4 INFORMAZIONE QUANTISTICA (ESEMPI DI BASE)

1 — 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,

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

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 $x_1x_2...x_n$ con $x_i = 0, 1$ e $i = 0, 1, ..., n$ tale che $x = x_1 2^{n-1} + x_2 2^{n-2} + ... + x_n 2^0$ (sec. 1.2 e [**nielsen-chuang_book**]). In maniera analoga, a livello quantistico useremo n qubit e assoceremo 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 quanstico 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

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

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

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

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 $|00...0\rangle$ e applicheremo n porte di Hadarmard $H^{\otimes n}$.

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

Nell'ultimo passaggio abbiamo definito $N = 2^n$ e siamo passati dalla notazione in termini di stringhe logiche (es. 0100...11) 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

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} U|x\rangle\,. \tag{4.1.5}$$

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 (Deutch, Deuthc-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 si 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 Impossibilitá di copiare stati quantistici (Teorema *no-cloning*)

Una delle operazioni fondamentali nei computer classici è quella di copiatura. Data una stringa di bit $x \equiv x_1 x_2 .... x_n$ è possibile copiarla un numero arbitrario di volte. É 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'indetità). Se il bit di controllo è acceso ($|1\rangle$) applicheremo una porta NOT al secondo. Di conseguenza, i qubit si trasformano come $|00\rangle \to |00\rangle$ e $|10\rangle \to |11\rangle$ e lo stato iniziale

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

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

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

Gli stati in Eq. (4.2.1) e (4.2.2) sono diversi perchè nel primo mancano i termini $|01\rangle$ e $|01\rangle$. 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 esista 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

$$|\psi s\rangle \xrightarrow{U_{COPY}} U_{COPY}\,|\psi s\rangle = |\psi\psi\rangle \tag{4.2.3}$$

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

$$|\varphi s\rangle \xrightarrow{U_{COPY}} = U_{COPY}\,|\varphi s\rangle = |\varphi\varphi\rangle \tag{4.2.4}$$

Se prendendo il prodotto scalare degli stati finali abbiamo

$$\langle\varphi s|\,U^{\dagger}_{COPY}U_{COPY}\,|\psi s\rangle = \langle\varphi s|\psi s\rangle = \langle\varphi|\psi\rangle\,\langle s|s\rangle = \langle\varphi|\psi\rangle \tag{4.2.5}$$

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

$$\langle\varphi|\psi\rangle = (\langle\varphi|\psi\rangle)^2. \tag{4.2.6}$$

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 Impossibilitá 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

$$|\psi\rangle_A |\psi\rangle_B |A\rangle_C \to U |\psi\rangle_A |\psi\rangle_B |A\rangle_C = |\psi\rangle_A |0\rangle_B |A'\rangle_C . \tag{4.2.7}$$

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 $|A'\rangle_C$.

É 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

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

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

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

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

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

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

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

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

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

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

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

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)]

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

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)

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

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 sui 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 eslpicito questo ragionamento astratto se Bob applica in sequeza una porta CNOT e una porta di Hadarmard al primo qubit. Sui qubit di sopra otterniamo

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

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 teletrasposto 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)]

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

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 $|\beta_{00}\rangle$

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

dove i primi due ket vanno intesi come di Alice mentre l'ultimo è quello di Bob; ovvero,i ket vanno intesi come $|0\rangle(|00\rangle = |0\rangle_A|0\rangle_A|0\rangle_B$ 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 $|100\rangle \to |110\rangle$ e $|111\rangle \to |101\rangle$. Lo stato viene trasformato in

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

Successivamente Alice applica una porta di Hadamard al primo qubit ottenendo

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

Questo può essere riscritto come

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

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

$$\begin{aligned}
&00 \text{ misura Alice} \quad \longrightarrow \quad \alpha|0\rangle + \beta|1\rangle \text{ stato Bob}\\
&01 \text{ misura Alice} \quad \longrightarrow \quad \alpha|1\rangle + \beta|0\rangle \text{ stato Bob}\\
&10 \text{ misura Alice} \quad \longrightarrow \quad \alpha|0\rangle - \beta|1\rangle \text{ stato Bob}\\
&11 \text{ misura Alice} \quad \longrightarrow \quad \alpha|1\rangle - \beta|0\rangle \text{ stato Bob}
\end{aligned} \tag{4.4.6}$$

Ognuno di queste misure capita con probabilità di 1/4. Quindi Bob con probabilità 1/4 riceveà 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 perchè 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 otterrebbe [3] 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 qualè 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

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

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

Queste però sono le probabilità che Bob avrebbe ottenuto prima che Alice manipolasse i sui 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 perchè 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 riportare 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 $f(x) : \{0,1\} \to \{0,1\}$, ovvero la funzione riceve un bit di input 0 o 1 e dà un bit fi 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 possibiltà 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

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

A questo punto, dobbiamo introdurre l'informazione sulla funzione f. Questo averrà tramite un operatore unitario che denotiamo con U_f. É conveniente trattare l'operatore U_f in modo generico anche perchè 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 $|x, y\rangle \to |x, y \oplus f(x)\rangle$. L'addizione modulo 2 da come risultato $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$ e $1 \oplus 1 = 0$. É 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 $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2} = |x\rangle|-\rangle$. Notiamo che

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

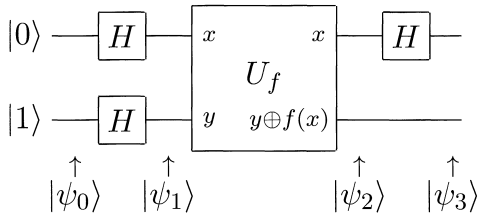

Figure 16: Schema di porte logiche quantistiche per l'algoritmo di Deutch.

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

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

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

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

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 *constante* 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

$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle . \tag{4.5.10}$$

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

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{4.5.11}$$

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

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{4.5.12}$$

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

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

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 $|x\rangle \equiv |x_1, x_2, x_3, ..., x_n\rangle$. Sul singolo qubit $|x_i\rangle$ la porta di Hadarmard agirà come in Eq. (4.5.13) con la sostituzione $k \to x_i$. Estendendo questo ragionamento a tutti gli n qubit abbiano

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

che può essere riscritta in forma compatta come

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

dove $x \cdot z$ è i 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

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

In questa equazione, il termine più importante è quello associato alla stringa con tutti i bit nulli: $|0\rangle \equiv |0, 0, ..., 0\rangle$. 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 constante 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 $f(x) = \bar{f}$)

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

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 constante, 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 $0, 0, 0, ..., 0$.

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

$$\sum_{x=0}^{N-1} \frac{(-1)^{f(x)}}{N} = \Big(\sum_{f(x)=0} \frac{1}{N} \Big) - \Big(\sum_{f(x)=1} \frac{1}{N} \Big) = \frac{1}{N} \Big(\frac{N}{2} - \frac{N}{2} \Big) = 0 \tag{4.5.18}$$

dove nelle somme abbiamo indicato che sono sugli elementi tale che $f(x) = 0$ o $f(x) = 1$. Quindi è zero e lo stato $|0\rangle \equiv |0, 0, ..., 0\rangle$ non comparirà in $|\psi_2\rangle$ e una misura dei primi n qubit darà una qualsiasi stringa tranne $0, 0, 0, ..., 0$. 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 constate. 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 funzione bilanciata 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 $f_a(x) = x \cdot a = x_1a_1 + x_2a_2 + ... + x_na_n$ 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

$$\begin{aligned} |\psi_2\rangle &= \sum_{x=0}^{N-1}\sum_{z=0}^{N-1} \frac{(-1)^{x\cdot z + x\cdot a}}{N} |z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \sum_{x=0}^{N-1}\sum_{z=0}^{N-1} \frac{(-1)^{(z\oplus a)\cdot x}}{N} |z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ &= \sum_{z=0}^{N-1} \Big(\sum_{x=0}^{N-1} \frac{(-1)^{(z\oplus a)\cdot x}}{N} \Big) |z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \sum_{z=0}^{N-1} \chi_z |z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \end{aligned} \tag{4.5.19}$$

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 $\chi_z = \sum_{x=0}^{N-1} \frac{(-1)^{(z\oplus a)\cdot x}}{N}$ 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 $z_i = a_i$, $z_i + a_i (\mathrm{mod}\ 2) = 0$ dato che $0 + 0 (\mathrm{mod}\ 2) = 0$ e $1 + 1 (\mathrm{mod}\ 2) = 0$. Quindi in questo

caso, la stringa di bit risultante sarà $z + a = 000...0$. 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

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

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 coeffiecienti devono essere annullarsi $\chi_{z\neq a} = 0$. Possiamo quindi scrivere in modo compatto $\chi_z = \sum_{x=0}^{N-1} \frac{(-1)^{(z\oplus a)\cdot x}}{N} = \delta_{z,a}$ [7].

Tornando all'Eq. (4.5.19) abbiamo che

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

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

$$f : \{0,1\}^n \to \{0,1\}^n. \tag{4.5.22}$$

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 possibiltà 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 $x \oplus y = x \oplus x \oplus a$. Conside-

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 domostrare **[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 addizional $|\psi_0\rangle = |0\rangle^{\otimes n} |0\rangle^{\otimes n}$ e di applicare N porte di Hadamard ai primi n qubit. Otterremo

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

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 $|0 \oplus f(x)\rangle = |f(x)\rangle$)

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

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

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

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 *sovrapposizione*

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

riamo il bit i-esimo del secondo membro. Per le proprietà dell'operatore XOR (sec. 1.1), abbiamo x_i XOR x_i XOR $a_i = (x_i$ XOR $x_i)$ XOR $a_i = 0$ XOR a_i. Se $a_i = 1$, 0 XOR $a_i = 1 = a_i$. Se $a_i = 0$, 0 XOR $a_i = 0 = a_i$. Da cui concludiamo che x_i XOR x_i 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

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

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 $\left[1-1\right] = 0$. Al contrario, se $a \cdot y = 0$, il coefficiente dello stato $|y\rangle$ è $\left[1+1\right] = 1$. Quindi nella somma precedente sono presenti solo gli stati $|y\rangle$ tali che $a \cdot y = 0$. La possiamo riscrivere come

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

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

La misura dei rimanenti n qubit, darà una stringa y tale the $a \cdot y = 0$. 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 $y_2, y_3, ..., y_n$ tali che $a \cdot y_i = 0$ per $i = 1, ..., n$. Con questi y_i possiamo risolvere il sistema di equazioni

$$\begin{aligned} a \cdot y_1 &= 0 \\ a \cdot y_2 &= 0 \\ &\vdots \\ a \cdot y_n &= 0 \end{aligned} \tag{4.5.29}$$

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.