l'operatore Z. con l'aiuto della figura 15, è possibile convincersi che in questo modo possiamo trasformare lo stato $\{x, y, z\} = \{0, 0, 1\}$ in uno stato generico $\{x_f, y_f, z_f\} = \{\cos \phi \sin \theta, \sin \phi \sin \theta, \cos \theta\}$. Lo stato iniziale $\{x, y, z\} = \{0, 0, 1\}$ non ha niente di particolare quindi scegliendo opportunamente θ e ϕ è possibile trasformare un qualsiasi stato iniziale in un qualsiasi stato finale.

IX – INIZIALIZZAZIONE DI UN SISTEMA A SINGOLO QUBIT

Per l'informazione quantistica è di fondamentale importanza la possibilità di inizializzare un sistema quantistico a due livelli in un generico stato $|\psi\rangle = \cos \alpha |0\rangle + e^{i\gamma} \sin \alpha |1\rangle$ con α, β e γ arbitrari.

Per fare questo abbiamo bisogno della porta logica di Hadamard H e di una nuova porta $U_{ph}(\gamma)$ detta *phase gate* che agisce nel seguente modo: $|0\rangle \rightarrow |0\rangle$ e $|1\rangle \rightarrow e^{i\gamma} |1\rangle$. La *phase gate* non cambia lo stato logico del qubit ma lo stato $|1\rangle$ acquista un fattore di fase $e^{i\gamma}$ (da cui il nome). Questa porta logica è talmente usata che spesso viene considerata come fondamentale⁴.

Partiamo dallo stato $|0\rangle$ e applichiamo una porta di Hadamard per ottenere $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$. A questo punto, applichiamo la *phase gate* $U_{ph}(-2\alpha)$ che genera uno sfasamento di -2α e una nuova porta H

$$\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \rightarrow \frac{1}{\sqrt{2}} (|0\rangle + e^{-i2\alpha} |1\rangle) \rightarrow \frac{1}{\sqrt{2}} (|+\rangle + e^{-i2\alpha} |-\rangle). \quad (3.9.1)$$

Esplicitiamo gli stati $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$ e raccogliamo i termini che moltiplicano $|0\rangle$ e $|1\rangle$

$$\begin{aligned} \frac{1}{\sqrt{2}} (|+\rangle + e^{-i2\alpha} |-\rangle) &= \frac{1}{2} [(1 + e^{-i2\alpha}) |0\rangle + (1 - e^{-i2\alpha}) |1\rangle] \\ &= \frac{e^{-i\alpha}}{2} [(e^{i\alpha} + e^{-i\alpha}) |0\rangle + (e^{i\alpha} - e^{-i\alpha}) |1\rangle] \\ &= \frac{e^{-i\alpha}}{2} [2 \cos \alpha |0\rangle + 2i \sin \alpha |1\rangle] \\ &= e^{-i\alpha} (\cos \alpha |0\rangle + i \sin \alpha |1\rangle). \end{aligned} \quad (3.9.2)$$

Negli ultimi passaggi abbiamo semplicemente raccolto il fattore esponenziale $e^{-i\alpha}$ e usato le relazioni $\cos x = \frac{e^{ix} + e^{-ix}}{2}$ e $\sin x = \frac{e^{ix} - e^{-ix}}{2i} = -i \frac{e^{ix} - e^{-ix}}{2}$.

⁴ Ricordiamo che bastano due porte logiche quantistiche ad un qubit per formare un set universale. La scelta delle porte che formano l'insieme à comunque una certa arbitarietà.

Applichiamo la porta $U_{ph}(-\pi/2)$. Il suo unico effetto è di aggiungere un fattore di fase $e^{-i\pi/2} = -i$ al ket $|1\rangle$. Infine, applichiamo l'operatore $U_{ph}(\gamma)$

$$e^{-i\alpha} (\cos \alpha |0\rangle + i \sin \alpha |1\rangle) \rightarrow \cos \alpha |0\rangle + \sin \alpha |1\rangle \rightarrow \cos \alpha |0\rangle + e^{i\gamma} \sin \alpha |1\rangle \quad (3.9.3)$$

dove negli ultimi passaggi abbiamo trascurato il fattore di fase globale $e^{-i\alpha}$ che non è osservabile (si veda la sezione 3.4.1).

Ricapitolando, partendo dallo stato iniziale $|0\rangle$, basta applicare in sequenza gli operatori H , $U_{ph}(-2\alpha)$, H , $U_{ph}(-\pi/2)$ e $U_{ph}(\gamma)$ per ottenere lo stato $\cos \alpha |0\rangle + e^{i\gamma} \sin \alpha |1\rangle$. Quindi, scegliendo opportunamente i parametri α e γ , è possibile costruire uno stato quantistico arbitrario.

X – ESERCIZI

3.10.1 Esercizio 1

1. Un sistema quantistico si trova nello stato $|0\rangle$. Si misura l'osservabile (operatore) $Z = |1\rangle\langle 1| - |0\rangle\langle 0|$. Quali sono i risultati della misura, le corrispondenti probabilità e lo stato del sistema dopo la misura?
2. Si consideri la stessa misura su un sistema nello stato $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.
3. Si consideri la misura dell'operatore $X = |1\rangle\langle 0| + |1\rangle\langle 0|$ sugli stati $|0\rangle$ e $|1\rangle$.

3.10.2 Esercizio 2: Misure sequenziali

1. Si consideri un sistema quantistico nello stato $|0\rangle$. Si misurano in sequenza gli osservabili $X = |1\rangle\langle 0| + |1\rangle\langle 0|$ e $Z = |1\rangle\langle 1| - |0\rangle\langle 0|$. Quali sono i risultati delle misure con le rispettive probabilità ?
2. Cosa succede se nell'esercizio precedente lo stato iniziale $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$?

4 | INFORMAZIONE QUANTISTICA (ESEMPI DI BASE)

I – PARALLELISMO QUANTISTICO

Come visto nella sezione 3.7.4, la porta di Hadamard H ci permette di costruire un qubit in sovrapposizione di stati logici. Ad esempio,

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \quad (4.1.1)$$

Come per il gatto di Schroedinger, questo qubit è allo stesso tempo nello stato logico 0 che nello stato logico 1. In questo modo, in un singolo qubit abbiamo racchiuso tutta l'informazione logica disponibile. Questa osservazione è alla base del parallelismo quantistico che è una delle proprietà che permette di ottenere dei vantaggi sulla computazione classica. Per comprenderlo a pieno la sua importanza è bene fare qualche esempio.

Ricordiamo che all'intero x associamo la stringa di bit $x_1x_2\dots x_n$ con $x_i = 0, 1$ e $i = 0, 1, \dots, n$ tale che $x = x_12^{n-1} + x_22^{n-2} + \dots + x_n2^0$ (sec. 1.2 e [[nielsen-chuang_book](#)]). In maniera analoga, a livello quantistico useremo n qubit e associeremo ad una stringa logica $x = 010..1$ lo stato quantistico $|x\rangle = |010..1\rangle$. Il vantaggio di usare stati quantistici è che in un *singolo* stato quantistico è possibile codificare *tutta* l'informazione logica, cioè tutte le possibili stringhe a n bit.

Per capire come questo possa succedere è conveniente partire da un sistema a due bit. Le stringhe logiche sono 00, 01, 10 e 11. Classicamente le possiamo trattare o manipolare singolarmente. Ad esempio, una sequenza di porte logiche può essere applicata ad un singolo stato alla volta. A livello quantistico le cose cambiano.

Supponiamo di partire dalla due qubit inizializzati nello stato $|00\rangle \equiv |0\rangle \otimes |0\rangle$ e di applicare due porte di Hadamard ai singoli qubit. Le due porte applicate contemporaneamente si denotano come $H \otimes H \equiv H^{\otimes 2}$ dove la notazione \otimes indica che la prima porta è applicata al primo qubit e la seconda al secondo qubit [[nielsen-chuang_book](#)]. Secondo le regole studiate in Sec. 3.7.4 e riportate sopra avremo

$$|0\rangle \otimes |0\rangle \xrightarrow{H^{\otimes 2}} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |10\rangle + |01\rangle + |11\rangle) \quad (4.1.2)$$

dove nell'ultima espressione abbiamo esplicitato il calcolo e usato la notazione compatta $|ij\rangle \equiv |i\rangle \otimes |j\rangle$. In Eq. (4.1.2) si vede che lo stato ottenuto applicando due porte di Hadamard è sovrapposizione di *tutti i possibili stati logici*.

Se adesso applichiamo un operatore unitario U , ad esempio una posta logica, ricordando le proprietà di linearità della meccanica quantistica, otterremo

$$\frac{1}{2}(|00\rangle + |10\rangle + |01\rangle + |11\rangle) \xrightarrow{U} \frac{1}{2}(U|00\rangle + U|10\rangle + U|01\rangle + U|11\rangle) \quad (4.1.3)$$

ovvero agirà contemporaneamente su tutti gli stati logici. In altre parole possiamo processare o manipolare *parallelamente* tutti gli stati logici allo stesso tempo.

Questo ragionamento si estende in maniera semplice al caso di n qubit. In questo caso, lo stato iniziale sarà $|00\dots0\rangle$ e applicheremo n porte di Hadarmard $H^{\otimes n}$.

$$\begin{aligned} |00\dots0\rangle &\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2^{\frac{n}{2}}}(|00..0\rangle + |10..0\rangle + \dots + |11..1\rangle) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle. \end{aligned} \quad (4.1.4)$$

Nell'ultimo passaggio abbiamo definito $N = 2^n$ e siamo passati dalla notazione in termini di stringhe logiche (es. $0100\dots11$) a quelle in termini di numeri interi x compresi fra 0 e $N - 1$. Anche in questo caso, applicando successivamente un operatore unitario U avremo

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} U|x\rangle. \quad (4.1.5)$$

Ovvero, possiamo manipolare *parallelamente* tutte le N stringhe logiche.

L'operazione di inizializzazione descritta in (4.1.4) è alla base della maggior parte degli algoritmi quantistici. Il fatto che si possa operare con un operatore unitario su tutti gli stati logici come mostrato in (4.1.5), è alla base di molti algoritmi quantistici (Deutsch, Deutch-Jozsa, Grover etc.).

Nota:

Il fatto che con il parallelismo quantistico è possibile manipolare o processare tutti gli stati logici contemporaneamente sembra suggerire immediatamente uno *speed-up* esponenziale rispetto a qualsiasi computer classico. Allora perchè esistono una solo manciata di algoritmi quantistici che permettono di velocizzare il calcolo? La risposta è nel fatto che, se da un punto certo punto di vista la meccanica quantistica permette una manipolazione parallela, l'estrazione dell'informazione è estremamente complicata. Questa avviene sempre tramite una misura che nel caso quantistico è probabilistica. Ad esempio, nello stato sovrapposizione di tutte le stringhe logiche (4.1.4), la probabilità di misurare una delle stringhe è $1/N = 1/2^n$ (che è esponenzialmente piccola). In sostanza gli algoritmi quantistici noti sono efficienti perchè riescono ad amplificare l'informazione che vogliamo estrarre prima di procedere alla misura.

II – DIFFERENZE FRA IL CALCOLO CLASSICO E QUANTISTICO

In questa sezione discuteremo due esempi che evidenziano alcune fondamentali differenze fra il calcolo classico e quello quantistico. Faremo vedere che due delle operazioni più comuni nel calcolo classico, ovvero la copiatura e la cancellazione di un bit di informazione, sono impossibili nel calcolo quantistico. Questi risultati sono risultati rigorosi e dipendono dalla struttura stessa della meccanica quantistica e vanno sotto il nome di teoremi *no-go* in quanto pongono delle limitazioni alle operazioni possibili nell'informatica quantistica.

4.2.1 Impossibilità di copiare stati quantistici (Teorema *no-cloning*)

Una delle operazioni fondamentali nei computer classici è quella di copiatura. Data una stringa di bit $x \equiv x_1x_2\dots x_n$ è possibile copiarla un numero arbitrario di volte. È possibile implementare una porta analoga su un computer quantistico?

La porta di NOT controllato (CNOT) introdotta nel precedente capitolo sembra fare al caso nostro. Supponiamo di avere un singolo qubit di informazione e che si trovi nello stato $|\psi\rangle = a|0\rangle + b|1\rangle$ (con $|a|^2 + |b|^2 = 1$). Per copiarlo, prendiamo un secondo qubit inizializzato nello stato $|0\rangle$. Avremo quindi lo stato $|\psi\rangle \otimes |0\rangle \equiv |\psi 0\rangle = a|00\rangle + b|10\rangle$. Applichiamo la porta CNOT considerando il primo bit come quello di controllo. Se questo è spento ($|0\rangle$) non applicheremo nessun operatore al secondo (oppure applichiamo l'identità). Se il bit di controllo è acceso ($|1\rangle$) applicheremo una porta NOT al secondo. Di conseguenza, i qubit si trasformano come $|00\rangle \rightarrow |00\rangle$ e $|10\rangle \rightarrow |11\rangle$ e lo stato iniziale

$$|\psi 0\rangle = a|00\rangle + b|10\rangle \xrightarrow{\text{CNOT}} a|00\rangle + b|11\rangle. \quad (4.2.1)$$

Analizziamo questo risultato nel dettaglio. Se lo stato iniziale è $|\psi\rangle = |0\rangle$ [ovvero $a = 1$ e $b = 0$ in Eq. 4.2.1] lo stato finale risulta $|00\rangle = |\psi\psi\rangle$. Se lo stato iniziale è $|\psi\rangle = |1\rangle$ [ovvero $a = 0$ e $b = 1$ in Eq. 4.2.1] lo stato finale risulta $|11\rangle = |\psi\psi\rangle$. Quindi in questi due casi abbiamo effettivamente copiato il bit iniziale.

Però la meccanica quantistica ci permette di avere stati più ricchi in cui i bit sono in una sovrapposizione di 0 e 1. Se consideriamo lo stato più generale $|\psi 0\rangle = a|00\rangle + b|10\rangle$ per copiarlo dovremmo avere un operatore il cui risultato sia

$$|\psi 0\rangle = a|00\rangle + b|10\rangle \xrightarrow{\text{COPY}} |\psi\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle. \quad (4.2.2)$$

Gli stati in Eq. (4.2.1) e (4.2.2) sono diversi perché nel primo mancano i termini $|01\rangle$ e $|10\rangle$. Quindi l'operazione CNOT produce una copia del bit iniziale solo in casi particolari ma non è un'effettiva operazione di copiatura.

Naturalmente, la singola operazione CNOT potrebbe essere troppo semplice e incompleta come operazione di copiatura. Quindi è lecito chiedersi se esiste un'operazione quantistica (quindi una sequenza di porta logiche quantistiche) che permetta di implementare una vera operazione di copiatura in cui $|\psi 0\rangle \xrightarrow{\text{COPY}} |\psi\psi\rangle$. La sorprendente risposta è che se lo stato da copiare è sconosciuto, non è possibile copiarlo. Questo risultato va sotto il nome di teorema *no-cloning*. Anche se c'è an-

cora dibattito su chi abbia derivato per la prima volta questo teorema, la sua paternità è di solito attribuita a Wootters e Zurek [Wootters1982].¹

La dimostrazione del teorema no-cloning è particolarmente semplice. Supponiamo di voler copiare lo stato $|\psi\rangle$ composta da una stringa arbitraria di qubit. Come sopra gli associamo uno stato $|s\rangle$ (della stessa dimensione in termini di qubit) dove vogliamo copiare l'informazione. L'operazione di copiatura sarà descritta da un'evoluzione unitaria U_{COPY} tale che

$$|\psi s\rangle \xrightarrow{U_{COPY}} U_{COPY} |\psi s\rangle = |\psi\psi\rangle \quad (4.2.3)$$

Supponiamo di voler copiare anche uno stato $|\varphi\rangle$. L'operatore U_{COPY} deve copiare tutti gli stati quindi avremo

$$|\varphi s\rangle \xrightarrow{U_{COPY}} U_{COPY} |\varphi s\rangle = |\varphi\varphi\rangle \quad (4.2.4)$$

Se prendendo il prodotto scalare degli stati finali abbiamo

$$\langle \varphi s | U_{COPY}^\dagger U_{COPY} |\psi s\rangle = \langle \varphi s | \psi s\rangle = \langle \varphi | \psi \rangle \langle s | s \rangle = \langle \varphi | \psi \rangle \quad (4.2.5)$$

visto che $U_{COPY}^\dagger U_{COPY} = \mathbb{1}$ e $\langle s | s \rangle = 1$. Dalle equazioni di sopra, questo deve essere uguale a ($\langle \psi\psi | \varphi\varphi \rangle = \langle \psi | \varphi \rangle \langle \psi | \varphi \rangle$)

$$\langle \varphi | \psi \rangle = (\langle \psi | \varphi \rangle)^2. \quad (4.2.6)$$

Questa equivale all'equazione $x^2 = x$ che ha soluzione solo se $x = 0$ o $x = 1$. Quindi può esistere un operatore unitario di copia U_{COPY} solo se gli stati $|\psi\rangle$ e $|\varphi\rangle$ sono ortogonali ($\langle \psi | \varphi \rangle = 0$) oppure sono identici ($\langle \psi | \varphi \rangle = 1$ per la normalizzazione equivale ad avere $|\psi\rangle = |\varphi\rangle$ ²). Ad esempio, non è possibile costruire un operatore U_{COPY} che possa copiare sia lo stato $|\psi\rangle = |0\rangle$ che lo stato $|\varphi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ dato che questi non sono ortogonali.

Concludiamo che se gli stati da copiare sono noti e ortogonali è possibile costruire un operatore unitario U_{COPY} che li copi. In genere, però non è possibile copiare stati quantistici qualsiasi; ovvero non esiste nessun operatore U_{COPY} capace di copiare tutti gli stati quantistici.

Il teorema no-cloning ha delle importanti conseguenze. Da un lato, rende un computer quantistico carente di una delle porte/operazioni fondamentali della logica classica. L'elaborazione dell'informazione quantistica deve essere sviluppata tenendo conto che non è possibile copiare lo stato quantistico e quindi duplicare l'informazione contenuta in esso.

D'altro canto però, l'impossibilità di copiare uno stato quantistico apre le porte a numerose applicazioni in termini di crittografia e sicurezza. Infatti, diventa impossibile per un "intercettatore" (*eavesdropper*), inserirsi in una conversazione

¹ Sembra che il fisico italiano Giancarlo Ghirardi derivò per primo una versione del teorema *no-cloning* in una risposta ad un articolo scientifico a cui faceva da *referee*. Non pubblicò mai la sua scoperta; quindi il teorema *no-cloning* viene in genere attribuito a Wootters e Zurek.

² In realtà sarebbe più corretto scrivere $\langle \psi | \varphi \rangle = e^{iX}$ e $|\psi\rangle = e^{-iX} |\varphi\rangle$ dove i due stati differiscono solo di una fase globale. Questa dettaglio però non invalida la discussione.

fra due parti, copiare l'informazione e riinviarla senza essere scoperto. Quindi, il teorema no-cloning è alla base della crittografia quantistica.

4.2.2 Impossibilità di distruggere stati quantistici (Teorema *no-deleting*)

Un altro risultato direttamente legato al teorema *no-cloning* è il cosiddetto Teorema *no-deleting*. Questo stabilisce che non è possibile distruggere l'informazione nei qubit. Quindi, un'altra operazione molto comune nei computer classici risulta invece impossibile nei computer quantistici.

Il processo di distruzione di cui parliamo prende due copie di uno stato quantistico *arbitrario* e *ignoto* come input e rende come output lo stato originale e uno stato specificato (ad esempio, lo stato $|0\rangle$) di un qubit.

Per rendere formale questa definizione prendiamo due sistemi quantistici A e B entrambi nello stato $|\psi\rangle$. Ad essi sarà associato lo stato della macchina C che deve distruggere il qubit che indichiamo con $|A\rangle_C$. Con queste notazioni, l'operazione di distruzione corrisponde a

$$|\psi\rangle_A |\psi\rangle_B |A\rangle_C \rightarrow U |\psi\rangle_A |\psi\rangle_B |A\rangle_C = |\psi\rangle_A |0\rangle_B |A'\rangle_C. \quad (4.2.7)$$

dove U è una trasformazione lineare ma non necessariamente unitaria. Si noti che il secondo qubit è stato distrutto (è passato da $|\psi\rangle_B$ a $|0\rangle_B$) e allo stesso tempo, abbiamo permesso che lo stato della macchina possa cambiare passando da $|A\rangle_C$ a $|A'\rangle_C$.

È importante sottolineare che lo stato $|A'\rangle_C$ non deve contenere informazione sullo stato $|\psi\rangle$. Infatti, se questo non fosse vero, l'informazione del qubit B sarebbe semplicemente trasferita a C e non distrutta come richiesto. Inoltre, un tipo di trasformazione di questo tipo per essere implementata richiederebbe di conoscere lo stato $|\psi\rangle$ cosa che è negata dall'ipotesi iniziali.

Per rimarcare l'importanza di queste ipotesi iniziali, facciamo un esempio identico a quello fatto per il teorema *no-cloning*. Supponiamo di sapere che il due qubit uguali negli stati $|0\rangle_A |0\rangle_B$ o $|1\rangle_A |1\rangle_B$. Applicando un operator CNOT otteniamo $|0\rangle_A |0\rangle_B$ o $|1\rangle_A |0\rangle_B$. Abbiamo quindi costruito un operatore che distrugge l'informazione nel secondo qubit inizializzandolo allo stato $|0\rangle_B$ (nel caso in cui questo sia inizialmente diverso). Si noti però che, come nel caso del teorema *no-cloning*, quest'operazione è possibile solo se gli stati iniziali sono noti; infatti, l'applicazione di una porta CNOT ad un sistema $|\psi\rangle_A |\psi\rangle_B$ non porterà in genere il secondo qubit nello stato $|0\rangle_B$.

A questo punto, possiamo passare alla dimostrazione del teorema *no-deleting*. Supponiamo che inizialmente $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. L'operazione di distruzione consisterebbe in

$$\begin{aligned} |\psi\rangle_A |\psi\rangle_B |A\rangle_C &\rightarrow |\psi\rangle_A |0\rangle_B |A'\rangle_C = (\alpha|0\rangle_A + \beta|1\rangle_A) |0\rangle_B |A'\rangle_C \\ &= (\alpha|0\rangle_A |0\rangle_B + \beta|1\rangle_A |0\rangle_B) |A'\rangle_C \end{aligned} \quad (4.2.8)$$

Dato che l'operazione di distruzione deve essere indipendente dallo stato iniziale, una trasformazione simile deve valere per gli stati della base canonica

$$\begin{aligned} |0\rangle_A |0\rangle_B |A\rangle_C &\rightarrow |0\rangle_A |0\rangle_B |A_0\rangle_C \\ |1\rangle_A |1\rangle_B |A\rangle_C &\rightarrow |1\rangle_A |0\rangle_B |A_1\rangle_C. \end{aligned} \quad (4.2.9)$$

Con queste relazioni, possiamo scrivere esplicitamente la trasformazione dello stato $|\Psi\rangle_A |\Psi\rangle_B |A\rangle_C$. Prima di tutto, è conveniente scriverlo in maniera estesa

$$\begin{aligned} |\Psi\rangle_A |\Psi\rangle_B |A\rangle_C &= \left[\alpha^2 |0\rangle_A |0\rangle_B + \beta^2 |1\rangle_A |1\rangle_B + \alpha\beta (|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B) \right] |A\rangle_C \\ &= \left[\alpha^2 |0\rangle_A |0\rangle_B + \beta^2 |1\rangle_A |1\rangle_B + \sqrt{2}\alpha\beta |\Psi_+\rangle \right] |A\rangle_C. \end{aligned} \quad (4.2.10)$$

Nell'ultima equazione abbiamo usato la definizione dello stato di Bell $|\Psi_+\rangle = 1/\sqrt{2}(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B)$.

Questa viene modificata in

$$|\Psi\rangle_A |\Psi\rangle_B |A\rangle_C \rightarrow \alpha^2 |0\rangle_A |0\rangle_B |A_0\rangle_C + \beta^2 |1\rangle_A |0\rangle_B |A_1\rangle_C + \sqrt{2}\alpha\beta |\Psi'_+\rangle_{ABC} \quad (4.2.11)$$

dove i primi due termini derivano direttamente dalle trasformazioni (4.2.9) mentre il terzo è la trasformazione $|\Psi_+\rangle \rightarrow |\Psi'_+\rangle_{ABC}$ dove $|\Psi'_+\rangle_{ABC}$ è uno stato ignoto che non specifichiamo. Infatti, le trasformazioni (4.2.9) non permettono di stabilire come viene trasformato lo stato di Bell $|\Psi_+\rangle$ dato che in esso non compaiono le copie di due stati $|0\rangle_A |0\rangle_B$ e $|1\rangle_A |1\rangle_B$ ma $|0\rangle_A |1\rangle_B$ e $|1\rangle_A |0\rangle_B$.

Nell'equazione (4.2.8) abbiamo ancora lasciato indicato lo stato finale $|A'\rangle_C$. Questo lo possiamo decomporre nella base $|A_0\rangle_C$ e $|A_1\rangle_C$ scrivendo il generico stato $|A'\rangle_C = \gamma |A_0\rangle_C + \delta |A_1\rangle_C$. L'equazione (4.2.8) può essere riscritta come

$$\begin{aligned} (\alpha |0\rangle_A |0\rangle_B + \beta |1\rangle_A |0\rangle_B) |A'\rangle_C &= \alpha\gamma |0\rangle_A |0\rangle_B |A_0\rangle_C + \beta\delta |1\rangle_A |0\rangle_B |A_1\rangle_C \\ &+ \alpha\delta |0\rangle_A |0\rangle_B |A_1\rangle_C + \beta\gamma |1\rangle_A |0\rangle_B |A_0\rangle_C. \end{aligned} \quad (4.2.12)$$

Confrontando le equazioni (4.2.12) e (4.2.11) possiamo determinare i coefficienti γ e δ . In particolare, confrontando i termini $|0\rangle_A |0\rangle_B |A_0\rangle_C$ e $|1\rangle_A |0\rangle_B |A_1\rangle_C$, otteniamo che $\gamma = \alpha$ e $\delta = \beta$. Di conseguenza, confrontando i rimanenti termini otteniamo che

$$|\Psi'_+\rangle_{ABC} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B |A_1\rangle_C + |1\rangle_A |0\rangle_B |A_0\rangle_C). \quad (4.2.13)$$

Dato che non abbiamo altri gradi di libertà, le soluzioni $\gamma = \alpha$ e $\delta = \beta$ sono le uniche che permettono di soddisfare entrambe le equazioni ma questo implica che $|A'\rangle_C = \alpha |A_0\rangle_C + \beta |A_1\rangle_C$. Come possiamo vedere, lo stato $|A'\rangle_C$ contiene tutta l'informazione riguardo allo stato da distruggere $|\Psi\rangle$ in quanto sono presenti entrambi i coefficienti α e β . Questo contraddice una delle assunzioni iniziali che $|A'\rangle_C$ debba essere indipendente dallo stato $|\Psi\rangle$. Infatti, la trasformazione che abbiamo trovato è possibile; tuttavia, non distrugge lo stato $|\Psi\rangle$ ma si limita a trasferirne l'informazione nel sistema C. Si noti inoltre che per implementare tale

trasformazione sarebbe necessario conoscere i coefficienti α e β (e quindi lo stato $|\psi\rangle$). Anche questo contraddice l'ipotesi che lo stato da distruggere sia ignoto.

III – superdense coding

Il *superdense coding* è un altro esempio di come la meccanica quantistica di base possa essere applicata all'informazione per ottenere dei vantaggi.

Supponiamo Alice (indicata con la lettera A) e Bob (indicato con la lettera B) debbano scambiarsi dei bit di informazione. In particolare, Alice vuole mandare due bit di informazione classica. Alice può, ad esempio, usare un canale classico *due e 'spedire'* a Bob i due bit di informazione. Se Alice e Bob possono usare la meccanica quantistica la stessa procedura (la trasmissione di due bit di informazione classica) può essere completata spedendo *un singolo qubit*. Questo protocollo che aumenta l'informazione scambiabile è detto *superdense coding*. Innanzitutto, Alice e Bob devono condividere uno stato *entangled* (di Bell) [sec. 3.6.2 e Eq. (3.6.5)]

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) \quad (4.3.1)$$

dove gli stati $|...\rangle_A$ e $|...\rangle_B$ sono rispettivamente di Alice e Bob. La procedura di Alice è di applicare una porta logica quantistica e poi di mandare il suo qubit (indicato con il pedice A) a Bob. La porta logica da applicare dipenderà dai bit di informazione che Alice vuole mandare. In uno spazio a due bit Alice può decidere di mandare i bit (o stringa) 00, 01, 10 o 11. Se vuole mandare la stringa 00 Alice non applica nessuna porta logica (che equivale all'identità) al suo qubit e poi manda il suo qubit a Bob. Se vuole mandare la stringa 10 Alice applica la porta logica Z al suo qubit e poi manda il suo qubit a Bob. Per le stringhe 01 e 11 Alice applicherà rispettivamente le porte logiche X e iY per poi mandare il suo qubit a Bob. Il risultato è che Bob si troverà in possesso di due qubit (il suo e quello di Alice)

$$\begin{aligned} 00 \text{ bit Alice : } |\beta_{00}\rangle &\xrightarrow{I} \frac{(|0\rangle_B \otimes |0\rangle_B + |1\rangle_B \otimes |1\rangle_B)}{\sqrt{2}} \text{ stato Bob} \\ 10 \text{ bit Alice : } |\beta_{00}\rangle &\xrightarrow{Z} \frac{(|0\rangle_B \otimes |0\rangle_B - |1\rangle_B \otimes |1\rangle_B)}{\sqrt{2}} \text{ stato Bob} \\ 01 \text{ bit Alice : } |\beta_{00}\rangle &\xrightarrow{X} \frac{(|1\rangle_B \otimes |0\rangle_B + |0\rangle_B \otimes |1\rangle_B)}{\sqrt{2}} \text{ stato Bob} \\ 11 \text{ bit Alice : } |\beta_{00}\rangle &\xrightarrow{iY} \frac{(|0\rangle_B \otimes |1\rangle_B - |1\rangle_B \otimes |0\rangle_B)}{\sqrt{2}} \text{ stato Bob} \end{aligned} \quad (4.3.2)$$

dove il pedice B indica che ora entrambi i qubit sono in possesso di Bob visto che Alice gli ha fisicamente mandato il suo qubit.

L'osservazione da fare è che ora le quattro possibilità in Eq. (4.3.2) rappresentano gli stati ortogonali di Bell [sec. 3.6.2 e Eq. (3.6.5)]. L'importanza dell'ortogonalità sta nel fatto che possono essere distinti inequivocabilmente con una misura. Questo significa che misurando i suoi due qubit Bob otterà un solo output con certezza.

Associando a tale output lo stato iniziale, sarà possibile determinare quale stringa fra le quattro possibili Alice gli ha mandato.

Possiamo rendere esplicito questo ragionamento astratto se Bob applica in sequenza una porta CNOT e una porta di Hadarmard al primo qubit. Sui qubit di sopra otteniamo

$$\begin{aligned} \frac{(|0\rangle_B \otimes |0\rangle_B + |1\rangle_B \otimes |1\rangle_B)}{\sqrt{2}} &\xrightarrow{\text{CNOT}} \frac{|0\rangle_B + |1\rangle_B}{\sqrt{2}} \otimes |0\rangle_B \xrightarrow{H} |00\rangle_B \\ \frac{(|0\rangle_B \otimes |0\rangle_B - |1\rangle_B \otimes |1\rangle_B)}{\sqrt{2}} &\xrightarrow{\text{CNOT}} \frac{|0\rangle_B - |1\rangle_B}{\sqrt{2}} \otimes |0\rangle_B \xrightarrow{H} |10\rangle_B \\ \frac{(|1\rangle_B \otimes |0\rangle_B + |0\rangle_B \otimes |1\rangle_B)}{\sqrt{2}} &\xrightarrow{\text{CNOT}} \frac{|1\rangle_B + |0\rangle_B}{\sqrt{2}} \otimes |1\rangle_B \xrightarrow{H} |01\rangle_B \\ \frac{(|0\rangle_B \otimes |1\rangle_B - |1\rangle_B \otimes |0\rangle_B)}{\sqrt{2}} &\xrightarrow{\text{CNOT}} \frac{|0\rangle_B - |1\rangle_B}{\sqrt{2}} \otimes |1\rangle_B \xrightarrow{H} |11\rangle_B \end{aligned} \quad (4.3.3)$$

In questo caso, la misura nella base canonica darà i due qubit che Alice voleva spedire a Bob.

IV – TELETRASPORTO QUANTISTICO

Un'altra sorprendente applicazione della meccanica quantistica alla manipolazione dell'informazione è il teletrasporto quantistico (*quantum teleportation*). Con teletrasporto quantistico si intende una procedura che permette di trasportare un qubit di informazione fra due parti senza modificarlo o misurarlo.

Anche in questo caso, l'elemento cruciale per il teletrasporto quantistico è la presenza di uno stato *entangled*. Come visto nella sezione 3.6.2, gli stati entangled hanno caratteristiche puramente quantistiche, sono delocalizzati (spazialmente separati).

Supponiamo che Alice (A) e Bob (B) condividano uno stato entangled $|\beta_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Questa notazione sta per la più precisa (e complessa) [sec. 3.6.2 e Eq. (3.6.5)]

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) \equiv \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (4.4.1)$$

dove gli stati $|...\rangle_A$ e $|...\rangle_B$ sono rispettivamente di Alice e Bob.

Supponiamo che Alice abbia un qubit di informazione $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (con $|\alpha|^2 + |\beta|^2 = 1$) che vuole mandare a Bob. Per far questo, lo accoppia allo stato entangled $|\beta_{00}\rangle$

$$|\psi_0\rangle = |\psi\rangle |\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left[\alpha|0\rangle (|00\rangle + |11\rangle) + \beta|1\rangle (|00\rangle + |11\rangle) \right] \quad (4.4.2)$$

dove i primi due ket vanno intesi come di Alice mentre l'ultimo è quello di Bob; ovvero, i ket vanno intesi come $|0\rangle (|00\rangle = |0\rangle_A |0\rangle_B)$ e così via.

Alice ha a disposizione due qubit e applica ad essi una porta CNOT usando il primo qubit come bit di controllo. La porta CNOT (3.7.6) agisce cambiando $|100\rangle \rightarrow |110\rangle$ e $|111\rangle \rightarrow |101\rangle$. Lo stato viene trasformato in

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle) \right]. \quad (4.4.3)$$

Successivamente Alice applica una porta di Hadamard al primo qubit ottenendo

$$|\psi_2\rangle = \frac{1}{2} \left[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle) \right]. \quad (4.4.4)$$

Questo può essere riscritto come

$$|\psi_2\rangle = \frac{1}{2} \left[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle) \right]. \quad (4.4.5)$$

Nel riscrivere lo stato $|\psi_2\rangle$ non abbiamo fatto altro che separare il qubit che appartiene a Bob (il terzo). Notiamo immediatamente che in $|\psi_2\rangle$ lo stato associato ai qubit $|00\rangle$ di Alice è associato allo stato $(\alpha|0\rangle + \beta|1\rangle)$ di Bob. Ma questo è esattamente lo stato che Alice voleva mandare a Bob. In realtà Bob possiede e può misurare una sovrapposizione di stati $(\alpha|0\rangle + \beta|1\rangle, \alpha|1\rangle + \beta|0\rangle, \alpha|0\rangle - \beta|1\rangle$ e $\alpha|1\rangle - \beta|0\rangle)$ in cui l'informazione sullo stato di Alice (caratterizzato da α e β) è sempre presente ma non direttamente accessibile. L'ultimo passo è quindi quello di rendere tale informazione accessibile a Bob.

Nell'ultimo passaggio è Alice misura i suoi due qubit. Dato che i qubit di Alice e Bob sono entangled, la misura di Alice induce un collasso dello stato di Bob (si veda 3.6.2). I possibili risultati della misura di Alice e i corrispondenti stati di Bob sono

00 misura Alice	\longrightarrow	$\alpha 0\rangle + \beta 1\rangle$	stato Bob
01 misura Alice	\longrightarrow	$\alpha 1\rangle + \beta 0\rangle$	stato Bob
10 misura Alice	\longrightarrow	$\alpha 0\rangle - \beta 1\rangle$	stato Bob
11 misura Alice	\longrightarrow	$\alpha 1\rangle - \beta 0\rangle$	stato Bob

(4.4.6)

Ognuno di queste misure capita con probabilità di 1/4. Quindi Bob con probabilità 1/4 riceverà lo stato $\alpha|0\rangle + \beta|1\rangle$ o lo stato $\alpha|1\rangle + \beta|0\rangle$ e così via. Affinchè Bob possegga sempre lo stato $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, Alice chiama attraverso un canale classico Bob e gli dice quale è stato il risultato della sua misura.

A questo punto, Bob non deve fare altro che applicare un'operatore correttivo. Questo sarà l'operatore X (σ_x) se la misura è 01, Z (σ_z) se la misura è 10, Y (σ_y) se la misura è 11 e Bob non farà niente se la misura è 00. Con quest'ultima operazione Bob si ritroverà sempre lo stato $|\psi\rangle$.

Ci sono due importanti osservazioni da fare sul teletrasporto quantistico. Lo stato passa $|\psi\rangle$ da Alice a Bob senza essere trasmesso. Questo è una caratteristica peculiare della meccanica quantistica; Alice può influenzare lo stato di Bob perché gli stati sono entangled. L'informazione però non può essere usata da Bob

fino a che Alice non gli comunica il risultato della sua misura. Questa comunicazione avviene secondo le leggi della teoria della relatività ristretta e quindi non è istantanea.

Per chiarire questo punto facciamo un ulteriore passo. All'inizio Alice e Bob condividono lo stato entangled $|\beta_{00}\rangle$. Se Bob facesse una misura sul suo qubit otterrebbe³ la metà delle volte 0 e l'altra metà 1, i.e., $\mathcal{P}(0) = 0.5$ e $\mathcal{P}(1) = 0.5$.

Supponiamo che Alice porti a termine la sua parte del protocollo (ovvero applichi ma porta CNOT, la porta di Hadamard e faccia la misura) ma non comunichi a Bob il suo risultato. La domanda che ci poniamo è: può Bob avere informazioni (statistiche) sullo stato $|\psi\rangle$ che Alice gli voleva mandare?

L'unica cosa sensata che Bob può fare è fare una misura nella base $\{|0\rangle, |1\rangle\}$ e cercare, ad esempio, di estrarre informazioni sui coefficienti α e β ⁴. Dall'equazioni (4.4.6) vediamo che se Alice ha misurato 00, Bob avrà probabilità $|\alpha|^2$ di misurare 0 e $|\beta|^2$ di misurare 1. Indichiamo queste probabilità con $\mathcal{P}_{00}(0) = |\alpha|^2$ e $\mathcal{P}_{00}(1) = |\beta|^2$. In modo analogo, nel caso Alice abbia misurato 01, Bob avrà $\mathcal{P}_{01}(0) = |\beta|^2$ e $\mathcal{P}_{01}(1) = |\alpha|^2$. Per gli altri casi avremo, $\mathcal{P}_{10}(0) = |\alpha|^2$ e $\mathcal{P}_{10}(1) = |\beta|^2$ e $\mathcal{P}_{11}(0) = |\beta|^2$ e $\mathcal{P}_{11}(1) = |\alpha|^2$.

Queste misure di Bob effettivamente contengono le informazioni su $|\alpha|^2$ e $|\beta|^2$. Il punto è che Bob non sa qual è il risultato delle misure di Alice quindi vedrà solo le misure aggregate dei casi in (4.4.6). Questo vuol di che la probabilità totale per Bob di misurare 0 è

$$\mathcal{P}_{\text{Bob}}(0) = \frac{1}{4}(\mathcal{P}_{00}(0) + \mathcal{P}_{01}(0) + \mathcal{P}_{10}(0) + \mathcal{P}_{11}(0)) = \frac{1}{4}(2|\alpha|^2 + 2|\beta|^2) = \frac{1}{2} \quad (4.4.7)$$

Allo stesso modo, la probabilità totale per Bob di misurare 1 è $\mathcal{P}_{\text{Bob}}(1) = 1/2$.

Queste però sono le probabilità che Bob avrebbe ottenuto prima che Alice manipolasse i suoi qubit. La conclusione è che sebbene Alice abbia modificato lo stato (o gli stati) di Bob, quest'ultimo non è in grado di estrarre nessuna informazione. Questa è la verifica diretta che l'informazione non può essere trasmessa istantaneamente con la misura degli stati entangled.

La seconda osservazione è che lo stato è trasmesso interamente quindi contiene moltissima informazione. Per capire meglio questo punto, è bene fare un paragone. Se Alice volesse trasmettere tramite un canale di comunicazione classico la stessa informazione sullo stato quantistico dovrebbe usare una quantità consistente di risorse. Potrebbe, ad esempio, misurare popolazione e fase degli stati $|0\rangle$ e $|1\rangle$ dello stato $|\psi\rangle$. La determinazione della popolazione e fase avverrebbe con la distruzione dello stato sovrapposizione che dovrebbe essere poi ricostruito. Inoltre, i numeri reali che descrivono popolazione e fase sarebbero comunque approssimati perché derivanti da una misura e trasmessi attraverso un canale classico. Al contrario, il teletrasporto quantistico permette di trasmettere *l'intero* stato senza distruggerlo.

³ In questo caso stiamo supponendo che Alice e Bob condividano un numero di qubit entangled sufficiente ad avere una statistica significativa.

⁴ Analogamente, Bob potrebbe voler stimare anche la fase relativa in $|\psi\rangle$. Le idee riportate qui si applicano anche in questo caso.

V – ALGORITMI QUANTISTICI SEMPLICI

4.5.1 Algoritmo di Deutch

L’algoritmo di Deutch è il più semplice degli algoritmi quantistici. Sebbene privo di interesse applicativo, è stato il primo ad evidenziare che la struttura della meccanica quantistica poteva effettivamente dare dei vantaggi sulla computazione classica. Inoltre si basa su due caratteristiche essenziali degli algoritmi quantistici: il *parallelismo quantistico* e l’*interferenza*. Questi sono alla base anche degli algoritmi più complessi.

Data una funzione f ad un bit, l’algoritmo di Deutch permette di capire se *costante* o no; nel caso in cui f non sia costante viene spesso chiamata *bilanciata*. Si consideri una funzione ad un bit $f(x) : \{0, 1\} \rightarrow \{0, 1\}$, ovvero la funzione riceve un bit di input 0 o 1 e dà un bit di output ($f(x) = 0$ o $f(x) = 1$). La funzione f sarà costante se $f(0) = f(1)$ e sarà *bilanciata* se $f(0) \neq f(1)$. Classicamente sono necessarie due chiamate della funzione f per determinare se è costante o no. In altri termini, l’unica possibilità è sondare tutto lo spazio degli input. Quantisticamente, l’algoritmo di Deutch prova che basta una sola chiamata della funzione f .

Lo stato iniziale dell’algoritmo di Deutch è costituito da due qubit: $|\psi_0\rangle = |01\rangle$. Ad entrambi viene applicata una porta di Hadarmard (3.7.4) per ottenere

$$|\psi_0\rangle \rightarrow |\psi_1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \quad (4.5.1)$$

A questo punto, dobbiamo introdurre l’informazione sulla funzione f . Questo avverrà tramite un operatore unitario che denotiamo con U_f . È conveniente trattare l’operatore U_f in modo generico anche perché lo stesso schema verrà poi utilizzato in altri contesti (ad esempio, per funzioni in cui l’input x è una stringa di molti bit).

Operatore U_f

Supponiamo di avere un dispositivo quantistico che dati due qubit $|x, y\rangle$ possa calcolare $f(x)$, l’addizione modulo 2 di $y \oplus f(x)$ e lo possa immagazzinare nel secondo qubit. L’effetto di questo operatore è quindi $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$. L’addizione modulo 2 da come risultato $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$ e $1 \oplus 1 = 0$. È quindi equivalente ad una porta XOR (*exclusive OR*) (sec. 1.1 e tab. 2).

Per capire come agisce l’operatore U_f nell’algoritmo di Deutch, lo applichiamo ad uno stato generico $|x\rangle (|0\rangle - |1\rangle)/\sqrt{2} = |x\rangle |-$. Notiamo che

$$\begin{aligned} \frac{1}{\sqrt{2}} |0\rangle (|0\rangle - |1\rangle) &= \frac{1}{\sqrt{2}} (|0, 0\rangle - |0, 1\rangle) \rightarrow \frac{1}{\sqrt{2}} (|0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle) \text{ se } x = 0 \\ \frac{1}{\sqrt{2}} |1\rangle (|0\rangle - |1\rangle) &= \frac{1}{\sqrt{2}} (|1, 0\rangle - |1, 1\rangle) \rightarrow \frac{1}{\sqrt{2}} (|1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(1)\rangle) \text{ se } x = 1. \end{aligned} \quad (4.5.2)$$

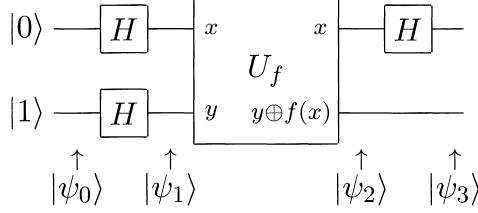


Figure 16: Schema di porte logiche quantistiche per l'algoritmo di Deutch.

Consideriamo il caso in cui $x = 0$. Se $f(0) = 0$ in Eq. (4.5.2) abbiamo lo stato

$$\frac{1}{\sqrt{2}}(|0, 0 \oplus 0\rangle - |0, 1 \oplus 0\rangle) = \frac{1}{\sqrt{2}}(|0, 0\rangle - |0, 1\rangle) = \frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle) = |0\rangle|-\rangle. \quad (4.5.3)$$

Se $f(0) = 1$,

$$\frac{1}{\sqrt{2}}(|0, 0 \oplus 1\rangle - |0, 1 \oplus 1\rangle) = \frac{1}{\sqrt{2}}(|0, 1\rangle - |0, 0\rangle) = -\frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle) = -|0\rangle|-\rangle. \quad (4.5.4)$$

Allo stesso modo, possiamo calcolare che per $x = 1$ e $f(x) = 0$

$$\frac{1}{\sqrt{2}}(|1, 0 \oplus 0\rangle - |1, 1 \oplus 0\rangle) = |1\rangle|-\rangle, \quad (4.5.5)$$

e per $x = 1$ e $f(x) = 1$

$$\frac{1}{\sqrt{2}}(|1, 0 \oplus 1\rangle - |1, 1 \oplus 1\rangle) = -|1\rangle|-\rangle. \quad (4.5.6)$$

In sostanza l'applicazione dell'operator U_f lascia invariato sia il primo qubit che il secondo ma lo stato acquista una fase $(-1)^{f(x)}$ che dipende dal valore della funzione f calcolata per x ⁵. Questi risultati si possono riassumere in una forma compatta

$$|x\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} = |x\rangle|-\rangle \rightarrow (-1)^{f(x)}|x\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} = (-1)^{f(x)}|x\rangle|-\rangle. \quad (4.5.7)$$

Torniamo adesso all'Eq. (4.5.1) che riscriviamo come $|\psi_1\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)|-\rangle$ e applichiamo l'operatore U_f con l'aiuto dell'Eq. (4.5.7). Otteniamo

$$|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)|-\rangle. \quad (4.5.8)$$

⁵ Possiamo dire che lo stato $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2} = |x\rangle|-\rangle$ è un autovettore dell'operatore U_f con autovalore $(-1)^{f(x)}$.

Applicando una porta di Hadamard al primo qubit abbiamo

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{2} \left[(-1)^{f(0)} (|0\rangle + |1\rangle) + (-1)^{f(1)} (|0\rangle - |1\rangle) \right] |-\rangle \\ &= \frac{1}{2} \left[((-1)^{f(0)} + (-1)^{f(1)}) |0\rangle + ((-1)^{f(0)} - (-1)^{f(1)}) |1\rangle \right] |-\rangle. \end{aligned} \quad (4.5.9)$$

Se la funzione è costante $f(0) = f(1)$, abbiamo che $(-1)^{f(0)} + (-1)^{f(1)} = 2$ e $(-1)^{f(0)} - (-1)^{f(1)} = 0$. Quindi $|\psi_3\rangle = |0\rangle$. Al contrario se la funzione è bilanciata $f(0) \neq f(1)$ e abbiamo che $(-1)^{f(0)} + (-1)^{f(1)} = 0$ e $(-1)^{f(0)} - (-1)^{f(1)} = \pm 2$ e $|\psi_3\rangle = \pm |1\rangle$. Visto che il segno \pm in $|\psi_3\rangle$ può essere visto come una fase globale, il suo valore è irrilevante quando andiamo a fare una misura (si veda la sezione 3.3) visto che misureremo sempre lo stato $|1\rangle$.

Concludiamo che una misura finale del primo qubit ci permetterà di distinguere il caso funzione costante (in cui misureremo lo stato $|0\rangle$) da quello di funzione bilanciata (in cui misureremo lo stato $|1\rangle$) con una singola chiamata dell'operatore U_f ⁶.

Perchè l'algoritmo di Deutch permette di migliorare le performance dell'algoritmo classico? La prima motivazione è che usa il *parallelismo quantistico*. Quando applichiamo l'operatore U_f (4.5.2), testiamo parallelamente i bit logici 0 e 1.

Il secondo punto è che l'informazione su f è immagazzinata nella fase accumulata. Ricordando che $e^{i\pi} = -1$, possiamo dire che se $f(0) = f(1)$ lo stato $|1\rangle$ del primo qubit in Eq. (4.7.1) non acquista nessuna fase. Mentre se $f(0) \neq f(1)$ lo stato $|1\rangle$ del primo qubit in Eq. (4.7.1) acquista una fase $e^{i\pi} = -1$. Questo cambiamento o accumulo di fase in fisica sia definiscono *interferenze*.

Queste proprietà sono comuni a quasi tutti gli algoritmi quantistici che sfruttano il parallelismo quantistico e le differenti fasi accumulate fra gli stati.

4.5.2 Algoritmo di Deutch-Jozsa

L'algoritmo di Deutch-Jozsa è un'estensione dell'algoritmo di Deutch appena visto. L'unica differenza è che la funzione f adesso accetta come input una stringa a n bit sebbene dia come output un singolo bit.

Per contestualizzare, potremmo associarlo ad un gioco che Alice e Bob hanno deciso di fare. Fissato il numero di bit n , Alice sceglie un intero compreso fra 0 e $2^n - 1$ e lo spedisce a Bob. Bob calcola una funzione $f(x)$ che dà come risultato 0 o 1. Bob ha promesso ad Alice di usare solo due tipi di funzioni; f può essere *costante* se assume lo stesso valore per tutti gli input o *bilanciata* se assume il valore 1 per *esattamente* metà dei possibili x e 0 per la rimanente metà. Alice deve indovinare se la funzione f scelta da Bob è costante o bilanciata.

A causa di assenza di informazione sulla funzione f , Alice non può fare altro che sondare gran parte dello spazio degli input x . Nel caso peggiore sono necessarie $2^n/2 + 1$ prove. Ad esempio, se la funzione è bilanciata (ovvero assume sia valore 0 che 1), Alice potrebbe comunque ricevere il valore 0 per i primi $2^n/2$ tentativi

⁶ Un calcolo diretto e alternativo dell'algoritmo di Deutch è presentato nell'appendice 4.7.

prima di ricevere con certezza il valore 1 e quindi poter affermare che f è bilanciata. Allo stesso modo, se la funzione è costante (e, ad esempio, assume sempre il valore 0), anche dopo aver ricevuto $2^n/2$ volte 0, Alice non può essere sicura fino a che al tentativo $2^n/2 + 1$ non riceve ancora 0. In termini di risorse classiche, diremo che sono necessarie $2^n/2 + 1$ chiamate alla funzione f per capire se è costante o bilanciata. Quindi, in questo senso, la complessità e le risorse necessarie per risolvere il problema scalano esponenzialmente con il numero di bit usati.

Usando dei qubit invece che dei bit classici, faremo vedere che lo stesso problema può essere risolto con una *singola* chiamata della funzione f . Questo è una velocizzazione (*speed-up*) esponenziale rispetto al caso classico.

L'algoritmo di Deutch-Jozsa segue i passaggi dell'algoritmo di Deutch. Lo stato iniziale è

$$|\Psi_0\rangle = |0\rangle^{\otimes n} |1\rangle. \quad (4.5.10)$$

Vengono applicate $n+1$ porte di Hadamard ai primi $n+1$ qubit. Come visto in Sec. 4.1 e in particolare nell'Eq. (4.1.4), in questo modo otteniamo la sovrapposizione di tutti le stringhe di bit con gli interi da 0 a $N-1 = 2^n - 1$. Lo stato diviene

$$|\Psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (4.5.11)$$

A questo punto a questo stato viene applicato l'operatore U_f (da Bob) che si comporta così $U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ e quindi (si veda l'algoritmo di Deutch in sec. 4.5.1)

$$|\Psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (4.5.12)$$

Successivamente Alice applica n porte di Hadamard ai primi n qubit. Per capire come queste agiscono, è utile considerare il singolo qubit $|k\rangle$ con $k = 0$ o 1. Conosciamo il risultato dal calcolo diretto ma è utile scriverlo in maniera compatta come

$$H|k\rangle = \frac{1}{\sqrt{2}} \sum_{z=0}^1 (-1)^{k z} |z\rangle. \quad (4.5.13)$$

La formula qui sopra si riconduce all'Eq. (3.7.4) per $k = 0$ o 1.

Ricordiamo che lo stato $|x\rangle$ è associato a una stringa di n bit e può essere scritto come $|x\rangle \equiv |x_1, x_2, x_3, \dots, x_n\rangle$. Sul singolo qubit $|x_i\rangle$ la porta di Hadamard agirà come in Eq. (4.5.13) con la sostituzione $k \rightarrow x_i$. Estendendo questo ragionamento a tutti gli n qubit abbiano

$$H^{\otimes n} |x_1, x_2, \dots, x_n\rangle = \sum_{z_1, z_2, \dots, z_n=0}^1 \frac{(-1)^{x_1 z_1 + x_2 z_2 + \dots + x_n z_n}}{\sqrt{N}} |z_1, z_2, \dots, z_n\rangle \quad (4.5.14)$$

che può essere riscritta in forma compatta come

$$H^{\otimes n} |x\rangle = \sum_{z=0}^{N-1} \frac{(-1)^{x \cdot z}}{\sqrt{N}} |z\rangle \quad (4.5.15)$$

dove $x \cdot z$ è il prodotto interno bit-per-bit (sec. 1.2.1).

Nell'eq. (4.5.12) era presente una somma su x ; quindi usando l'Eq. (4.5.15) per ogni x in Eq. (4.5.12), otteniamo

$$|\psi_2\rangle = \sum_{x=0}^{N-1} \sum_{z=0}^{N-1} \frac{(-1)^{x \cdot z + f(x)}}{N} |z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (4.5.16)$$

In questa equazione, il termine più importante è quello associato alla stringa con tutti i bit nulli: $|0\rangle \equiv |0, 0, \dots, 0\rangle$. Dato che $z = 0$ sicuramente $x \cdot z = 0$ e il coefficiente di $|0\rangle$ sarà $\sum_{x=0}^{N-1} \frac{(-1)^{f(x)}}{N}$. Se f è costante deve assumere lo stesso valore per tutti gli x . Questo implica che il termine $(-1)^{f(x)}$ non dipende più da x e può essere portato fuori dalla somma. Il coefficiente dello stato $|0\rangle$ diviene (denotando $f(x) = \bar{f}$)

$$\sum_{x=0}^{N-1} \frac{(-1)^{f(x)}}{N} = (-1)^{\bar{f}} \sum_{x=0}^{N-1} \frac{1}{N} = (-1)^{\bar{f}}. \quad (4.5.17)$$

Nell'ultimo passaggio abbiamo sfruttato il fatto che nella somma in x ci sono N termini che, divisi per $1/N$ si sommano a 1. Riassumendo, se f è costante, il coefficiente dello stato $|0\rangle$ è $(-1)^{\bar{f}}$. Il suo modulo quadro (che determina la probabilità della misura dello stato sec. 3.3) è 1. Visto che lo stato $|\psi_2\rangle$ deve essere normalizzato, questo implica immediatamente che gli altri stati devono avere tutti coefficiente zero e quindi non compaiono in $|\psi_2\rangle$. In altri termini, se la funzione è costante $|\psi_2\rangle = |0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ e una misura dei primi n qubit darà la stringa $0, 0, 0, \dots, 0$.

Se la funzione f è bilanciata, il coefficiente di $|0\rangle$ sarà sempre $\sum_{x=0}^{N-1} \frac{(-1)^{f(x)}}{N}$. In questo caso, il fattore $(-1)^{f(x)}$ non può essere portato fuori dalla somma ma sappiamo che varrà +1 ($f(x) = 0$) per $N/2$ stringhe e -1 ($f(x) = 1$) per le altre $N/2$ stringhe. Il coefficiente dello stato $|0\rangle$ sarà

$$\sum_{x=0}^{N-1} \frac{(-1)^{f(x)}}{N} = \left(\sum_{f(x)=0} \frac{1}{N} \right) - \left(\sum_{f(x)=1} \frac{1}{N} \right) = \frac{1}{N} \left(\frac{N}{2} - \frac{N}{2} \right) = 0 \quad (4.5.18)$$

dove nelle somme abbiamo indicato che sono sugli elementi tale che $f(x) = 0$ o $f(x) = 1$. Quindi è zero e lo stato $|0\rangle \equiv |0, 0, \dots, 0\rangle$ non comparirà in $|\psi_2\rangle$ e una misura dei primi n qubit darà una qualsiasi stringa tranne $0, 0, 0, \dots, 0$. Quindi, se nella misura finale anche solo uno dei bit assume il valore 1, la funzione è bilanciata.

Ricapitolando, alla fine dell'algoritmo Alice misura uno stato $|z\rangle$ (composto da n di qubit). Se $|z\rangle$ è la stringa di 0, la funzione è constata. Se è presente anche un solo qubit con il valore 1, la funzione è bilanciata.

A livello di risorse, l'algoritmo ha chiamato una sola volta la funzione f . Come nell'algoritmo di Deutch, il parallelismo quantistico unito all'interferenza ha permesso di ottenere la soluzione con un numero di chiamate inferiore a quelle necessarie nel caso classico.

Come discusso, l'algoritmo di Deutch-Jozsa da uno *speed-up* esponenziale rispetto agli algoritmi classici. Bisogna però aggiungere due importanti precisazioni. Se si considerano le ipotesi sulla funzione f non sembra strano che la soluzione del problema si ottenga con una sola chiamata di f . In maniera effettiva, per le funzioni bilanciate queste dividono lo spazio degli input in due sole possibilità : le stringhe x per cui $f(x) = 0$ e quelle per cui $f(x) = 1$. Esattamente come nell'algoritmo di Deutch.

Inoltre, anche in questo caso l'algoritmo non è molto più utile in termini applicativi dell'algoritmo di Deutch visto che funziona solo se le funzioni f assumono valore 0 e 1 per metà degli input o per tutti gli input (a seconda che siano bilanciate o costanti).

4.5.3 Algoritmo di Bernstein-Vazirani

Un procedimento simile a quello proposto da Deutch e Jozsa fu proposto da Bernstein e Vazirani per risolvere un problema analogo.

Supponiamo nuovamente di avere uno spazio logico a n bit e di avere una funzione che per ogni input x calcola $f_a(x) = x \cdot a = x_1 a_1 + x_2 a_2 + \dots + x_n a_n$ dove la stringa a n bit a è ignota. Ovvero, la funzione f_a calcola il prodotto interno (AND) bit-a-bit (sec. 1.2.1) fra un input generico x e una stringa ignota a . Il nostro compito è determinare a .

La sequenza di operazioni logiche è esattamente la stessa dell'algoritmo di Deutch-Jozsa ma, in questo caso, l'azione dell'oracolo non sarà quello di aggiungere una fase $(-1)^{f(x)}$ come in Eq. (4.5.16) ma una fase $(-1)^{x \cdot a}$ (dato che $f_a(x) = x \cdot a$). L'equazione (4.5.16) diventerà

$$\begin{aligned} |\Psi_2\rangle &= \sum_{x=0}^{N-1} \sum_{z=0}^{N-1} \frac{(-1)^{x \cdot z + x \cdot a}}{\sqrt{N}} |z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \sum_{x=0}^{N-1} \sum_{z=0}^{N-1} \frac{(-1)^{(z \oplus a) \cdot x}}{\sqrt{N}} |z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ &= \sum_{z=0}^{N-1} \left(\sum_{x=0}^{N-1} \frac{(-1)^{(z \oplus a) \cdot x}}{\sqrt{N}} \right) |z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \sum_{z=0}^{N-1} \chi_z |z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \end{aligned} \quad (4.5.19)$$

Negli esponenti della prima riga siamo passati da $x \cdot z + x \cdot a$ a $(z \oplus a) \cdot x$ sfruttando le proprietà delle operazioni bit-a-bit. In particolare, la somma formale $z \oplus a$ è da intendere come la XOR bit-a-bit (modulo 2) (sec. 1.2.2). Nell'ultima riga abbiamo semplicemente invertito l'ordine delle somme per evidenziare che $\chi_z = \sum_{x=0}^{N-1} \frac{(-1)^{(z \oplus a) \cdot x}}{\sqrt{N}}$ è il coefficiente associato allo stato z .

Se $z = a$ vuol dire che le due stringhe hanno tutti gli n bit uguali ($z_i = a_i$). Per l' i -esimo bit dovremmo calcolare $z_i + a_i$ (modulo 2) (questo equivale all'operazione logica z_i XOR a_i fra bit come in sec. 1.2.2). Se $z_i = a_i$, $z_i + a_i \pmod{2} = 0$ dato che $0 + 0 \pmod{2} = 0$ e $1 + 1 \pmod{2} = 0$. Quindi in questo

caso, la stringa di bit risultante sarà $z + a = 000\dots0$. Il passo successivo è calcolare $(z + a) \cdot x$ che darà 0 visto che per i singoli bit avremo $(z_i + a_i)x_i = 0$. Conseguentemente abbiamo che

$$\chi_{z=a} = \sum_{x=0}^{N-1} \frac{1}{N} = 1 \quad (4.5.20)$$

Ma dato che lo stato $\sum_{z=0}^{N-1} \chi_z |z\rangle$ deve essere normalizzato, se $\chi_{z=a} = 1$ tutti gli altri coefficienti devono essere annullarsi $\chi_{z \neq a} = 0$. Possiamo quindi scrivere in modo compatto $\chi_z = \sum_{x=0}^{N-1} \frac{(-1)^{(z+a)\cdot x}}{N} = \delta_{z,a}$ ⁷.

Tornando all'Eq. (4.5.19) abbiamo che

$$|\psi_2\rangle = \sum_{z=0}^{N-1} \delta_{z,a} |z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |a\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (4.5.21)$$

Quindi una misura dei primi n qubit logici darà lo stato (o stringa) $|a\rangle$ con probabilità 1. Con un computer quantistico possiamo risolvere il problema di Bernstein-Vazirani con una sola chiamata dell'oracolo. Classicamente sono invece necessarie n chiamate dell'oracolo abbiamo quindi uno *speed-up* polinomiale (lineare).

4.5.4 Algoritmo di Simon

Come abbiamo visto l'algoritmo di Bernstein-Vazirani da uno *speed-up* rispetto al corrispondente classico che è solo lineare. Il vero vantaggio (e con esso lo stimolo) di costruire un computer quantistico si avrebbe con uno *speed-up* maggiore. In questa categoria ricade l'algoritmo di Simon [Simon1997] che permette di avere uno *speed-up esponenziale* rispetto agli analoghi classici.⁸

Supponiamo nuovamente di avere un oracolo o Black Box che calcola una funzione che ha come input una stringa a n bit e dà come output un'altra stringa a n bit

$$f : \{0, 1\}^n \rightarrow \{0, 1\}^n. \quad (4.5.22)$$

La funzione f ha la caratteristica che per ogni x esiste un solo y tale che $f(x) = f(y)$. Tale y non è casuale ma sappiamo che è calcolato secondo la regola $y = x \oplus a$ dove a è una stringa a n bit e $x \oplus a$ rappresenta l'operazione XOR bit-a-bit fra le stringhe x e a (sec. 1.2.2). Il nostro scopo è trovare la stringa a , ovvero, la periodicità della funzione f .

Il problema è classicamente difficile dato che non esiste un algoritmo efficiente per risolverlo. L'unica possibilità che abbiamo è di dare all'oracolo una serie di stringhe fino a che non troviamo una coppia x e y tale che $f(x) = f(y)$. Una volta trovate tali stringhe, il periodo può essere calcolato come $a = x \oplus y$ ⁹.

⁷ $\delta_{z,a}$ è la delta di Kronecker che ha le proprietà $\delta_{a,a} = 1$ e $\delta_{z,a} = 0$ se $z \neq a$.

⁸ Secondo alcune fonti [Preskill_Lecture_notes], originalmente è stato proposto dagli stessi Bernstein e Vazirani. L'algoritmo è però in genere attribuito ad Daniel Simon [Simon1997].

⁹ Questo può essere dimostrato nel seguente modo. Supponiamo di aver trovato x e y tali che $y = x \oplus a$. Sommiamo a destra e a sinistra x in modo tale da avere $x \oplus y = x \oplus x \oplus a$. Consideriamo

Visto che l'unico modo di risolvere il problema è di provare diversi input, per trovare i giusti x e y dovremmo in media sondare tutto lo spazio logico che è composto da 2^n stringhe. Sulla base di questo ragionamento si può dimostrare [Preskill_Lecture_notes] che, in media, sono necessari $2^{n/2}$ tentativi e chiamate dell'oracolo. Possiamo quindi dire che la complessità cresce esponenzialmente con il numero di bit n .

Con un computer e oracolo (Black Box) quantistici potremmo fare decisamente meglio. Supponiamo come nell'algoritmo di Deutch-Jozsa di partire da n bit logici più n qubit addizionali $|\psi_0\rangle = |0\rangle^{\otimes n} |0\rangle^{\otimes n}$ e di applicare N porte di Hadamard ai primi n qubit. Otterremo

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |0\rangle^{\otimes n}. \quad (4.5.23)$$

con, come al solito, $N = 2^n$.

A questo punto, applichiamo l'oracolo che per ogni $|x\rangle$ calcola $f(x)$ e immagazzina il suo valore (ricordiamo che in questo caso è una stringa a n bit) negli n bit finali (dato che $|0 \oplus f(x)\rangle = |f(x)\rangle$)

$$|\psi_1\rangle \xrightarrow{O} |\psi_2\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle. \quad (4.5.24)$$

Dato che per ogni x esiste un $x \oplus a$ tale che $f(x) = f(x \oplus a)$, nella somma precedente lo stato $|f(x)\rangle$ sarà associato sia allo stato $|x\rangle$ che allo stato $|x \oplus a\rangle$. Possiamo quindi riscriverla come

$$|\psi_2\rangle = \frac{1}{\sqrt{N/2}} \sum_{x=0}^{N-1} \frac{|x\rangle + |x \oplus a\rangle}{\sqrt{2}} |f(x)\rangle. \quad (4.5.25)$$

Misurando gli ultimi n qubit, otterremo una stringa casuale $f(x_0)$ con probabilità $1/2^{n-1} = 2/N$. Il valore di questa stringa così come di x_0 non è importante. Ciò che ci interessa è che i primi n qubit dopo la misura si troveranno nello stato *sovraposizione*

$$|\psi_3\rangle = \frac{|x_0\rangle + |x_0 \oplus a\rangle}{\sqrt{2}}. \quad (4.5.26)$$

riamo il bit i -esimo del secondo membro. Per le proprietà dell'operatore XOR (sec. 1.1), abbiamo $x_i \text{ XOR } x_i \text{ XOR } a_i = (x_i \text{ XOR } x_i) \text{ XOR } a_i = 0 \text{ XOR } a_i$. Se $a_i = 1$, $0 \text{ XOR } a_i = 1 = a_i$. Se $a_i = 0$, $0 \text{ XOR } a_i = 0 = a_i$. Da cui concludiamo che $x_i \text{ XOR } x_i \text{ XOR } a_i = a_i$ e quindi $x \oplus y = a$.

Se gli applichiamo n porte di Hadarmad come in Eq. (4.5.15) otteniamo

$$\begin{aligned} |\psi_3\rangle \xrightarrow{H^{\otimes n}} |\psi_4\rangle &= \frac{1}{\sqrt{2N}} \sum_{y=0}^{N-1} \left[(-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus a) \cdot y} \right] |y\rangle \\ &= \frac{1}{\sqrt{2N}} \sum_{y=0}^{N-1} \left[(-1)^{x_0 \cdot y} + (-1)^{x_0 \cdot y + a \cdot y} \right] |y\rangle \\ &= \frac{1}{\sqrt{2N}} \sum_{y=0}^{N-1} (-1)^{x_0 \cdot y} \left[1 + (-1)^{a \cdot y} \right] |y\rangle. \end{aligned} \quad (4.5.27)$$

Il prodotto interno bit-per-bit $a \cdot y$ può essere uguale a 1 o 0 (sec. 1.2.1). Per le stringhe y per cui $a \cdot y = 1$, il coefficiente dello stato $|y\rangle$ è $[1 - 1] = 0$. Al contrario, se $a \cdot y = 0$, il coefficiente dello stato $|y\rangle$ è $[1 + 1] = 1$. Quindi nella somma precedente sono presenti solo gli stati $|y\rangle$ tali che $a \cdot y = 0$. La possiamo riscrivere come

$$|\psi_4\rangle = \frac{1}{\sqrt{2N}} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y} \left[1 + (-1)^{a \cdot y} \right] |y\rangle \quad (4.5.28)$$

dove abbiamo incluso il vincolo $a \cdot y = 0$ come pedice della somma.

La misura dei rimanenti n qubit, darà una stringa y tale che $a \cdot y = 0$. Supponiamo che questa sia y_1 . La conoscenza di y_1 non ci permette di avere immediatamente a . Per questo dobbiamo iterare la procedura per ottenere diversi valori y_2, y_3, \dots, y_n tali che $a \cdot y_i = 0$ per $i = 1, \dots, n$. Con questi y_i possiamo risolvere il sistema di equazioni

$$\begin{aligned} a \cdot y_1 &= 0 \\ a \cdot y_2 &= 0 \\ &\cdot \\ &\cdot \\ &\cdot \\ a \cdot y_n &= 0 \end{aligned} \quad (4.5.29)$$

Se le equazioni $a \cdot y_i = 0$ sono linearmente indipendenti esiste una sola stringa a che le soddisfa tutte e può essere facilmente determinata. Si può dimostrare [Preskill_Lecture_notes] che bastano $O(n)$ iterazioni del protocollo per ottenere n equazioni linearmente indipendenti e determinare a .

Abbiamo quindi visto che se un algoritmo classico impiegherebbe $O(2^{n/2})$ iterazioni (o chiamate all'oracolo) per risolvere il problema di Simon, un computer quantistico impiegherebbe solo $O(n)$ iterazioni (o chiamate all'oracolo). Un computer quantistico permetterebbe quindi uno *speed-up* esponenziale rispetto ad uno classico.

5

CRITTOGRAFIA QUANTISTICA

I – CRITTOGRAFIA CLASSICA

Uno degli algoritmi quantistici più importanti è quello di Shor [Shor1999] per la fattorizzazione di numeri interi. La sua importanza sta nel fatto che è un algoritmo quantistico che ha uno *speed-up* esponenziale rispetto agli algoritmi classici e risolve un problema di enorme importanza per la crittografia.

Il protocollo maggiormente usato per lo scambio di informazioni sicure è l'RSA (dalle iniziali degli scopritori Rivest-Shamir-Adleman). Questo si basa sul fatto che dato un numero intero (grande) prodotto di due numeri interi e primi, i.e., $m = p \cdot q$ con p e q primi, sia computazionalmente difficile trovare la sua fattorizzazione, ovvero p e q . L'algoritmo di Shor ha mostrato che un eventuale computer quantistico potrebbe fattorizzare m in tempi esponenzialmente brevi rispetto ai computer attuali. Questo significa che le chiavi crittografiche basate sulla RSA che oggi si pensano sicure per svariati anni (si pensi alle carte di credito che sono cambiate ogni tre anni) potrebbero essere decrittate in settimane o mesi rendendole inservibili¹. Tuttavia, se da una parte la meccanica quantistica potrebbe rendere insicuri gli schemi crittografici odierni come l'RSA, dall'altra apre le porte a nuovi protocolli crittografici che sono sicuri perché sfruttano le leggi di base della fisica quantistica.

Il protocolli crittografici quantistici sono a chiave privata (*private key cryptography*); ovvero, Alice e Bob devono avere una chiave criptografica comune e sicura. Uno dei codici a chiave privata più semplici è il *Vernam cipher* (figura 18). Alice e Bob condividono una chiave privata (*encryption key*). Alice la usa per criptare il messaggio originale (*encrypted message*) e spedirlo a Bob attraverso un canale pubblico. Bob usando la stessa chiave può decriptare il messaggio di Alice. In questo caso, se il messaggio viene intercettato da Eve, questa non riuscirà a decifrare il messaggio. Infatti, visto che la chiave criptografica è ignota (e quindi per Eve è random), l'unico approccio è cercare di trovarla mediante forza bruta; quindi, per chiavi criptografiche sufficientemente complesse, con tempi lunghi e grande potenza di calcolo.

La crittografia a chiave privata ha però degli enormi difetti pratici. Se si usa la stessa chiave per criptare un numero elevato di messaggi, Eve può accumulare abbastanza informazione e riuscire a scoprirla. Quindi le chiavi private vanno cambiate periodicamente ma anche questo comporta delle complicazioni. Infatti, la stessa chiave, ad esempio mandata tramite un canale di comunicazione, può essere intercettata e rubata. Queste motivazioni e difficoltà hanno favorito negli anni intorno al 1970, lo sviluppo della crittografia a chiave pubblica.

¹ È per questo che settori che maneggiano dati sensibili come i militari o le banche si sono interessati da subito nell'informazione quantistica.

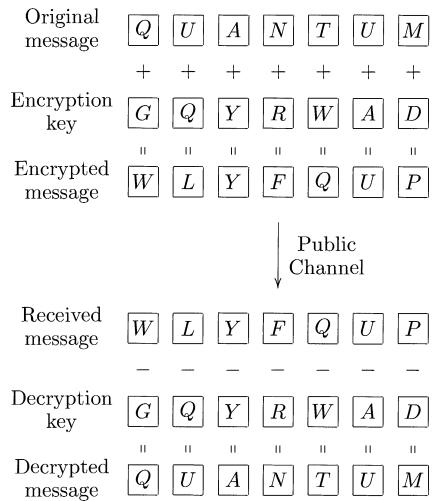


Figure 18: Il *Vernam cipher*: un esempio di crittografia a chiave privata. Immagine presa da [\[nielsen-chuang_book\]](#).

La crittografia quantistica segue uno schema a chiave privata e, in particolare, si focalizza sullo scambio delle chiavi private (si parla infatti di *Quantum Key Distribution* o QKD). Come nel caso classico, lo scambio della chiave avviene attraverso un canale pubblico (quindi insicuro e intercettabile). La differenza che, per le leggi fisiche che governano la meccanica quantistica, è possibile stabilire con estrema precisione se il messaggio è stato intercettato.

II – CRITTOGRAFIA QUANTISTICA

La crittografia quantistica è il settore dell'informazione quantistica più sviluppato e più vicino alla produzione di massa. Al momento di scrivere, i settori della sicurezza militare e il settore bancario stanno pensando di implementare protocolli di crittografia quantistica per rendere (più) sicuri gli scambi di informazioni interni. Progetti più avveniristici prevedono la costruzione di reti per lo scambi di dati critografici nazionali, transnazionali e addirittura con satelliti orbitanti intorno alla terra.

La ragione per questo veloce sviluppo è legata alla semplicità dei protocolli e al numero limitato di operazioni che sono necessarie per implementarli. Per un protocollo crittografico è necessario solo riuscire a inizializzare i qubit e fare delle misure in basi diverse. Non servono quindi porte logiche che permettono di costruire un'arbitraria sovrapposizione di stati logici o operazioni complesse.

Questa è una semplificazione enorme e soprattutto permette di implementare i protocolli crittografici in sistemi ottici che usano la polarizzazione dei fotoni per codificare l'informazione quantistica. I fotoni hanno la proprietà di essere stabili

e robusti rispetto a perturbazioni esterne (ambientali), facili da manipolare e da trasmettere anche su lunghe distanze (ad esempio, attraverso una fibra ottica).

Il primo protocollo per la crittografia quantistica fu proposto da Charles Bennett and Gilles Brassard nel 1984 ed è chiamato comunemente protocollo BB84 (dalle iniziali degli autori e dall'anno di pubblicazione) [bb84]. È il più semplice dei protocolli ma ha in se tutte le caratteristiche e le idea essenziali tanto che gli altri si possono considerare delle ottimizzazioni del BB84.

5.2.1 Protocollo BB84: idee di base

Il protocollo BB84 è un protocollo sicuro per la distribuzione di chiavi crittografiche. L'idea è che Alice e Bob possano scambiarsi una chiave crittografica sicura con cui criptare il messaggio che si vogliono scambiare. La meccanica quantistica ha due proprietà fondamentali che permettono la sua implementazione: Un eventuale *hacker* (che chiameremo Eve)

1. non può copiare un generico qubit contenente l'informazione a causa del teorema *no-cloning* in sec. (4.2.1).
2. una misura del qubit lo perturba a causa del collasso della funzione d'onda **sec:measurement**.

A livello classico, se Eve si inserisse nel canale di comunicazione fra Alice e Bob, potrebbe copiare l'informazione mandata da Alice e rispedire tutto a Bob che non potrebbe accorgersi della copia. Oppure potrebbe fare una misura diretta sui bit trasmessi senza che Bob si accorga di niente. Queste due procedure sono impossibili se l'informazione è trasmessa tramite qubit invece che con bit classici.

L'implementazione del protocollo per lo scambio di una chiave crittografia sicura è complicato dal fatto che si devono stabilire con criteri quantitativi se c'è stato l'intervento di Eve o no.

L'idea alla base del protocollo BB84 è che dato uno stato quantistico esiste una base in cui l'output della misura è certo e non probabilistico 3.3. Ad esempio, se il sistema si trova nello stato $|0\rangle$ una misura nella base canonica darà il valore 1 con probabilità 1. Al contrario, se il sistema si trova nello stato $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$ una misura darà il valore 1 con probabilità 1/2 e il valore -1 con probabilità 1/2. Però, se il sistema è nello stesso stato $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$ ma misuriamo nella base $\{|+\rangle, |-\rangle\}$ (si veda sec. 3.3) otterremo il valore 1 con probabilità 1. Quindi, l'output della misura è certo o meno a seconda dello stato e della base in cui si fa la misura ².

Dobbiamo aggiungere un'ulteriore precisazione l'informazione logica "astratta" è costituita da due bit 0 e 1. Questa però può essere fisicamente codificata in diversi stati. Ad esempio, in un sistema classico potremmo stabilire che lo stato logico 1 corrisponde al passaggio di corrente in un filo e lo 0 all'assenza di corrente. La stessa informazione potrebbe essere codificata in termini di voltaggio.

² Nel linguaggio della Fisica si dice che viene misurato l'operatore di Pauli Z o σ_z nel primo caso, X o σ_x nel secondo. Il risultato della misura è certo se lo stato è un autostato dell'operatore da misurare ed è invece probabilistico se è sovrapposizione di autostati dell'operatore da misurare.

In meccanica quantistica abbiamo un elemento in più perché nello stesso sistema fisico possiamo scegliere diverse basi in cui codificare l'informazione e fare la misura. Ad esempio, potremmo stabilire che il bit logico 0 è codificato da uno stato con polarizzazione (sez. 3.1.2) verso l'alto $|0\rangle = |\uparrow\rangle$. Ma potremmo anche decidere di usare la polarizzazione a 45° per cui dire che $|0\rangle = |\nearrow\rangle$. Questi due stati non sono ortogonali quindi ricadiamo nella distinzione discussa sopra.

Per il protocollo BB84 possiamo identificare due basi indicate con B_1 e B_2 : **Base** $B_1 : \{|0\rangle, |1\rangle\}$ e **Base** $B_2 : \{|0_+\rangle, |1_+\rangle\}$. La relazione fra le due basi è

$$\begin{aligned} |0\rangle &= \frac{|+\rangle + |-\rangle}{\sqrt{2}} = \frac{|0_+\rangle + |1_+\rangle}{\sqrt{2}} \\ |1\rangle &= \frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{|0_+\rangle - |1_+\rangle}{\sqrt{2}} \end{aligned} \quad (5.2.1)$$

e

$$\begin{aligned} |0_+\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \\ |1_+\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle. \end{aligned} \quad (5.2.2)$$

Con questa notazione vogliamo evidenziare che l'informazione logica 0 può essere codificata in due stati fisici $|0\rangle$ e $|0_+\rangle$. A questo scopo, abbiamo usato una notazione leggermente diversa. Gli stati che nel capitolo 3 erano denotati con $|+\rangle$ e $|-\rangle$ ora sono, rispettivamente, $|0_+\rangle$ e $|1_+\rangle$. Da relazioni di sopra vediamo che se misuriamo nella base B_1 gli stati $|0\rangle$ e $|1\rangle$ otterremo il corrispondente autovalore con probabilità 1; se invece gli stessi stati vengono misurati nella base B_2 l'output sarà l'autovalore associato a $|+\rangle$ il 50% di volte e l'autovalore associato a $|-\rangle$ il rimanente 50%. In maniera analoga, nella base B_2 gli stati $|0_+\rangle = |+\rangle$ e $|1_+\rangle = |-\rangle$ otterremo il corrispondente autovalore con probabilità 1; mentre una misura nella base canonica B_1 darà l'autovalore associato con probabilità del 50%.

Protocollo BB84: implementazione

Punto 1

Fissato a n il numero di qubit da usare nel protocollo, Alice estrae due sequenze di n numeri casuali di 0 e 1. La prima sequenza n rappresenta una stringa logica associata al messaggio mentre la seconda rappresenta la base in cui codificare il messaggio. Ad esempio, potremmo decidere di usare la base B_1 ogni qual volta nella seconda stringa compare lo 0 e la base B_2 quando compare 1. Quindi l'unione delle due stringhe ci dice bit-per-bit l'informazione che dobbiamo codificare e la base in cui dobbiamo codificarla. Un esempio è mostrato in tabella 5. Seguendo questo schema, Alice prepara una serie di qubit e li manda a Bob.

stringa logica A	o	1	1	o	1	1	1	o
stringa base A	o	o	1	o	o	o	1	o
qubit A	$ 0\rangle$	$ 1\rangle$	$ 1_+\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$	$ 1_+\rangle$	$ 0\rangle$

Table 5: Codifica dei qubit da parte di Alice

stringa logica A	o	(1)	(1)	o	(1)	1	1	(0)
stringa base A	o	0	1	o	0	o	1	0
qubit A	$ 0\rangle$	$ 1\rangle$	$ 1_+\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$	$ 1_+\rangle$	$ 0\rangle$
stringa base B	1	0	1	1	0	1	o	0
misura B	o^*	(1)	(1)	1^*	(1)	o^*	1^*	(0)

Table 6: Misura dei qubit da parte di Bob. I casi in cui la base di misura di Alice e Bob coincide sono segnalati con \square . Questi portano ad un output della misura certo e in cui il valore trovato da Bob coincide con quello codificato da Alice (segnalati con \circlearrowright).**Punto 2**

Bob riceve i qubit da Alice ed estrae n numeri random. Questi determinano la base in cui Bob fa la misura dei qubit. Ad esempio, se il primo numero random estratto è 1, Bob misura nella base B_2 . Bob non sa la sequenza di basi che Alice ha usato per la codifica, quindi la sua stringa e le successive misure saranno scorrelate e coincideranno solo statisticamente con quelle di Alice. Rimane però vero che se quando i bit nella stringa delle basi di Alice e Bob coincidono, la misura di Bob darà un risultato con probabilità 1. Se invece non coincidono ogni out-put avrà probabilità 1/2.

Un esempio è mostrato in Tabella 6. La riga più interessante è l'ultima (misura di B). Qui con l'asterisco sono segnati i risultati della misura che sono probabilistici (escono con il 50% di probabilità) perchè le stringhe delle basi di Alice e Bob non coincidono. Invece sono cerchiati i risultati della misura di Bob per cui l'output è certo dato che le stringhe delle basi di Alice e Bob coincidono (segnalati con un quadrato). Il punto fondamentale è che in questo caso il valore misurato da Bob è lo stesso di quello codificato inizialmente da Alice (come evidenziato nell'ultima riga in Tabella 6).

Punto 3

Alice e Bob pubblicano apertamente la stringhe di bit con cui hanno scelto, rispettivamente, la base di codifica e misura. A questo punto, sanno i bit logici associati saranno gli stessi per entrambi e quindi condividono una chiave segreta (perchè solo loro conoscono il valore effettivo dei bit che non è stato pubblicato).

Nell'esempio in tabella 6, Alice e Bob sanno che i bit 2, 3, 5 e 7 sono associati alla stessa base e come si deduce dalla tabella la stringa associata a questi sarà 1110 e potrà essere usata per criptare un messaggio.

Fino a questo punto abbiamo esaminato, come Alice e Bob possono scambiarsi una chiave pubblica usando qubit. La vera forza della QKD sta nel fatto che, a differenza di quella classica, può essere resa sicura rispetto agli attacchi di Eve.

Intervento di Eve

Visto che Eve non può copiare i qubit per il teorema *no-cloning*, l'unica cosa che può fare è inserirsi nella comunicazione fra Alice e Bob e sostituirsi a Bob nella misura per poi mandare a Bob dei qubit. Eve può estrarre una sua stringa di numeri random, in base a questa scegliere la base in cui misurare e mandare un'informazione a Bob. Come nel caso di Bob, i risultati della misura di Eve saranno gli stessi del bit logico codificato da Alice solo nel caso in cui le stringhe delle basi di Alice e Eve coincidono. Per minimizzare la perturbazione dell'informazione (e quindi non essere scoperta) Eve manderà a Bob il risultato della sua misura. Ad esempio, se misura un qubit nella base B_2 e il risultato è 0, manderà a Bob lo stato $|0_+\rangle$. Se per tale qubit la base di Eve coincide con quella di Alice, la misura non perturberà lo stato e Bob riceverà esattamente lo stesso qubit mandato da Alice. Eve è riuscita nell'intento di rubare l'informazione senza essere osservata.

Allo stesso tempo, nei casi in cui la base di Eve e Alice non coincidono, Eve misurerà, distruggerà lo stato originale e manderà a Bob un qubit logico che è quello originale solo il 50% delle volte. Facciamo un esempio, supponiamo che Eve misuri il qubit 2 nella base B_2 (Alice aveva usato la base B_1) e che il sistema collassi nello stato $|0_+\rangle$. Eve manderà a Bob lo stesso stato e Bob che, secondo la tabella 6 sceglie la base la stessa base di Alice B_1 , non misurerà con certezza lo stato 1 ma solo con probabilità 1/2.

Da questa analisi arriviamo alla conclusione che, statisticamente, Eve perturba la metà dei qubit in cui Alice e Bob dovrebbero avere uguali. Quindi la presenza di Eve può essere svelata con il seguente

Punto 4

Fra i qubit che sono stati misurati nella stessa base, Alice e Bob selezionano la prima metà e svelano pubblicamente i risultati delle misure. In assenza di Eve la correlazione fra i risultati dovrebbe essere completa. La presenza di Eve si rivela quando le misure fra questi qubit danno risultati diversi. Una volta che Alice e Bob stabiliscono che il minimo di correlazione per la sicurezza è, ad esempio, del 90%, decidono che la comunicazione è stata "disturbata" ogni volta che le correlazioni scende sotto tale soglia. Se è così, il protocollo viene annullato e viene riattivato usando altri canali non intercettabili.

Quanti qubit sono necessari per scambiare una chiave crittografica di m bit? Se si parte da n qubit iniziali, solo nella metà dei casi Alice e Bob sceglieranno la stessa base di misura; quindi, i qubit correlati sono solo $n/2$. Per stabilire o escludere la presenza di Eve, vengono pubblicati la metà di questi. Quindi se il controllo della sicurezza va a buon fine, solo $n/4$ sono correlati e non pubblicati e possono essere usati come chiave crittografica. Quindi per avere una chiave crittografica sicura di m bit, è necessario usare in partenza $n = 4m$ qubit.

III – PROTOCOLLO EPR CON STATI ENTANGLED.

Nel 1991 Arthur Ekert propose un protocollo di crittografia quantistica che usa gli stati entangled. Questo protocollo è detto EPR dai nomi di Einstein-Poldosky e Rosen che discussero per la prima volta le proprietà degli stati entangled.

Il protocollo BB84 è intrinsecamente asimmetrico: Alice genera la chiave che poi, criptata, viene mandata a Bob. Inoltre all'atto della generazione della chiave c'è lo scambio di qubit (Alice manda i suoi qubit a Bob dopo averli criptati). Il protocollo EPR elimina queste due condizioni.

Supponiamo che Alice e Bob condividano n qubit entangled come

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (5.3.1)$$

Questi potrebbero essere, ad esempio, generati da Alice che poi ne manda la metà a Bob, vice versa, o addirittura potrebbe essere un operatore esterno addetto alla generazione.

Alice genera un bit random classico b e, a seconda del suo valore, misura il suo qubit nella base $B_1 = \{|0\rangle, |1\rangle\}$ o nella base $B_2 = \{|+\rangle, |-\rangle\}$. Supponiamo che il valore di questa misura sia a . Allo stesso modo, Bob genera un bit random classico b' e, a seconda del suo valore, misura nella base B_1 o B_2 .

Supponiamo che il bit random di Alice sia $b = 0$ e che Alice misuri nella base B_1 . Se misura 0 (cosa che capita) il 50% delle volte, il sistema collasserà nello stato $|00\rangle$. Se Bob estrae il numero $b' = 0$ e misura nella base B_1 , il suo risultato sarà 0 il 100% delle volte. Allo stesso modo se Alice misura 1 il sistema collassa nello stato $|11\rangle$ e se $b' = 0$, Bob misurerà sempre 1. Ne consegue che se $b = b' = 0$ i qubit di Alice e Bob sono perfettamente correlati.

Supponiamo ora che Alice estragga il numero $b = 1$ e decida di misurare nella base B_2 . Abbiamo che lo stato entangled può essere scritto come

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} \left[\frac{|+\rangle + |-\rangle}{\sqrt{2}} \otimes |0\rangle + \frac{|+\rangle - |-\rangle}{\sqrt{2}} \otimes |1\rangle \right]. \quad (5.3.2)$$

Raccogliendo gli stati $|+\rangle$ e $|-\rangle$ abbiamo che

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} \left[|+\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} + |-\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] = \frac{|++\rangle + |--\rangle}{\sqrt{2}}. \quad (5.3.3)$$

Seguendo il ragionamento precedente è chiaro che se Bob estrae $b' = 1$, le misure di Alice e Bob sono perfettamente correlate. Ovvvero, se il qubit di Alice collassa in $|\pm\rangle$ anche quello di Bob si troverà nello stato $|\pm\rangle$.

Concludiamo che se $b = b'$ (indipendentemente dallo specifico valore) le misure di Alice e Bob sono perfettamente correlate e quindi $a = a'$. Questi sono i bit che andranno a formare la chiave crittografica segreta.

I qubit per i quali $b \neq b'$ vengono scartati perché statisticamente scorrelati. Infatti, supponiamo che Alice abbia $b = 0$ e $b' = 1$ e che la misura di Alice faccia collassare i qubit nello stato $|00\rangle$. Questo può essere scritto come

$$|00\rangle = |0\rangle \otimes \frac{|+\rangle + |-\rangle}{\sqrt{2}}. \quad (5.3.4)$$

È chiaro che una misura di Bob nella base B_2 darà la metà delle volte lo stato $|+\rangle$ e il risultato $a' = 0$ e la rimanente metà lo stato $|-\rangle$ e il risultato $a' = 1$. Quindi solo il la metà delle volte $a = a'$ e questi qubit non possono essere usati per costruire una chiave segreta. In maniera analoga, si può far vedere che è necessario scartare tutti i qubit per i quali $b \neq b'$.

È importante notare che il protocollo è completamente simmetrico. Non è importante ai fini del protocollo se la prima misura è fatta da Alice o Bob e, addirittura, le misure potrebbero essere simultanee.

In secondo luogo, la chiave è completamente random ed in questo caso è generata nel momento della misura. Infatti, è completamente indeterminata fino a quando Alice e Bob non misurano i qubit.

Terzo, anche questo protocollo crittografico è sicuro in presenza di Eve. Ci sono infatti tecniche che permettono di stabilire se i qubit sono statisticamente correlati o se hanno perso le correlazioni quantistiche a causa dell'intervento di Eve.

6

ALGORITMI QUANTISTICI

I – ALGORITMO DI GROVER PER LA RICERCA IN DATABASE

6.1.1 Algoritmi con "oracolo" o "Black Box"

Il primo passo per arrivare all'algoritmo per la ricerca in database è introdurre il concetto di *oracolo* o *Black Box* (scatola nera) in maniera analoga (ma più generica) a quella introdotta nella sezione 4.5.3.

Supponiamo di avere un database di N elementi. Invece di classificare e distinguere gli elementi in base all'informazione che contengono, a livello astratto, è utile associare ad ogni elemento un numero intero. La ricerca nel database si ridurrà quindi a trovare l'intero che soddisfa le proprietà desiderate. Per descrivere tutto il database avremmo bisogno di n bit o qubit con $N = 2^n$. Gli interi associati saranno nell'intervallo compreso fra 0 e $N - 1$.

Tutta l'informazione sul problema che vogliamo risolvere è codificata in una funzione f che ha come input un intero x (o volendo una stringa di n bit) e come output un singolo bit. In altre parole, $f : \{0, 1\}^{\otimes n} \rightarrow \{0, 1\}$. Per definizione, $f(x) = 1$ se x è soluzione del nostro problema (ovvero è uno degli elementi che stiamo cercando) e $f(x) = 0$ se x non è soluzione del nostro problema.

Per fissare le idee, facciamo un esempio. Supponiamo di voler cercare il numero di un utente in un elenco telefonico *non ordinato* che comprende N utenti. L'elenco è costruito in modo tale da codificare per ogni utente le informazioni {Nome, Cognome, Numero di telefono}. Vogliamo trovare il numero di Mario Rossi. Possiamo costruire una funzione f che, per ogni utente, legga il nome e il cognome, lo confronti con il nome (Mario) e il cognome (Rossi) cercato. La funzione f darà come output 1 se nome e cognome sono quelli dell'utente cercato e 0 in tutti gli altri casi.

Lo schema è molto simile nel caso quantistico. Qui dobbiamo supporre di avere un dispositivo quantistico detto *oracolo* o *Black Box* che sia in grado di *riconoscere* la soluzione e di *segnalare* o *marcare* la soluzione agendo su un qubit addizionale. Prima di andare avanti, è bene chiarire il significato dei termini in italico nella frase precedente.

L'*oracolo* non conosce la soluzione del problema (del resto è una funzione scritta da noi che non sappiamo quale sia la soluzione) ma sa riconoscerla quando viene interrogato sottoponendogli un elemento del database. Un esempio illustrativo è la fattorizzazione dei numeri interi. Supponiamo che ci sia dato un numero intero m e che ci sia detto che è il prodotto di due numeri primi p e q : $m = p \cdot q$. Dobbiamo trovare quali sono p e q . L'algoritmo più usato di crittografia classica (RSA) si basa sul fatto che questo è un problema computazionalmente difficile da risolvere e che, fino ad ora, non è stato individuato nessun algoritmo

classico che sia efficiente¹. Il problema della fattorizzazione dei numeri primi può essere riformulato come un problema di ricerca in un database. Fra tutti i possibili input² dobbiamo trovare quelli per cui m è divisibile. In questo caso la funzione f implementata dall'oracolo non fa altro che prendere un intero x come input, dividere m per x e controllare se la divisione è esatta. Quindi l'oracolo non conosce la soluzione ma è in grado di verificare velocemente (mediante una divisione) se un numero è soluzione o no del problema (in questo caso, è un fattore di m)³.

La seconda proprietà che deve avere l'oracolo è di poter *marcare* la soluzione del problema. Vediamo come questo può essere fatto in maniera relativamente semplice (si veda anche l'algoritmo di Deutch in sec. 4.5.1). Allo stato generico $|x\rangle$ associamo un qubit aggiuntivo detto spesso *qubit oracolo* o *ancilla*: $|q\rangle$. Lo stato totale sarà quindi $|x\rangle|q\rangle$. Il qubit ancilla non porta informazione logica ma serve solo per immagazzinare l'informazione su $f(x)$, ovvero sul fatto che x sia o no soluzione del nostro problema. In maniera analoga a quanto visto nel problema si Deutch, questa operazione viene fatta usando l'addizione modulo 2 per cui l'effetto dell'oracolo è di applicare la seguente trasformazione

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle. \quad (6.1.1)$$

Nel caso più semplice, $q = 0$. Se x è soluzione, $f(x) = 1$ e $|0 \oplus 1\rangle = |1\rangle$. Al contrario, se x non è soluzione, $f(x) = 0$ e $|0 \oplus 0\rangle = |0\rangle$. Riassumendo abbiamo che

$$|x\rangle|0\rangle \xrightarrow{O} \begin{cases} |x\rangle|1\rangle & \text{se } x \text{ è soluzione} \\ |x\rangle|0\rangle & \text{se } x \text{ non è soluzione.} \end{cases} \quad (6.1.2)$$

In sostanza l'effetto dell'oracolo è quello di *marcare* solo gli stati soluzione associandolo ad un qubit aggiuntivo con valore 1.

L'esempio precedente è stato fatto scegliendo $q = 0$. Questo però è una scelta arbitraria. Potremmo scegliere ad esempio di inizializzare il qubit ancilla nello stato $|q\rangle = |1\rangle$. In questo caso, se x è soluzione, $f(x) = 1$ e $|1 \oplus 1\rangle = |0\rangle$ e se x non è soluzione, $f(x) = 0$ e $|1 \oplus 0\rangle = |1\rangle$. Quindi

$$|x\rangle|1\rangle \xrightarrow{O} \begin{cases} |x\rangle|0\rangle & \text{se } x \text{ è soluzione} \\ |x\rangle|1\rangle & \text{se } x \text{ non è soluzione.} \end{cases} \quad (6.1.3)$$

¹ Come discusso nel Capitolo 5, esiste un algoritmo *quantistico* (di Shor) che permette di risolvere il problema della fattorizzazione degli interi in modo efficiente. [nielsen-chuang_book, Rieffel2011, Yanofsky2008].

² In realtà basta cercare fra gli interi compresi fra 2 e \sqrt{m} [nielsen-chuang_book, Rieffel2011, Yanofsky2008].

³ Questo concetto (e quindi quello dell'oracolo o della Black Box) è alla base della teoria della complessità computazionale. Si pensi, ad esempio, alla classe di problemi NP per i quali il trovare una soluzione è difficile mentre il controllo se un dato input (istanza) è soluzione o no può essere fatto velocemente (con risorse polinomiali nella dimensione dell'input) [nielsen-chuang_book].

Questa osservazione ci permette di studiare in altri casi dove il qubit ancilla nello stato $|q\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Lo stato totale si può scrivere come

$$|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} [|x\rangle \otimes |0\rangle - |x\rangle \otimes |1\rangle]. \quad (6.1.4)$$

Usando le equazioni (6.1.2) e (6.1.5), vediamo che se x è soluzione il bit ancilla cambia stato mentre rimane ugualse se x non è soluzione. Con questa osservazione otteniamo che l'effetto dell'oracolo è

$$\frac{1}{\sqrt{2}} [|x\rangle \otimes |0\rangle - |x\rangle \otimes |1\rangle] \xrightarrow{O} \begin{cases} \frac{1}{\sqrt{2}} (|x\rangle \otimes |1\rangle - |x\rangle \otimes |0\rangle) & \text{se } x \text{ è soluzione} \\ \frac{1}{\sqrt{2}} (|x\rangle \otimes |0\rangle - |x\rangle \otimes |1\rangle) & \text{se } x \text{ non è soluzione.} \end{cases} \quad (6.1.5)$$

I due stati ottenuti differiscono solo per un segno meno che possiamo fattorizzare come una fase. L'effetto dell'oracolo in questo caso è

$$|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{O} (-1)^{f(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (6.1.6)$$

Anche in questo caso lo stato soluzione viene *marcato* dall'applicazione dell'oracolo. La differenza consta nella scelta dello stato iniziale del qubit ancilla che si riflette nella maniera in cui l'oracolo agisce. Se usando $|q\rangle = |0\rangle$, lo stato $|x\rangle |q\rangle$ viene modificato, usando $|q\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ acquista solo una fase $(-1)^{f(x)}$ mentre la struttura non viene cambiata. In quest'ultimo caso possiamo addirittura dimenticarci del qubit ancilla (visto che non viene modificato ed è uguale per tutti gli stati $|x\rangle$) e scrivere l'effetto solo sui qubit logici

$$|x\rangle \xrightarrow{O} (-1)^{f(x)} |x\rangle. \quad (6.1.7)$$

6.1.2 Algoritmo di ricerca in database (Grover)

Ora possiamo discutere l'implementazione e le performance dell'algoritmo di Grover per la ricerca in un database. Per semplicità considereremo solo il caso in cui c'è un unico stato che soddisfa i requisiti richiesti fra i possibili N elementi del database. (il problema ha un'unica soluzione). Il caso con M soluzioni è ugualmente trattabile ma richiede l'introduzione di tecniche e algoritmi più complicati [nielsen-chuang_book].

L'algoritmo di Grover inizia con la costruzione dello stato quantistico sovrapposizione di tutti i possibili stati logici (sec. 4.1). Se lo spazio di ricerca è costituito da N elementi che possono essere codificati in n qubit (quindi $N = 2^n$), questo può essere costruito partendo dallo stato di soli zeri $|000\dots 0\rangle$ con l'applicazione di n porte di Hadamard (3.7.4). Il nostro stato di partenza sarà

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle. \quad (6.1.8)$$

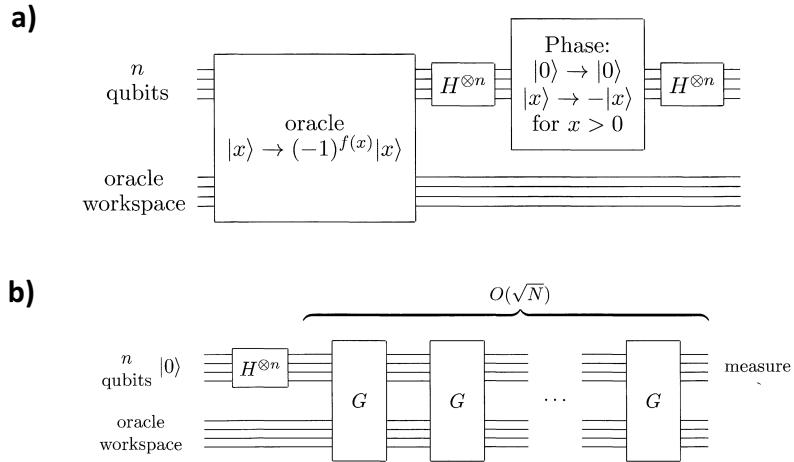


Figure 19: a) Schema circuitale per l'implementazione dell'operatore di Grover. b) Schema circuitale per l'implementazione dell'algoritmo di Grover.

Il cuore dell'algoritmo è nella costruzione di un operatore detto di *Grover* che sfrutta l'idea di oracolo come discussa nella sezione 6.1.1

Implementazione dell'operatore di Grover G:

- Applicare allo stato l'oracolo (6.1.7) che cambia la fase allo stato soluzione:

$$|x\rangle \xrightarrow{\text{O}} (-1)^{f(x)}|x\rangle. \quad (6.1.9)$$

- Applicare n porte di Hadamard.
- Applicare un cambio di fase a tutti gli stati tranne allo stato $|000\dots 0\rangle$:

$$|x\rangle \rightarrow -(-1)^{\delta_{x0}}|x\rangle \quad (6.1.10)$$

(dove δ_{x0} è la delta di Kronecker tale che $\delta_{ij} = 1$ se $i = j$ e $\delta_{ij} = 0$ se $i \neq j$).
Ovvero, $|0\rangle \rightarrow |0\rangle$ e, per $x \neq 0$, $|x\rangle \rightarrow -|x\rangle$.

- Applicare n porte di Hadamard.

La sequenza di operazioni per costruire l'operatore di Grover è mostrata in Figura 19 a).

Una volta costruito il circuito logico quantistico per implementare l'operatore di G , l'algoritmo per la ricerca in un database si riduce alla sua applicazione per un numero $\sqrt{N} = 2^{n/2}$ di volte come mostrato in Figura 19 b).

Stati "soluzione" e "non-soluzione".

Lo spazio logico può essere diviso in due sottospazi. Quello generato da $|x\rangle$ con x soluzione del nostro problema (ovvero quelli a cui l'oracolo cambia segno) e quelli che non sono soluzione del nostro problema. Supponiamo che ci siano M stati soluzione e, di conseguenza $N - M$ stati non-soluzione. La sovrapposizione di tutti gli stati soluzione viene indicata da un vettore $|\beta\rangle$ mentre quella degli stati non-soluzione viene indicata con $|\alpha\rangle$. In modo più formale, definiamo

$$\begin{aligned} |\alpha\rangle &= \frac{1}{\sqrt{N-M}} \sum_{x \in \text{non-sol}} |x\rangle \\ |\beta\rangle &= \frac{1}{\sqrt{M}} \sum_{x \in \text{sol}} |x\rangle \end{aligned} \quad (6.1.11)$$

Con questa notazione lo stato iniziale $|\psi\rangle$ in Eq. (6.1.8) si scrive come

$$|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle. \quad (6.1.12)$$

Questo può essere verificato anche direttamente inserendo le definizioni (6.1.11) nella (6.1.12).

Operatore di Grover

Così come è stato presentato, l'operatore G e la sua azione risultano ancora misteriosi. Per rendere più concreta la trasformazione indotta scriviamo tutto in termini di operatori quantistici sfruttando la distinzione fra stati soluzione e stati non-soluzione in Eq. (6.1.11).

Come detto l'oracolo cambia segno solo agli stati soluzione, quindi cambierà segno allo stato $|\beta\rangle$ lasciando $|\alpha\rangle$ invariato. Se lo facciamo agire su uno stato generico $a|\alpha\rangle + b|\beta\rangle$ otteniamo

$$O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle \quad (6.1.13)$$

Nella notazione braket questo può essere scritto come

$$O = |\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta|. \quad (6.1.14)$$

Una scrittura ancora più conveniente è quella in termini di matrici nello spazio $\{|\alpha\rangle, |\beta\rangle\}$. Abbiamo

$$O = \begin{pmatrix} |\alpha\rangle & |\beta\rangle \\ \langle\alpha| & \langle\beta| \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (6.1.15)$$

Per la rimanente parte dell'operatore di Grover abbiamo l'applicazione di n porte di Hadarmard intermezzate dall'operatore che cambia di segno a tutti gli

stati tranne lo stato $|\bar{0}\rangle \equiv |00\dots 0\rangle$. Quest'ultimo nella notazione braket si scrive come

$$U = 2|\bar{0}\rangle\langle\bar{0}| - Id \quad (6.1.16)$$

(dove Id è l'operatore identità). Possiamo verificare che se $|x\rangle \neq |\bar{0}\rangle$,

$$U|x\rangle = (2|\bar{0}\rangle\langle\bar{0}| - Id)|x\rangle = -|x\rangle \quad (6.1.17)$$

e che

$$U|\bar{0}\rangle = (2|\bar{0}\rangle\langle\bar{0}| - Id)|\bar{0}\rangle = 2|\bar{0}\rangle - |\bar{0}\rangle = |\bar{0}\rangle \quad (6.1.18)$$

come ci aspettavamo.

A questo punto possiamo scrivere la parte rimanente dell'operatore di Grover come

$$H^{\otimes n}UH^{\otimes n} = H^{\otimes n}(2|\bar{0}\rangle\langle\bar{0}| - Id)H^{\otimes n} = 2|\psi\rangle\langle\psi| - Id. \quad (6.1.19)$$

L'ultimo passaggio deriva dal fatto che $H^{\otimes n}|\bar{0}\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = |\psi\rangle$ e che $H^{\otimes n}IdH^{\otimes n} = Id$. Infatti, $H^{\otimes n}IdH^{\otimes n} = (H^2)^{\otimes n} = Id$ dato che $H^2 = Id$.

Ne consegue che l'operatore di Grover può essere scritto come

$$G = (2|\psi\rangle\langle\psi| - Id)O. \quad (6.1.20)$$

6.1.3 Interpretazione geometrica dell'algoritmo

Lo stato $|\psi\rangle$ in Eq. (6.1.12) è normalizzato e può essere riscritto in termini di funzioni seno e coseno come

$$|\psi\rangle = \cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle \quad (6.1.21)$$

con

$$\begin{aligned} \cos \frac{\theta}{2} &= \sqrt{\frac{N-M}{N}} \\ \sin \frac{\theta}{2} &= \sqrt{\frac{M}{N}} \end{aligned} \quad (6.1.22)$$

Questa riscrittura ci permette di rappresentare lo stato del sistema in uno spazio bidimensionale e legarlo agli angoli come in figura 20.

I casi più importanti a livello computazionale (e più difficili da risolvere) sono quelli in cui lo spazio di ricerca è molto grande e le soluzioni sono poche; ovvero, $N \gg M$.

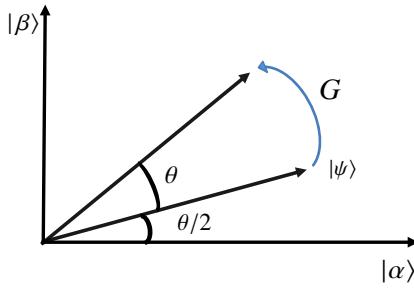


Figure 20: Rappresentazione geometrica dell'algoritmo di Grover. Il sistema è descritto in un piano bidimensionale in cui gli assi sono le proiezioni sul subspazio delle soluzioni $|\beta\rangle$ e delle non-soluzioni $|\alpha\rangle$. L'operatore di Grover induce una rotazione di un angolo θ .

Riscriviamo ora l'operatore $2|\psi\rangle\langle\psi| - \text{Id}$ in termini delle funzioni seno e coseno. Dall'Eq. (6.1.21), abbiamo che $\langle\psi|\alpha\rangle = \cos\frac{\theta}{2}$ e $\langle\psi|\beta\rangle = \sin\frac{\theta}{2}$. Quindi,

$$\begin{aligned} (2|\psi\rangle\langle\psi| - \text{Id})|\alpha\rangle &= 2|\psi\rangle\langle\psi|\alpha\rangle - |\alpha\rangle = 2\cos\frac{\theta}{2}|\psi\rangle - |\alpha\rangle \\ &= 2\cos\frac{\theta}{2}\left(\cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle\right) - |\alpha\rangle \\ &= \cos\theta|\alpha\rangle + \sin\theta|\beta\rangle. \end{aligned} \quad (6.1.23)$$

Dove abbiamo usato le relazioni $2\sin\frac{\theta}{2}\cos\frac{\theta}{2} = \sin\theta$ e $2\cos^2\frac{\theta}{2} - 1 = \cos\theta$.

In maniera del tutto analoga abbiamo

$$\begin{aligned} (2|\psi\rangle\langle\psi| - \text{Id})|\beta\rangle &= 2|\psi\rangle\langle\psi|\beta\rangle - |\beta\rangle = 2\sin\frac{\theta}{2}|\psi\rangle - |\beta\rangle \\ &= 2\sin\frac{\theta}{2}\left(\cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle\right) - |\beta\rangle \\ &= \sin\theta|\alpha\rangle - \cos\theta|\beta\rangle. \end{aligned} \quad (6.1.24)$$

Questo ci permette di scrivere l'operatore U in forma matriciale come

$$U = \begin{bmatrix} |\alpha\rangle & |\beta\rangle \\ \langle\alpha| & \langle\beta| \end{bmatrix} \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}. \quad (6.1.25)$$

Ne consegue che l'operatore di Grover nello spazio $\{|\alpha\rangle, |\beta\rangle\}$ e in forma matriciale si scrive come

$$G = U O = \begin{bmatrix} |\alpha\rangle & |\beta\rangle \\ \langle\alpha| & \langle\beta| \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}. \quad (6.1.26)$$

6.1.4 Effetto dell'operatore di Grover

L'operatore di Grover nella rappresentazione (6.1.26) è immediatamente associabile ad una rotazione nel piano definito dagli stati $\{|\alpha\rangle, |\beta\rangle\}$ ⁴.

Per capire meglio questo punto, supponiamo di applicarlo allo stato $|\phi\rangle = \cos\delta|\alpha\rangle + \sin\delta|\beta\rangle$:

$$G |\phi\rangle = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \cdot \begin{bmatrix} \cos\delta \\ \sin\delta \end{bmatrix} = \begin{bmatrix} \cos(\theta + \delta) \\ \sin(\theta + \delta) \end{bmatrix} \quad (6.1.27)$$

dove abbiamo usato le formule $\sin(a \pm b) = \sin a \cos b \pm \cos a \sin b$ e $\cos(a \pm b) = \cos a \cos b \mp \sin a \sin b$. Quindi lo stato descritto dall'angolo δ viene ruotato di un angolo θ .

Ne consegue che se applichiamo k volte l'operatore di Grover, genereremo nello spazio $\{|\alpha\rangle, |\beta\rangle\}$ una rotazione di un angolo $k\theta$. Se lo stato iniziale è $|\psi\rangle$ in Eq. (6.1.21) (associato ad un angolo $\theta/2$) dopo k applicazioni dell'operatore di Grover avremo

$$G^k |\psi\rangle = \begin{bmatrix} \cos\left(\frac{2k+1}{2}\theta\right) \\ \sin\left(\frac{2k+1}{2}\theta\right) \end{bmatrix} = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle. \quad (6.1.28)$$

6.1.5 Performance dell'algoritmo di Grover

L'Eq. (6.1.28) ci dà lo stato del sistema dopo k applicazioni dell'operatore di Grover. Affinchè l'algoritmo sia efficace deve aumentare la probabilità di misurare uno degli stati soluzione; quindi deve aumentare il coefficiente dello stato $|\beta\rangle$. Per avere la certezza di misurare uno degli stati in $|\beta\rangle$ dobbiamo avere

$$\sin\left(\frac{2k+1}{2}\theta\right) \approx 1 \quad (6.1.29)$$

che equivale ad richiedere che $\frac{2k+1}{2}\theta \approx \frac{\pi}{2}$ e quindi

$$k = \frac{1}{2}\left(\frac{\pi}{\theta} - 1\right). \quad (6.1.30)$$

In altre parole, l'Eq. (6.1.30) ci fornisce il numero di iterazioni necessarie all'algoritmo di Grover per rendere molto probabile la misura di uno degli stati soluzione.

Che valore assume θ ? Dall'Eq. (6.1.22) abbiamo che $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$. Nei casi più interessanti e difficili dove ci sono poche soluzioni, $M \ll N$. Di conseguenza, anche l'angolo $\theta/2$ dovrà essere piccolo e otterremo

$$\sin\frac{\theta}{2} \approx \frac{\theta}{2} = \sqrt{\frac{M}{N}}. \quad (6.1.31)$$

⁴ Si veda, ad esempio, https://en.wikipedia.org/wiki/Rotation_matrix.

Usando questa relazione nell'Eq. (6.1.30), otteniamo

$$k = \frac{1}{2} \left(\frac{\pi}{2} \sqrt{\frac{N}{M}} - 1 \right) \approx \frac{\pi}{4} \sqrt{\frac{N}{M}}. \quad (6.1.32)$$

Ricordando che per un sistema a n bit $N = 2^n$, abbiamo ottenuto che l'algoritmo di Grover riesce a trovare una soluzione corretta con $\sqrt{N} = 2^{\frac{n}{2}}$ chiamate alla funzione f . Questo è da confrontare alle $N = 2^n$ chiamate alla funzione f , per la ricerca classica in un database non strutturato. Ne consegue che l'algoritmo di Grover dà una velocizzazione (*speed-up*) quadratico rispetto agli analoghi classici.

6.1.6 Applicazione alla ricerca in un database di 4 elementi

Consideriamo la ricerca in un database di 4 elementi. Supponiamo che fra i 4 elementi ce ne sia solo uno indicato con \bar{x} che soddisfi le condizioni richieste. Quindi avremo che $f(\bar{x}) = 1$ e $f(x) = 0$ se $x \neq \bar{x}$.

Per l'implementazione dell'algoritmo di Grover, è necessario specificare le caratteristiche dell'elemento che stiamo cercando e la funzione f ⁵. Tuttavia per capire in senso astratto come funziona l'algoritmo di Grover e calcolare quante applicazioni sono necessarie per risolvere il problema, questo non è necessario dato che si può usare il formalismo più astratto usato nella sezione precedente.

In questo caso, abbiamo che $N = 4$ e $M = 1$. Di conseguenza,

$$\begin{aligned} \cos \frac{\theta}{2} &= \frac{N - M}{N} = \frac{\sqrt{3}}{2} \\ \sin \frac{\theta}{2} &= \frac{M}{N} = \frac{1}{2} \end{aligned} \quad (6.1.33)$$

che corrisponde ad un angolo $\theta = \pi/3$ (ovvero $\theta/2 = \pi/6$)

Possiamo scrivere lo stato iniziale in Eq. (6.1.21) come

$$|\Psi\rangle = \frac{\sqrt{3}}{2} |\alpha\rangle + \frac{1}{2} |\beta\rangle = \begin{bmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix} \quad (6.1.34)$$

Quindi dall'Eq. (6.1.26)

$$G = \frac{1}{2} \begin{bmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{bmatrix}. \quad (6.1.35)$$

Applicando una sola volta l'operatore di Grover allo stato iniziale $|\Psi\rangle$ otteniamo

$$G |\phi\rangle = \frac{1}{2} \begin{bmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{bmatrix} \cdot \frac{1}{2} \begin{bmatrix} \sqrt{3} \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |\beta\rangle. \quad (6.1.36)$$

Quindi con una sola applicazione dell'operatore G siamo arrivati a trovare la soluzione del problema.

⁵ Si noti che, come discusso in sezione 6.1.1, questo non significa conoscere la soluzione del problema ma saperla riconoscere.

7

INTRODUZIONE AI CODICI DI CORREZIONE DEGLI ERRORI PER COMPUTER QUANTISTICI

I – CORREZIONE DEGLI ERRORI NEI COMPUTER CLASSICI

Sebbene molto stabili i computer e le reti classiche possono andare in conto ad errori. Ad esempio, se noi immagazziniamo in un hardisk o mandiamo attraverso una rete una stringa di bit, è possibile che l'inevitabile rumore generi dei *bit flip*; ovvero trasformi alcuni bit che inizialmente avevano valore 0 in bit con valore 1 e viceversa.

Uno dei metodi più semplici e allo stesso tempo più efficaci per ovviare a questi errori è immagazzinare l'informazione logica in un numero maggiore di bit fisici. Ad esempio, il bit logico 0 può essere codificato con una stringa di tre 0, ovvero 000. Analogamente il bit logico 1 verrà codificato con la stringa 111.

Supponiamo adesso che a causa del rumore uno dei bit fisici che identificano il bit logico 0 subisca uno *bit flip*: $000 \rightarrow 100$. Grazie alla ridondanza di informazione usata, è possibile riconoscere e correggere l'errore. Basta ad esempio misurare tutti e tre i bit e usare il protocollo di *voto di maggioranza* (*majority voting*): se la maggioranza dei bit ha valore 0 assumiamo che il bit logico sia 0 e correggiamo l'errore trovato; analogamente, se la maggioranza dei bit ha valore 1 assumiamo che il bit logico sia 1.

Da questo esempio, è chiaro che il numero di bit usati deve essere dispari. Inoltre, il loro numero dipende da quanto è importante il rumore. Questa secondo punto necessita di un piccolo approfondimento. Riprendiamo l'esempio di sopra. Possiamo usare tre bit fisici solo se la probabilità che due bit cambino contemporaneamente è piccola. Infatti, se due bit contemporaneamente andassero incontro ad un *flip* ci ritroveremo con la stringa, ad esempio, 101. A questo punto, il protocollo di voto di maggioranza, ci indurrebbe a considerare il bit logico come 1 mentre inizialmente era 0.

In maniera più quantitativa, se la probabilità di un singolo *bit flip* è p , la probabilità che due bit vengano trasformati è $3p^2(1-p)$ mentre quella che tutti e tre vengano trasformati è p^3 ¹. La probabilità che due bit saltino è la somma delle due probabilità : $3p^2(1-p) + p^3 = 3p^2 - 2p^3$. Questa deve essere più piccola della probabilità p di un singolo salto. Arriviamo quindi alla condizione

$$3p^2 - 2p^3 < p \quad (7.1.1)$$

che è verificata se $p < 1/2$.

¹ Nel calcolo della probabilità dobbiamo tener conto anche dei modi in cui i bit possono saltare. La probabilità che saltino due bit ma che il terzo rimanga uguale è $p^2(1-p)$. In questo processo potrebbero saltare il primo e il secondo (mentre il terzo rimane stabile), il primo e il terzo (mentre il secondo rimane stabile) oppure il secondo e il terzo (mentre il primo rimane stabile). Dato che abbiamo tre modi in cui il processo può avvenire, la probabilità totale sarà $3p^2(1-p)$.

Siamo arrivati alla conclusione che per un qualsiasi processo in cui la probabilità di *bit flip* è minore di $1/2$, bastano tre bit affinché il protocollo di voto di maggioranza dia buoni risultati. Vorremo però poter diminuire la probabilità di errore in modo tale da poter rendere stabili e sicuri la trasmissione, l'immagazzinamento e l'elaborazione dei dati. Ci sono due modi per farlo. Il primo è usare un hardware che sia più stabile e quindi che abbia una probabilità più bassa di subire *bit flip* contemporanei.

L'alternativa più interessante è usare un numero di bit maggiore. Se la probabilità che un singolo bit salti è $P = 1/2 + \epsilon$ (quindi arbitrariamente vicina alla soglia $1/2$), si può dimostrare che per un numero N grande di bit fisici, la probabilità di errore decresce come $P_{\text{errore}} \propto e^{-Ne^2}$.

Siamo arrivati alla conclusione che, con un numero grande di bit, è possibile rendere i nostri dati stabili anche se sottoposti ad una sorgente di rumore. Il numero di bit da usare sarà determinato dalla probabilità di errore del nostro hardware.

II – CASO QUANTISTICO: I PROBLEMI

Rispetto ai computer classici, quelli quantistici sembrano avere degli svantaggi intrinseci. Innanzitutto, i sistemi quantistici sono più delicati e instabili dei corrispondenti classici. Si aggiungono però altre limitazioni legate alla struttura stessa della meccanica quantistica. In particolare,

1. Lo stato del sistema non può essere copiato come dimostrato dal teorema no-cloning (se c. 4.2.1). Questo impedisce di duplicare l'informazione e sfruttare le copie per estrarre l'informazione corretta.
2. In generale, il sistema non può essere misurato senza disturbare lo stato del sistema. Dobbiamo fare particolare attenzione nell'estrarrre informazione perché la misura potrebbe portare al collasso e distruggere la sovrapposizione di stati quantistici. In sostanza, dobbiamo trovare un modo di estrarre l'informazione senza disturbare lo stato.
3. Ci sono altri tipo di errore di cui dobbiamo tenere conto:
 - a) Come nel caso classico, il *bit flip* corrisponde alla transizione $|0\rangle \rightarrow |1\rangle$ e $|1\rangle \rightarrow |0\rangle$.
 - b) errori piccoli in cui il sistema non ha una transizione completa ma transisce verso una sovrapposizione di stati; per esempio, $|0\rangle \rightarrow \gamma|0\rangle + \delta|1\rangle$.
 - c) La fase relativa fra gli stati può essere modificata per effetto del rumore; per esempio, $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle + e^{i\phi}\beta|1\rangle$

III – CODICI DI CORREZIONE DEGLI ERRORI QUANTITICI

Il più semplice codice di correzione degli errori quantistico sfrutta, come l'analogo classico, il voto di maggioranza. Per prima cosa dobbiamo moltiplicare l'informazione.

A questo proposito definiamo i qubit logici come stati composti da un numero dispari di qubit fisici. Ad esempio, se si usano tre qubit avremo

$$\begin{aligned} |0_L\rangle &\equiv |000\rangle \\ |1_L\rangle &\equiv |111\rangle \end{aligned} \quad (7.3.1)$$

Lo stato quantistico generico sarà dunque scritto come $\alpha|0_L\rangle + \beta|1_L\rangle$ e si può ottenere a partire dallo stato a singolo qubit con delle semplici porte CNOT

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |00\rangle \xrightarrow{\text{C}_1 \text{NOT}_2} (\alpha|00\rangle + \beta|11\rangle) \otimes |0\rangle \xrightarrow{\text{C}_1 \text{NOT}_3} \alpha|0_L\rangle + \beta|1_L\rangle \quad (7.3.2)$$

Si noti che una misura diretta dello stato, ad esempio nella base canonica, distruggerebbe la sovrapposizione e quindi parte dell'informazione. È necessario quindi trovare degli osservabili che permettano di estrarre l'informazione desiderata senza perturbare lo stato del sistema.

Concentriamoci prima sui primi due qubit. Un operatore di questo tipo è $Z_1 \otimes Z_2$; ovvero l'operatore che misura *contemporaneamente* il valore dell'operatore Z di Pauli del primo e del secondo qubit. Si noti che gli stati della base a due qubit $\{|00\rangle, |10\rangle, |01\rangle, |11\rangle\}$ sono tutti autostati dell'operatore $Z_1 \otimes Z_2$. Inoltre ricordando che $Z_i|0\rangle_i = -|0\rangle_i$ e $Z_i|1\rangle_i = |1\rangle_i$ abbiamo che, ad esempio, misurando $Z_1 \otimes Z_2$ per lo stato $|00\rangle$ avremo $(-1)^2 = 1$. Riassumendo

$$\begin{aligned} Z_1 \otimes Z_2 |00\rangle &= |00\rangle \\ Z_1 \otimes Z_2 |01\rangle &= -|01\rangle \\ Z_1 \otimes Z_2 |10\rangle &= -|10\rangle \\ Z_1 \otimes Z_2 |11\rangle &= |11\rangle. \end{aligned} \quad (7.3.3)$$

Dalla teoria della misura deduciamo che se dovessimo avessimo solo stati della base a due qubit, una misura di $Z_1 \otimes Z_2$ non disturberebbe lo stato. In generale però dovremmo tener conto che il sistema sarà in una sovrapposizione di stati della base.

7.3.1 Errore *bit flip*

Vediamo cosa succede se il sistema va incontro ad un *bit flip* per il primo qubit. Lo stato del sistema sarà

$$|\Psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle = \alpha|000\rangle + \beta|111\rangle \xrightarrow{\text{errore}} \alpha|100\rangle + \beta|011\rangle = |\Phi\rangle \quad (7.3.4)$$

Applicando l'operatore $Z_1 \otimes Z_2$ allo stato $|\Phi\rangle$ (usando le regole ottenute sopra) abbiamo

$$Z_1 \otimes Z_2 (\alpha|100\rangle + \beta|011\rangle) = (-\alpha|100\rangle - \beta|011\rangle) = -|\Phi\rangle. \quad (7.3.5)$$

Facendo lo stesso sullo stato senza errori $|\Psi\rangle$ abbiamo

$$Z_1 \otimes Z_2(\alpha|000\rangle + \beta|111\rangle) = (\alpha|000\rangle + \beta|111\rangle) = |\Psi\rangle. \quad (7.3.6)$$

Concludiamo che entrambi gli stati sono autostati dell'operatore $Z_1 \otimes Z_2$ ma con autovalore diverso. Quindi, una misura dell'operatore $Z_1 \otimes Z_2$ distruggerà la sovrapposizione di stati $|\Psi\rangle$ e $|\Phi\rangle$. Però nel caso il sistema sia in $|\Psi\rangle$ oppure in $|\Phi\rangle$ la misura di $Z_1 \otimes Z_2$ permetterà di estrarre l'informazione desiderata. Se dalla misura otteniamo l'autovalore +1 deduciamo che non ci sono stati errori; se otteniamo -1 deduciamo che c'è stato un errore.

Lo schema però non è ancora completo. Infatti se ci fosse un errore nel secondo qubit avremmo

$$|\Psi\rangle = \alpha|000\rangle + \beta|111\rangle \xrightarrow{\text{errore}} \alpha|010\rangle + \beta|101\rangle = |\Phi\rangle \quad (7.3.7)$$

In questo caso, la misura dell'operatore $Z_1 \otimes Z_2$ darà esattamente gli stessi risultati di sopra. In sostanza la singola misura di $Z_1 \otimes Z_2$ evidenzia che c'è stato un errore ma non ci permette di sapere se è avvenuto sul primo o sul secondo qubit. Questa incertezza ci impedisce di correggere l'errore.

Per identificare anche la posizione in cui è avvenuto l'errore è necessario misurare un altro operatore complementare come $Z_1 \otimes Z_3$. Supponiamo che l'errore sia avvenuto sul primo qubit; avremo

$$Z_1 \otimes Z_3(\alpha|100\rangle + \beta|011\rangle) = (-\alpha|100\rangle - \beta|011\rangle) = -|\Phi\rangle (\alpha|100\rangle + \beta|011\rangle). \quad (7.3.8)$$

Quindi otterremo l'autovalore -1. Se invece l'errore fosse avvenuto sul secondo qubit, avremo

$$Z_1 \otimes Z_3(\alpha|010\rangle + \beta|101\rangle) = \alpha|010\rangle + \beta|101\rangle \quad (7.3.9)$$

che è associato all'autovalore e alla misura +1. Una misura combinata di $Z_1 \otimes Z_2$ e di $Z_1 \otimes Z_3$ darà quindi la coppia di risultati $\{-1, -1\}$ se l'errore è avvenuto sul primo qubit e $\{-1, 1\}$ se è avvenuto sul secondo. Una volta identificato il qubit perturbato, potremmo intervenire applicando una porta di correzione; X_1 nel primo caso e X_2 nel secondo caso.

7.3.2 Errori "piccoli"

Un sistema quantistico può andare incontro a perturbazioni (errori) che non modificano completamente il valore del qubit ma generano sovrapposizioni indesiderate. Ad esempio, $|0\rangle \rightarrow \gamma|0\rangle + \delta|1\rangle$ dove, per semplicità consideriamo γ e δ reali e, visto che la perturbazione è considerata piccola abbiamo che $|\gamma| \gg |\delta|$. Se il $|0\rangle$ va incon-

tro alla trasformazione di sopra, dovremmo per forza avere che $|1\rangle \rightarrow \gamma|1\rangle - \delta|0\rangle$ ².

Se questo tipo di errore avviene sul primo qubit si avrà una sovrapposizione di più stati

$$|\Psi\rangle = \alpha|000\rangle + \beta|111\rangle \xrightarrow{\text{errore}} \alpha\gamma|000\rangle + \alpha\delta|100\rangle + \beta\gamma|111\rangle - \beta\delta|011\rangle = |\Phi\rangle. \quad (7.3.10)$$

Usando le regole di sopra abbiamo che

$$Z_1 \otimes Z_2 |\Phi\rangle = \alpha\gamma|000\rangle - \alpha\delta|100\rangle + \beta\gamma^*|111\rangle + \beta\delta^*|011\rangle \neq |\Phi\rangle. \quad (7.3.11)$$

Ne consegue che $|\Phi\rangle$ non è un autostato di $Z_1 \otimes Z_2$ e che quindi verrà perturbato dalla misura. Per vedere come, lo scriviamo evidenziando gli autostati di $Z_1 \otimes Z_2$ aventi lo stesso valore

$$\begin{aligned} |\Phi\rangle &= \gamma[\alpha|000\rangle + \beta|111\rangle] + \delta[\beta|011\rangle - \alpha|100\rangle] \\ &= \gamma|\phi_+\rangle + \delta|\phi_-\rangle. \end{aligned} \quad (7.3.12)$$

Lo stato $|\phi_+\rangle$ (sovrapposizione di $|00\rangle$ e $|11\rangle$) è un autostato di $Z_1 \otimes Z_2$ con autovalore +1 e lo stato $|\phi_-\rangle$ (sovrapposizione di $|01\rangle$ e $|10\rangle$) è un autostato di $Z_1 \otimes Z_2$ con autovalore -1. Dalla teoria della misura (sezione 3.3) sappiamo che la misura di $Z_1 \otimes Z_2$ darà +1 con probabilità γ^2 e il sistema collasserà sullo stato $|\phi_+\rangle$ oppure otterremo -1 con probabilità δ^2 se il sistema collassa sullo stato $|\phi_-\rangle$.

Data la condizione di errore "piccolo" $\gamma^2 \gg \delta^2$, la maggior parte delle volte otterremo +1 e il sistema dopo la misura si troverà nello stato $|\phi_+\rangle = \alpha|000\rangle + \beta|111\rangle$. Questo è lo stato logico iniziale senza errore. Quindi la misura proiettiva ha automaticamente corretto l'errore senza ulteriori modifiche.

Cosa succede se otteniamo -1? In questo caso, il sistema si troverà nello stato con errore $|\phi_-\rangle = \beta|011\rangle - \alpha|100\rangle$. Però l'output -1 ci segnala la presenza dell'errore che può essere eliminato con l'applicazione di porte logiche correttive. Ad esempio, in questo caso, l'applicazione di una porta X_1 (NOT sul primo qubit) da $|\phi_-\rangle \rightarrow |\phi_+\rangle$ che è lo stato originale.

È importante evidenziare che, come sopra, la singola misura di $Z_1 \otimes Z_2$ non è sufficiente per sapere che c'è stato un errore ma non per individuarne la posizione (l'errore potrebbe essere anche sul secondo qubit). Quindi per poter applicare le porte correttive è necessario misurare anche l'osservabile $Z_1 \otimes Z_3$.

Riassumendo, le misure degli osservabili $Z_1 \otimes Z_2$ e $Z_1 \otimes Z_3$ permettono di controllare se e dove è avvenuto un errore e correggerlo.

² Si noti che questa è una trasformazione unitaria che preserva il prodotto scalare. Dato che gli stati iniziali $|0\rangle$ e $|1\rangle$ sono ortogonali, gli stati finali devono essere ortogonali. Ne consegue la regola di trasformazione per lo stato $|1\rangle$.

7.3.3 Errore sulla fase

Nella meccanica quantistica la differenza di fase fra gli stati è osservabile. Ne consegue che anche la fase relativa può essere perturbata e portare ad un disturbo o distruzione dell'informazione originale. Oltre agli errori trattati fin ora, i qubit possono incorrere in un *errore di fase*. Questo è un errore puramente quantistico visto che non c'è alcuna corrispondenza classica.

Consideriamo gli errori in cui la fase relativa fra due stati sovrapposizione cambia di segno detto di *phase flip*; questo può essere schematizzato come

$$\begin{aligned} |0\rangle &\xrightarrow{\text{phase error}} |0\rangle \\ |1\rangle &\xrightarrow{\text{phase error}} -|1\rangle \end{aligned} \quad (7.3.13)$$

ovvero, come una trasformazione unitaria in cui solo lo stato $|1\rangle$ cambia segno.

Se anche uno solo dei qubit che compongono lo stato logico $|\Phi\rangle$ andasse incontro a un *phase flip* si avrebbe

$$\alpha|000\rangle + \beta|111\rangle \xrightarrow{\text{phase flip}} \alpha|000\rangle - \beta|111\rangle. \quad (7.3.14)$$

Si noti che la misura degli osservabili $Z_1 \otimes Z_2$ e $Z_1 \otimes Z_3$ non permette di identificare l'errore. Notiamo però che se invece di avere gli stati della base canonica $\{|0\rangle, |1\rangle\}$ avessimo gli stati della base $\{|+\rangle, |-\rangle\}$ si avrebbe

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \xleftrightarrow{\text{phase flip}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle. \quad (7.3.15)$$

Quindi, nella base $\{|+\rangle, |-\rangle\}$, il *phase flip* è equivalente ad un *bit flip* che scambia gli stati della base. Ne consegue che per identificare e correggere i *phase flip* è sufficiente implementare lo stesso schema dei *bit flip* nella base $\{|+\rangle, |-\rangle\}$.

Nello specifico, se partiamo dallo stato $|\Phi\rangle = \alpha|000\rangle + \beta|111\rangle$, applichiamo tre porte di Hadamard ai tre qubit

$$|\Phi\rangle \xrightarrow{H^{\otimes 3}} \alpha|+++ \rangle + \beta|--- \rangle. \quad (7.3.16)$$

Dato $\{|+\rangle, |-\rangle\}$ sono autostati dell'operatore X , i.e., $X|+\rangle = |+\rangle$ e $X|-\rangle = -|-\rangle$, dovremmo misurare gli operatori $X_1 \otimes X_2$ e $X_1 \otimes X_3$. Esattamente come discusso prima, in assenza di errori (ovvero sullo stato $|\Phi\rangle$) otterremo semplicemente gli autovalori +1 e +1.

Supponiamo che il primo qubit vada incontro ad un *phase flip*

$$\alpha|+++ \rangle + \beta|--- \rangle \xrightarrow{\text{phase flip}} \alpha|-++ \rangle + \beta|+-- \rangle. \quad (7.3.17)$$

In questo caso, le misure di $X_1 \otimes X_2$ e $X_1 \otimes X_3$ daranno come risultati -1 e -1, rispettivamente, e permetteranno di individuare l'errore e di correggerlo appli-

cando l'operatore Z_1 ³. Dopo aver fatto le misure e, nel caso, applicati gli operatori di correzione, è necessario tornare alla base canonica applicando altre tre porte di Hadamard.

I protocolli presentati permettono di individuare e correggere gli errori indotti dal rumore. Dato che però non si sa quando questi possono avvenire, è necessario applicarli con una certa frequenza in modo tale da mantenere il sistema nello spazio logico.

IV – PROTOCOLLO COMPLETO

Fino ad questo punto abbiamo discusso le idee fondamentali dei codici di correzione degli errori. Abbiamo mostrato che si possono trovare degli operatori che permettono di stabilire (tramite la misura) se e dove c'è stato un errore. Il punto cruciale è di codificare gli stati logici in modo tale che siano autostati degli operatori che poi andiamo a misurare. In questo modo, la misura permette di estrarre l'informazione riguardante l'errore senza distruggere la sovrapposizione di stati.

Queste idee possano essere usate per i *bit flip* e *phase flip* (con differenti operatori da misurare). Sebbene contengano le idee fondamentali, i protocolli discussi non sono completi. Per poter implementare contemporaneamente i protocolli di correzione per i *bit flip* e *phase flip*, tre qubit non sono sufficienti ed è necessario usare 9 qubit. Il protocollo completo per la correzione degli errori fu proposto da Peter Shor nel 1995 [Shor1995] ed è quello che discutiamo nel seguito del capitolo.

In questo protocollo i 9 qubit sono divisi in 3 blocchi e i qubit logici $|0_L\rangle$ e $|1_L\rangle$ sono definiti con

$$\begin{aligned} |0_L\rangle &\equiv \frac{|000\rangle + |111\rangle}{\sqrt{2}} \frac{|000\rangle + |111\rangle}{\sqrt{2}} \frac{|000\rangle + |111\rangle}{\sqrt{2}} \\ |1_L\rangle &\equiv \frac{|000\rangle - |111\rangle}{\sqrt{2}} \frac{|000\rangle - |111\rangle}{\sqrt{2}} \frac{|000\rangle - |111\rangle}{\sqrt{2}} \end{aligned} \quad (7.4.1)$$

È conveniente introdurre una notazione speciale per indicare i blocchi di tre qubit

$$\begin{aligned} |\bar{0}\rangle &\equiv \frac{|000\rangle + |111\rangle}{\sqrt{2}} \\ |\bar{1}\rangle &\equiv \frac{|000\rangle - |111\rangle}{\sqrt{2}} \end{aligned} \quad (7.4.2)$$

In questo modo, i qubit logici si possono riscrivere come $|0_L\rangle = |\bar{0}\rangle|\bar{0}\rangle|\bar{0}\rangle$ e $|1_L\rangle = |\bar{1}\rangle|\bar{1}\rangle|\bar{1}\rangle$ e il generico stato (logico) del qubit come

$$|\Psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle = \alpha|\bar{0}\rangle|\bar{0}\rangle|\bar{0}\rangle + \beta|\bar{1}\rangle|\bar{1}\rangle|\bar{1}\rangle. \quad (7.4.3)$$

A questo punto possiamo fare alcune osservazioni. La prima è che i blocchi sono sovrapposizioni equipesate (e normalizzate) degli stati $|000\rangle$ e $|111\rangle$ e differiscono solo per la fase relativa. La seconda è che lo stato logico in eq. 7.4.3 rassomiglia a

³ L'operatore Z_1 scambia gli stati $|+\rangle \leftrightarrow |-\rangle$.

quello discusso nella sezione 7.3; possiamo quindi aspettarci, con i dovuti cambiamenti, di poter implementare un codice di correzione simile a quello già discusso.

7.4.1 Bit flip

Supponiamo che avvenga un *bit flip* su primo qubit (naturalmente lo stesso schema si può usare per determinare l'errore su ogni qubit). In questo caso ci basta considerare l'effetto sul primo blocco

$$\begin{aligned} |\bar{0}\rangle &= \frac{|000\rangle + |111\rangle}{\sqrt{2}} \rightarrow \frac{|100\rangle + |011\rangle}{\sqrt{2}} \\ |\bar{1}\rangle &= \frac{|000\rangle - |111\rangle}{\sqrt{2}} \rightarrow \frac{|100\rangle - |011\rangle}{\sqrt{2}}. \end{aligned} \quad (7.4.4)$$

Anche in questo caso, misuriamo gli operatori $Z_1 \otimes Z_2$ e $Z_1 \otimes Z_3$.

Analogamente alla discussion in sez. 7.3, si può dimostrare che gli stati $|\bar{0}\rangle$ e $|\bar{1}\rangle$ sono autostati di $Z_1 \otimes Z_2$ entrambi con autovalore +1 mentre gli stati con l'errore (a destra nell'equazione) sono autostati di $Z_1 \otimes Z_2$ con autovalore -1.

Quindi, la misura di questi osservabili non distruggerà lo stato $|\psi\rangle$ né la sovrapposizione nel blocco ma il differente valore ottenuto, ovvero ± 1 , permetterà di capire se c'è stato un errore.

Allo stesso modo, la misura successiva e combinata dell'operatore $Z_1 \otimes Z_3$ permetterà di individuare la posizione l'errore che quindi potrà essere successivamente corretto.

7.4.2 Phase flip

Per individuare e correggere l'errore sulla fase *si confrontano i blocchi* invece che i qubit. Un *phase flip* sul primo blocco (è irrilevante quale dei primi tre qubit subisca l'errore) genera la trasformazione

$$\begin{aligned} |\bar{0}\rangle &= \frac{|000\rangle + |111\rangle}{\sqrt{2}} \rightarrow \frac{|000\rangle - |111\rangle}{\sqrt{2}} = |\bar{1}\rangle \\ |\bar{1}\rangle &= \frac{|000\rangle - |111\rangle}{\sqrt{2}} \rightarrow \frac{|000\rangle + |111\rangle}{\sqrt{2}} = |\bar{0}\rangle \end{aligned} \quad (7.4.5)$$

che è equivalente al *flip del blocco* $|\bar{0}\rangle \leftrightarrow |\bar{1}\rangle$.

L'operatore che ci interessa in questo caso è $X_1 \otimes X_2 \otimes X_3$. Ricordando che $X_i |0\rangle = |1\rangle$ e $X_i |1\rangle = |0\rangle$, possiamo verificare che

$$\begin{aligned} X_1 \otimes X_2 \otimes X_3 |\bar{0}\rangle &= X_1 \otimes X_2 \otimes X_3 \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}} \right) = \frac{|000\rangle + |111\rangle}{\sqrt{2}} = |\bar{0}\rangle \\ X_1 \otimes X_2 \otimes X_3 |\bar{1}\rangle &= X_1 \otimes X_2 \otimes X_3 \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}} \right) = -\frac{|000\rangle - |111\rangle}{\sqrt{2}} = -|\bar{1}\rangle. \end{aligned} \quad (7.4.6)$$

Quindi i blocchi $|\bar{0}\rangle$ e $|\bar{1}\rangle$ sono autostati di $X_1 \otimes X_2 \otimes X_3$ rispettivamente con autovalore +1 e -1. In altri termini, se misuriamo l'operatore $X_1 \otimes X_2 \otimes X_3$, possiamo ottenere l'informazione sulla fase relativa del blocco senza tuttavia distruggere la sovrapposizione di stati.

In maniera analoga, l'operatore $(X_1 \otimes X_2 \otimes X_3)(X_4 \otimes X_5 \otimes X_6)$ ci darà informazione *contemporanea* sulla fase del primo e del secondo blocco. In altri termini, ci permette di sapere se le fasi relative del primo e del secondo blocco sono uguali o diverse fra loro.

Si può verificare direttamente che gli stati senza errore $|0_L\rangle = |\bar{0}\rangle|\bar{0}\rangle|\bar{0}\rangle$ e $|1_L\rangle = |\bar{1}\rangle|\bar{1}\rangle|\bar{1}\rangle$ sono autostati dell'operatore $(X_1 \otimes X_2 \otimes X_3)(X_4 \otimes X_5 \otimes X_6)$ con autovalore +1. Allo stesso modo, gli stati in cui la fase è cambiata nel primo blocco $|\bar{1}\rangle|\bar{0}\rangle|\bar{0}\rangle$ e $|\bar{0}\rangle|\bar{1}\rangle|\bar{1}\rangle$ hanno fase diversa e sono autostati dell'operatore $(X_1 \otimes X_2 \otimes X_3)(X_4 \otimes X_5 \otimes X_6)$ con autovalore -1.

Quindi la misura dell'operatore $(X_1 \otimes X_2 \otimes X_3)(X_4 \otimes X_5 \otimes X_6)$ ci permette di stabilire se la fase del primo o secondo blocco è cambiata. Esattamente come nel caso di *bit flip*, la misura dell'operatore $(X_1 \otimes X_2 \otimes X_3)(X_7 \otimes X_8 \otimes X_9)$ ci permetterà di individuare la posizione dell'errore. Una volta individuato il blocco in cui la fase è cambiata basterà applicare un operatore Z_i (dove, per il primo blocco, i può essere uguale a 1, 2 o 3) per correggere l'errore.

7.4.3 Errori piccoli

Le osservazioni appena fatte, ci permettono di chiarire anche cosa succede nel caso di errori piccoli. Come visto in sez. 7.3.2, la misura dell'operatore $Z_1 \otimes Z_2$ permette con probabilità $|\gamma|^2 \gg |\delta|^2$ di correggere automaticamente l'errore avvenuto.

Abbiamo pur sempre una (piccola) probabilità $|\delta|^2$ di far collassare il sistema nello stato $\beta|011\rangle - \alpha|100\rangle$. In questo caso, la misura di $Z_1 \otimes Z_2$ e $Z_1 \otimes Z_3$ permetterà di stabilire che c'è stato un *bit flip* nel primo qubit e di correggerlo applicando un operatore X_1 per ottenere $-(\alpha|000\rangle - \beta|111\rangle)$.

Sebbene gli stati logici siano adesso corretti (ovvero $|000\rangle$ e $|111\rangle$ con i rispettivi coefficienti α e β), la fase relativa è diversa dallo stato logico ideale ed è necessario un ulteriore passaggio.

Con l'estensione del protocollo di correzione a 9 qubit questo è relativamente semplice. Infatti il nuovo stato corretto è $|\bar{1}\rangle$ (invece di $|\bar{0}\rangle$ come vorremmo). Quindi basterà usare il protocollo appena discusso per individuare e correggere il *phase flip* e riottenere lo stato logico corretto.

7.4.4 Protocollo di Shor

Vediamo ora un protocollo di correzione degli errori alternativo al precedente. Anche esso è stato proposto da Peter Shor e prende quindi il suo nome.

L'idea di base è simile: l'informazione di un singolo qubit viene codificata in 9 qubit divisi in blocchi da 3. La differenza sostanziale sta nel fatto che il codice restituisce il qubit iniziale corretto senza necessità di misura e correzione. Gli otto

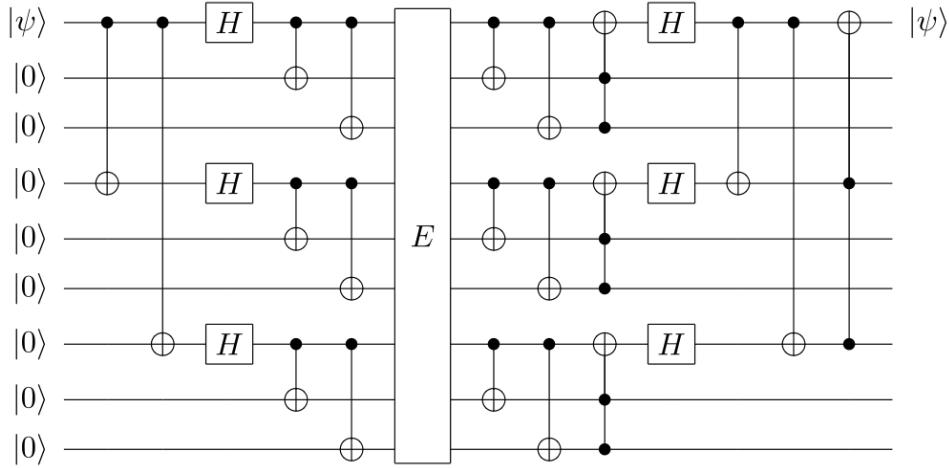


Figure 21: Il protocollo di Shor con 9 qubit. Il blocco centrale rappresenta l'errore. Le altre porte sono mostrate in Fig. 22

qubit aggiuntivi devono essere scartati o riinizializzati allo stato $|0\rangle$. Quindi il risparmio in termini di misure e correzioni viene pagato in termini di dimensione del hardware o di complessità nella procedura di riinizializzazione⁴

Il protocollo come sequenza di porte logiche è mostrato in Fig. 21. Le porte controllate utilizzate sono mostrate in Fig. 22 a) e sono la porta CNOT e quella di Toffoli. Visto che lavoriamo in uno spazio a molti qubit, per queste porte sarà necessario indicare il o i qubit di controllo e quelli *target*. Denoteremo quindi con $C_{i,j,k}$ una porta CNOT con il controllo sul qubit i e target j e con $T_{i,j,k}$ la porta di Toffoli con controllo sui qubit i e j e target sul qubit k [Fig. 22 a)]

Per capire il funzionamento del protocollo di Shor è conveniente dividerlo in piccole sequenze di porte logiche. Ad esempio, la sequenza in Fig. 22 b) permette di costruire il blocchi in Eq. (7.4.2). Se, ad esempio, partiamo dallo stato $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ e gli associamo due qubit $|00\rangle$, con la sequenze Fig. 22 b) otterremo

$$|\psi\rangle \rightarrow \frac{1}{\sqrt{2}} [\alpha(|000\rangle + |111\rangle) + \beta(|000\rangle - |111\rangle)] = \alpha|0\rangle + \beta|1\rangle = |\psi_1\rangle. \quad (7.4.7)$$

⁴ La procedura di riinizializzazione allo stato $|0\rangle$ non può essere fatto con un operatore unitario e quindi con una normale porta logica. È necessario usare l'ambiente esterno e far "decadere" i qubit eccitati, i.e., nello stato $|1\rangle$, nello stato $|0\rangle$.

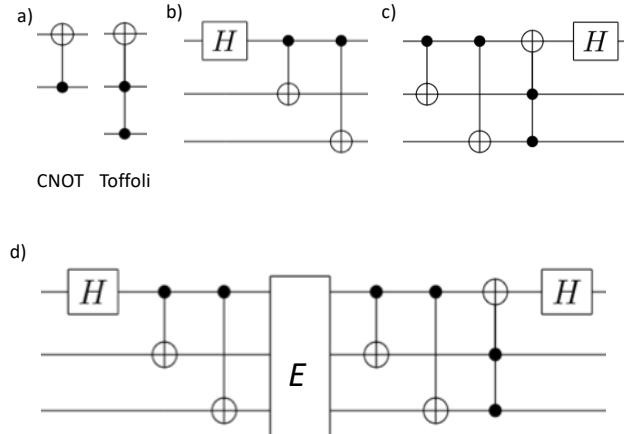


Figure 22: a) La rappresentazione grafica delle porte CNOT e di Toffoli. b) La sequenza di porte logiche per duplicare l'informazione logica su 3 qubit. c) La sequenza di porte logiche per correggere l'errore di *bit flip* su tre qubit.

7.4.5 Bit flip

Supponiamo adesso che ci sia un *bit flip* sul primo qubit. Come al solito questo viene descritto con l'applicazione di una porta X_1 (dove l'indice indica il qubit su cui è applicata). La sequenza di porte in Fig. 22 c) darà

$$\begin{aligned} |\psi_1\rangle &\xrightarrow{X_1} \frac{1}{\sqrt{2}} [\alpha(|100\rangle + |011\rangle) + \beta(|100\rangle - |011\rangle)] \\ &\xrightarrow{\frac{C_1 \text{NOT}_2}{C_1 \text{NOT}_3}} \frac{1}{\sqrt{2}} [\alpha(|1\rangle + |0\rangle)|11\rangle + \beta(|1\rangle - |0\rangle)|11\rangle] = |\psi_2\rangle. \end{aligned} \quad (7.4.8)$$

Gli ultimi due qubit sono entrambi "accesi" quindi la porta di Toffoli T_{231} agirà come una porta NOT sul primo qubit. Con la successiva porta di Hadamard H_1 otteniamo

$$\begin{aligned} |\psi_2\rangle &\xrightarrow{T_{231}} \frac{1}{\sqrt{2}} [\alpha(|0\rangle + |1\rangle) + \beta(|0\rangle - |1\rangle)]|11\rangle \\ &\xrightarrow{H_1} (\alpha|0\rangle + \beta|1\rangle)|11\rangle = |\psi\rangle|11\rangle. \end{aligned} \quad (7.4.9)$$

Come possiamo vedere, il risultato finale è che il primo qubit è tornato quello originale ma i due qubit ancilla hanno cambiato il loro valore.

Per completezza riportiamo anche il calcolo nel caso di un errore sul secondo qubit

$$\begin{aligned}
 |\psi_1\rangle &\xrightarrow{X_2} \frac{1}{\sqrt{2}} [\alpha(|010\rangle + |101\rangle) + \beta(|010\rangle - |101\rangle)] \\
 &\xrightarrow{\frac{C_1 \text{NOT}_2}{C_1 \text{NOT}_3}} \frac{1}{\sqrt{2}} [\alpha(|0\rangle + |1\rangle)|10\rangle + \beta(|0\rangle - |1\rangle)|10\rangle] \\
 &\xrightarrow{T_{231}} \frac{1}{\sqrt{2}} [\alpha(|0\rangle + |1\rangle) + \beta(|0\rangle - |1\rangle)]|10\rangle \\
 &\xrightarrow{H_1} (\alpha|0\rangle + \beta|1\rangle)|10\rangle = |\psi\rangle|10\rangle. \tag{7.4.10}
 \end{aligned}$$

Si noti che in questo caso la porta di Toffoli agisce come l'identità. Nuovamente, il risultato finale è che il primo qubit è quello originale mentre i secondi due vengono cambiati in $|10\rangle$. Analogamente, si può dimostrare che nel caso di errore sul terzo qubit del blocco lo stato finale sarà $|\psi\rangle|01\rangle$ mentre in assenza di errori si avrà (banalmente) $|\psi\rangle|00\rangle$.

Possiamo fare un'osservazione. La prima è che mentre il primo qubit ritorna quello originale, gli altri due sono usati per ampliare lo spazio e per immagazzinare l'informazione indesiderata. Dovranno quindi essere eliminati e non potranno essere riutilizzati. Un'ulteriore applicazione del codice di correzione dovrebbe quindi prevedere nuovi qubit con un considerevole aumento del hardware quantistico. Un'alternativa è riinizializzare gli stessi qubit nello stato $|00\rangle$ lasciando che decadano per effetto del rumore esterno.

7.4.6 Phase flip

Come nel protocollo in sec. 7.4, l'errore di *phase flip* viene corretto con il confronto fra i blocchi (non fra i qubit). Ricordiamo che, se il *phase flip* avviene su uno dei tre qubit che compongono il blocco, questo induce la trasformazione in Eq. (7.4.5): $|\bar{0}\rangle \leftrightarrow |\bar{1}\rangle$. Notiamo inoltre che la trasformazione in Fig. 22 b) e in Eq. (7.4.7) darà

$$\begin{aligned}
 |000\rangle &\xrightarrow{\text{Fig 22 b)}} \frac{|000\rangle + |111\rangle}{\sqrt{2}} = |\bar{0}\rangle \\
 |100\rangle &\xrightarrow{\text{Fig 22 b)}} \frac{|000\rangle - |111\rangle}{\sqrt{2}} = |\bar{1}\rangle \tag{7.4.11}
 \end{aligned}$$

Per la trasformazione inversa Fig. 22 c) dobbiamo tenere in conto la presenza della porta di Toffoli T_{231} . Sul blocco $|\bar{0}\rangle$ otteniamo

$$|\bar{0}\rangle \xrightarrow{\frac{C_1 \text{NOT}_2}{C_1 \text{NOT}_3}} \frac{|000\rangle + |100\rangle}{\sqrt{2}} \xrightarrow{T_{231}} \frac{|000\rangle + |100\rangle}{\sqrt{2}} \xrightarrow{H_1} |000\rangle. \tag{7.4.12}$$

Quindi la porta di Toffoli agisce come l'identità. In modo analogo si ottiene

$$|\bar{1}\rangle \xrightarrow{\frac{C_1 \text{NOT}_2}{C_1 \text{NOT}_3}} \frac{|000\rangle - |100\rangle}{\sqrt{2}} \xrightarrow{T_{231}} \frac{|000\rangle - |100\rangle}{\sqrt{2}} \xrightarrow{H_1} |100\rangle. \tag{7.4.13}$$

Quindi abbiamo verificato che la sequenza in Fig. 22 c) è l'opposta di quella in in Fig. 22 b) per i suddetti stati.

Siamo in grado ora di verificare che la trasformazione in Fig. 22 d) corregge anche gli errori di *phase flip*. Scriviamo lo stato a 9 qubit come $|\psi\rangle = \alpha|\bar{0}\bar{0}\bar{0}\rangle + \beta|\bar{1}\bar{1}\bar{1}\rangle$ e supponiamo che avvenga un *phase flip* sul primo blocco

$$|\psi\rangle \xrightarrow{\text{phase flip}} \alpha|\bar{1}\bar{0}\bar{0}\rangle + \beta|\bar{0}\bar{1}\bar{1}\rangle = |\psi_1\rangle. \quad (7.4.14)$$

Come visto sopra, le porte di Toffoli T_{231} , T_{564} e T_{897} in Fig. 21 agiscono come l'identità. Usando la trasformazione in inversa in Fig. 22 c), abbiamo

$$|\psi_1\rangle \rightarrow \alpha|100\rangle|000\rangle|000\rangle + \beta|000\rangle|100\rangle|100\rangle = |\psi_2\rangle. \quad (7.4.15)$$

Le successive porte $C_1\text{NOT}_4$, $C_1\text{NOT}_7$ e T_{471} agiranno come

$$\begin{aligned} |\psi_2\rangle &\xrightarrow[C_1\text{NOT}_4]{C_1\text{NOT}_7} \alpha|100\rangle|100\rangle|100\rangle + \beta|000\rangle|100\rangle|100\rangle \\ &\xrightarrow{T_{471}} \alpha|000\rangle|100\rangle|100\rangle + \beta|100\rangle|100\rangle|100\rangle \\ &= (\alpha|0\rangle + \beta|1\rangle)|00\rangle|100\rangle|100\rangle = |\psi\rangle|00\rangle|100\rangle|100\rangle. \end{aligned} \quad (7.4.16)$$

Abbiamo verificato che il circuito ripristina lo stato iniziale $|\psi\rangle$ a discapito degli altri qubit.

8

INTRODUZIONE AI QUANTUM GAMES

I – INTRODUZIONE

John von Neumann è stato un matematico, fisico, *computer scientist* e uno dei più importanti scienziati (nell'ambito di tali rami) del ventesimo secolo e ha dato contributi fondamentali a diversi rami della matematica, della fisica matematica e della meccanica quantistica¹.

Durante il suo coinvolgimento nel Progetto Manhattan per la produzione delle armi nucleari, il suo interesse arrivò anche all'informatica. Oltre mettere le basi dell'architettura dei primi computer (architettura dei computer infatti viene detta "di Von Neumann"), si dedicò anche alla parte di software. Da questo suo interesse nacque la moderna teoria dei giochi. La data di nascita di questo settore di ricerca a cavallo fra la matematica, l'informatica e l'economica è il 1944 quando von Neumann insieme a Oskar Morgenstern pubblicò il libro *Theory of Games and Economic Behavior*.

La teoria dei giochi è considerata una branca della matematica applicata che studia le decisioni di un soggetto che interagisce con altri soggetti e ha come meta il massimo guadagno (dove guadagno è da intendere in senso lato). La teoria dei giochi ha in realtà moltissime sfaccettature e applicazioni. Come suggerisce il titolo del libro di von Neumann, la più evidente è in ambito economico dove viene usata per cercare di modellizzare il comportamento di singoli individui per descrivere diversi fenomeni economici. L'estensione più naturale è quella alle scienze sociali dove si usa per modellizzare i comportamenti sociali su piccola e grandi scale (dalla scelta di comprare casa in un determinato quartiere alle elezioni nazionali).

Dato che la meccanica quantistica introduce ha diversa struttura matematica che permette una manipolazione profondamente diversa dell'informazione, nella prima decade del ventunesimo secolo i ricercatori hanno iniziato a chiedersi se e come la teoria dei giochi tradizionale poteva essere modificata quando sono inclusi i fenomeni quantistici. Questo nuovo ramo di ricerca dell'informatica quantistica comprende quelli che oggi si chiamano *quantum games*. In questo capitolo ne discutiamo due che possono considerarsi prototipi.

¹ https://en.wikipedia.org/wiki/John_von_Neumann

II – *spin-flip* IN STAR TREK

Discutiamo un modello di *quantum game* proposto dal fisico David Meyer nel 1999 [meyer1999, piotrowski2003]. Il capitano Picard e Q che sono due personaggi della series televisiva Star Trek. Supponiamo che si sfidino ad un gioco denominato *spin-flip*. Lo spin è una caratteristica delle particelle quantistiche. Per quanto ci interessa sarà sufficiente considerare il caso in cui ci sono due stati di spin: $|\uparrow\rangle$ e $|\downarrow\rangle$. Per uniformare la notazione con quella usata, li denoteremo come $|\uparrow\rangle = |1\rangle$ e $|\downarrow\rangle = |0\rangle$.

Nella versione classica Picard e Q possono agire sullo spin facendolo saltare oppure lo possono lasciare invariato. Queste due operazioni corrispondono applicazione dell'operatore identità $\mathbb{1}$ oppure della una porta X (o NOT):

$$\begin{aligned} |i\rangle &\xrightarrow{\mathbb{1}} |i\rangle \\ |1\rangle &\xrightarrow{X} |0\rangle \end{aligned} \tag{8.2.1}$$

con $i = 0, 1$.

Il gioco a cui si sfidano Picard e Q è il seguente.

1. Il capitano Picard inizializza lo spin nello stato $|1\rangle$.
2. Q manipola il qubit (applica X o $\mathbb{1}$).
3. Picard applica manipola il qubit (applica X o $\mathbb{1}$).
4. Q manipola il qubit (applica X o $\mathbb{1}$).

Le operazioni fatte da Picard e Q sono ignote all'avversario. Q vince (e Picard perde) se lo stato finale è $|1\rangle$ mentre Picard vince (e Q perde) se lo stato finale è $|0\rangle$.

Facciamo un esempio. Se la sequenza di operazioni è X (da Q), $\mathbb{1}$ (da Picard) e $\mathbb{1}$ (da Q). In totale al qubit verrà applicata la porta X quindi $|1\rangle \rightarrow |0\rangle$, lo stato finale sarà $|0\rangle$ e Picard vince.

Si può intuire che, dato che lo stato iniziale è sempre $|1\rangle$ e che $X^2 = \mathbb{1}$, tutte le volte che viene applicato un numero dispari di operatori X vincerà Q mentre se il numero è pari vincerà Picard. In ogni caso, dato che la scelta dell'avversario è ignota, *non esiste una strategia vincente* né per Q né per Picard.

A questo punto facciamo una modifica ai punti 2 – 4 del precedente gioco. Supponiamo che Q possa applicare delle generica porta logica quantistica (ai punti 2 e 4) mentre Picard decida con probabilità p di applicare la porta X e con probabilità $1 - p$ di applicare l'identità .

La struttura del nuovo gioco (quantistico) è

1. Il capitano Picard inizializza lo spin nello stato $|1\rangle$.
2. Q applica al qubit con una porta U_1 .
3. Picard con probabilità p applica X e con probabilità $1 - p$ applica l'identità .
4. Q applica al qubit con una porta U_2 .

Considerando un generico operatore quantistico U_1 possiamo scrivere l'evoluzione dello stato iniziale come

$$|\psi_0\rangle = |1\rangle \xrightarrow{U_1} a|1\rangle + b|0\rangle \quad (8.2.2)$$

Per semplificare la discussione supporremo che a e b siano reali. Per coefficienti complessi è possibile fare una discussione analoga. Questa trasformazione unitaria può essere associata alla matrice (scritta nella base $\{|0\rangle, |1\rangle\}$)²

$$U_1 = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}. \quad (8.2.3)$$

Per descrivere l'azione di Picard (che è classica) dobbiamo dividere l'evoluzione in due parti. Dato che Picard applica la porta X (NOT) con probabilità p e l'indietà con probabilità $1-p$, lo stato evolverà secondo le regole

$$\begin{cases} a|0\rangle + b|1\rangle & \text{con probabilità } p \text{ applica } X \\ a|1\rangle + b|0\rangle & \text{con probabilità } 1-p \text{ applica } \mathbb{1}. \end{cases} \quad (8.2.4)$$

Per il suo secondo turno, Q supponiamo che applichi una trasformazione una porta di Hadamard; cioè $U_2 = H$. Nei due casi discussi prima, lo stato evolverà in

$$\begin{cases} \frac{1}{\sqrt{2}}[(a-b)|1\rangle + (a+b)|0\rangle] & \text{con probabilità } p \\ \frac{1}{\sqrt{2}}[(a+b)|0\rangle + (-a+b)|1\rangle] & \text{con probabilità } 1-p. \end{cases} \quad (8.2.5)$$

Da quest'ultima espressione, si vede immediatamente che se Q decide di applicare anche la prima volta una porta di Hadamard ($U_1 = H$), si avrà $|1\rangle \rightarrow 1/\sqrt{2}(|0\rangle - |1\rangle)$ a di conseguenza, usando le notazioni di sopra, $a = b = -1/\sqrt{2}$ ³. Ne consegue che lo stato finale sarà in entrambi i casi $|1\rangle$ e Q vincerà sempre.

Concludiamo che, scegliendo $U_1 = H$ tale che $a = b = -1/\sqrt{2}$ e $U_2 = H$, Q vince sempre indipendentemente dalla scelta che fa Picard. Questo è un incredibile miglioramento (per Q) rispetto al caso classico ed è dovuto al fatto che Q possa sfruttare a pieno la meccanica quantistica mentre Picard no.

Un'analisi matematica più attenta della struttura del gioco svela il "trucco" di Q. Come passo iniziale Q applica una porta di Hadamard che trasforma lo stato iniziale $|1\rangle$ nello stato $|-\rangle$. Gli operatori che Picard può applicare classicamente sono X e $\mathbb{1}$. Lo stato $|-\rangle$ è autostato sia di X che di $\mathbb{1}$; di conseguenza l'operazione di Picard non cambia lo stato ma genera solamente una (irrilevante) fase globale:

$$|-\rangle \xrightarrow{\text{X oppure } \mathbb{1}} \pm|-\rangle. \quad (8.2.6)$$

La seconda operazione di Q (un'altra porta H) cancella l'effetto della prima dato che $H^2 = \mathbb{1}$ e quindi riporta lo stato in quello originale: $|-\rangle \rightarrow |1\rangle$.

² Questa è la generica matrice unitaria che conserva il prodotto scalare con a e b reali.

³ Si noti che l'unica richiesta è che i coefficienti a e b abbiano segno opposto. Il loro segno assoluto è irrilevante.

	Bob: C	Bob: D
Alice: C	(3,3)	(0,5)
Alice: D	(5,0)	(1,1)

Table 7: Ricompensa combinata di Alice e Bob nel dilemma del prigioniero.**III – DILEMMA DEL PRIGIONIERO****8.3.1 Caso classico**

Uno degli esempi prototipo della teoria dei giochi è il dilemma del prigioniero originalmente proposto da proposto da Albert Tucker negli anni cinquanta del ventesimo secolo.

Ritorniamo ai consueti Alice (A) e Bob (B) che in questo caso sono complici, sono stati arrestati e vengono interrogati separatamente. Entrambi hanno due scelte o strategie: collaborare fra di loro (*cooperate* in inglese e indicata con la lettera C) oppure non cooperare e accusare l'altro (*defect* in inglese e indicata con la lettera D).

La ricompensa (*payoff*) è espressa con un numero. Lo scopo del gioco è massimizzare questo la ricompensa ⁴. Le possibilità che A e B hanno a disposizione sono

1. se solo uno dei due accusa l'altro (ad esempio, Alice sceglie D e Bob sceglie C), quello che accusa ha la massima ricompensa 5 mentre l'altro (che collabora) ha la minima ricompensa 0. Queste vengono rappresentate come strategie $(A, B) = (D, C)$ e $(A, B) = (C, D)$.
2. se entrambi accusano l'altro [strategia $(A, B) = (D, D)$], hanno entrambi una ricompensa ridotta di 1.
3. se entrambi collaborano [strategia $(A, B) = (C, C)$], hanno entrambi una ricompensa ridotta di 3.

Le possibilità sono riassunte in tabella 7 [eisert1999].

A livello razionale c'è una strategia dominante che è l'accusa (strategia D). Alice non sa cosa deciderà Bob ma sa che se Bob coopera e lei lo accusa [strategia $(A, B) = (D, C)$] otterrà una ricompensa di 5 contro i 3 che otterebbe se cooperasse [strategia $(A, B) = (C, C)$]. Allo stesso tempo, se Bob la accusasse e anche lei lo accusasse [strategia $(A, B) = (D, D)$], la ricompensa sarebbe 1 contro 0 se cooperasse [strategia $(A, B) = (C, D)$]. Quindi, indipendentemente dalla scelta di Bob, Alice sa che riuscirà a massimizzare la ricompensa se accusa Bob ⁵.

Possiamo rendere più formale questo discorso introducendo il formalismo della meccanica quantistica che ci servirà anche dopo. In questo caso, usiamo due qubit uno di Alice e uno di Bob in cui loro "scriverranno" la loro scelta. Lo stato totale

⁴ Nel caso specifico, la ricompensa potrebbe rappresentare lo sconto di pena in anni.

⁵ Il dilemma del prigioniero è completamente simmetrico quindi il discorso fatto per Alice vale anche per Bob. Ne consegue che anche per Bob la strategia migliore sarebbe la D e la scelta combinata (D, D) è quella migliore. nella teoria dei giochi si dice che la strategia (D, D) è un punto di equilibrio di Nash [eisert1999]

sarà $|i\rangle_A \otimes |j\rangle_B \equiv |ij\rangle$ dove gli indici A e B indicano il qubit di Alice e di Bob. Gli stati che descrivono tutto lo spazio delle strategie e ne costituiscono una base sono $\{|DD\rangle, |DC\rangle, |CD\rangle, |CC\rangle\}$.

Come stato iniziale fissiamo (in maniera arbitraria) $|CC\rangle$. Indicheremo le operazioni di Alice e Bob con gli operatori U_A e U_B e l'operatore totale con $U_A \otimes U_B$. Si noti che il prodotto tensore evidenzia che le operazioni di Alice e Bob sono separate e indipendenti. Lo stato finale dopo le scelte di Alice e Bob sarà

$$|CC\rangle \rightarrow U_A \otimes U_B |CC\rangle$$

La ricompensa sarà associata ad un operatore. Per Alice tale operatore/ricompensa sarà

$$P_A = |DD\rangle\langle DD| + 5|DC\rangle\langle DC| + 3|CC\rangle\langle CC| = \begin{bmatrix} 1 & & & \\ & 5 & & \\ & & 0 & \\ & & & 3 \end{bmatrix}. \quad (8.3.1)$$

dove nell'ultimo membro abbiamo indicato la rappresentazione matriciale nella base di sopra tralasciando gli elementi nulli.

Per Bob tale operatore/ricompensa sarà

$$P_B = |DD\rangle\langle DD| + 5|CD\rangle\langle CD| + 3|CC\rangle\langle CC| = \begin{bmatrix} 1 & & & \\ & 0 & & \\ & & 5 & \\ & & & 3 \end{bmatrix}. \quad (8.3.2)$$

Si noti che gli operatori P_A e P_B sono definiti nello spazio totale delle strategie ma hanno forma diversa.

Nel caso più semplice e vicino a quello classico, A e B possono i) non fare niente e quindi cooperare (visto che il qubit iniziale è C) oppure ii) applicare (indipendentemente l'uno dall'altra) la trasformazione $|C\rangle \rightarrow |D\rangle$ e accusare il compagno. Queste due scelte corrispondono ad applicare l'operatore identità $\mathbb{1}$ (strategia C) oppure l'operatore $D = iY$ (strategia D) che nella base $\{|D\rangle, |C\rangle\}$ assume la forma

$$D = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

L'effetto di D è $D|D\rangle \rightarrow -|C\rangle$ e $D|C\rangle \rightarrow |D\rangle$.

Facciamo qualche esempio.

La strategia di $(A, B) = (D, D)$, sarà rappresentata dall'operatore (totale) $D \otimes D$ che genererà lo stato finale $D \otimes D|CC\rangle = |DD\rangle$. In questo caso, la ricompensa di Alice sarà $\langle DD|P_A|DD\rangle = 3$ e quella di Bob $\langle DD|P_B|DD\rangle = 3$. Se $(A, B) = (C, D)$, l'operatore (totale) sarà $\mathbb{1} \otimes D$ che genererà lo stato finale $\mathbb{1} \otimes D|CC\rangle = |CD\rangle$. In questo caso, le ricompense saranno $\langle CD|P_A|CD\rangle = 0$ e quella di Bob $\langle CD|P_B|CD\rangle = 5$. Esattamente come ci aspettavamo.

8.3.2 Caso quantistico

Passando al regime quantistico si hanno più possibilità . Prima di tutto, Alice e Bob possono applicare ai propri qubit un numero maggiore di trasformazioni. Infatti, il più generico operatore unitario agente su un qubit si scrive come

$$U(\theta, \phi) = \begin{bmatrix} e^{i\phi} \cos \frac{\theta}{2} & \sin \frac{\theta}{2} \\ -\sin \frac{\theta}{2} & e^{-i\phi} \cos \frac{\theta}{2} \end{bmatrix}. \quad (8.3.3)$$

Questo comprende come casi particolari gli operatori usati nel caso classico dato che $C = U(0,0)$ e $D = U(\pi,0)$.

É comunque importante notare che esistono strategie puramente quantistiche. Se prendiamo $\theta = 0$ e $\phi = \pi/2$ abbiamo un operatore che chiamiamo Q

$$Q = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}.$$

Pur non cambiano la strategia (infatti $|C\rangle \rightarrow -i|C\rangle$ e $|D\rangle \rightarrow i|D\rangle$), cambia la fase del qubit. Questo non avrebbe effetto con stati classici ma su stati quantistici in sovrapposizione questa diventa ha un effetto osservabile e quindi una nuova strategia puramente quantistica. Ad esempio, Q trasforma $(|C\rangle + |D\rangle)/\sqrt{2} \rightarrow -i(|C\rangle - |D\rangle)/\sqrt{2}$ che sono stati ortogonali e quindi possono essere distinti con una misura.

La meccanica quantistica offre però anche la possibilità di partire da stati diversi e, in particolare, di partire da stati *entangled*. Si può comprendere immediatamente che questo fatto può avere un impatto sul gioco. Infatti, nel caso classico, le azioni di A e B sono completamente indipendenti e scorrelate. Se A e B condividono uno stato entangled, non solo i loro qubit correlati ma la correlazione è quantitica. Sebbene le operazioni di A e B siano ancora indipendenti, la correlazione quantistica può modificare il risultato del gioco. Come vedremo, questo ha importanti conseguenze.

Per introdurre l'entanglement fra A e B, supponiamo che i qubit forniti ad entrambi siano stati modificati tramite l'operatore $J = \exp[i(\gamma/2)D \otimes D]$. In termini di matrici questo può essere scritto nella base $\{|DD\rangle, |DC\rangle, |CD\rangle, |CC\rangle\}$ come

$$J = \begin{bmatrix} \cos \frac{\gamma}{2} & 0 & 0 & i \sin \frac{\gamma}{2} \\ 0 & \cos \frac{\gamma}{2} & -i \sin \frac{\gamma}{2} & 0 \\ 0 & -i \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} & 0 \\ i \sin \frac{\gamma}{2} & 0 & 0 & \cos \frac{\gamma}{2} \end{bmatrix}. \quad (8.3.4)$$

Si noti che nel caso $\gamma = 0$, $J = \mathbb{1}$ è semplicemente la matrice identità nello spazio delle strategie.

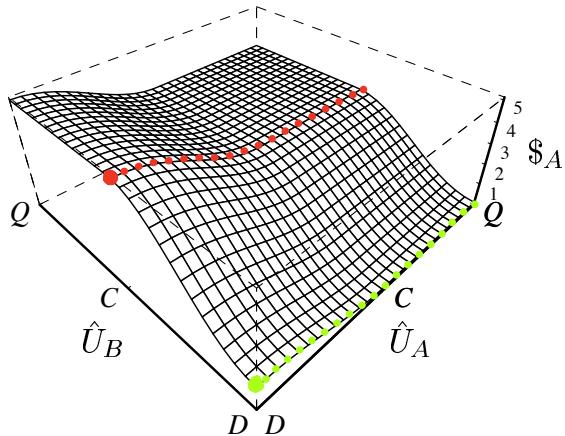


Figure 23: Dilemma del prigioniero. Caso quantistico senza entanglement. Quello mostrato con $\$_A$ è la ricompensa di Alice. Le curve tratteggiate sulla superficie mostrano che, fissata l'operazione di B (quindi una determinata \hat{U}_B), la massima ricompensa di A è massima nel caso lei accusi B, i.e., strategia D e $U_A = D$. Le operazioni Q (si veda il testo) sono puramente quantistiche (non hanno corrispettivo classico) ma in questo caso non danno alcun vantaggio rispetto alle scelte di Alice e Bob. La figura è presa da [eisert1999].

Se invece prendiamo $\gamma = \pi/2$

$$J\left(\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & i \\ 0 & 1 & -i & 0 \\ 0 & -i & 1 & 0 \\ i & 0 & 0 & 1 \end{bmatrix} \quad (8.3.5)$$

che, applicata allo stato $|CC\rangle$, darà

$$J\left(\frac{\pi}{2}\right)|CC\rangle = \frac{1}{\sqrt{2}}(i|DD\rangle + |CC\rangle). \quad (8.3.6)$$

Questo è uno stato massimamente entangled⁶. Concludiamo che l'operatore J è un operatore che permette di generare entanglement fra i qubit che poi saranno consegnati ad Alice e Bob.

Consideriamo prima il caso in cui $\gamma = 0$, $J = 1$ e gli stati di A e B non siano entangled. L'analisi dettagliata della ricompensa di Alice (e di Bob) per il caso quantistico è più complessa perché abbiamo a che fare con strategie continue e non discrete [come lo sono gli operatori unitari (8.3.3) che A e B possono usare]. Un modo di rappresentare la ricompensa di Alice è mostrata in Fig. 23 in uno

⁶ Lo stato ottenuto non è uno stato di Bell ma può essere ottenuto dello stato di Bell $1/\sqrt{2}(|DD\rangle + |CC\rangle)$ applicando l'operatore di phase $U_{ph}(\delta)$ [introdotto nella sezione 3.9] che trasforma $|0\rangle \rightarrow |0\rangle$ e $|1\rangle \rightarrow e^{i\delta}|1\rangle$ con $\delta = \pi/2$. Tale operatore può essere applicato al primo o al secondo qubit. Dato che tale operatore agisce "localmente" su un solo qubit, non può modificare l'entanglement. Ne consegue che lo stato generato è già massimamente entangled come quelli di Bell.

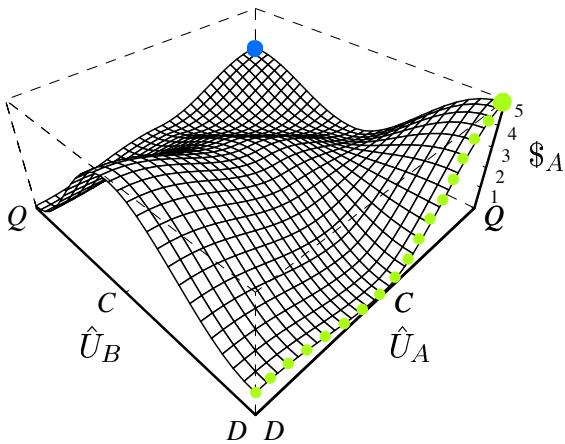


Figure 24: Dilemma del prigioniero. Caso quantistico con entanglement. Quello mostrato con $\$_A$ è la ricompensa di Alice. La curva verde mostra le possibili strategie di Alice quando Bob sceglie D . Al contrario dei casi classico e senza entanglement dove la strategia migliore per Alice era D , in questo caso risulta essere quella puramente quantistica Q con una ricompensa di 5. Il punto blu mostra la strategia globale $(A, B) = (Q, Q)$. Questa è simmetrica e risulta essere quella che massimizza sia la ricompensa di Alice sia quella di Bob (per un valore di 3). Essendo una strategia puramente quantistica non è accessibile nel gioco classico e il vantaggio nella ricompensa è ottenibile solo con stati entangled. La figura è presa da [eisert1999].

spazio tridimensionale. La ricompensa di Alice è mostrata sull'asse z mentre sugli assi x e y sono rappresentate, rispettivamente, le scelte di Alice (\hat{U}_A) e Bob (\hat{U}_B)⁷.

Le scelte "classiche" in Tab. 7 sono rappresentate con i punti C e D sugli assi. La strategia puramente quantistica Q in Eq. (8.3.4) è indicata esplicitamente.

Supponiamo che Bob scelga la strategia (classica) D . Alice ha anche in questo caso uno spettro continuo di possibilità (curva verde in Fig. 23). Come si può vedere, la ricompensa di Alice è massima quando $\hat{U}_A = D$; ovvero anche Alice sceglie di accusare Bob. Questa è esattamente quello che si aveva nel caso classico.

Se Bob sceglie la strategia (classica) C (curva rossa in Fig. 23), per massimizzare la propria ricompensa Alice dovrà scegliere $\hat{U}_A = D$. Anche in questo caso, il risultato è uguale a quello classico.

Come si vede in Fig. 23, questo è vero per ogni strategia di Bob e nemmeno la strategia quantistica Q porta differenze. Concludiamo che *indipendentemente* da quello che sceglie Bob, la strategia migliore per Alice è la D . Dato che il problema è simmetrico, lo stesso vale per Bob. Quindi, riotteniamo il risultato classico per il quale, la strategia individuale migliore è la D e quella globale migliore è la (D, D) .

Consideriamo adesso il caso massimamente entangled con $\gamma = \pi/2$. Con le stesse indicazioni di sopra, in Fig. 24 è mostrato la ricompensa di Alice.

⁷ Una discussione più approfondita necessiterebbe l'introduzione di una parametrizzazione di \hat{U}_A e \hat{U}_B . Questa complicherebbe la discussione e quindi non viene discussa. Per i dettagli ci si può comunque riferire al lavoro originale [eisert1999].

In questo caso, la strategia D non è più la migliore per Alice. Se Bob sceglie la strategia D, Alice ha la ricompensa minima (uguale a 0) con la strategia C e 1 se sceglie D, esattamente come nel caso classico. Ma la strategia migliore di Alice risulta quella puramente quantistica Q per la quale la ricompensa è 5 (massima).

Nel caso Bob scelga C, la strategia migliore per Alice è D (come nel caso classico). Ma la strategia D per Alice non solo non è quella che massimizza la ricompensa ma è anche rischiosa in quanto la ricompensa va a zero se Bob scegli la strategia Q. Ne deduciamo che la strategia di Alice per massimizzare la ricompensa *non è indipendente* dalla scelta di Bob come invece accadeva nel caso classico.

Ritornando ad una visione globale del gioco (ricordando che il gioco è simmetrico), si può osservare l'emergere di una nuova strategia di equilibrio. La strategia $(A, B) = (Q, Q)$ permette sia ad A che B di avere una ricompensa di 3⁸. Si noti che in questo caso è la ricompensa è il triplo di quella ottenibile nel caso classico [in cui per la strategia (D, D) la ricompensa era di 1]. Questa combinazione di strategia così come la ricompensa è puramente quantistica e non compare nel caso classico.

⁸ Questo è un punto di equilibrio di Nash come discusso in Ref. [eisert1999].

IV – COME VINCERE CON LA MECCANICA QUANTISTICA

Discutiamo un altro *quantum game* che rivela una delle proprietà fondamentali della meccanica quantistica e ha importantissime implicazioni nel settore noto come *fondamenti di meccanica quantistica*.

Supponiamo che Alice (A), Bob (B) e Charlie (C) siano stati separati, imprigionati e non abbiano la possibilità di comunicare gli uni con gli altri. Per poter essere liberati, devono vincere ad un strano gioco.

Ognuno ha a disposizione due variabili X e Y a cui possono attribuire valore 1 o -1. Separatamente gli viene chiesto quale valore vogliono attribuire ad X oppure quale valore vogliono attribuire a Y. Vengono però informati che le domande fatte hanno una struttura ben precisa. O a tutti viene chiesto "che valore attribuisci a X" oppure a uno viene chiesto "che valore attribuisci a X" e agli altri "che valore attribuisci a Y". In sostanza può essere chiesto il valore di una fra le seguenti terne $\{X_A, X_B, X_C\}$, $\{X_A, Y_B, Y_C\}$, $\{Y_A, X_B, Y_C\}$ o $\{Y_A, Y_B, X_C\}$.

Il gioco consiste nel scegliere i valori attribuiti in maniera tale che i prodotti dei numeri scelti abbiano un preciso valore. Infatti, verranno liberati solo se prendendo i prodotti dei valori assegnati saranno

$$\begin{aligned} X_A X_B X_C &= -1 \\ X_A Y_B Y_C &= 1 \\ Y_A X_B Y_C &= 1 \\ Y_A Y_B X_C &= 1. \end{aligned} \tag{8.4.1}$$

Naturalmente A, B e C non sono a conoscenza né della domanda né delle risposte degli altri. La domande che ci poniamo è :

Esiste una strategia per cui A, B e C sono sicuri di vincere?

La risposta è "no": non esiste nessuna strategia che permetta di vincere con sicurezza. Infatti, non sapendo quale domanda è stata posta, la certezza di vincere si avrebbe solo verificando contemporaneamente tutte le equazioni (8.4.1). Questo è però impossibile.

Oltre alla verifica mediante calcolo diretto, una dimostrazione più semplice e veloce consistente nel moltiplicare tutti i membri di *sinistra* nelle equazioni (8.4.1)

$$(X_A X_B X_C)(X_A Y_B Y_C)(Y_A X_B Y_C)(Y_A Y_B X_C) = X_A^2 X_B^2 X_C^2 Y_A^2 Y_B^2 Y_C^2 = 1. \tag{8.4.2}$$

L'ultimo passaggio abbiamo sfruttato il fatto che le variabili X_i e Y_i possono assumere solo i valori ± 1 . Quindi i loro quadrati saranno tutti 1 ($X_i^2 = 1$ e $Y_i^2 = 1$) e il prodotto in Eq. (8.4.2) sarà uguale a 1, i.e., $(\prod_i X_i^2)(\prod_i Y_i^2) = 1$.

D'altro canto, questo deve essere uguale al prodotto dei membri di *destra* dell'Eq. (8.4.1). Dato che questo è -1, concludiamo che il sistema (8.4.1) non ha soluzione e le quattro equazioni non possono essere soddisfatte contemporaneamente.

Ora mostriamo che se A, B e C possono condividere uno stato quantistico entangled esiste una strategia che permette di vincere con sicurezza. Supponiamo che A, B e C condividano lo stato

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B |0\rangle_C - |1\rangle_A |1\rangle_B |1\rangle_C) \equiv \frac{1}{\sqrt{1}}(|000\rangle - |111\rangle) \quad (8.4.3)$$

(dove nella seconda equazione gli indici A, B e C sono sottintesi per semplificare la notazione). Questo stato ricorda da vicino gli stati entangled di Bell e prende il nome dalle iniziali dei fisici (D. Greenberger, M. Horne e A. Zeilinger) che lo usarono per studiare le caratteristiche della meccanica quantistica.

Tornando al gioco, il protocollo che A, B, e C applicano usando lo stato quantistico è il seguente:⁹

1. se la domanda posta è "che valore attribuisci a X", si misura l'operatore σ_x
2. se la domanda posta è "che valore attribuisci a Y", si misura l'operatore σ_y .

Ad esempio, se ad A viene chiesto "che valore attribuisci a X" e a C "che valore attribuisci a Y", loro misureranno rispettivamente gli osservabili $\sigma_{x,A}$ e $\sigma_{y,C}$ (dove con gli indici abbiamo esplicitamente la relazione con la misura di A e C).

Si noti che la domanda e l'azione di A, B e C sono indipendenti; loro non sanno cosa è stato chiesto agli altri ma devono solo preoccuparsi di misurare il qubit a loro disposizione nella base opportuna.

Supponiamo che a tutti e tre sia chiesto il valore di X, i.e., $\{X_A, X_B, X_C\}$. In questo caso, A, B e C misureranno $\sigma_{x,A}$, $\sigma_{x,B}$ e $\sigma_{x,C}$. Per stabilire il risultato di queste misure e quindi la risposta data, è necessario scrivere lo stato (8.4.3) nella base di degli autostati degli operatori misurati, i.e., $\sigma_{x,i}$ che, come al solito, indichiamo con $|\pm\rangle$ e che si scrivono come $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ e $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$. Lo stato (8.4.3) si scriverà

$$\begin{aligned} |GHZ\rangle &= \frac{1}{4}[(|+\rangle + |-\rangle)^{\otimes 3} - (|+\rangle - |-\rangle)^{\otimes 3}] = \\ &= \frac{1}{4}[|+++ \rangle + |++-\rangle + |+-+ \rangle + |-++ \rangle + |+-- \rangle + |-+- \rangle + |--+ \rangle + |--- \rangle \\ &\quad - |+++\rangle + |+-\rangle + |+-+ \rangle + |-++ \rangle - |+-- \rangle - |-+- \rangle - |--+ \rangle + |--- \rangle] \\ &= \frac{1}{2}[|++-\rangle + |+-+ \rangle + |-++ \rangle + |--- \rangle] \end{aligned} \quad (8.4.4)$$

Supponiamo che a causa della misura di $\sigma_{x,A}$, $\sigma_{x,B}$ e $\sigma_{x,C}$ di da parte di A, B e C, lo stato collassi (con probabilità 1/4) nello stato $|++-\rangle$ ¹⁰. I valori che A, B e C otterranno e che poi daranno come risposta sono $X_A = 1$ (legato alla misura di $|+\rangle$ sul primo qubit), $X_B = 1$ (legato alla misura di $|+\rangle$ sul secondo qubit) e $X_C = -1$ (legato alla misura di $|-\rangle$ sul terzo qubit). Quindi il loro prodotto sarà $X_A X_B X_C = -1$.

⁹ Per evitare confusione fra la variabile X, Y e i corrispondenti operatori di Pauli, useremo per quest'ultimi rispettivamente i simboli σ_x e σ_y .

¹⁰ Non è necessario che la misura sia contemporanea così come non è importante la sequenza temporale delle misure.

In maniera analoga, se il sistema collassasse sullo stato $|+ - +\rangle$ (con probabilità 1/4) si otterrà $\{X_A, X_B, X_C\} = \{1, -1, 1\}$ e prodotto $X_A X_B X_C = -1$. In questo modo, si vede che qualsiasi sia il risultato della misura il prodotto $X_A X_B X_C$ sarà sempre -1 e A, B e C vinceranno al gioco.

Supponiamo ora che la domanda riguardi la terna $\{X_A, Y_B, Y_C\}$ ¹¹. Secondo il protocollo, A misurerà $\sigma_{x,A}$ mentre B e C misureranno $\sigma_{y,B}$ e $\sigma_{y,C}$. Per comprendere quale sarà il risultato di tali misure, è necessario scrivere lo stato $|GHZ\rangle$ in Eq. (8.4.3) in termini degli autostati di $\sigma_{x,A}$, $\sigma_{y,B}$ e $\sigma_{y,C}$.

A tal proposito denotiamo gli autostati di $\sigma_{y,i}$ con $|\pm\rangle$ e ricordiamo la loro relazione con gli stati $|0\rangle$ e $|1\rangle$

$$\begin{aligned} |0\rangle &= \frac{|\bar{+}\rangle + |\bar{-}\rangle}{\sqrt{2}} \\ |1\rangle &= -i \frac{|\bar{+}\rangle - |\bar{-}\rangle}{\sqrt{2}}. \end{aligned} \quad (8.4.5)$$

In questo caso, lo stato (8.4.3) si scriverà

$$|GHZ\rangle = \frac{1}{4} \left[(|+\rangle + |-\rangle) \otimes (|\bar{+}\rangle + |\bar{-}\rangle)^{\otimes^2} - (|+\rangle - |-\rangle) \otimes (-i)^2 (|\bar{+}\rangle + |\bar{-}\rangle)^{\otimes^2} \right]. \quad (8.4.6)$$

Si noti che la struttura è analoga all'espressione (8.4.4) con l'unica differenza che il termine $(-i)^2 = -1$ cambia di segno della terza riga dell'equazione. Dal calcolo esplicito si ottiene

$$\begin{aligned} |GHZ\rangle &= \frac{1}{4} \left[|+\bar{+}\bar{+}\rangle + |+\bar{+}\bar{-}\rangle + |+\bar{-}\bar{+}\rangle + |-\bar{+}\bar{+}\rangle + |+\bar{-}\bar{-}\rangle + |-\bar{+}\bar{-}\rangle + |-\bar{-}\bar{+}\rangle + |-\bar{-}\bar{-}\rangle \right. \\ &\quad \left. + |+\bar{+}\bar{-}\rangle - |+\bar{+}\bar{-}\rangle - |+\bar{-}\bar{+}\rangle - |-\bar{+}\bar{+}\rangle + |+\bar{-}\bar{-}\rangle + |-\bar{+}\bar{-}\rangle + |-\bar{-}\bar{+}\rangle - |-\bar{-}\bar{-}\rangle \right] \\ &= \frac{1}{2} \left[|+\bar{+}\bar{+}\rangle + |+\bar{-}\bar{-}\rangle + |-\bar{+}\bar{-}\rangle + |-\bar{-}\bar{+}\rangle \right]. \end{aligned} \quad (8.4.7)$$

A seguito delle misure di $\sigma_{x,A}$, $\sigma_{y,B}$ e $\sigma_{y,C}$ da parte di A, B e C, il sistema collasserà in uno degli stati scritti sopra. Se, ad esempio, collassasse (con probabilità 1/4) nello stato $|+\bar{+}\bar{+}\rangle$, la terna data da A, B e C sarà $\{X_A, Y_B, Y_C\} = \{1, 1, 1\}$ e il prodotto $X_A Y_B Y_C = 1$. È evidente che anche per tutte le altre possibili terne estratte dalla misura ($\{X_A, Y_B, Y_C\} = \{1, 1, 1\}$, $\{X_A, Y_B, Y_C\} = \{1, -1, -1\}$, $\{X_A, Y_B, Y_C\} = \{-1, 1, -1\}$ e $\{X_A, Y_B, Y_C\} = \{-1, -1, 1\}$), il prodotto sarà sempre $X_A Y_B Y_C = 1$. Di conseguenza anche in questo caso A, B e C vinceranno il gioco e saranno liberati.

Dato che lo schema del gioco è simmetrico per A, B e C, il protocollo funzionerà anche per le altre domande (ad esempio, qual'è la terna $\{Y_A, X_B, Y_C\}$) restituendo sempre un prodotto uguale a 1.

Abbiamo quindi dimostrato che, per il gioco in questione, non esiste un protocollo classico che assicuri la vincita ma sfruttando la meccanica quantistica esiste una strategia vincente. Il vantaggio quantistico è determinato dall'entanglement

¹¹ Ovvero si chieda ad A che valore assume X e a B e C che valore assume Y.

che permette di avere delle correlazioni quantistiche fra le misure non presenti con stati classici.

V – TEST DI NON-CLASSICITÀ DELLA MECCANICA QUANTISTICA

Il gioco discusso nel paragrafo precedente è stato introdotto dal fisico L. Vaidman partendo da un articolo divulgativo di D. Mermin. In realtà ha implicazioni molto profonde e ci permette di discutere uno degli esperimenti cruciali per stabilire che la meccanica quantistica non può essere ricondotta a teorie classiche ma che ha una struttura intrinsecamente diversa. Si tenga conto che la discussione qui sotto è, per ovvi motivi, semplificata. si cercherà comunque di evidenziare l'essenza dei risultati trascurando a volte la precisione nel linguaggio (si veda per maggiori dettagli e precisione l'articolo divulgativo di D. Mermin su *Physics Today* del 1990 [mermin1990]).

Il dibattito sulla struttura della meccanica quantistica risale alla nascita stessa della teoria hanno coinvolto e Einstein, Bohr, Schrödinger e, più in avanti negli anni, John Bell. Senza entrare nei dettagli tecnici e concettuali del dibattito, è comunque importante fare un'analisi cronologica e storica.

Einstein credeva che la meccanica quantistica fosse incompleta e che le predizioni controintuitive che la teoria faceva fossero in realtà una manifestazione di questa incompletezza. Era in particolare turbato dagli effetti "non-locali" della teoria.

8.5.1 Nonlocalità e entanglement in meccanica quantistica

Come abbiamo visto nei capitoli precedenti, gli stati entangled mostrano delle correlazioni quantistiche. Ad esempio, se lo stato di Bell $(|00\rangle + |11\rangle)/\sqrt{2}$ è condiviso fra Alice e Bob, dopo la misura del suo qubit Alice sa esattamente quale sarà il risultato della misura di Bob. Nell'interpretazione standard della meccanica quantistica, questo implica i) che ci sia una correlazione fra le misure e ii) che la teoria sia nonlocale (una misura di Alice perturba lo stato di Bob anche se abbastanza lontano da non interagire con Alice).

La soluzione che Einstein, Poldoski e Rosen (EPR) proposero è che le quantità fisiche avessero sempre un valore definito che si manifestava solo all'atto della misura. Dato che la teoria completa che include questi dettagli, è ignota l'unica cosa che possiamo fare è trattare le misure come statistiche¹².

Il problema delle correlazioni può essere facilmente risolto aggirato usando le correlazioni classiche. Ad esempio, supponiamo di avere una scatola con due palline. Le palline possono avere colore blu o rosso e sappiamo che nella scatola sono state messe palline dello stesso colore. A questo punto, l'estrazione (ovvero

¹² La statistica della teoria microscopica completa che include la meccanica quantistica è determinata da altre variabili (o gradi di libertà) che sono sconosciute. Vengono di solito chiamate *variabili nascoste*. Una volta note tali variabili e il loro comportamento, la meccanica quantistica cesserebbe di essere una teoria probabilistica e diventerebbe completamente deterministica.

la misura) di una pallina rivelerà immediatamente il colore della seconda pallina anche se questa non è stata ancora estratta dalla scatola.

Se poi supponiamo di avere N scatole e di mettere in metà palline blue e nelle restanti palline rosse, gli esperimenti descriveranno esattamente la statistica attesa: il 50% delle volte estrarremo i colori blu-blu (che possiamo associare alla misura che porta allo stato $|11\rangle$) e il restante 50% estrarremo i colori rosso-rosso (corrispondente allo stato $|00\rangle$).

Molti fisici stentavano a credere nella nonlocalità della meccanica quantistica soprattutto perchè sembra in contrasto con il principio della relatività ristretta ("niente può viaggiare più voleve della luce")¹³.

Se però, come proposero EPR, gli stati quantistici hanno sempre un valore definito e la misura non fa altro che rivelarlo, non c'è un problema di nonlocalità e la misura di Alice non cambia lo stato del sistema di Bob ma ne evidenzia solo il valore. Questo è naturalmente diverso da quanto assume l'interpretazione convenzionale per la quale il valore del sistema di Alice e quello di Bob viene definito (istantaneamente) solo all'atto della misura.

Fino al 1964 sembrava che fosse impossibile distinguere fra queste due possibili interpretazioni. In quell'anno, in un suo famosissimo lavoro [Bell1964], J. Bell dimostrò che esisteva un esperimento che permetteva di stabilire se fossero presenti delle variabili nascoste o meno. L'esperimento fu portato a termine negli anni 80 dal fisico francese A. Aspect e confermò l'assenza delle variabili nascoste e la nonlocalità della meccanica quantistica.

Noi non tratteremo il lavoro di Bell ma una situazione analoga ma più immediata e diretta proposta da GHZ nel 1989.

8.5.2 Esperimento GHZ (basato su [mermin1990])

Usando tre qubit, supponiamo di preparare uno stato $|GHZ\rangle$ come in Eq. (8.4.3). Dalla riscrittura dello stato in Eq. (8.4.7) si può vedere che lo stato $|GHZ\rangle$ è autostato dell'operatore $\sigma_{x,A} \otimes \sigma_{y,B} \otimes \sigma_{y,C}$. Dato che $\{|\pm\rangle\}$ sono autostati di $\sigma_{x,i}$ e $\{|\mp\rangle\}$ sono autostati di $\sigma_{y,i}$, abbiamo che

$$\begin{aligned}\sigma_{x,A} \otimes \sigma_{y,B} \otimes \sigma_{y,C} |+\bar{\tau}\bar{\tau}\rangle &= |+\bar{\tau}\bar{\tau}\rangle \\ \sigma_{x,A} \otimes \sigma_{y,B} \otimes \sigma_{y,C} |+\bar{\tau}\bar{\tau}\rangle &= |+\bar{\tau}\bar{\tau}\rangle \\ \sigma_{x,A} \otimes \sigma_{y,B} \otimes \sigma_{y,C} |-\bar{\tau}\bar{\tau}\rangle &= |-\bar{\tau}\bar{\tau}\rangle \\ \sigma_{x,A} \otimes \sigma_{y,B} \otimes \sigma_{y,C} |-\bar{\tau}\bar{\tau}\rangle &= |-\bar{\tau}\bar{\tau}\rangle\end{aligned}\quad (8.5.1)$$

(si veda l'importantissima precisazione alla nota¹⁴). Dato che tutti gli stati ($|+\bar{\tau}\bar{\tau}\rangle$, $|+\bar{\tau}\bar{\tau}\rangle$, $|-\bar{\tau}\bar{\tau}\rangle$ e $|-\bar{\tau}\bar{\tau}\rangle$) sono autostati dell'operatore con lo stesso autovalore +1, anche la loro sovrapposizione nello stato $|GHZ\rangle$ in (8.4.7), sarà autostato con lo

¹³ Come visto nell'esempio del teletrasposto quantistico, la soluzione è nell'interpretare il principio di relatività ristretta in un altro senso. Ovvero che nessuna informazione può essere scambiata a velocità maggiore di quella della luce.

¹⁴ ricordiamo che quello che questo corrisponde a *verificare* che gli stati sono autostati dell'operatore *NON* vuol dire applicare l'operatore allo stato.

stesso autovalore. Un analogo ragionamento e calcolo può essere fatto per gli operatori $\sigma_{y,A} \otimes \sigma_{x,B} \otimes \sigma_{y,C}$ e $\sigma_{y,A} \otimes \sigma_{y,B} \otimes \sigma_{x,C}$.

Arriviamo quindi a stabilire che lo stato $|GHZ\rangle$ è autostato di tutti e tre gli operatori con autovalore +1:

$$\begin{aligned}\sigma_{x,A} \otimes \sigma_{y,B} \otimes \sigma_{y,C} |GHZ\rangle &= |GHZ\rangle \\ \sigma_{y,A} \otimes \sigma_{x,B} \otimes \sigma_{y,C} |GHZ\rangle &= |GHZ\rangle \\ \sigma_{y,A} \otimes \sigma_{y,B} \otimes \sigma_{x,C} |GHZ\rangle &= |GHZ\rangle.\end{aligned}\quad (8.5.2)$$

possiamo quindi misurare in sequenza gli operatori *composti* $\sigma_{x,A} \otimes \sigma_{y,B} \otimes \sigma_{y,C}$, $\sigma_{y,A} \otimes \sigma_{x,B} \otimes \sigma_{y,C}$ e $\sigma_{y,A} \otimes \sigma_{y,B} \otimes \sigma_{x,C}$ senza cambiare o perturbare lo stato $|GHZ\rangle$. In tutte e tre le misure otterremo l'autovalore +1.

Si noti che in questo caso, dato che gli operatori sono composti,¹⁵ non possiamo attribuire un valore preciso alle misure sui *singoli* qubit. Ovvero, dato che misuriamo l'operatore $\sigma_{x,A} \otimes \sigma_{y,B} \otimes \sigma_{y,C}$, non è possibile determinare quale sia il valore di $\sigma_{x,A}$. Infatti l'unica informazione che abbiamo è sul prodotto composto delle misure questo potrebbe essere sia +1 che -1.

Usando una interpretazione classica del risultato delle misure (come nella teoria delle variabili nascoste discussa sopra), potremmo dire che i qubit hanno un valore specificato (determinato a *priori*) lungo gli assi x e y. Usando la notazione del paragrafo precedente, indicheremo con X_i e Y_i per il qubit i. Ribadiamo che questi valori non sono determinati dalla misura che ha solo il compito di "rivelarli".

Con queste notazioni e interpretazioni, arriviamo a dire che la misura di $\sigma_{x,A} \otimes \sigma_{y,B} \otimes \sigma_{y,C}$ non determina il valore di X_A , Y_B e Y_C univocamente ma solo il loro prodotto che è +1. Come visto in precedenza, questo potrebbe essere attribuito, ad esempio, sia alla terna $\{X_A, Y_B, Y_C\} = \{1, 1, 1\}$ che $\{X_A, Y_B, Y_C\} = \{1, -1, -1\}$ che a cui associamo valori diversi per i singoli qubit.

Nonostante ciò, le misure dei tre operatori di sopra impongono dei vincoli perché devono soddisfare le seguenti equazioni

$$\begin{aligned}X_A Y_B Y_C &= 1 \\ Y_A X_B Y_C &= 1 \\ Y_A Y_B X_C &= 1.\end{aligned}\quad (8.5.3)$$

Come fatto in precedenza moltiplichiamo i membri di sinistra ottenendo

$$(X_A Y_B Y_C)(Y_A X_B Y_C)(Y_A Y_B X_C) = X_A X_B X_C Y_A^2 Y_B^2 Y_C^2 = X_A X_B X_C \quad (8.5.4)$$

dove nell'ultima equazione abbiamo usato il fatto che $Y_i = \pm 1$ e quindi $Y_i^2 = 1$. Uguagliando questo al prodotto dei membri di sinistra otteniamo che necessariamente

$$X_A X_B X_C = 1. \quad (8.5.5)$$

¹⁵ È importante notare che qui stiamo supponendo di misurare l'operatore composto sui tre qubit mentre nel paragrafo precedente la misura era pensata come fatta separatamente sui tre qubit.

In altre parole, pur non essendo in grado di stabilire i valori dei singoli X_i , sappiamo che il loro prodotto deve essere uguale a +1. Questo è la predizione di una teoria con variabili nascoste in cui i valori X_i (qualsiasi essi siano) sono determinati inizialmente.

A questo punto, dopo aver fatto le prime tre misure (che, ricordiamo, non distruggono lo stato $|GHZ\rangle$) e ottenuto sempre +1, misuriamo l'operatore $\sigma_{x,A} \otimes \sigma_{x,B} \otimes \sigma_{x,C}$. Riscrivendo tale stato nella base degli autostati $\{| \pm \rangle\}$ come in Eq. (8.4.4), possiamo verificare che

$$\begin{aligned}\sigma_{x,A} \otimes \sigma_{x,B} \otimes \sigma_{x,C} |++-\rangle &= -|++-\rangle \\ \sigma_{x,A} \otimes \sigma_{x,B} \otimes \sigma_{x,C} |+-\rangle &= -|+-\rangle \\ \sigma_{x,A} \otimes \sigma_{x,B} \otimes \sigma_{x,C} |-+\rangle &= -|-+\rangle \\ \sigma_{x,A} \otimes \sigma_{x,B} \otimes \sigma_{x,C} |--\rangle &= -|--\rangle.\end{aligned}\quad (8.5.6)$$

Quindi tutti questi stati sono autostati di $\sigma_{x,A} \otimes \sigma_{x,B} \otimes \sigma_{x,C}$ con autovalore -1. Di conseguenza $|GHZ\rangle$ sarà autostato con lo stesso autovalore. La misura darà quindi risultato -1 senza perturbare lo stato.

Interpretando i risultati in senso classico come sopra, arriviamo a dire che, dalla misura risulta che

$$X_A X_B X_C = -1 \quad (8.5.7)$$

che è in contraddizione con quello che ci saremmo aspettati dall'equazione (8.5.5) che, ricordiamo, derivava come conseguenza delle prime tre misure.

Siamo arrivati alla conclusione le prime tre misure sono incompatibili con il risultato della quarta misura. Questa apparente contraddizione deriva dall'aver supposto che si possa attribuire agli stati dei valori fissati per le variabili X_i e, in questo senso, classici (ad esempio, assumere che il valore di X_A sia fissato ma che sia solamente "sconosciuto"). Nella interpretazione tradizionale della meccanica quantistica, i valori di X_i non sono determinati a priori ma durante la misura. Questo implica immediatamente la nonlocalità della meccanica quantistica.

Da questo punto di vista, l'esperimento discusso permette di discriminare fra questa visione (classica) e una visione puramente quantistica. La misura dell'osservabile $\sigma_{x,A} \otimes \sigma_{x,B} \otimes \sigma_{x,C}$ determina quale delle due interpretazioni sia quella vera. In questo senso basta la misura $X_A X_B X_C = -1$ per escludere l'interpretazione classica.

L'esperimento è stato effettivamente portato a termine nel laboratorio di Anton Zeilinger nel 2000 e ha confermato che la meccanica quantistica non ammette una descrizione in termini di variabili classiche. L'esperimento ha come conseguenza la conferma che la meccanica quantistica è una teoria intrinsecamente nonlocale.

VI – IL GIOCO DI *mermin-peres* (*pseudo-telepathy game*)

Un altro gioco in cui c'è un evidente vantaggio ad usare la meccanica quantistica è quello proposto da Mermin e Peres e, a volte chiamato, *pseudo-telepathy game*. Come nel caso precedente, nel caso classico non c'è una strategia che permetta ai giocatori di vincere sempre mentre questa è possibile nella versione quantistica del gioco.

8.6.1 Struttura del gioco

Alice e Bob che sono separati e non possono comunicare. Un arbitro ha una matrice (o tabella) con 3 righe e 3 colonne. Ogni casella della tabella viene identificata con il numero della riga i e della colonna j (con $i, j = 1, 2, 3$).

L'arbitro sceglie casualmente il numero della riga i e il numero della colonna j e comunica ad Alice il numero della riga e a Bob il numero della colonna.

Alice e Bob devono fornire una terna ciascuno che andranno a formare i valori della riga i -esima (dati da Alice) e della colonna j -esima dati da Bob. In altre parole, se Alice a Bob hanno mandato rispettivamente le terne $\{a_{i,1}, a_{i,2}, a_{i,3}\}$ e $\{b_{i,1}, b_{i,2}, b_{i,3}\}$ (con $a_{i,k}, b_{i,k} = \pm 1$), l'arbitro compila la i -esima riga e la j -esima colonna della matrice M . Ad esempio, se $i = 3$ e $j = 4$ abbiamo (8.6.1)

$$M = \begin{bmatrix} & b_{1,2} \\ & b_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3}/b_{3,3} \end{bmatrix}. \quad (8.6.1)$$

Come si può vedere, per qualsiasi scelta di i e j c'è sempre un elemento di sovrapposizione fra la terna di Alice e quella di Bob: l'elemento $M_{i,j}$. La condizione per vincere il gioco è che l'elemento $M_{i,j}$ della matrice sia definito univocamente ovvero che $a_{i,j} = b_{j,i}$.

Ci sono due vincoli sui numeri che Alice e Bob possono scegliere

1. possono essere solo $+1$ e -1 .
2. per Alice il prodotto dei numeri scelti deve essere uguale a $+1$ e per Bob deve essere uguale a -1 . Ovvero,

$$\begin{aligned} \prod_{k=1}^3 a_{i,k} &= a_{i,1}a_{i,2}a_{i,3} = +1 \\ \prod_{k=1}^3 b_{j,k} &= b_{j,1}b_{j,2}b_{j,3} = -1. \end{aligned} \quad (8.6.2)$$

Riassumendo, scelti i e j a caso ($i, j = 1, 2, 3$)

- Alice e Bob vincono se scelgono $a_{i,j} = b_{j,i}$.
- $a_{i,k} = \pm 1$ $b_{j,k} = \pm 1$ (con $k = 1, 2, 3$).
- $\prod_{k=1}^3 a_{i,k} = +1$ e $\prod_{k=1}^3 b_{j,k} = -1$.

8.6.2 Caso classico

Come detto Alice e Bob sono separati e non possono comunicare. Possono però aver stabilito una strategia prima di essere separati. La domanda è : esiste una strategia classica (prestabilita) che permetta ad Alice e bob di vincere sempre?

Alice e Bob riescono a vincere sempre se per ogni i e j riescono ad avere $a_{i,j} = b_{j,i}$ con i vincoli ???. Questo corrisponderebbe ad riuscire a costruire una matrice tale che gli elementi delle righe moltiplicati diano +1 e gli elementi delle colonne moltiplicati diano -1. Tale strategia non esiste. Per dimostrarlo prendiamo la matrice

$$M = \begin{bmatrix} +1 & +1 & +1 \\ +1 & -1 & -1 \\ -1 & +1 & +1/-1 \\ -1 & -1 & -1/+1 \end{bmatrix}_{+1 \atop -1/+1 \atop -1/-1/+1}$$

A destra delle righe è riportato il prodotto $\prod_{k=1}^3 a_{i,k}$ e sotto le colonne $\prod_{k=1}^3 b_{j,k}$. Come si può vedere, le prime due righe e colonne soddisfano i vincoli richiesti. L'ultima riga e colonna invece hanno vincoli incompatibili. Se scegliamo l'elemento $M_{3,3} = +1$ possiamo soddisfare la condizione $\prod_{k=1}^3 b_{3,k} = -1$ ma avremmo $\prod_{k=1}^3 a_{3,k} = -1$. Al contrario, scegliendo $M_{3,3} = -1$ avremo $\prod_{k=1}^3 a_{3,k} = +1$ come richiesto ma $\prod_{k=1}^3 b_{3,k} = +1$. Si può dimostrare che anche con altre scelte è impossibile costruire una matrice M che soddisfi tutte le condizioni richieste.

Alice e Bob possono stabilire una strategia a priori (che equivale a scegliere una particolare matrice M) ma non la possono cambiare dopo perchè non possono comunicare. Dato che la scelta di i e j è casuale, statisticamente Alice e Bob potranno vincere 8 volte su 9 (esattamente come gli elementi di M che soddisfano tutte le richieste) ma non potranno vincere sempre.

8.6.3 Caso quantistico

La versione quantistica del gioco segue le stesse regole della controparte classica in Sez. 8.6.1 con i vincoli (8.6.1) ma Alice e Bob possono condividere e misurare stati quantistici.

Supponiamo che condividano quattro qubit denominati con le lettere minuscole a, b, c, d *entangled* a coppie (stati di Bell); ovvero,

$$\begin{aligned} |\Psi_0\rangle &= \frac{1}{2} \left(|0\rangle_a \otimes |0\rangle_b + |1\rangle_a \otimes |1\rangle_b \right) \otimes \left(|0\rangle_c \otimes |0\rangle_d + |1\rangle_c \otimes |1\rangle_d \right) \\ &= \frac{1}{2} \left(|0\rangle_a |0\rangle_b |0\rangle_c |0\rangle_d + |0\rangle_a |0\rangle_b |1\rangle_c |1\rangle_d + |1\rangle_a |1\rangle_b |0\rangle_c |0\rangle_d + |1\rangle_a |1\rangle_b |1\rangle_c |1\rangle_d \right) \end{aligned} \quad (8.6.3)$$

dove nell'ultimo passaggio, per semplicità , abbiamo omesso e sottinteso il simbolo di prodotto tensore \otimes .

I qubit a e c saranno di Alice mentre quelli b e d saranno di Bob. È conveniente riscrivere lo stato $|\Psi_0\rangle$ raccogliendo i qubit di Alice e Bob $|i\rangle_a |j\rangle_b |k\rangle_c |l\rangle_d \equiv$

$|i\rangle_a |k\rangle_c |j\rangle_b |l\rangle_d = |ij\rangle_A |kl\rangle_B$ dove gli indici A e B indicano l'appartenenza ad Alice e Bob, rispettivamente. Con queste notazioni, lo stato $|\Psi_0\rangle$ si può riscrivere

$$\begin{aligned} |\Psi_0\rangle &= \frac{1}{2} \left(|0\rangle_a |0\rangle_c |0\rangle_b |0\rangle_d + |0\rangle_a |1\rangle_c |0\rangle_b |1\rangle_d + |1\rangle_a |0\rangle_c |1\rangle_b |0\rangle_d + |1\rangle_a |1\rangle_c |1\rangle_b |1\rangle_d \right) \\ &= \frac{1}{2} \left(|00\rangle_A |00\rangle_B + |01\rangle_A |01\rangle_B + |10\rangle_A |10\rangle_B + |11\rangle_A |11\rangle_B \right) \end{aligned} \quad (8.6.4)$$

Come possiamo notare, *nei singoli contributi* lo stato di Alice è uguale a quello di Bob; ovvero, lo stato $|\Psi_0\rangle$ è la somma di contributi del tipo $|ij\rangle_A |ij\rangle_B$.

Prima di andare avanti facciamo una breve osservazione matematica. Gli stati di Bell che compongono $|\Psi_0\rangle$ in eq. (8.6.3) hanno la stessa struttura nelle basi di σ_z ($\{|0\rangle, |1\rangle\}$), σ_x ($\{|+\rangle, |-\rangle\}$) e σ_y ($\{|+_y\rangle, |-_y\rangle\}$) (dove $|\pm_y\rangle = 1/\sqrt{2}(\mp i|0\rangle + |1\rangle)$)¹⁶. In altri termini, abbiamo che

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|++\rangle + |--\rangle}{\sqrt{2}} = \frac{|+_y+_y\rangle - |-_y-_y\rangle}{\sqrt{2}}. \quad (8.6.5)$$

Questo significa che lo stato iniziale può essere scritto nelle tre basi differenti come

$$\begin{aligned} |\Psi_0\rangle &= \frac{1}{2} \left(|00\rangle_A |00\rangle_B + |01\rangle_A |01\rangle_B + |10\rangle_A |10\rangle_B + |11\rangle_A |11\rangle_B \right) \\ &= \frac{1}{2} \left(|++\rangle_A |--\rangle_B + |+-\rangle_A |+-\rangle_B + |-+\rangle_A |-+\rangle_B + |--\rangle_A |--\rangle_B \right) \\ &= \frac{1}{2} \left(|+_y+_y\rangle_A |+_y+_y\rangle_B - |+_y-_y\rangle_A |+_y-_y\rangle_B \right. \\ &\quad \left. - |-_y+_y\rangle_A |-_y+_y\rangle_B + |-_y-_y\rangle_A |-_y-_y\rangle_B \right). \end{aligned} \quad (8.6.6)$$

Fatte queste premesse possiamo passare alla strategia quantistica che Alice e Bob adottano. Prima di essere separati, decidono di misurare lo stato entangled secondo la matrice M

$$M = \begin{bmatrix} \text{Id} \otimes \sigma_z & \sigma_z \otimes \text{Id} & -\sigma_z \otimes \sigma_z \\ \sigma_x \otimes \text{Id} & \sigma_x \otimes \text{Id} & -\sigma_x \otimes \sigma_x \\ \sigma_x \otimes \sigma_z & \sigma_z \otimes \sigma_x & -\sigma_y \otimes \sigma_y \end{bmatrix}. \quad (8.6.7)$$

e di mandare all'arbitro i risultati delle misure. La matrice (8.6.7) va interpretata nel seguente modo. Una volta ricevuto l'indice i , Alice fa in sequenza le misure indicate nella riga i . Ad esempio, se $i = 2$, Alice misurerà in sequenza gli osservabili $\text{Id} \otimes \sigma_x$, $\sigma_x \otimes \text{Id}$ e $-\sigma_x \otimes \sigma_x$ e manderà i risultati all'arbitro. Allo stesso modo, ricevuto l'indice $j = 1$, Bob misurerà $\text{Id} \otimes \sigma_z$, $\text{Id} \otimes \sigma_x$ e $\sigma_x \otimes \sigma_z$ e manderà i risultati della misura.

Per semplificare la discussione facciamo un esempio pratico e supponiamo che l'arbitro abbia estratto i due numeri $i = 1$ e $j = 1$. Alice quindi dovrà misurare gli operatori $\text{Id} \otimes \sigma_z$, $\sigma_z \otimes \text{Id}$ e $-\sigma_z \otimes \sigma_z$ mentre Bob $\text{Id} \otimes \sigma_z$, $\sigma_z \otimes \text{Id}$ e $-\sigma_z \otimes \sigma_z$.

Supponiamo che Alice faccia la prima misura di $\text{Id} \otimes \sigma_z$. Notiamo che lo stato $|\Psi_0\rangle$ non è autostato di $\text{Id} \otimes \sigma_z$ ed i qubit di Alice e Bob sono *entangled*. Con-

¹⁶ Questo lo si può dimostrare con il calcolo diretto. Ad esempio WRITE

Alice	$ 00\rangle$	$ 01\rangle$	$ 10\rangle$	$ 11\rangle$
$\text{Id} \otimes \sigma_z$	-1	+1	-1	+1
$\sigma_z \otimes \text{Id}$	-1	-1	+1	+1
$-\sigma_z \otimes \sigma_z$	-1	+1	+1	+1
$\prod_{k=1}^3 a_{i,k}$	-1	-1	-1	-1

Table 8: Tabella della misure di Alice quando viene chiesta la riga $i = 1$. Le righe rappresentano gli osservabili che Alice misura. Questi sono tutti diagonali nella stessa base mostrata nella parte superiore della tabella. La prima misura di Alice fa collassare lo stato in uno degli stati riportati (con uguale probabilità di 1/4). Le misure successive non alterano lo stato. I rispettivi risultati delle misure sono mostrati nella tabella e il prodotto delle misure è riportato nell'ultima riga. Come si vede, questo è sempre uguale a -1.

cludiamo che alla misura di Alice i) con probabilità 1/4, il sistema composta dai quattro qubit collassa in uno dei seguenti stati $|00\rangle_A |00\rangle_B$, $|01\rangle_A |01\rangle_B$, $|10\rangle_A |10\rangle_B$ o $|11\rangle_A |11\rangle_B$, ii) anche il sistema di Bob collassa.

La prima importante osservazione è che *indipendentemente* dallo stato in cui il sistema collassa, gli stati di Alice e Bob sono uguali, i.e., come notato prima $|ij\rangle_A |ij\rangle_B$. Dato che la matrice delle misure M (8.6.7) impone ad Alice e Bob di misurare lo stesso osservabile sullo stesso stato, concludiamo che *per ogni i e j il risultato della misura sarà lo stesso* e quindi $a_{i,j} = b_{j,i}$. La prima condizione per la vincita è dunque soddisfatta.

Un discorso analogo si può fare per gli altri osservabili. Come mostrato in eq. (8.6.6), in qualsiasi base i termini di Alice e Bob sono identici quindi una misura dello stesso osservabile, farà collassare il sistema ma darà lo stesso valore.

La seconda condizione in 8.6.1 è banalmente soddisfatta perché i risultati della misura sono due e quindi possono immediatamente essere associati ai valori \pm . Rimane quindi l'ultima condizione $\prod_{k=1}^3 a_{i,k} = +1$ e $\prod_{k=1}^3 b_{j,k} = -1$ che è la più complicata da verificare.

Supponiamo per semplificare che Alice faccia prima tutte le sue misure. Si può dimostrare che i tre osservabili che Alice misura possiedono una base comune; ovvero, esiste una base in cui tutti e tre sono diagonali¹⁷.

Nello specifico, la la base comune ai tre osservabili che Alice misura per $i = 1$ è riportata in tabella 8 con i rispettivi autovalori (è immediato verificare che questi sono effettivamente autostati e autovalori). In termini di misura, questo significa che quando Alice farà la prima misura il sistema collasserà in uno degli stati riportati nella tabella (si ricordi che $|\psi_0\rangle$ non è autostato degli osservabili che Alice misura). Una volta avvenuto il collasso, le successive misure non saranno probabilistiche ma daranno un risultato certo. Ad esempio, se dopo la misura dell'osservabile $\text{Id} \otimes \sigma_z$, il sistema collassa in $|10\rangle$, Alice ottiene il valore +1. Dato che $|10\rangle$ è autostato di $\sigma_z \otimes \text{Id}$, il risultato della misura sarà certamente -1. Allo stesso modo la terza misura ($-\sigma_z \otimes \sigma_z$), darà con certezza il risultato +1.

¹⁷ In maniera più formale, si può dimostrare che gli operatori delle righe e delle colonne commutano. Dati due operatori A e B, si dice che commutano se $[A, B] \equiv AB - BA = 0$ (dove il simbolo [...] indica l'operatore di commutazione). si può dimostrare che se due operatori commutano esiste una base in cui sono entrambi diagonali.

Bob	$ +0\rangle$	$ +1\rangle$	$ -0 \rangle$	$ -1 \rangle$
$\text{Id} \otimes \sigma_z$	-1	+1	-1	+1
$\sigma_x \otimes \text{Id}$	+1	+1	-1	-1
$\sigma_x \otimes \sigma_z$	-1	+1	+1	-1
$\prod_{k=1}^3 b_{i,k}$	+1	+1	+1	+1

Table 9: Tabella della misure di Bob quando viene chiesta la riga $j = 1$. Le righe rappresentano gli osservabili che Bob misura. Questi sono tutti diagonali nella stessa base mostrata nella parte superiore della tabella. La prima misura di Bob fa collassare lo stato in uno degli stati riportati (con uguale probabilità di 1/4). Le misure successive non alterano lo stato. I rispettivi risultati delle misure sono mostrati nella tabella e il prodotto delle misure è riportato nell'ultima riga. Come si vede, questo è sempre uguale a +1.

Come si può vedere il prodotto dei risultati delle misure di Alice è $(+1)(-1)(+1) = -1$. Si può facilmente verificare che questo accade per un qualsiasi stato in tabella 8.

Un discorso analogo può essere fatto per Bob. Sempre nel caso in cui $j = 1$, gli osservabili da misurare hanno un base di autostati comuni mostrata in tabella 9. Dopo la prima misura e rispettivo collasso, le misure seguenti saranno deterministiche e daranno un risultato certo. Come si può vedere dalla tabella 9, indipendentemente dallo stato su cui collassa il sistema, il prodotto delle tre misure sarà $\prod_{k=1}^3 b_{i,k} = +1$ come richiesto.

Dobbiamo fare una precisazione. Prendiamo ancora il caso in cui $i = 1$ e $j = 1$, supponiamo che Alice prima faccia la prima misura e che ottenga il risultato -1 quando misura $\text{Id} \otimes \sigma_z$. Per capire meglio, dobbiamo scrivere lo stato $|\psi_0\rangle$ in termini di autostati di $\text{Id} \otimes \sigma_z$ facendo però attenzione ai rispettivi autovalori. Otteniamo

$$|\psi_0\rangle = \frac{1}{2} \left[\left(|00\rangle_A |00\rangle_B + |01\rangle_A |01\rangle_B \right) + \left(|10\rangle_A |10\rangle_B + |11\rangle_A |11\rangle_B \right) \right] \quad (8.6.8)$$

dove abbiamo separato gli autostati con autovalore -1 da quelli con autovalore +1. La misura di $\text{Id} \otimes \sigma_z$ farà collassare il sistema nella sovrapposizione $(|00\rangle_A |00\rangle_B + |01\rangle_A |01\rangle_B)$ perché non può distinguere stati con stesso autovalore. In ogni caso, la misura successiva dell'osservabile $\sigma_z \otimes \text{Id}$ distinguerà i due stati stato che $|00\rangle_A$ ha autovalore -1 e $|01\rangle_A$ ha autovalore +1. Quindi, è la sequenza completa di misura di Alice che seleziona uno degli autostati in tabella 8.

L'ultimo punto da chiarire è cosa succede con le misure in sequenza di Alice e di Bob. Supponiamo che Alice abbia fatto le sue misure e selezionato lo stato $|01\rangle_A$. Come discusso [si veda eq. (8.6.6) e relativi commenti], anche lo stato di Bob sarà $|01\rangle_B$. Questo però non è un autostato degli osservabili che Bob deve misurare (tabella 9). Cosa succederà?

Per capirlo basta riscrivere lo stato $|01\rangle_B$ nella base in tabella 9. Abbiamo (ricordiamo che $|0\rangle = 1/\sqrt{2}(|+\rangle + |-\rangle)$)

$$|01\rangle_B = \frac{1}{\sqrt{2}}(|+1\rangle_B + |-1\rangle_B). \quad (8.6.9)$$

La misura di Bob di $\text{Id} \otimes \sigma_z$ non distingherà e non farà collassare lo stato (questo è già autostato con autovalore 1). La seconda misura di $\sigma_x \otimes \text{Id}$ farà collassare (con uguale probabilità) il sistema nello stato $|+1\rangle_B$, nel qual caso Bob otterrà +1, o $| -1\rangle_B$, nel qual caso Bob otterrà -1. Quindi, anche in questo caso, sono le misure sequenziali che individuano (statisticamente) uno degli stati in tabella 9. Il fatto che ci sia o meno un collasso e quando questo avvenga (durante la prima o seconda misura) è irrilevante perché il prodotto delle tre misure sarà sempre +1.

Naturalmente, la discussione fatta non dipende dal fatto di aver scelto $i = 1$ e $j = 1$. Discorsi analoghi con identiche conclusioni si possono fare per generici i e j . Abbiamo quindi dimostrato che nel caso quantistico esiste una strategia che permette ad Alice e Bob di vincere sempre contro una probabilità massima di $8/9$ nel caso classico.

9

ELITZUR-VAIDMAN BOMB TESTER

I – INTRODUZIONE

La meccanica quantistica è ricca di fenomeni poco intuitivi se interpretati nell’ambito della fisica classica a cui siamo abituati. Alcuni di questi, come l’entanglement e la sovrapposizione di stati, sono alla base delle applicazioni informatiche. Altri stanno ancora trovando piano piano applicazioni nuove e inaspettate.

Quello che discutiamo in questo capitolo è un esperimento proposto da Elitzur e Vaidman nel 1993 [EV_bomb1993]. Quello che notarono è che ci sono situazioni in meccanica quantistica si può ottenere informazione su un oggetto senza misurarlo direttamente (o meglio senza interagire con esso). Per questo motivo chiamarono questo fenomeno "misura senza interazione" (*interaction-free measurement*). Per evidenziare l’apparente situazione paradossale (o meglio controiduitiva), immaginarono di costruire un *bomb tester* quantistico per testare lo stato di una bomba senza farla esplodere.

Quello che sembrava una pura idea da laboratorio, ha fatto la sua apparizione nel campo dell’informatica quantistica. In Fig. 25 è mostrata una *challenge* comparsa su un sito di informatici che pone il problema su come usare il *bomb tester* quantistico in un aeroporto.

II – INTERFEROMETRI

In figura 26 (a) è mostrato un tipo di esperimento di ottica. Un fascio di luce *beam splitter* che lo divide in due fasci aventi intensità dimezzata. I due fasci vengono riflessi da due specchi (*mirror*) e si ricongiungono su un secondo *beam splitter* che li ricombina. La luce uscente dal secondo *beam splitter* viene infine misurata da due *detector*.

A seconda della lunghezza dei percorsi dei fasci di luce nei due bracci dell’interferometro, si hanno diversi fenomeni di interferenza. In particolare, i percorsi possono essere aggiustati in modo da far sì che solo il *detector 1* rilevi il fascio mentre il *detector 2* non riceve nessuna illuminazione. Questo è un tipico fenomeno di interferenza in fisica in cui si ha interferenza costruttiva per il fascio che raggiunge il *detector 1* e interferenza distruttiva per quello che raggiunge il *detector 2*.

Se diminuiamo l’intensità del fascio si raggiunge il regime quantistico dove entra nell’interferometro un solo fotone alla volta. La fenomenologia dell’effetto è la stessa ma in questo caso diremo che arrivato sul *beam splitter* il fotone avrà il

UTCTF 2019 - Airport Security (1750pt)

MARCH 10, 2019
CRYPTO QUANTUM

Airport Security (1750pt)

Crypto

Description: nc quantumbomb.live 1337

You have a bomb and will receive a random qubit to query the bomb. You're allowed to apply any unitary matrix to this query, and it'll query the bomb in superposition of whether or not it's a bomb. If the bomb measures $|1\rangle$, it will explode. If the bomb measures $|0\rangle$, it does nothing. Nothing is measured if there is no bomb.

gates are inputed as:

```
numbers = np.matrix([[complex(numbers[0]), complex(numbers[1])], [complex(numbers[2]), complex(numbers[3])]])
```

Figure 25: Una challenge comparsa su un sito informatico. Dedicata alla sicurezza aeroportuale immagina di usare il *bomb tester* quantistico proposto da Elitzur e Vaidman.

50% di possibilità di passare in un ramo e il 50% di andare nell'altro. Il fotone verrà poi riflesso dagli specchi e "ricombinato" dal secondo *beam splitter*. Anche in questo caso l'interferenza farà in modo che sia misurato solo dal detector 1.

Possiamo formalizzare questo fenomeno usando la notazione della quantum information:

1. i fotoni nei rami orizzontali sono associati allo stato $|0\rangle$.
2. i fotoni nei rami verticali sono associati allo stato $|1\rangle$.

Un fascio/fotone che incide in un *beam splitter* viene "diviso" nei due rami con probabilità del 50%. Lo specchio trasforma i fotoni "orizzontali" in fotoni "verticali". Quindi possiamo fare l'associazione con porte le logiche quantistiche

1. il *beam splitter* è associato ad una porta di Hadamard H .
2. lo specchio è associato ad una porta X (NOT).

Con queste notazioni abbiamo che la dinamica dell'interferometro in Fig. 26 (a) è

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{X} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{H} |0\rangle. \quad (9.2.1)$$

Come si vede, il fotone finale esce dall'interferometro orizzontalmente ed è quindi assorbito (misurato) sempre dal detector 1. Si noti inoltre che gli specchi (porte

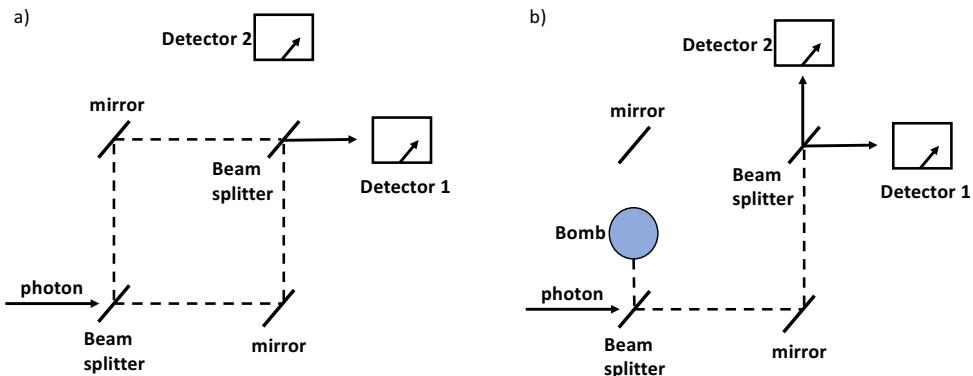


Figure 26: a) Un interferometro costituito da due *beam splitter* e due specchi riflettenti. I bracci dell'interferometro sono costruiti in modo tale che i fotoni arrivino solo al detector 1. b) Lo stesso interferometro in cui è stato posto un oggetto in uno dei bracci. L'oggetto assorbe tutti i fotoni passanti lungo la traiettoria. Questo distrugge il fenomeno di interferenza fra i due percorsi e di conseguenza i fotoni che arrivano al secondo *beam splitter* sono misurati da entrambi i detector.

logiche X) non hanno effetto sullo stato visto che lo stato $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ è autostato (con autovalore 1) dell'operatore X.

Adesso supponiamo che un oggetto assorbente venga posto nel ramo verticale come mostrato in figura 26 (b). Il fotone incidente sul primo *beam splitter* andrà la metà delle volte nel ramo orizzontale e l'altra metà nel ramo verticale. Questi ultimi varranno assorbiti mentre quelli nel ramo orizzontale invece verranno riflessi e poi "divisi" dal secondo *beam splitter*. In questo caso però non ci sarà interferenza con il fotone del ramo verticale dato che questo è stato assorbito. Quindi il fotone incidente sul secondo *beam splitter* potrà essere assorbito sia dal detector 1 che dal detector 2 come mostrato in Fig. 26 (b).

Possiamo anche stimare con che probabilità i fotoni verranno assorbiti dai detector. Il 50% dei fotoni verranno assorbiti dopo il passaggio attraverso il primo *beam splitter*. Della metà passanti nel ramo inferiore, la metà varrà deviata e assorbita dal detector 1 e l'altra metà dal detector 2 (per un totale del 25% in entrambi i casi). Concludiamo che

1. il 25% delle volte si attiverà il detector 1.
2. il 25% delle volte si attiverà il detector 2 .
3. il 50% nessun detector si attiverà .

Notiamo che la differenza fra le due situazioni descritte in Fig. 26, sta nella possibilità di misurare dei fotoni con il detector 2. Questo avviene con probabilità 0.25 se l'oggetto assorbente è presente e non può avvenire quando è assente. Concludiamo che, se un fotone (passando nel ramo inferiore) viene successivamente

misurato dal detector 2, siamo sicuri che ci sia un oggetto assorbente senza che il fotone abbia interagito con esso¹.

Possiamo vedere questo fenomeno a livello più preciso introducendo un terzo stato $|a\rangle$ che rappresenta il fotone assorbito. Il fenomeno in Fig. 26 (b) sarà

$$\begin{aligned} |0\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{\text{assorbimento}} \frac{1}{\sqrt{2}}(|0\rangle + |a\rangle) \\ &\xrightarrow{X} \frac{1}{\sqrt{2}}(|1\rangle + |a\rangle) \xrightarrow{H} \frac{1}{2}(|0\rangle - |1\rangle) + \frac{1}{\sqrt{2}}|a\rangle \end{aligned} \quad (9.2.2)$$

Si noti che le porte X e H agiscono solo sullo stato $|0\rangle$ e 1 dato che non ha senso applicarle al fotone assorbito. Se vengono misurati i fotoni in direzione orizzontali (dal detector 1) e quelli in direzione verticale (dal detector 2), avremo

1. Probabilità 0.25 di misurare $|0\rangle$ con il detector 1.
2. Probabilità 0.25 di misurare $|1\rangle$ con il detector 2.
3. Probabilità 0.5 di non misurare niente con i detector (lo stato $|a\rangle$ non è misurabile con i detector).

Notiamo che la differenza fra le due situazioni descritte in Fig. 26, sta nella possibilità di misurare dei fotoni con il detector 2. Questo avviene con probabilità 0.25 se l'oggetto assorbente è presente e non può avvenire quando è assente. Esattamente quello che ci aspettavamo dalla discussione più fenomenologica dell'esperimento.

III – BOMB DETECTOR

Per rendere più evidente quanto questo risultato sia controintuitivo, Elitzur e Vaidman proposero di usarlo in una situazione pratica.

Supponiamo di avere un certo numero di bombe che vengono attivate da un detector di fotoni. Se il detector è rotto e la bomba risulta inattiva.

Problema: Vogliamo sapere quali bombe sono attive senza farle esplodere.

Classicamente il problema non è risolvibile. Infatti, l'unico modo per sapere se una bomba è attiva è mandare un fotone ma questo farebbe esplodere la bomba.

Il problema è (parzialmente) risolvibile usando la meccanica quantistica e l'esperimento discusso. Se la bomba è inattiva i fotoni che passano nel ramo verticale dopo il primo *beam splitter* non interagiscono con il detonatore e continuano senza interagire. La bomba inattiva coincide quindi con la situazione in fig. 26 (a) e, a causa dell'interferenza, solo il detector 1 misurerà i fotoni.

Se la bomba è attiva, il 50% delle volte il fotone passerà nel ramo verticale, verrà assorbito e farà esplodere la bomba. In questi casi il nostro protocollo fallisce dato che la bomba era attiva ma esplode durante il controllo.

¹ Da qui la terminologia usata del lavoro originale: *interaction-free measurement*.

Il restante 50% delle volte il fotone passerà nel ramo orizzontale e da qui (dopo il *beam splitter*) sarà misurato dal detector 1 nel 25% dei casi e nel rimanente 25% dei casi dal detector 2. Se il detector 1 misura il fotone non abbiamo alcuna informazione sulla bomba; infatti, avremmo lo stesso segnale dal detector 1 sia in presenza di una bomba inattiva che in presenza di una bomba attiva.

La discriminazione può avvenire quando è il detector 2 che misura il fotone. Infatti, in questo caso, una bomba attiva non attiverebbe mai questo detector. Concludiamo che, se il detector 2 riceve un fotone, la bomba è attiva. Si noti che però il fotone non ha interagito con la bomba dato che è passato nel ramo orizzontale.

Per quanto sorprendente questo fatto è naturale nella meccanica quantistica ed è simile a quello visto nell'esperimento della doppia fenditura in sec. 3.1.1. Infatti, gli stati quantistici sono descritti da funzioni d'onda; tralasciando per un momento la precisione nel linguaggio, possiamo dire che queste, come le onde nei sistemi fisici, sono "non-locali" e una perturbazione in una parte della funzione d'onda genera o distrugge l'interferenza.

9.3.1 Estensione e miglioramento

Nel caso discusso fino ad ora, il 50% delle volte la bomba esplode, 25% la bomba non esplode ma non abbiamo informazione utile e solo il restante 25% riusciamo ad sapere che la bomba è attiva senza farla esplodere. Sebbene questi risultati siano sorprendenti e migliori di quanto non si possa fare classicamente non sono soddisfacenti in termini assoluti. La domanda naturale è se si può fare meglio. Seguendo la referenza [Kwiat1995] mostreremo che la risposta è affermativa.

Supponiamo di fare due modifiche all'interferometro in Fig. 26. La prima è nei *beam splitter* che possono essere costruiti in modo tale che la maggior parte dei fotoni passi nel ramo orizzontale e soli pochi nel ramo verticale.

A livello formale, questo significa che non avremo più un operatore di Hadamard associato al *beam splitter* ma un generico operatore di rotazione scrivibile come

$$U_{BS}(\theta) = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}. \quad (9.3.1)$$

nella base $\{|0\rangle, |1\rangle\}$. Si noti che per $\theta = \pi/4$, otteniamo la matrice di Hadamard.

La matrice $U_{BS}(\theta)$ è una matrice di rotazione di un angolo θ nello spazio $\{|0\rangle, |1\rangle\}^2$.

La seconda modifica da apportare all'interferometro è di non misurare i fotoni dopo un passaggio ma riprendere i fotoni e farli passare attraverso N *beam splitter* prima di misurarli³. Indipendentemente dalla struttura fisica utilizzata, questo equivale ad applicare l'operatore $U_{BS}(\theta)$ e quindi indurre una rotazione di un angolo $N\theta$.

² Si veda, ad esempio, https://en.wikipedia.org/wiki/Rotation_matrix.

³ Questo può essere fatto utilizzando una sequenza di *beam splitter* oppure prendendo il fotoni nei due rami e, con delle fibre ottiche, reindirizzarli verso il *beam splitter* iniziale.

Supponiamo quindi che la bomba sia inattiva e di applicare $U_{BS}^N(\theta)$. Avremo

$$|0\rangle \xrightarrow{U_{BS}(\theta)} \cos \theta |0\rangle + \sin \theta |1\rangle \xrightarrow{U_{BS}(\theta)} \dots \xrightarrow{U_{BS}(\theta)} \cos(N\theta) |0\rangle + \sin(N\theta) |1\rangle \quad (9.3.2)$$

A questo punto si vede che se sceglieremo $\theta = \pi/(2N)$, lo stato finale sarà $|1\rangle$ e solo un detector misurerà i fotoni.

Supponiamo adesso che la bomba sia attiva. Dopo il primo passaggio attraverso il *beam splitter*, il fotone nel ramo verticale (stato $|1\rangle$) verrà assorbito. Come sopra, descriviamo questo effetto introducendo la trasformazione $|1\rangle \rightarrow |\alpha\rangle$ dovuta all'assorbimento. Il primo passaggio sarà

$$|0\rangle \xrightarrow{U_{BS}(\theta)} \cos \theta |0\rangle + \sin \theta |1\rangle \xrightarrow{\text{assorbimento}} \cos \theta |0\rangle + \sin \theta |\alpha\rangle \quad (9.3.3)$$

Come visto sopra la seconda applicazione del *beam splitter* cambierà solo i fotoni negli stati $|0\rangle$ e $|1\rangle$. Avremo quindi

$$\begin{aligned} \cos \theta |0\rangle + \sin \theta |\alpha\rangle &\xrightarrow{U_{BS}(\theta)} \cos \theta (\cos \theta |0\rangle + \sin \theta |1\rangle) + \sin \theta |\alpha\rangle \\ &\xrightarrow{\text{assorbimento}} \cos^2 \theta |0\rangle + (\cos \theta \sin \theta + \sin \theta) |\alpha\rangle \end{aligned} \quad (9.3.4)$$

L'effetto di aver applicato due *beam splitter* (seguiti dall'assorbimento) è di avere lo stato del fotone $|0\rangle$ (quello che è ancora nella fibra ottica o nell'interferometro) con un'ampiezza di probabilità di $\cos^2 \theta$. Questo fissa attraverso la normalizzazione anche il coefficiente dello stato assorbito $|\alpha\rangle$.

Estendendo questa osservazione al caso di N applicazioni del *beam splitter*, otterremo lo stato

$$|0\rangle \xrightarrow{U_{BS}^N(\theta)} \cos^N \theta |0\rangle + (\dots) |\alpha\rangle \quad (9.3.5)$$

Per $N \gg 1$ e ricordando che abbiamo scelto $\theta = \pi/(2N)$, la probabilità di misurare $|0\rangle$ è

$$\cos^{2N} \theta = \left[\cos \left(\frac{\pi}{2N} \right) \right]^{2N} \approx \left[1 - \left(\frac{\pi}{2N} \right)^2 \right]^{2N} \approx 1 - \frac{\pi^2}{8N} \quad (9.3.6)$$

Quindi, in presenza della bomba attiva, la probabilità di misurare $|0\rangle$ si approssima a 1 se prendiamo θ sufficientemente piccolo e N (il numero di *beam splitter*) sufficientemente grande.

Riassumendo per N grande, se la bomba non è attiva misureremo $|1\rangle$ (con certezza) mentre se la bomba è attiva misureremo $|0\rangle$ con una probabilità prossima a 1. Questo schema ci permette quindi di distinguere fra i due casi senza far esplodere la bomba.

Questo schema migliorato è stato proposto e verificato sperimentalmente da ricercatori austriaci e statunitensi [Kwiat1995]. Lo schema ottico usato è presentato in figura 27. L'idea è quella di far passare il fotone in una serie di *beam splitter* (rappresentati nella zona centrale delle figure) e di specchi (posti superiormente e inferiormente nelle figure).

In figura 27 a) è mostrato il set-up sperimentale in cui il singolo *beam splitter* fa passare nel ramo superiore dell'interferometro pochi fotoni che nella mag-

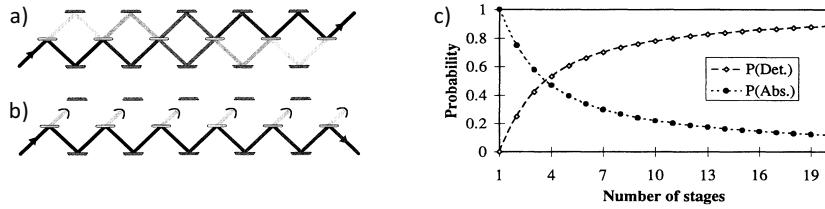


Figure 27: a) Un interferometro costituito da due *beam splitter* e due specchi riflettenti. I bracci dell'interferometro sono costruiti in modo tale che i fotoni arrivino solo al detector 1. b) Lo stesso interferometro in cui è stato posto un oggetto in uno dei bracci. L'oggetto assorbe tutti i fotoni passanti lungo la traiettoria. Questo distrugge il fenomeno di interruzione fra i due percorsi e di conseguenza i fotoni che arrivano al secondo *beam splitter* sono misurati da entrambi i detector.

gior parte dei casi vengono riflessi verso il basso. Sebbene l'effetto del singolo *beam splitter* sia piccolo, la successione unita agli effetti di interruzione fanno uscire il fotone verso il ramo superiore.

Lo schema in figura 27 b) rappresenta il caso in cui sia presente la bomba. Questa è descritta da un detector che assorbe i fotoni che, attraversando il *beam splitter*, passano nel ramo superiore dell'interferometro. In questo caso, dopo la successione di interferometri, il fotone esce dal ramo inferiore.

La figura 27 c) rappresenta i risultati sperimentali ottenuti in funzione del numero di interferometri usati. Le funzioni $P(\text{Det.})$ e $P(\text{abs.})$ sono rispettivamente la probabilità di ottenere informazione senza interagire con l'oggetto e la probabilità che il fotone venga assorbito. Come si può vedere, all'aumentare del numero di interferometri si riduce la probabilità di assorbimento del fotone mentre si riesce ad ottenere informazione (con probabilità crescente).