



# APPUNTI PER ORALE

## ▼ STATI ENTANGLED

Considero sistema a due qubit descritto dal prodotto tensore di due spazi vettoriali  $V \otimes W$

$$|v\rangle_V \otimes |w\rangle_W$$

Questo è uno stato separabile in quanto una misura al primo qubit non influenza il secondo e viceversa

Un sistema **entangled** è tale quando due qubit sono fortemente correlati; la misura di uno influenza l'altro qubit.

Uno stato entangled, **non essendo fattorizzabile**, la **misura sul sistema  $V$  influenza anche il sistema  $W$** .

## Stati di Bell

Sono stati entangled molto importanti:

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

Gli stati di Bell costituiscono una base ortonormale nello spazio a due qubit.

Per descrivere il sistema posso usare la base canonica  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$  oppure la base di Bell  $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$

## ▼ TRASFORMAZIONI UNITARIE

In meccanica quantistica le sole trasformazioni ammissibili sono unitarie ovvero

- lineari
- invertibili: lascia invariati i prodotti scalari e quindi anche la norma dei vettori

## Porte quantistiche

Ovvero trasformazioni unitarie che possono essere implementate fisicamente.

### Trasformazioni di Pauli

Identità, X, Y e Z:

$$\begin{array}{ll}
Id|0\rangle := |0\rangle & Id|1\rangle := |1\rangle \\
X|0\rangle := |1\rangle & X|1\rangle := |0\rangle \\
Y|0\rangle := -i|1\rangle & Y|1\rangle := i|0\rangle \\
Z|0\rangle := -|0\rangle & Z|1\rangle := |1\rangle
\end{array}$$

$$\begin{aligned}
Id &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
X &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\
Y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\
Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}
\end{aligned}$$

Nella base canonica:

- **X** corrisponde al not classico
- **Z** genera un cambio della fase relativa
- **Y** può essere visto come una combinazione dei precedenti

## Trasformazione di Hadamard

Opera su singolo qubit:

$$H|0\rangle = |+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$$

$$H|1\rangle = |-\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

## C-NOT

Opera su due qubit:

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

Cambiando base (ad esempio utilizzando  $|\pm\rangle$ ) il risultato della CNOT non cambia, utilizza il primo qubit come controllo sul secondo.

CNOT può generare entanglement, posso farlo con prodotto tensore tra un qubit + e 0 e poi metterli in porta CNOT; il + come controllo sullo 0. A questo punto ho ottenuto lo stato entangled

## Inizializzazione di un qubit

Serve porta **Hadamard** e **phase gate** che lascia invariato 0 e cambia la fase allo stato 1 che diventa  $e^{i\gamma}|1\rangle$

### ▼ TEOREMA NO-CLONING

## *L'impossibilità di copiare stati quantistici*

Una delle operazioni fondamentali dei computer classici che non è possibile realizzare sui computer quantistici è quella di copiatura.

Inizialmente si pensava che realizzare una porta capace di copiare un qubit fosse possibile in quanto il NOT controllato, CNOT, sembrava fare proprio questo.

Preso infatti un qubit  $|\Psi\rangle = a|0\rangle + b|1\rangle$  e un qubit  $|0\rangle$  se proviamo ad applicare il CNOT usando come bit di controllo quelli di  $|\Psi\rangle$  e come target quelli di  $|0\rangle$  sembra effettivamente di fare un'operazione di copiatura dei qubit, il risultato infatti è  $a|00\rangle + b|11\rangle$ .

Tuttavia la meccanica quantistica spesso e volentieri ci permette di lavorare con stati più ricchi di quelli presi come esempio, e pertanto la porta CNOT ci permette di effettuare un'operazione di copiatura solo in casi particolari.

La domanda sull'esistenza di una porta più complessa che permetta effettivamente di copiare i qubit tuttavia può sorgere, **ma la risposta è che se lo stato da copiare è sconosciuto non è possibile copiarlo**, e questo è conosciuto come teorema del no-cloning

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

Questo teorema porta vantaggi e svantaggi poiché da un lato priva i computer quantistici di una delle operazioni fondamentali e anche più semplici della computazione classica, d'altro canto però apre innumerevoli porte nel campo della crittografia e della sicurezza, in quanto rende impossibile intercettare le informazioni spedite.

Pertanto il teorema del no cloning possiamo affermare che sia alla base della crittografia quantistica.

## *È come fare uno screenshot ad un video*

### ▼ TEOREMA NO-DELETING

## Ovvero l'impossibilità di distruggere stati quantistici

Deriva dal teorema no-cloning.

Vorremmo poter eliminare l'informazione su un qubit utilizzando delle trasformazioni **non necessariamente unitarie**. Per fare questo ci servirebbe una macchina con un proprio stato interno.

$$|\Psi\rangle_A |\Psi\rangle_B |A\rangle_C \rightarrow \mathcal{U} |\Psi\rangle_A |\Psi\rangle_B |A\rangle_C = |\Psi\rangle_A |0\rangle_B |A'\rangle_C$$

Dalla dimostrazione fatta a lezione, l'operatore  $\mathcal{U}$  dovrebbe poter cancellare le informazioni sullo stato di B ma questo non è possibile in quanto cancellando lo stato di B in realtà si andrebbe soltanto a “spostare” l'informazione nello stato interno della macchina di cancellazione C.

## ▼ SUPER DENSE CODING

Supponiamo che Alice e Bob si vogliono scambiare **due bit** di informazione.

Nel caso classico Alice dovrebbe spedire i due bit separatamente.

Nel caso quantistico è possibile codificare i due bit classici in un unico qubit quantistico con all'interno l'informazione originale.

Alice e Bob devono **condividere uno stato entangled**. Alice avrà un qubit e Bob avrà l'altro.

Le possibili combinazioni di due bit sono 4: 00, 01, 10 e 11

Il protocollo di comunicazione del super dense coding definisce **porte logiche da applicare allo stato quantistico** in base ai bit che si vogliono trasmettere.

In base alla combinazione di due bit che A vuole trasmettere a B, **Alice applica una determinata porta** al suo qubit **dopodiché lo invia a Bob**.

Bit da inviare	Porta applicata da A	Stato di Bob
00	$\mathbb{I}$	$\frac{( 0\rangle_B \otimes  0\rangle_B +  1\rangle_B \otimes  1\rangle_B)}{\sqrt{2}}$
01	$\mathbb{X}$	$\frac{( 0\rangle_B \otimes  0\rangle_B -  1\rangle_B \otimes  1\rangle_B)}{\sqrt{2}}$
10	$\mathbb{Z}$	$\frac{( 1\rangle_B \otimes  0\rangle_B +  0\rangle_B \otimes  1\rangle_B)}{\sqrt{2}}$
11	$i\mathbb{Y}$	$\frac{( 0\rangle_B \otimes  1\rangle_B -  1\rangle_B \otimes  0\rangle_B)}{\sqrt{2}}$

nota: gli stati ottenuti rappresentano i quattro stati ortogonali di Bell, che quindi possono essere distinti con una misura.

Ora Bob ha entrambi i qubit. Gli basta applicare una porta CNOT seguita da un Hadamard per ottenere i due bit che Alice voleva trasmettergli.



La potenza del protocollo super dense coding sta nell'inviare la metà di informazione. Alice manda un solo qubit per spedire due bit di informazione classica.

## ▼ TELETRASPORTO QUANTISTICO

Consiste nel trasferire informazione da uno stato ad un altro.

Classicamente per trasferire informazioni è sufficiente prendere il valore di uno o più bit e replicarlo/i in un altro, mentre quantisticamente occorre utilizzare due qbit entangled.

Alice deve inviare un qbit (messaggio) a Bob, entrambi condividono uno stato entangled. Per mandare questo qbit, Alice applica una CNOT e una H al qbit da inviare insieme a quello entangled, in questo modo, istantaneamente il qbit di Bob cambierà stato, ottenendo una sovrapposizione di tutti i possibili stati, tutti con 1/4 di possibilità.

A questo punto Alice può fare una misura sui due qbit per ottenere due bit classici.

Questi bit andranno comunicati a Bob per mezzo di un canale di trasmissione classico (Salvo la relatività speciale) e indicheranno le porte che deve applicare al suo qbit per ricostruire lo stato che voleva mandare Alice.

bit (Misura Alice)	Stato qbit Bob	Porta da applicare	Stato ottenuto (msg Alice)
00	$\alpha 0\rangle + \beta 1\rangle$	$\mathbb{I}$	$\alpha 0\rangle + \beta 1\rangle$
01	$\alpha 0\rangle + \beta 1\rangle$	$X$	$\alpha 0\rangle + \beta 1\rangle$
10	$\alpha 0\rangle - \beta 1\rangle$	$Z$	$\alpha 0\rangle + \beta 1\rangle$
11	$\alpha 1\rangle - \beta 0\rangle$	$iY/XZ$	$i(-i\alpha 0\rangle - i\beta 1\rangle) = \alpha 0\rangle + \beta 1\rangle (i^2 = -1)$

La teoria della **relatività speciale di Einstein si salva** in quanto, è vero che lo stato di Bob cambia istantaneamente, ma se andasse a misurarlo otterrebbe il collasso in uno stato casuale visto che tutti hanno la stessa probabilità, inoltre Bob non sa quando Alice ha applicato le porte ai suoi qbit quindi dovrà attendere che gli arrivi un messaggio classico.

Anche il **no cloning theorem è salvo** perchè quando Alice fa la misura, questa va a far collassare la funzione d'onda dei qbit e di conseguenza lo stato iniziale verrà perso.

## ▼ DEUTSCH

*Algoritmo per verificare in una sola esecuzione se una funzione è costante o è bilanciata*

Utilizza il parallelismo quantistico e l'interferenza per avere notevoli vantaggi sui metodi computazionali classici.

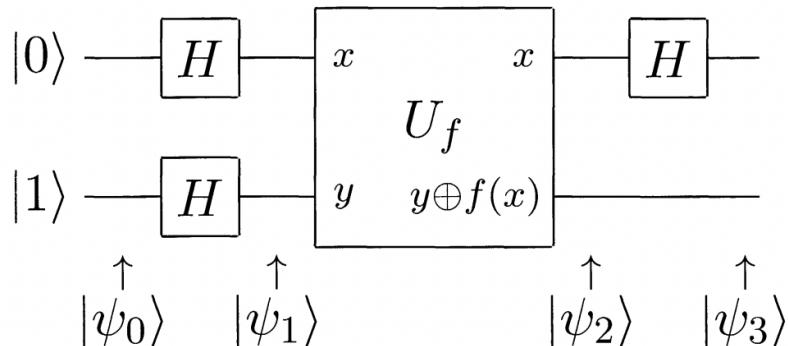
Una funzione si dice costante se  $f(0) = f(1)$  e bilanciata altrimenti.

Classicamente sarebbero necessarie due chiamate alla funzione per determinare tali proprietà, sondando tutto lo spazio degli input.

Quantisticamente invece basta una sola chiamata.

Prendendo infatti due qubit  $|\Psi_0\rangle = |01\rangle$  in input e applicando la Hadamard a entrambi otteniamo una sovrapposizione di tutti gli input.

A questo punto applica  $U_f$  che presi due qubit  $|x, y\rangle$  restituisce  $|x, y \oplus f(x)\rangle$ .



Dopo un serie di calcoli ci accorgeremo che **se la funzione è costante**

$$(-1)^{f(0)} + (-1)^{f(1)} = 2 \quad \text{e} \quad (-1)^{f(0)} - (-1)^{f(1)} = 0 .$$

se è bilanciata invece

$$(-1)^{f(0)} + (-1)^{f(1)} = 2 \quad \text{e} \quad (-1)^{f(0)} - (-1)^{f(1)} = \pm 2 .$$

Quindi la misura del primo qubit ci permetterà di distinguere se la funzione è costante ( misuriamo  $|0\rangle$  ) o è bilanciata ( misuriamo  $|1\rangle$  ).

L'algoritmo di deutsch permette di migliorare l'algoritmo classico sfruttando il parallelismo quantistico, in quanto quando applichiamo  $U_f$  la stiamo testando parallelamente sui bit logici 1 e 0. E poi grazie all'interferenza l'informazione sulla funzione viene immagazzinata nella fase globale, infatti se la funzione è costante non acquista nessuna fase, se è bilanciata lo stato del primo qubit acquista una fase pari a  $e^{i\pi} = -1$ .

## ▼ DEUTSCH-JOZSA

Evoluzione dell'algoritmo di Deutch che permette di capire se la funzione oracolo è costante o bilanciata chiamandola ogni volta con una stringa di n bit.

Quindi Alice sceglie un numero compreso tra 0 e  $2^n - 1$  cioè il numero massimo rappresentabile con n bit e Bob risponde con un bit.

Nella soluzione classica l'unica soluzione è sondare piano piano lo spazio e sperare di trovare due output diversi in modo da capire subito che è bilanciata, nel caso peggiore però, Alice, dovrà effettuare  $\frac{2^n}{2} + 1$  chiamate cioè metà dello spazio più 1.

Il corrispettivo quantistico, invece, permette di scoprire se l'oracolo è bilanciato o costante con una sola chiamata e utilizzando n qbit.

Per funzionare questi qbit vengono messi in una sovrapposizione tra  $|0\rangle$  e  $|1\rangle$  al 50% in modo da poter sondare tutto lo spazio disponibile, per farlo applichiamo Hadamard a tutti i qbit che abbiamo.

A questo punto possiamo chiamare la funzione che dovrà essere opportunamente modificata per poter funzionare con dei qbit. Questa funzione non farà altro che modificare o meno la fase (cosa che possiamo misurare riapplicando Hadamard) e facendo collassare il qbit in  $|0\rangle$  o  $|1\rangle$ . A questo punto se misuriamo  $|0\rangle$  sapremo che la funzione è costante, altrimenti è bilanciata.

## ▼ BERNSTEIN-VAZIRANI

*Abbiamo una stringa x e facciamo il prodotto bit a bit con una stringa ignota a, il nostro obiettivo è trovare a*

Classicamente avremmo bisogno di n chiamate mentre quantisticamente abbiamo bisogno di una sola chiamata all'oracolo pertanto abbiamo uno speed-up polinomiale.

N chiamate perchè prendo gli n bit e li metto tutti a zero tranne 1 e questo lo vado a spostare di volta in volta.

Es n=4 → 1000/0100/0010/0001

Applico H ha tutti i qbit inizializzati a 0 in modo da creare sovrapposizione poi chiamo la funzione oracolo, riapplico H e vado a misurare tutti i qbit ottenendo la stringa s.

La sequenza di operazioni logiche è la stessa dell'algoritmo di Deutsch-Jozsa ma in questo caso l'oracolo ( funzione ) non aggiunge una fase globale  $(-1)^{f(x)}$  ma una fase  $(-1)^{x \cdot a}$ .

Infatti dove prima in D-J avevamo  $|\psi 2\rangle$ , ovvero il risultato dell'applicazione di  $U_f$  a  $|\psi 1\rangle$ , questo aveva come esponenti  $x * z + x * a$ , mentre adesso avrà  $(z \oplus a) * x$  che sfrutta le proprietà degli operatori bit a bit.

Quindi se  $z = a$  avremo vuol dire che le stringhe avranno tutti gli n bit uguali e per l'i-esimo bit dovremo calcolare  $z_i + a_i \pmod{2}$  ovvero  $z_i \text{ XOR } a_i$ .

ma dato che lo stato  $|z\rangle$  deve essere normalizzato, se  $X_{z=a} = 1$  allora tutti gli altri coefficienti devono annullarsi  $X_{z \neq a} = 0$ , quindi una misura dei primi qubit logici restituirà lo stato  $|a\rangle$  con probabilità 1.

La cosa davvero importante è che la fase che introduciamo serve a eliminare tutti i bit ottenuti che non ci interessano, ovvero quelli per cui  $z \neq a$ . Poiché non sono utili al risultato infatti vengono scartati attraverso la fase.

## ▼ SIMON

Abbiamo una funzione che mappa un input a n bit in un output a n bit.

$$f : \{0,1\}^n \rightarrow \{0,1\}^n$$

L'input che diamo alla funzione viene però messo in XOR bit a bit con una stringa s segreta di n bit.

Il nostro obiettivo è trovare la stringa s.

Gli output sono a coppie cioè abbiamo n/2 output differenti e n/2 output collegati all'altra metà.

Per trovare la stringa s dobbiamo riuscire a farci restituire due output uguali, in questo modo mettendo in XOR i due input che restituiscono lo stesso output riusciamo ad ottenere la stringa s.

Per ottenere due output uguali, classicamente, potrei arrivare a fare  $2^{\frac{n}{2}}$  chiamate che scala come  $\sqrt{2^n}$  dove n/2 indica il fatto che gli output univoci sono solo metà rispetto a n.

Quantisticamente invece possiamo mettere i qbit di input sovrapposizione formata da  $x$  e da  $x \oplus s$ . La stringa messa in XOR andrà a determinare una fase che possiamo poi leggere riconvertendo in base 0,1.

$$\frac{|x\rangle + |x \oplus s\rangle}{\sqrt{2}}$$

Per capire l'intera stringa  $s$  dovremo fare  $n$  **chiamate** contro le  $2^{\frac{n}{2}}$  classiche.

### ▼ BB84

#### *Protocollo sicuro per la distribuzione di chiavi crittografiche*

Sfrutta due importanti proprietà della meccanica quantistica:

- teorema no-cloning:  
non posso copiare un generico qubit contenente l'informazione
- proprietà della misura:  
una misura su un qubit provoca il collasso della funzione d'onda

L'idea alla base è che dato uno stato quantistico esiste una base il cui **output della misura è certo** e non probabilistico

## Implementazione

1. Alice - estrazione e misura
  - a. viene fissato  $n$  numero di qubit da usare.
  - b. Alice estrae due sequenze di numeri casuali in 0 e 1
    - **prima** sequenza è **stringa logica**
    - **seconda** sequenza è **base in cui codificare**
  - c. Seguendo le due sequenze Alice prepara una serie di qubit e li manda a Bob.
    - Stringa logica 0 e base 0 allora crea qubit  $|0\rangle$ ,
    - stringa logica 1 e base 0 allora crea qubit  $|1\rangle$ ,
    - stringa logica 0 e base 1 allora crea qubit  $|+\rangle$ ,
    - stringa logica 1 e base 1 allora crea qubit  $|-\rangle$
2. Bob - ricezione, estrazione e misura
  - a. Bob riceve i qubit di Alice ed estrae a caso  $n$  **bit della base**, questi sono la base su cui misurare i qubit di Alice.
  - b. Effettua la misura sulla stringa di qubit ed in media  $\frac{n}{2}$  saranno congruenti a quelli di Alice.

### 3. Alice e Bob - pubblicazione

- a. Pubblicano le stringhe di bit con cui hanno scelto la base per misurare
- b. Confrontano e capiscono quali qubit della stringa logica hanno in comune. **Questa è la chiave segreta tra AeB.**



La potenza di BB84 sta che se un attaccante prova a fare un attacco MITM (non potendo copiare i qubit) dovrà per forza scegliere una stringa di bit base per misurare i qubit (di Alice per Bob) per poi inviarli a Bob.  
A questo punto Bob effettuerà la misura come detto nel punto precedente e quando AeB pubblicheranno le stringhe di codifica e misura. Si scoprirà che c'è stato un attaccante in quanto Eve ha distrutto lo stato originale del 50% dei qubit.

### 4. Alice e Bob - analisi e scelta della chiave

- a. Tra i qubit misurati nella stessa base, Alice e Bob scelgono la prima metà per svelarne pubblicamente il risultato.
- b. Se non c'è stato nessun attaccante la correlazione tra i qubit sarà completa.
- c. A questo punto possono usare la seconda parte dei qubit (quelli non pubblicati) da utilizzare come chiave.



Nel caso in cui ci sia stata Eve la correlazione tra i qubit sarà molto minore ed Alice e Bob riescono a capire che c'è stato un problema.

Per garantire la sicurezza Alice e Bob scelgono una soglia (es 90%) di correlazione dei loro qubit, al di sotto della quale si considera invalidato lo scambio della chiave.

## ▼ EPR

Evoluzione del protocollo crittografico EPR, si basa sull'utilizzo degli stati entangled; in questo modo è possibile bypassare l'invio dei qbit di Alice a Bob dopo averli criptati.

Supponiamo che Alice e Bob condividano n qbit entangled fatti così:

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Alice genera randomicamente un bit classico e lo usa come base per misurare il suo qbit. Bob fa la medesima cosa.

Il principio è il medesimo del BB84 ma non occorre scambiare qbit, infatti, Alice estrae a caso le basi in cui misurare, Bob fa lo stesso e dove le basi sono congruenti si possono tenere i qbit (e usarli come chiave crittografica) mentre dove sono diverse i qbit vengono scartati.

Questo protocollo è **completamente simmetrico** in quanto non è importante chi fa la misura per primo. Inoltre la **chiave è al 100% randomica** in quanto è indeterminata fino a che non viene effettuata la misura e anche questo, **come il BB84, è sicuro in presenza di un man in the middle** in quanto è possibile verificare se i qbit sono correlati o se hanno perso la correlazione per colpa di un'intervento di Eve.

## ▼ GROVER

### *Algoritmo per la ricerca di un elemento all'interno di un database*

Ogni elemento all'interno di un database può essere rappresentato attraverso un numero pertanto per descrivere tutto un database avremo bisogno di n bit/qubit con  $N = 2^n$ , e gli elementi compresi tra 0 e N-1.

Supponiamo infatti di voler cercare un elemento all' interno di un database non ordinato e di avere una funzione di riconoscimento che restituisce 1 se l'elemento corrente corrisponde con quello cercato e 0 in caso contrario.

Nel caso quantistico avremo bisogno di *marcare* gli elementi che corrispondono all'elemento cercato. Un esempio molto significativo potrebbe essere la ricerca dei fattori primi di un numero.

Questo problema è associabile alla ricerca di elementi all'interno di un database in cui dobbiamo *segnare* gli elementi che sono fattori primi del numero preso in input.

Per marcare gli elementi possiamo utilizzare un qubit ancilla inizializzato magari a  $|0\rangle$  che non viene toccato nel caso in cui l'elemento preso in considerazione non sia l'elemento cercato e viene trasformato in  $|1\rangle$  in caso contrario.

Se però come qubit ancilla utilizzassimo uno stato più complesso come il  $|-\rangle$  Hadamardiano allora nel momento in cui riconosciamo un elemento analogo a quello cercato possiamo applicare un fattore di fase che non modifica la struttura dell'elemento e possiamo anche dimenticarci del qubit ancilla.

( Il fattore di fase introdotto è dato da  $(-1)^{f(x)}$  )

Quindi inizialmente dobbiamo creare la sovrapposizione di tutti i possibili input applicando n porte di Hadamard se cosideriamo come stato di partenza il ket  $|000\dots 0\rangle$ .

Pertanto lo stato di partenza sarà

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

Ciò che ci permette davvero di realizzare l'algoritmo tuttavia è la realizzazione del cosidetto operatore di Grover.

Infatti possiamo pensare lo spazio logico come diviso in due sottoporzioni, quella generata da  $|x\rangle$  con x soluzione del nostro problema e quella con x non soluzione del nostro problema.

Possiamo indicare la sovrapposizione di tutti gli stati soluzione come il vettore  $|\beta\rangle$  e quella degli stati non soluzione come il vettore  $|a\rangle$ .

Ora, immaginando il problema all'interno di uno spazio bidimensionale dove in ordinata abbiamo il vettore degli stati soluzione e in ascissa il vettore degli stati non soluzione, il ruolo dell'operatore di grover è quello di **spostare il vettore degli elementi del nostro database che sono soluzione del nostro problema sempre di più verso il vettore degli stati soluzione.**

Così facendo andremo ad **innalzare sempre di più la possibilità** di essere estratti al momento della misura degli **elementi che stiamo effettivamente cercando** all'interno del nostro database.

L'algoritmo di grover risulta eccezionale in termini di costo computazionale in quanto provvede uno **speed-up esponenziale**. Se in un database sono presenti un milione di elementi classicamente dovremmo fare (nel caso peggiore) un milione di iterazioni prima di verificare se l'elemento sia presente o meno.

Grazie all'algoritmo di grover è necessario solamente fare 1000 iterazioni  $(\sqrt{N})$ .

### ▼ CORREZIONE DEGLI ERRORI

Nei computer classici possiamo usare bit in più di ridondanza ed utilizzare il **voto di maggioranza** per correggere un eventuale bit-flip

es:  $010 \rightarrow 000, 110 \rightarrow 111$

Problema: se avvengono due bit-flip perdiamo l'informazione!

Ovviamente il numero di bit totale deve essere dispari.

## Computer Quantistici - errori

possono essere di 3 tipi

1. bit-flip: sono transizioni  $|0\rangle \rightarrow |1\rangle$  o  $|1\rangle \rightarrow |0\rangle$
2. errori piccoli:  $|0\rangle \rightarrow \gamma|0\rangle + \delta|1\rangle$  ovvero sovrapposizione di stati
3. errori di fase relativa:  $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle + e^{i\phi}\beta|1\rangle$  ad esempio per effetto di rumore

## Codici di correzione errori quantistici

Sfruttano il voto di maggioranza, utilizzano tre qubit per

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

Per l'**inizializzazione** basta utilizzare **due porte CNOT**, la prima dal qubit di partenza verso il secondo e poi dal qubit dello stato verso il terzo.

**Osservabili**  $Z_1 \otimes Z_2$

$$\begin{aligned}
 Z_1 \otimes Z_2 |00\rangle &= |00\rangle \\
 Z_1 \otimes Z_2 |01\rangle &= -|01\rangle \\
 Z_1 \otimes Z_2 |10\rangle &= -|10\rangle \\
 Z_1 \otimes Z_2 |11\rangle &= |11\rangle
 \end{aligned}$$

**Genera un autovalore “–” (meno) quando i due qubit sono diversi**  
e lascia invariati se sono uguali

## Errore bit-flip

Posso identificare un eventuale errore di bit-flip **misurando** prima l'osservabile  $Z_1 \otimes Z_2$  e poi l'osservabile  $Z_1 \otimes Z_3$  per stabilire con certezza “se” e “dove” si è verificato il flip.

Identificato l'errore posso correggerlo **applicando una porta correttiva  $X_n$**  in base al qubit “flippato”.

## Errori “piccoli”

Quando un sistema quantistico subisce perturbazione che genera sovrapposizioni indesiderate  
es:  $|0\rangle \rightarrow \gamma|0\rangle + \delta|1\rangle$

Misurando come nel caso precedente gli operatori  $Z$  se l'errore è piccolo allora il qubit modificato ha alta probabilità di collassare nello stato originale (in quanto lo stato errato non è autostato dell'operatore  $Z$ )

Se così non fosse, la misura di  $Z$  genera un bit flip che potrà essere corretto utilizzando una porta  $X$  sul qubit perturbato

## Errori di fase

Gli errori di fase non sono presenti classicamente.

Un errore di fase provoca un cambio di segno nello stato. Se siamo nella base 01 la misura degli osservabili  $Z_1 \otimes Z_2$  e  $Z_1 \otimes Z_3$  non permette di identificare l'errore.

L'errore di fase è un errore bit flip nella base +- quindi prima cambio la base di 01 in +- con una porta di Hadamard e poi misuro gli osservabili  $Z_1 \otimes Z_2$  e  $Z_1 \otimes Z_3$  per capire quale qubit è stato perturbato.

Una volta trovato il qubit sbagliato posso applicare una porta correttiva  $X$  sul qubit errato.



Gli osservabili  $Z_1 \otimes Z_2$  e  $Z_1 \otimes Z_3$  non vanno applicati ma vanno misurati.  
**MISURARE NON APPLICARE**

### ▼ ALGORITMO DI SHOR - correzione completa a 9 bit

Vengono effettuate le stesse operazioni dell'algoritmo di correzione degli errori però su un numero maggiore di qubit (9) poichè 3 non sono abbastanza

Vengono fatte le stesse operazioni.

Per verificare la presenza di un bit flip si **misurano** i bit con le porte Z e **in base all'autovalore** che otterremo sapremo se si sarà verificato un errore.

Per verificare la presenza di un phase flip invece occorrerà cambiare base da  $|0\rangle$  e  $|1\rangle$  a  $|+\rangle$  e  $|-\rangle$  e poi misurare con le porte X e osservare gli autovalori.

### ▼ DILEMMA DEL PRIGIONIERO

## Caso classico

Alice e Bob vengono interrogati separatamente. Possono cooperare o meno (*Cooperate or Defect*)

Nel caso classico abbiamo la matrice delle ricompense:

	Bob: C	Bob: D
Alice: C	(3, 3)	(0, 5)
Alice: D	(5, 0)	(1, 1)

La scelta di non cooperare sembrerebbe la strada vincente in quanto nel caso peggiore otterrei sempre un punto mentre nel caso migliore ne prenderei 5

## Caso quantistico

Nel caso quantistico assumiamo che Alice e Bob dispongano di due qubit in entanglement.

Questo permette ad A&B di poter accedere ad un numero maggiore di trasformazioni rispetto al caso classico.

Nel caso in qubit siano massimamente in entanglement si nota che la strategia vincente per Alice non è più quella di “non-cooperare” ma diventa una strategia puramente quantistica dove la ricompensa è 5.

La meccanica quantistica ci permette di trovare nuove strategie di gioco non osservabili e non accessibili nel caso classico

### ▼ MERMIN

Un altro gioco quantistico che dimostra come è possibile vincere sfruttando tecniche puramente quantistiche in ambienti che non permetterebbero la vittoria utilizzando computazioni classiche

In questo gioco ci ritroviamo con Alice Bob e Charlie imprigionati in stanze non comunicanti.

Per essere liberati devono rispondere ad alcune domande in modo che la somma delle risposte dia risultati precisi.

Le domande in questione sono :

- Che valore vuoi assegnare ad X (domanda fatta a tutti e tre)
- Che valore vuoi assegnare ad X (ad uno solo ) e che valore vuoi assegnare ad Y ( agli altri due)

Ad X e ad Y possono solo assegnare i valori 1 e -1.

Per essere liberati se siamo nell'ambito della prima domanda il risultato finale deve essere -1.

Nell'ambito dell'altra domanda invece il risultato deve essere 1.

Classicamente non esiste una strategia vincente in quanto sarebbe necessario verificare contemporaneamente tutte le equazioni non sapendo quale domanda è stata posta.

Introducendo però uno stato quantistico massimamente entangled

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B|0\rangle_C + |1\rangle_A|1\rangle_B|1\rangle_C)$$

possiamo attuare una strategia che ci permette di vincere con sicurezza

In questo caso infatti la domanda e l'azione di A,B,C sono completamente indipendenti e l'unica cosa di cui si devono preoccupare è di misurare il qubit a loro disposizione nella base opportuna.

Se ricadessimo nella prima domanda allora A,B e C dovrebbero misurare

$$\sigma_{X,A}, \sigma_{X,B}, \sigma_{X,C}$$

poi per rilevare il risultato bisognerà scrivere i valori ottenuti nella base  $+ -$ .

Qualsiasi combinazione abbiano scelto possiamo osservare che termineranno sempre ottenendo -1 come risultato e pertanto vinceranno sempre.

Se ricadessimo nella seconda domanda allora la situazione cambierà e A misurerà  $\sigma_{X,A}$  mentre B e C misureranno  $\sigma_{y,B}$  e  $\sigma_{y,C}$ .

Anche in questo caso vedremo che alla fine cambiando la base in  $+ -$  per qualsiasi combinazione alla fine si otterrà sempre come valore 1 pertanto vinceranno anche in questo caso.

Abbiamo quindi dimostrato che utilizzando la meccanica quantistica si può attuare una strategia vincente.

## ▼ BOMB TESTER

Si tratta di un esperimento prettamente quantistico in cui si è visto che si possono ottenere informazioni su un oggetto senza interagire con esso ('interaction-free measurement').

Il bomb test è un chiaro esempio di questa situazione paradossale.

Immaginiamo di avere un fascio di fotoni, questi vanno in un beam splitter (H) che li divide in due fasci con intensità dimezzata. Entrambi i fasci vengono riflessi tramite un mirror (X) e dopo essere stati ricombinati tramite un secondo beam splitter vengono misurati da uno dei due detector.

Immaginiamo ora che ci sia un corpo assorbente sul ramo verticale subito dopo il primo beam splitter, in questo caso al secondo beam splitter ci sarà una suddivisione del fascio e quindi entrambi i detector riceveranno dei fotoni.

Avremo quindi una divisione di questo tipo:

- 25% detector 1
- 25% detector 2
- 50% nessun detector

Immaginiamo ora di avere una bomba e non più un corpo assorbente.

Se finisco nel ramo verticale, cioè, la bomba esploderà se attiva. Se finisco nel ramo orizzontale ho due possibilità cioè essere rilevato dal detector 1 o dal detector 2. Nel caso del detector 1 non avrò nessuna informazione sullo stato della bomba perché potrei ricevere il segnale da una bomba attiva o da una inattiva ma se rilevo con il detector 2 questa sarà sicuramente attiva ma non avrò interagito con essa.

#### ▼ SPIN FLIP

Q e P giocano con qbit

qbit può essere spin up o spin down (consideriamo come 0 e 1)

possono applicare Id o X

in base allo stato finale del qubit se 1 vince P, 0 vince Q

L'altro non sa quali porte vengono applicate dall'altro

Strategia quantistica

- Q può applicare porta H  $0 \rightarrow + 1 \rightarrow -$
- A questo punto la porta X non ha effetto su stato $+$  (in quanto autostato)
- Prima della fine del gioco Q riapplica Hadamard per ritornare alla base 01

Q con questo metodo vince sempre