FISICA COMPUTAZIONALE & MODELLI ALTERNATIVI DI COMPUTER

① PORTE LOGICHE UNIVERSALI

NOT $A = \bar{A}$

A AND B $\equiv A \wedge B \equiv A \cdot B$ (prodotto se A,B binari)

A OR B $\equiv A \vee B$

A NAND B $\equiv \overline{A \wedge B}$

A NOR B $= \overline{A \vee B}$

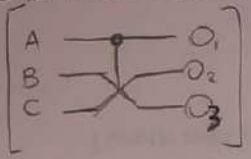
A XOR B $= A \oplus B = A+B \pmod 2$

} tutte non reversibili

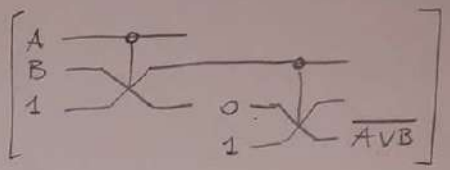
def INSIEMI [UNIVERSALI] di PORTE: combinazioni delle porte possono implementare qualsiasi funzione booleana
es. AND, NOT / OR, NOT

def PORTE LOGICHE [REVERSIBILI]: applicando porta REVERSIBILE e poi suo inverso si ottiene informazione originale

⊙ PORTA di FREDKING-TOFFOLI: è REVERSIBILE → inverso di se stesso
e UNIVERSALE



combinandone 2 si ottiene NOR



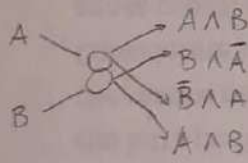
② OPERAZIONI BIT-A-BIT

stringa n bit $x_1 x_2 \dots x_n \iff$ intero $x = x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$ con $0 \le x \le 2^n - 1 = N-1$

- [PRODOTTO] interno o SCALARE $x \cdot z = x_1 z_1 + x_2 z_2 + \dots + x_n z_n \pmod 2$
  = AND BITWISE
- [SOMMA] = XOR BITWISE $x \oplus z = x+z \pmod 2 = x_1+z_1 \pmod 2, \dots, x_n+z_n \pmod 2 = x_1 \text{ XOR } z_1 \pmod 2, \dots, x_n \text{ XOR } z_n \pmod 2$

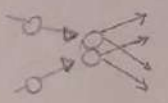
③ COMPUTER BILLARDO

porta logica elementare



- urti ELASTICI e PRECISI
- 1 = palla PRESENTE
- 0 = palla ASSENTE

collisioni gate



insieme ad altre porte si può ottenere FREDKING-TOFFOLI ⇒ computer UNIVERSALE REVERSIBILE

④ COMPUTER & DNA

[DNA]
- doppia elica
- basi azotate A-T/C-G
- DNA polimerasi: enzima x duplicazione da primer di attivazione

↓ Macchina di Turing UNIVERSALE

[PROBLEMA CAMMINO HAMILTONIANO] } cammino tra 2 nodi che passa ∀ nodo solo 1 volta

NODI: città ATL ACATGCAG — TGAACGTC
BOS TCGGACTG — AGCCTGAC

ARCHI: voli ATL-BOS: GCAGTCGG

algoritmo per cammino da A a B:
1) genero insieme cammini casuali ⇒ fare mapire stringhe città_voli
2) ∀ cammino
   a. controllo se è da A a B ⇒ polimerasi con primer che duplica solo da A a B
   b. controllo se n vertici ⇒ colla elettroforetica, troppo lenti/pesanti: numero nodi! Troppi vertici
   c. ∀ vertice controllo se cammino ci passa ⇒ MICROSFERE FERRO
   d. insieme rimasto contiene CAMMINO HAMILTONIANO

APPARATO MATEMATICO

1) PREREQUISITI MATEMATICI

$i = \sqrt{-1}$ $\quad z \in \mathbb{C} \Rightarrow z = a + ib \quad a, b \in \mathbb{R}$ $\quad$ [MODULO]

$z = |z| e^{i\theta} = |z|\cos\theta + i|z|\sin\theta \rightarrow |z| = \sqrt{a^2+b^2}$ [θ FASE]

[COMPLESSO CONIUGATO $z^* = a - ib$] $\Rightarrow z \cdot z^* = a^2 + b^2 = |z|^2$

- VETTORI
  - caratterizzati da MODULO, DIREZIONE, VERSO
  - operazioni: - SOMMA $\Rightarrow$ regola parallelogramma $\vec{v} + \vec{w}$
    - PRODOTTO per SCALARE $\alpha \vec{v}$
    - PRODOTTO SCALARE: funzione $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{C}$

$$\Rightarrow \langle v|w\rangle = v^\dagger w$$

t.c. $\langle u, v\rangle \in \mathbb{R}^+$, $\langle u, v\rangle = 0$ sse $\vec{v} = 0$; $\langle u, v\rangle = \langle v, u\rangle^*$; $\langle u, \alpha v + \beta v\rangle = \alpha\langle u, v\rangle + \beta\langle u, v\rangle$

$\langle v, w\rangle = 0 \Leftrightarrow v \perp w$ cioè v e w ORTOGONALI

- Spazi vettoriali: v e w non multipli l'uno dell'altro $\Rightarrow V = \{v, w\}$ SPAZIO generato da v e w $\rightarrow$ BASE di V
- Trasposto coniugato $v = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad v^\dagger = [1 \;\; 0] \Rightarrow \begin{bmatrix} v = |v\rangle & v^\dagger = \langle v| \\ \text{KET} & \text{BRA} \end{bmatrix}$ $\rightarrow$ SONO NORMALIZZATI cioè $|v| = 1$

- SPAZI VETTORIALI

$V = \{|\alpha_1\rangle, |\alpha_2\rangle, \ldots |\alpha_N\rangle\}$

$W = \{|\beta_1\rangle, |\beta_2\rangle, \ldots |\beta_M\rangle\}$

- SOMMA DIRETTA $V \oplus W = \{(|v\rangle, |w\rangle) : |v\rangle \in V \,\&\, |w\rangle \in W\}$
- PRODOTTO TENSORE $V \otimes W = \{|\alpha_1\rangle_v \otimes |\beta_1\rangle_w, |\alpha_1\rangle_v \otimes |\beta_2\rangle_w, \ldots |\alpha_1\rangle_v \otimes |\beta_M\rangle_w,$

$|\alpha_N\rangle_v \otimes |\beta_1\rangle_w, \ldots |\alpha_N\rangle_v \otimes |\beta_M\rangle_w\}$

AMMETTONO PRODOTTO SCALARE come SOMMA/PRODOTTO dei prodotti scalari definiti su V e W

$\langle u|u'\rangle = (\langle v| \otimes \langle w|)(|v'\rangle \otimes |w'\rangle) = \langle v|v'\rangle\langle w|w'\rangle$

proprietà:

1) $\forall |v\rangle, |v'\rangle \in V, |w\rangle \in W \quad (|v\rangle + |v'\rangle) \otimes |w\rangle = (|v\rangle \otimes |w\rangle) + (|v'\rangle \otimes |w\rangle)$

$|w\rangle \otimes (|v\rangle + |v'\rangle) = (|w\rangle \otimes |v\rangle) + (|w\rangle \otimes |v'\rangle)$

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

$\langle u|u'\rangle = (\langle v| \oplus \langle w|)(\langle v'| \oplus \langle w'|) = \langle v|v'\rangle + \langle w|w'\rangle$

2) OPERATORI LINEARI

$O : V \rightarrow V \quad O|v\rangle = |w\rangle$

con $V = \{|\alpha_1\rangle, \ldots |\alpha_N\rangle\}$

matrice $O_{ij} = \langle\alpha_i|O|\alpha_j\rangle$

$$O = \sum_{ij} O_{ij} |\alpha_i\rangle\langle\alpha_j|$$

def $O = O^\dagger \Rightarrow O$ AUTOAGGIUNTO/HERMITIANO

def $O|v\rangle = \lambda|v\rangle \Rightarrow |v\rangle$ AUTOVETTORE, λ AUTOVALORE

proprietà:

1) O Hermitt. ha AUTOVALORI REALI
2) Autovettori di Hermitt. associati a autovalori $\neq$ SONO ORTOGONALI
3) Se O diagonale, O_{ii} AUTOVALORI e

$$O = \sum_i O_{ii} |\alpha_i\rangle\langle\alpha_i|$$

INTRODUZIONE AI FENOMENI QUANTISTICI

sistema fisico a 2 stati descritto da: $|V_0\rangle, |V_1\rangle$ → base ORTONORMALE di UNO SPAZIO VETTORIALE

STATO QUANTISTICO = QUANTUM BIT = QUBIT $|a\rangle = a_0|V_0\rangle + a_1|V_1\rangle$ con $|a_0|^2 + |a_1|^2 = 1$ } è SOVRAPPOSIZIONE DI STATI del SISTEMA

∞ stati possibili in cui si può trovare il sistema

① POSTULATO DELLA MISURA

1) per misurare un OSSERVABILE (= operatore hermitiano) O servono
- AUTOSTATI $|\phi_i\rangle$ e *AUTOVALORI λ_i di O
- STATO del SISTEMA su cui effettuare misura, DECOMPOSTO NELLA BASE dei $\{|\phi_i\rangle\}$

$|a\rangle = \sum_i a_i |\phi_i\rangle$ con $a_i = \langle\phi_i|a\rangle$

2) Risultato = λ_i con probabilità $|a_i|^2$

3) dopo misura SISTEMA COLLASSA in $|\phi_i\rangle$ ⟹ [MISURA DISTRUGGE SOVRAPPOSIZIONE STATI]

② ESPERIMENTO LUCE POLARIZZATA

[in $B_1 = \{|\uparrow\rangle, |\rightarrow\rangle\}$ fotone è in stato $|a\rangle = a|\uparrow\rangle + b|\rightarrow\rangle$ $P_1 = |\uparrow\rangle\langle\uparrow| - |\rightarrow\rangle\langle\rightarrow|$

1) polarizzatore "↑" / misura di P_1: con prob $= |a|^2$ sistema collassa in $|\psi_1\rangle = |\uparrow\rangle$

[in $B_2 = \{|\nwarrow\rangle, |\nearrow\rangle\}$ fotone è in stato $|\psi_1\rangle = |\uparrow\rangle = \frac{|\nearrow\rangle + |\nwarrow\rangle}{\sqrt{2}}$ $P_2 = |\nearrow\rangle\langle\nearrow| - |\nwarrow\rangle\langle\nwarrow|$

2) polarizzatore "↗" / misura di P_2: con prob $= \frac{1}{2}$ sistema collassa in $|\psi_2\rangle = |\nearrow\rangle$

[in B_1, fotone in stato $|\psi_2\rangle = |\nearrow\rangle = \frac{|\uparrow\rangle + |\rightarrow\rangle}{\sqrt{2}}$

3) polarizzatore "→", misura di P_1: con prob $= \frac{1}{2}$ sistema collassa in $|\psi_3\rangle = |\rightarrow\rangle$

intensità luce FINALE $= \frac{1}{4} \cdot a \cdot 100\% \cdot$ luce INIZIALE

③ FASE GLOBALE

NON è OSSERVABILE / MISURABILE

$|U\rangle = \sum_i a_i |\phi_i\rangle \longrightarrow \lambda_i$ con prob $= |a_i|^2$

$|V\rangle = \sum_i e^{i\theta} a_i |\phi_i\rangle \longrightarrow \lambda_i$ con prob $= |e^{i\theta} a_i|^2 =$
$= e^{i\theta} a_i \cdot (e^{i\theta} a_i)^* =$
$= e^{i\theta} a_i \cdot e^{-i\theta} a_i = |a_i|^2$

④ FASE RELATIVA

È OSSERVABILE (misurando un operatore sui suoi AUTOSTATI) (es)

$|U\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \xrightarrow[\boxed{\sigma_x}]{X} (1)$ prob = 100%

$|V\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle \xrightarrow[\boxed{\sigma_x}]{X} (-1)$ prob = 100%

⑤ STATI A 2 QUBIT e ENTANGLEMENT

data base $B=\{|0\rangle,|1\rangle\}$ di ogni qubit

- per n qubit SPAZIO VETTORIALE è DATO DAL PRODOTTO TENSORE: $\{|0\rangle,|1\rangle\}^{\otimes n} = \{|0\rangle,|1\rangle\}_1 \otimes \dots \otimes \{|0\rangle,|1\rangle\}_n$
- per 2 qubit SPAZIO VETTORIALE

$$V \otimes W = \{|0\rangle_v, |1\rangle_v\} \otimes \{|0\rangle_w, |1\rangle_w\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

$$= \{|0\rangle_1 \otimes |0\rangle_2 \otimes \dots \otimes |0\rangle_n,\ |1\rangle_1 \otimes |0\rangle_2 \otimes \dots \otimes |0\rangle_n,\ \dots,\ |1\rangle_1 \otimes |1\rangle_2 \otimes \dots \otimes |1\rangle_n\}$$ 2^n STATI

es $|00\dots0\rangle = \begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}$ } 2^n valori

es $|11\dots1\rangle = \begin{bmatrix}0\\\vdots\\0\\1\end{bmatrix}$

A) STATI SEPARABILI/FATTORIALIZZABILI:

dati stati generici $|V\rangle = \alpha|0\rangle_v + \beta|1\rangle_v$ degli spazi V e W, $|W\rangle = \gamma|0\rangle_w + \delta|1\rangle_w$ $\Rightarrow |\psi\rangle = |V\rangle_v \otimes |W\rangle_w = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$ è STATO SEPARABILE

misura su V NON influenza stato di W

$|\psi\rangle = \alpha|0\rangle_v(\gamma|0\rangle_w + \delta|1\rangle_w) + \beta|1\rangle_v(\gamma|0\rangle_w + \delta|1\rangle_w)$ — misura su V →
- prob $= |\alpha|^2$, $\lambda_0 \Rightarrow |0\rangle_v(\gamma|0\rangle_w + \delta|1\rangle_w)$
- prob $= |\beta|^2$, $\lambda_1 \Rightarrow |1\rangle_v(\gamma|0\rangle_w + \delta|1\rangle_w)$

stato di W uguale sempre

B) STATI ENTANGLED

NON possono essere scritti come prodotto $|V\rangle_v \otimes |W\rangle_w$ es $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

misura su V PERTURBA LO STATO di W

$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ — misura su V →
- prob $= \frac{1}{2}$, $\lambda_0 \Rightarrow |01\rangle$
- prob $= \frac{1}{2}$, $\lambda_1 \Rightarrow |10\rangle$

→ stato di W cambia!

es [BASE DI BELL] base ORTONORMALE di STATI MASSIMAMENTE ENTANGLED

$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \sim |00\rangle$ $\quad |\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \sim |10\rangle$

$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \sim |01\rangle$ $\quad |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \sim |11\rangle$

distinguibili con misura di $A = \lambda_0|\phi^+\rangle\langle\phi^+| + \lambda_1|\phi^-\rangle\langle\phi^-| + \lambda_2|\psi^+\rangle\langle\psi^+| + \lambda_3|\psi^-\rangle\langle\psi^-|$ diagonale nella base di Bell

⑥ TRASFORMAZIONI UNITARIE

- LINEARE: $U|a\rangle = a_0 U|0\rangle + a_1 U|1\rangle$
- INVERTIBILE con TRASPOSTA CONIUGATA $UU^\dagger = \mathbb{I}$
- CONSERVA PRODOTTO SCALARE: dati $|a\rangle, |b\rangle$ e $|a'\rangle = U|a\rangle$, $|b'\rangle = U|b\rangle$ $\cdot \langle b'|a'\rangle = \langle b|U^\dagger U|a\rangle = \langle b|a\rangle$

[ELABORAZIONI CLASSICHE DISSIPATIVE ≠ ELABORAZIONI QUANTISTICHE REVERSIBILI]

[TRASFORMAZIONI DI PAULI]

$|1\rangle$ $|0\rangle$

$Id|0\rangle = |0\rangle$ $\quad Id|1\rangle = |1\rangle$ $\quad Id = \begin{bmatrix}1&0\\0&1\end{bmatrix}$

$X|0\rangle = |1\rangle$ $\quad X|1\rangle = |0\rangle$ $\quad X = \begin{bmatrix}0&1\\1&0\end{bmatrix}$

$Y|0\rangle = -i|1\rangle$ $\quad Y|1\rangle = i|0\rangle$ $\quad Y = \begin{bmatrix}0&-i\\i&0\end{bmatrix}$

$Z|0\rangle = -|0\rangle$ $\quad Z|1\rangle = |1\rangle$ $\quad Z = \begin{bmatrix}1&0\\0&-1\end{bmatrix}$

OSS SONO HERMITIANI?

OSS X = NOT, Z = CAMBIO FASE RELATIVA $\quad Y = -iXZ$

FORMA MATRICIALE IN BASE $\{|1\rangle, |0\rangle\}$?

[GENERICO OPERATORE UNITARIO U]

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

↳ [TRASFORMAZIONE DI HADAMARD] · cambio di base

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

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

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \quad \begin{matrix} |1\rangle & |0\rangle \end{matrix}$$

↳ [PORTA C-NOT] : definito in $\{|0\rangle, |1\rangle\}$, applicato a 2 qubit, 1° controllo, 2° Target

$\text{CNOT}\ |0\rangle_A \otimes |0\rangle_B := |0\rangle_A \otimes |0\rangle_B$

$\text{CNOT}\ |0\rangle_A \otimes |1\rangle_B = |0\rangle_A \otimes |1\rangle_B$

$\text{CNOT}\ |1\rangle_A \otimes |0\rangle_B := |1\rangle_A \otimes |1\rangle_B$

$\text{CNOT}\ |1\rangle_A \otimes |1\rangle_B := |1\rangle_A \otimes |0\rangle_B$

$\text{CNOT}\ |++\rangle = |++\rangle$

$\text{CNOT}\ |+-\rangle = |--\rangle$

$\text{CNOT}\ |-+\rangle = |-+\rangle$

$\text{CNOT}\ |--\rangle = |+-\rangle$

[OSS] se applicato a $\{|+\rangle, |-\rangle\}$ 1°-bit Target 2°-bit controllo

e $|+\rangle = 0$ $|-\rangle = 1$

[OSS] CNOT GENERA ENTANGLEMENT!

(ES) $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\phi^+\rangle$ STATO di BELL

SEPARABILE perché $= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle$

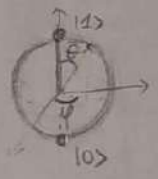
ENTANGLED!

(7) RAPPRESENTAZIONE SFERA DI BLOCH

stato generico $|\psi\rangle = \cos\frac{\theta}{2}|1\rangle + \text{sen}\frac{\theta}{2} e^{i\varphi}|0\rangle$ con $e^{i\varphi}$ FASE RELATIVA

• rappresentato con coordinate con $0 \le \theta \le \pi$ $0 \le \varphi < 2\pi$

$$\begin{cases} x = \cos\varphi \,\text{sen}\theta \\ y = \text{sen}\varphi \,\text{sen}\theta \\ z = \cos\theta \end{cases}$$



• operatore unitario = ROTAZIONE su sfera Bloch

es. $U = \cos\frac{\alpha}{2}\,Id - i\,\text{sen}\frac{\alpha}{2} Y \Rightarrow U|1\rangle = \cos\frac{\alpha}{2}|1\rangle + \text{sen}\frac{\alpha}{2}|0\rangle$ $(\varphi = 0, \theta = \alpha)$

↓ ROTAZIONE RISPETTO ASSE y

⇐ cioè punto di coordinate $\begin{cases} x = \text{sen}\alpha \\ y = 0 \\ z = \cos\alpha \end{cases}$

[OSS] 2 operatori tra X, Y, Z sono sufficienti x RUOTARE ATTORNO a ASSE GENERICO

(8) INIZIALIZZAZIONE SISTEMA QUANTISTICO

$U_{PA}(\gamma) \begin{cases} |0\rangle \to |0\rangle \\ |1\rangle \to e^{i\gamma}|1\rangle \end{cases}$ α, γ PARAMETRI ARBITRARI

$|0\rangle \xrightarrow{H} |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{U_R(-2\alpha)} \frac{1}{\sqrt{2}}(|0\rangle + e^{-i2\alpha}|1\rangle) \xrightarrow{H} e^{-i\alpha}\left[\cos\alpha|0\rangle + i\,\text{sen}\alpha|1\rangle\right]$

$\xrightarrow{U(-\pi/2)} \cos\alpha|0\rangle + \text{sen}\alpha|1\rangle \xrightarrow{U_R(\gamma)} \cos\alpha|0\rangle + e^{i\gamma}\text{sen}\alpha|1\rangle$ $\quad \left[H\,U(-2\alpha)\,H\,U(-\pi/2)\,U_R(\gamma)\right]$

INFORMAZIONE QUANTISTICA

① PARALLELISMO QUANTISTICO

[VANTAGGIO rispetto computazione classica: 1 QUBIT può CODIFICARE TUTTA INFORMAZIONE LOGICA]

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

n qubit $|00\ldots0\rangle \xrightarrow{H^{\otimes n}} |++\ldots+\rangle = \frac{1}{\sqrt{2^n}}\underbrace{(|000\ldots0\rangle+|0\ldots1\rangle+\ldots+|111\ldots1\rangle)}_{\text{TUTTI i possibili } 2^n \text{ STATI logici}} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$ con $N=2^n$

OSS operatore UNITARIO è LINEARE $\Rightarrow$ MANIPOLA PARALLELAMENTE TUTTI GLI STATI LOGICI

[è VANTAGGIO ma estrazione INFORMAZIONE avviene con misura che è PROBABILISTICA]

② NO-CLONING

- è possibile COSTRUIRE OPERATORE di COPIA di stati quantistici solo se gli stati sono NOTI e ORTOGONALI
- $\nexists$ operatore capace di COPIARE QUALSIASI STATO

dim dati stati $|\psi\rangle, |\varphi\rangle$, generico $|S\rangle$, operatore U_{copy}

$|\psi S\rangle \longrightarrow U_{copy}|\psi S\rangle = |\psi\psi\rangle$
$|\varphi S\rangle \longrightarrow U_{copy}|\varphi S\rangle = |\varphi\varphi\rangle$
$\Longleftrightarrow \langle\psi S|U^{\dagger}_{copy}U_{copy}|\varphi S\rangle = \langle\psi\psi|\varphi\varphi\rangle$

$\langle\psi S|\varphi S\rangle = \langle\psi|\varphi\rangle\langle\psi|\varphi\rangle$

$\langle\psi|\varphi\rangle = 0$ cioè $|\psi\perp|\varphi\rangle$ ①
$\langle\psi|\varphi\rangle = 1$ cioè $|\psi\rangle = |\varphi\rangle$ ②
$\Rightarrow \langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2 \Leftarrow \langle\psi|\varphi\rangle\langle S|S\rangle = (\langle\psi|\varphi\rangle)^2$

③ SUPERDENSE CODING: protocollo per trasferire informazione sfruttando entanglement

[VANTAGGIO: inviare 2 bit di info classica con 1 SOLO QUBIT]

A e B condividono $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A\otimes|0\rangle_B + |1\rangle_A\otimes|1\rangle_B) = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ [è STATO di BELL, ENTANGLED]

A vuole mandare		B riceve
00	$\|\phi^+\rangle \xrightarrow{Id}$	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}} = \|\phi^+\rangle$
10	$\|\phi^+\rangle \xrightarrow{Z}$	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}} = \|\phi^-\rangle$
01	$\|\phi^+\rangle \xrightarrow{X}$	$\frac{\|10\rangle+\|01\rangle}{\sqrt{2}} = \|\psi^+\rangle$
11	$\|\phi^+\rangle \xrightarrow{iY}$	$\frac{\|01\rangle-\|10\rangle}{\sqrt{2}} = \|\psi^-\rangle$

4 STATI ORTONORMALI di Bell! distinguibili univocamente con misura

[oppure applicando CNOT e Hadamard al 1° QUBIT e misura Z in base canonica]

[applicati agli stati di A]

④ TELETRASPORTO QUANTISTICO: procedura x trasportare 1 qubit di informazione tra 2 punti senza violare principio di indeterminazione

7

A e B condividono STATO ENTANGLED $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A + |1\rangle_B) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

A ha ALTRO QUBIT da TRASMETTERE $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Per inviarlo lo accoppia a $|\phi^+\rangle$

$|\psi_0\rangle = |\psi\rangle|\phi^+\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)]$

(~) qubit di A ⇒ sono 2!
(−) qubit di B

↓ [Alice. CNOT] (1° controllo, 2° Target)

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

↓ [Alice: Hadamard] 1° qubit

$|\psi_2\rangle = \frac{1}{\sqrt{2}}[\alpha|+\rangle(|00\rangle + |11\rangle) + \beta|-\rangle(|10\rangle + |01\rangle)] =$

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

↓ [Alice MISURA]: misura INDUCE COLLASSO STATO Bob

A misura	Stato Bob
$\|00\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$
$\|01\rangle$	$\alpha\|1\rangle + \beta\|0\rangle$
$\|10\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$
$\|11\rangle$	$\alpha\|1\rangle - \beta\|0\rangle$

} tutte con prob $= \frac{1}{4}$
} A comunica risultato a B

↓ [Bob applica PORTA CORRETTIVA]

$\alpha|0\rangle + \beta|1\rangle$ — Id
$\alpha|1\rangle + \beta|0\rangle$ — X
$\alpha|0\rangle - \beta|1\rangle$ — Z
$\alpha|1\rangle - \beta|0\rangle$ — Y

[STATO FINALE Bob: $\alpha|0\rangle + \beta|1\rangle = |\psi\rangle$]

OSS

1. Stato Bob cambia senza essere trasmesso (ENTANGLEMENT)
2. Info su risultato misura Alice serve a Bob, altrimenti non può ottenere info su α e β

⑤ ALGORITMO DI DEUTCH: stabilire se $f: \{0,1\} \to \{0,1\}$ COSTANTE/BILANCIATA

[VANTAGGIO: CASO CLASSICO 2 chiamate di f (VS) caso QUANTISTICO 1 chiamata SOLA]

· Operatore U_f: $|x,y\rangle \longrightarrow |x, y \oplus f(x)\rangle \Rightarrow \boxed{U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle}$

$$|\psi_0\rangle = |01\rangle \xrightarrow{H\otimes H} |\psi_1\rangle = |+-\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|-\rangle$$

$$\xrightarrow{U_f} |\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle \overset{\circledast}{+} (-1)^{f(1)}|1\rangle\right)|-\rangle$$

$$\xrightarrow{H(1^\circ \text{ qubit})} |\psi_3\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}\frac{|0\rangle+|1\rangle}{\sqrt{2}} + (-1)^{f(1)}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|-\rangle =$$

$$= \frac{1}{2}\left(\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right)|-\rangle$$

2 CASI 1) COSTANTE $\begin{cases} =0 : |\psi_3\rangle = \frac{1}{2}(2|0\rangle)|-\rangle = |0\rangle|-\rangle \\ =1 : |\psi_3\rangle = \frac{1}{2}(-2|0\rangle)|-\rangle = -|0\rangle|-\rangle \end{cases} \Big\} \pm|0\rangle|-\rangle$

2) BILANCIATA

$f(0)=0$ e $f(1)=1$: $|\psi_3\rangle = \frac{1}{2}(2|1\rangle)|-\rangle = |1\rangle|-\rangle$

$f(0)=1$ e $f(1)=0$: $|\psi_3\rangle = \frac{1}{2}(-2|1\rangle)|-\rangle = -|1\rangle|-\rangle$ $\Big\} \pm|1\rangle|-\rangle$

[MISURA 1° qubit di $|\psi_3\rangle$ $\begin{cases} \lambda_0 \Rightarrow f \text{ COSTANTE} \\ \lambda_1 \Rightarrow f \text{ BILANCIATA} \end{cases}$]

OBS ① PARALLELISMO QUANTISTICO U_f applicato contemp. a $|0\rangle$ e $|1\rangle$

② se $f(0) \neq f(1)$, $\circledast$ qui si crea INTERFERENZA = FASE RELATIVA

---

⑥ ALGORITMO DI DEUTCH - JOZSA: come prima ma $f: \{0,1\}^{\otimes M} \to \{0,1\}$ $\begin{cases} \text{COSTANTE} \\ \text{BILANCIATA (50/50)} \end{cases}$

[VANTAGGIO: caso classico $2^{M}/2 + 1$ chiamate (VS) caso QUANTISTICO 1 SOLA chiam]

$$|\psi_0\rangle = |0\rangle^{\otimes M}|1\rangle \xrightarrow{H^{\otimes M+1}} |\psi_1\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \xrightarrow{U_f} |\psi_2\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}(-1)^{f(x)}|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

$$\left[H|k\rangle = \frac{1}{\sqrt{2}}\sum_{z=0}^{1}(-1)^{kz}|z\rangle \longrightarrow H^{\otimes M}|x_1 x_2 \dots x_M\rangle = \frac{1}{\sqrt{N}}\sum_{z_1,z_2\dots z_M=0}^{1}(-1)^{x_1z_1+x_2z_2+\dots+x_Mz_M}|z_1,z_2\dots z_M\rangle = \sum_{z=0}^{N-1}\frac{(-1)^{x\cdot z}}{\sqrt{N}}|z\rangle\right]$$

$$|\psi_2\rangle \xrightarrow{H^{\otimes M}} |\psi_3\rangle = \sum_{x=0}^{N-1}\sum_{z=0}^{N-1}\frac{(-1)^{x\cdot z+f(x)}}{N}|z\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \quad \text{Coeff di } |z\rangle=|0\rangle: \sum_{x=0}^{N-1}\frac{(-1)^{f(x)}}{N}$$

2 CASI 1) COSTANTE $f(0)=f(1)=\bar{f}$ (NON DIP. DA x) $\Rightarrow \sum_{x=0}^{N-1}\frac{(-1)^{f(x)}}{N} = (-1)^{\bar{f}} \Rightarrow |(-1)^{\bar{f}}|^2 = 1 =$

$\Rightarrow |\psi_3\rangle = (-1)^{\bar{f}}|0\rangle|-\rangle$

2) BILANCIATA $\sum_{x=0}^{N-1}\frac{(-1)^{f(x)}}{N} = \sum_{f(x)=0}\frac{1}{N} - \sum_{f(x)=1}\frac{1}{N} = 0 \Rightarrow |\psi\rangle$ NON ha componente $|0\rangle$

[MISURA 1° qubit di $|\psi_3\rangle$ $\begin{cases} \to \lambda_0 \Rightarrow f \text{ COSTANTE} \\ \to \neq\lambda_0 \Rightarrow f \text{ BILANCIATA} \end{cases}$]

OSS speed-up ESPONENZIALE rispetto CASO CLASSICO!

(7) ALGORITMO DI BERNSTEIN-VAZIRANI: dato $f_a(x) = x \cdot a = x_1 a_1 + \dots + x_n a_n$ trovare a ignoto

Stesse porte logiche di prima (Deutch-Jozsa)

$$|\psi_3\rangle = \sum_{x=0}^{N-1}\sum_{z=0}^{N-1} \frac{(-1)^{x\cdot z + f(x)}}{N}|z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \sum_{x=0}^{N-1}\sum_{z=0}^{N-1} \frac{(-1)^{x\cdot z + x\cdot a}}{N}|z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} =$$

$$= \sum_{z=0}^{N-1}\left(\sum_{x=0}^{N-1} \frac{(-1)^{(z\oplus a)\cdot x}}{N}\right)|z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad \text{con } \chi_z = \sum_{x=0}^{N-1} \frac{(-1)^{(z\oplus a)\cdot x}}{N}$$

Se $z = a \Rightarrow z_1 z_2 \dots z_n = a_1 a_2 \dots a_n \Rightarrow (z \oplus a) = 0 \Rightarrow \chi_a = \sum_{x=0}^{N-1} \frac{1}{N} = 1$

$\Rightarrow |\chi_{z=a}|^2 = 1 \Rightarrow \chi_{z\neq a} = 0 \Rightarrow \chi_z = \begin{cases} 1 & \text{se } z=a \\ 0 & \text{se } z\neq a \end{cases} = \delta_{z,a}$

$$\Rightarrow |\psi_3\rangle = \sum_{z=0}^{N-1} \delta_{z,a}|z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |a\rangle|-\rangle \xrightarrow[\text{primi } n \text{ qubit}]{\text{misura}} \lambda_a \quad \underline{\text{prob} = 100\%}$$

[OSS: speed-up polinomiale $n \to 1$]

(8) ALGORITMO DI SIMON: dato $f: \{0,1\}^n \to \{0,1\}^m$ t.c $\forall x\ \exists! y$ t.c. $y = x \oplus a \wedge f(x) = f(y)$ (PERIODICITÀ di f) trovare a ignota

[VANTAGGIO. CASO CLASSICO $2^{N/2}$ chiamate oracolo (VS) CASO QUANTISTICO N chiamate oracolo]

$$|\psi_0\rangle = |0\rangle^{\otimes n}|0\rangle^{\otimes m} \xrightarrow{H^{\otimes n}} |\psi_1\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|0\rangle^{\otimes m}$$

spazio fatto n bit ancilla

Considero oracolo/black-box O che calcola $f(x)$ e scrive risultato in ultimi m qubit

$$|\psi_1\rangle \xrightarrow{O} |\psi_2\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|f(x)\rangle \xrightarrow{\text{prop. di } f} |\psi_2\rangle = \frac{1}{\sqrt{N/2}}\sum_{x=0}^{N-1}\frac{|x\rangle + |x\oplus a\rangle}{\sqrt{2}}|f(x)\rangle$$

$$\xrightarrow[\text{ultimi } m \text{ qubit}]{\text{misura}} |\psi_3\rangle = \frac{|x_0\rangle + |x_0\oplus a\rangle}{\sqrt{2}} \quad \text{stato primi } n \text{ qubit}$$

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

$$\left[H^{\otimes n}|x\rangle = \frac{1}{\sqrt{N}}\sum_{z=0}^{N-1}(-1)^{x\cdot z}|z\rangle\right]$$

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

$\left[1 + (-1)^{a\cdot y}\right] = 0 \Leftrightarrow a\cdot y = 1$, $\neq 0 \Leftrightarrow a\cdot y = 0$

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

misura $\Rightarrow$ risultato y_i t.c. $a\cdot y_i = 0$

RIPETO n volte $\Rightarrow$ ottengo n y_i t.c. $\begin{cases} a\cdot y_1 = 0 \\ a\cdot y_2 = 0 \\ \vdots \\ a\cdot y_n = 0 \end{cases}$ SISTEMA LINEARE n eq.ni n incognite $\Rightarrow$ (a)

CRITTOGRAFIA QUANTISTICA

10

QKD: Quantum Key Distribution
scambio chiave segr. PRIVATA su canale pubblico
proprietà quantistiche garantiscono segretezza

(1) PROTOCOLLO BB84: asimmetrico + scambio qubit A→B

Quale SICUREZZA su: 1) NO-CLONING: Eve NON può copiare generico qubit che contiene info crittografica

2) MISURA CAUSA COLLASSO: se Eve fa misura, effetti sono EVIDENTI quindi A e B se ne accorgono

$B_1 = \{|0\rangle, |1\rangle\}$ $B_2 = \{|+\rangle, |-\rangle\} = \{|0_+\rangle, |1_+\rangle\}$ $\left[|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \quad |1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}\right]$

[ALICE]: 1) sceglie n bit random ⇒ STRINGA LOGICA DA CODIFICARE
2) sceglie n bit random ⇒ STRINGA BASI IN CUI CODIFICARE ($0 \to B_1$, $1 \to B_2$)
3) codifica STRINGA LOGICA:

bit \ base	B_1	B_2
0	$\|0\rangle$	$\|0_+\rangle$
1	$\|1\rangle$	$\|1_+\rangle$

⇒ produce n qubit

4) invia i qubit a Bob

[BOB]: 1) sceglie n bit random ⇒ STRINGA BASI IN CUI MISURARE ($0 \to B_1$, $1 \to B_2$)
2) misura qubit di Alice nelle basi scelte

qubit \ base	B_1	B_2
$\|0\rangle$	0	$\nearrow^0_1$
$\|1\rangle$	1	$\nearrow^1_0$
$\|0_+\rangle$	$\nearrow^0_1$	0
$\|1_+\rangle$	$\nearrow^0_1$	1

se $BASE_{ALICE} = BASE_{BOB}$, bit codificato$_{ALICE}$ = bit misurato$_{BOB}$

[A&B]: 1) pubblicano STRINGHE BASI ⇒ bit relativi a basi uguali POSSONO essere usati x chiave
2) pubblicano METÀ QUBIT misurati in stessa base ⇒ se NON c'è stato Eve DEVONO essere uguali (cioè c'è CORRELAZIONE tra risultati)
3) verificano correlazione ⇒ soglia scelta → se OK usano altra metà bit come chiave
se NO ripetono protocollo

[OSS] ~ metà bit SCORRELATI
metà bit CORRELATI pubblicati ⇒ $\frac{1}{4}$ bit scartato ⇒ $n = 4m$ (n: qubit iniziali, m: bit chiave)

[EVE] può fare MAN-IN-THE MIDDLE
misurando qubit di A e mandando a Bob stato misurato
⇒ COLLASSO PERTURBA STATI ! (circa metà ricevuti)

② PROTOCOLLO EPR: simmetrico + No scambio qubit

A e B condividono n qubit $|\Phi^+\rangle = \frac{|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ [OSS stessa struttura nelle 2 basi $= \frac{|{+}{+}\rangle + |{-}{-}\rangle}{\sqrt{2}}$]

$B_1 = \{|0\rangle, |1\rangle\}$ $B_2 = \{|+\rangle, |-\rangle\}$

11

$\forall$ qubit: 1) A sceglie BASE MISURA q_A } $(0 \to B_1, 1 \to B_2)$
2) B sceglie BASE MISURA q_B }
3) A MISURA qubit condiviso
4) B MISURA qubit condiviso + 5) A e B condividono bit BASI $\Rightarrow$ [chiave = bit per cui $B_A = B_B$]

2 CASI · $q_A = q_B$ → = 0: $|\Phi^+\rangle \xrightarrow[A]{B_2}$ λ_0 prob ½ $|00\rangle \xrightarrow[B]{B_1}$ prob = 1 $|00\rangle \Rightarrow \emptyset$
λ_1 prob ½ $|11\rangle \xrightarrow[B]{B_1}$ prob = 1 $|11\rangle \Rightarrow 1$

= 1 $|\Phi^+\rangle \xrightarrow[A]{B_2}$ λ_+ prob ½ $|{+}{+}\rangle \xrightarrow[B]{B_2}$ prob = 1 $|{+}{+}\rangle \Rightarrow \emptyset$
λ_- prob ½ $|{-}{-}\rangle \xrightarrow[B]{B_2}$ prob = 1 $|{-}{-}\rangle \Rightarrow 1$

· $q_A \neq q_B$: MISURE NON CORRELATE $\Rightarrow$ bit SCARTATI

[OSS 1) Simmetrico: NON importa chi misura prima
2) chiave RANDOM: prodotta dalla misura
3) EVE scoperta come in BB84 (✓)]

ALGORITMO DI GROVER

ricerca in database di N elementi → associati a interi $0 \le x \le N-1$

(12)

① ORACOLO / BLACK-BOX

data funzione $f: \{0,1\}^m \to \{0,1\}$

1) RICONOSCE se input è SOLUZIONE: $f(x) = \begin{cases} 1 & \text{se } x \text{ SOLUZIONE} \\ 0 & \text{se } x \underline{\text{NON}} \text{ SOLUZIONE} \end{cases}$

2) MARCA SOLUZIONE con QUBIT ANCILLA

↳ $|x\rangle|q\rangle \longrightarrow |x\rangle|q \oplus f(x)\rangle \Rightarrow$ Se $q=|0\rangle, |1\rangle$ CAMBIA STATO se x SOLUZIONE; ALTRIM RIMANE INVARIATO

Se $q=|-\rangle$ AGGIUNGE FASE $(-1)^{f(x)}$

3) se x soluzione

$|x\rangle|0\rangle = |x\rangle|1\rangle$ $\quad |x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle = -|x\rangle|-\rangle$ → anello trascurabile xk invariato

② OPERATORE DI GROVER: algoritmo parte da $|\psi\rangle = H^{\otimes m}|\bar{0}\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$

1) O : $|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle$
2) $H^{\otimes m}$
3) OPERATORE CAMBIO FASE P: $|x\rangle \xrightarrow{P} -(-1)^{\delta_{x0}}|x\rangle$ con $\delta_{x0} = \begin{cases} 1 \text{ se } x=0 \\ 0 \text{ se } x\neq 0 \end{cases}$
4) $H^{\otimes m}$

U

$$\boxed{G = UO = H^{\otimes m} P H^{\otimes m} O}$$

spazio logico divisibile in $|\alpha\rangle = \frac{1}{\sqrt{N-M}}\sum_{x}^{\text{NON sol}}|x\rangle$ $\quad |\beta\rangle = \frac{1}{\sqrt{M}}\sum_{x}^{\text{sol}}|x\rangle \Rightarrow$ SPAZIO LOGICO $a|\alpha\rangle + b|\beta\rangle$

- O cambia segno SOLO a stati soluzione

$O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle \iff O = |\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta| = \begin{matrix} |\alpha\rangle & |\beta\rangle \end{matrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

- P cambia segno a TUTTI TRANNE a $|\bar{0}\rangle = |00\ldots0\rangle$

$$P = |0\rangle\langle 0| - \sum_{x\neq 0}|x\rangle\langle x| = |0\rangle\langle 0| - \sum_{x\neq 0}|x\rangle\langle x| + |0\rangle\langle 0| - |0\rangle\langle 0| = 2|0\rangle\langle 0| - \sum_{x}|x\rangle\langle x| = 2|\bar{0}\rangle\langle\bar{0}| - Id$$

- $U = H^{\otimes m} P H^{\otimes m} = H^{\otimes m}(2|0\rangle\langle 0| - Id)H^{\otimes m} = 2H^{\otimes m}|0\rangle\langle 0|H^{\otimes m} - H^{\otimes m} Id H^{\otimes m} = 2|\psi\rangle\langle\psi| - Id$
- $\boxed{G = UO = (2|\psi\rangle\langle\psi| - Id)O}$

③ INTERPRETAZIONE GEOMETRICA

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \operatorname{sen}\frac{\theta}{2}|\beta\rangle \quad \text{con} \begin{cases} \cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}} \\ \operatorname{sen}\frac{\theta}{2} = \sqrt{\frac{M}{N}} \end{cases}$$

$$U|\alpha\rangle = \cos\theta|\alpha\rangle + \operatorname{sen}\theta|\beta\rangle$$
$$U|\beta\rangle = \operatorname{sen}\theta|\alpha\rangle - \cos\theta|\beta\rangle \Rightarrow U = \begin{matrix} |\alpha\rangle & |\beta\rangle \end{matrix} \begin{bmatrix} \cos\theta & \operatorname{sen}\theta \\ \operatorname{sen}\theta & -\cos\theta \end{bmatrix}$$

$$\Downarrow$$

$$G = \begin{bmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{bmatrix}$$

ROTAZIONE SENSO ANTIORARIO di angolo θ

$$\begin{cases} \langle\psi|\alpha\rangle = \langle\alpha|\cos\frac{\theta}{2}|\alpha\rangle + \langle\beta|\operatorname{sen}\frac{\theta}{2}|\alpha\rangle = \cos\frac{\theta}{2} \\ \langle\psi|\beta\rangle = \operatorname{sen}\frac{\theta}{2} \end{cases}$$

④ PERFORMANCE ALGORITMO

algoritmo EFFICACE se aumenta PROBABILITÀ di MISURARE lo STATO SOLUZIONE $(\in |\beta\rangle)$
$\Rightarrow$ deve aumentare coefficiente di $|\beta\rangle$

$$|\psi_0\rangle = \cos\tfrac{\theta}{2}|\alpha\rangle + \operatorname{sen}\tfrac{\theta}{2}|\beta\rangle \xrightarrow{G} \cos\left(\tfrac{\theta}{2}+\theta\right)|\alpha\rangle + \operatorname{sen}\left(\tfrac{\theta}{2}+\theta\right)|\beta\rangle$$

$$\xrightarrow{G^k} \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \operatorname{sen}\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$

$$\Rightarrow \operatorname{sen}\left(\frac{2k+1}{2}\theta\right) \approx 1 \iff \frac{2k+1}{2}\theta \approx \frac{\pi}{2} \iff k = \frac{1}{2}\left(\frac{\pi}{\theta} - 1\right)$$

$$\overset{(*)}{\Rightarrow} k = \frac{1}{2}\left(\frac{\pi}{2}\sqrt{\frac{N}{M}} - 1\right) \approx \frac{\pi}{4}\sqrt{\frac{N}{M}}$$

$\Rightarrow$ SONO necessarie $\sqrt{N}$ chiamate di f

[SPEED-UP QUADRATICO RISPETTO CASO CLASSICO]

(*) [casi interessanti
$M \ll N \Rightarrow \sqrt{\frac{M}{N}}$ piccolo
$\Rightarrow \operatorname{sen}\frac{\theta}{2}$ piccolo
$\Rightarrow \operatorname{sen}\frac{\theta}{2} \approx \frac{\theta}{2} = \sqrt{\frac{M}{N}}$]

13

CODICI DI CORREZIONE DEGLI ERRORI

① COMPUTER CLASSICI

Rumore può generare BIT FLIP: $0 \to 1$, $1 \to 0$ $\Rightarrow 0_L = 000$ $1_L = 111$ e VOTO DI MAGGIORANZA

2 assunzioni: - n° bit DISPARI
- p 1 solo bit flip $\gg$ p 2 bit flip

(14)

② CASO QUANTISTICO

1) NO-CLONING impedisce duplicazione informazione e estrazione info da copie
2) MISURA DISTURBA STATO, perdita informazione
3) vari tipi di errore: BIT-FLIP, ERRORI PICCOLI, PHASE FLIP

anche qui, voto maggioranza: $|0_L\rangle = |000\rangle$ $|1_L\rangle = |111\rangle$

$(\alpha|0\rangle + \beta|1\rangle) \otimes |00\rangle \xrightarrow{C_1NOT_2} (\alpha|00\rangle + \beta|11\rangle) \otimes |0\rangle \xrightarrow{C_1NOT_3} (\alpha|000\rangle + \beta|111\rangle) = [\alpha|0_L\rangle + \beta|1_L\rangle$ STATO GENERICO$]$

($|00\rangle$: qubit ANCILLA)

$Z_1 \otimes Z_2 |00\rangle = |00\rangle$
$Z_1 \otimes Z_2 |01\rangle = -|01\rangle$
$Z_1 \otimes Z_2 |10\rangle = -|10\rangle$
$Z_1 \otimes Z_2 |11\rangle = |11\rangle$

BIT-FLIP $|\psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle \rightsquigarrow |\phi\rangle = \alpha|100\rangle + \beta|011\rangle$

$(Z_1 \otimes Z_2)|\psi\rangle = \alpha|000\rangle + \beta|111\rangle = |\psi\rangle$ $\quad (Z_1 \otimes Z_2)|\phi\rangle = -\alpha|100\rangle - \beta|011\rangle = -|\phi\rangle$

$|\alpha\rangle$ — $Z_1 \otimes Z_2$ → $\lambda = 1 \Rightarrow |\psi\rangle$ NO BIT FLIP 1°/2°
→ $\lambda = -1 \Rightarrow |\phi\rangle$ C'È BIT FLIP 1°/2°

$|\alpha\rangle$ — $Z_1 \otimes Z_3$ → $\lambda = 1 \Rightarrow |\psi\rangle$ NO BIT FLIP 1°/3°
→ $\lambda = -1 \Rightarrow |\phi\rangle$ C'È BIT FLIP 1°/3°

	$\|\psi\rangle$	$\|\phi_1\rangle$	$\|\phi_2\rangle$	$\|\phi_3\rangle$
$Z_1 \otimes Z_2$	+1	−1	−1	+1
$Z_1 \otimes Z_3$	+1 ✓	−1 ⇓	+1 ⇓	−1 ⇓
PORTA CORRETTIVA $\Rightarrow$		X_1	X_2	X_3

PHASE-FLIP $|0\rangle \to |0\rangle$, $|1\rangle \to -|1\rangle$ $\} \alpha|0_L\rangle + \beta|1_L\rangle \rightsquigarrow \alpha|0_L\rangle - \beta|1_L\rangle$

OSS $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \rightsquigarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle \Rightarrow [$PHASE FLIP in $\{|0\rangle, |1\rangle\} \equiv$ BIT-FLIP in $\{|+\rangle, |-\rangle\}]$

$|\psi\rangle = \alpha|000\rangle + \beta|111\rangle \xrightarrow{H^{\otimes 3}} |\phi\rangle = \alpha|+++\rangle + \beta|---\rangle \rightsquigarrow |\eta'\rangle = \alpha|-++\rangle + \beta|+--\rangle$

$(X_1 \otimes X_2)|\phi\rangle = \alpha|+++\rangle + \beta|---\rangle = |\phi\rangle$ $\quad (X_1 \otimes X_2)|\eta\rangle = -\alpha|-++\rangle - \beta|+--\rangle = -|\eta\rangle$

$|\alpha\rangle$ — $X_1 \otimes X_2$ → $\lambda = +1$ NO PHASE FLIP 1°/2°
→ $\lambda = -1$ C'È PHASE FLIP 1°/2°

$|\alpha\rangle$ — $X_1 \otimes X_3$ → $\lambda = +1$ NO PHASE-FLIP 1°/3°
→ $\lambda = -1$ C'È PHASE-FLIP 1°/3°

	$\|\phi\rangle$	$\|\eta_1\rangle$	$\|\eta_2\rangle$	$\|\eta_3\rangle$
$X_1 \otimes X_2$	+1	−1	−1	+1
$X_1 \otimes X_3$	+1	+1	−1	−1
		⇓	⇓	⇓
		Z_1	Z_2	Z_3
		↓	↓	↓
		$H^{\otimes 3} \to |\psi\rangle$ ✓		

$X_1 \otimes X_2 |++\rangle = |++\rangle$
$X_1 \otimes X_2 |+-\rangle = -|+-\rangle$
$X_1 \otimes X_2 |-+\rangle = -|-+\rangle$
$X_1 \otimes X_2 |--\rangle = |--\rangle$

ERRORI DEBOLI $|0\rangle \rightsquigarrow \gamma|0\rangle + \delta|1\rangle$ con $|\delta| \ll |\gamma|$
$|1\rangle \rightsquigarrow \gamma|1\rangle - \delta|0\rangle$

$|\psi\rangle = \alpha|000\rangle + \beta|111\rangle \rightsquigarrow \alpha(\gamma|0\rangle + \delta|1\rangle)|00\rangle + \beta(\gamma|1\rangle - \delta|0\rangle)|11\rangle =$
$= \alpha\gamma|000\rangle + \alpha\delta|100\rangle + \beta\gamma|111\rangle - \beta\delta|011\rangle =$
$= \gamma(\underbrace{\alpha|000\rangle + \beta|111\rangle}_{|\psi\rangle}) + \delta(\underbrace{\alpha|100\rangle - \beta|011\rangle}_{|\phi^-\rangle}) = |\eta\rangle$

$(Z_1 \otimes Z_2)|\psi\rangle = \alpha|000\rangle + \beta|111\rangle = |\psi\rangle$ $\quad (Z_1 \otimes Z_2)|\phi^-\rangle = -\alpha|100\rangle + \beta|011\rangle = -|\phi^-\rangle$

$Z_1 \otimes Z_2$ → $\lambda = 1 \Rightarrow |\psi\rangle$ MISURA AUTOCORRETTIVA con prob $|\gamma|^2$ ⇒ MOLTO PIÙ FREQUENTE
→ $\lambda = -1 \Rightarrow |\phi^-\rangle$ c'è ancora BIT FLIP e PHASE FLIP con prob $|\delta|^2$

③ PROTOCOLLO COMPLETO DI SHOR : x correggere TUTTI TIPI di errore visti

definisco BLOCCHI $|\bar{0}\rangle = \dfrac{|000\rangle + |111\rangle}{\sqrt{2}}$ $\quad |\bar{1}\rangle = \dfrac{|000\rangle - |111\rangle}{\sqrt{2}}$ ⇒ BLOCCHI da 3 qubit

QUBIT LOGICI $|0_L\rangle = |\bar{0}\rangle|\bar{0}\rangle|\bar{0}\rangle$ $\quad |1_L\rangle = |\bar{1}\rangle|\bar{1}\rangle|\bar{1}\rangle$ ⇒ 9 qubit

GENERICO STATO LOGICO $|\psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle = \alpha|\bar{0}\bar{0}\bar{0}\rangle + \beta|\bar{1}\bar{1}\bar{1}\rangle$

BIT-FLIP $|\bar{0}\rangle \rightsquigarrow \dfrac{|100\rangle + |011\rangle}{\sqrt{2}}$ $\quad |\bar{1}\rangle \rightsquigarrow \dfrac{|100\rangle - |011\rangle}{\sqrt{2}}$ [BLOCCO ESCE DA SPAZIO LOGICO]

controllo blocco per blocco, procedimento di prima

1° BLOCCO: $Z_1 \otimes Z_2$, $Z_1 \otimes Z_3$ → X_1, X_2, X_3 ; 2° BLOCCO: $Z_4 \otimes Z_5$, $Z_4 \otimes Z_6$ → X_4, X_5, X_6 ; 3° BLOCCO: $Z_7 \otimes Z_8$, $Z_7 \otimes Z_9$ → X_7, X_8, X_9

PHASE-FLIP qui NON importa se flip avviene su 1°,2°,3° qubit del blocco
$|\bar{0}\rangle \rightsquigarrow \dfrac{|000\rangle - |111\rangle}{\sqrt{2}} = |\bar{1}\rangle$ $\quad |\bar{1}\rangle \rightsquigarrow \dfrac{|000\rangle + |111\rangle}{\sqrt{2}} = |\bar{0}\rangle$ [BLOCCO RIMANE IN SPAZIO LOGICO]

[INFO SU FASE RELATIVA SINGOLO BLOCCO] $(X_1 \otimes X_2 \otimes X_3)|\bar{0}\rangle = \dfrac{|111\rangle + |000\rangle}{\sqrt{2}} = |\bar{0}\rangle$ $\quad (X_1 \otimes X_2 \otimes X_3)|\bar{1}\rangle = \dfrac{|111\rangle - |000\rangle}{\sqrt{2}} = -|\bar{1}\rangle$

$|\psi\rangle = \alpha|\bar{0}\bar{0}\bar{0}\rangle + \beta|\bar{1}\bar{1}\bar{1}\rangle \rightsquigarrow |\phi\rangle = \alpha|\bar{1}\bar{0}\bar{0}\rangle + \beta|\bar{0}\bar{1}\bar{1}\rangle \neq \alpha|0_L\rangle + \beta|1_L\rangle$ [STATO ESCE DA SPAZIO LOGICO]

[INFO SU FASE RELATIVA 2 BLOCCHI DIVERSI] $\bar{X}_1 = X_1 \otimes X_2 \otimes X_3$ $\quad \bar{X}_2 = X_4 \otimes X_5 \otimes X_6$ $\quad \bar{X}_3 = X_7 \otimes X_8 \otimes X_9$

$(\bar{X}_1 \otimes \bar{X}_2)|\psi\rangle = \alpha|\bar{0}\bar{0}\bar{0}\rangle + \beta|\bar{1}\bar{1}\bar{1}\rangle = |\psi\rangle$ $\quad (\bar{X}_1 \otimes \bar{X}_2)|\phi\rangle = -\alpha|\bar{1}\bar{0}\bar{0}\rangle - \beta|\bar{0}\bar{1}\bar{1}\rangle = -|\phi\rangle$

$\bar{X}_1 \otimes \bar{X}_2$ → $\lambda = 1 \Rightarrow$ 1° e 2° BLOCCO STESSA FASE RELATIVA
→ $\lambda = -1 \Rightarrow$ 1° e 2° BLOCCO DIVERSA FASE RELATIVA

$\bar{X}_1 \otimes \bar{X}_3$ → $\lambda = 1 \Rightarrow$ 1° e 3° STESSA F.R.
→ $\lambda = -1 \Rightarrow$ 1° e 3° DIVERSA F.R.

	$\|\psi\rangle$	$\|\phi_2\rangle$	$\|\phi_1\rangle$	$\|\phi_3\rangle$
$\bar{X}_1 \otimes \bar{X}_2$	+1	−1	−1	+1
$\bar{X}_1 \otimes \bar{X}_3$	+1	−1	+1	−1
	✓	↓	↓	↘
		$Z_1 \otimes Z_2$	$Z_1 \otimes Z_3 \otimes Z_4 \otimes Z_5$	$Z_7 \otimes Z_8 \otimes Z_9$

ERRORI DEBOLI $|\bar{0}\rangle \rightsquigarrow \frac{1}{\sqrt{2}}\left[(\gamma|0\rangle+\delta|1\rangle)|000\rangle+(\gamma|1\rangle-\delta|0\rangle)|111\rangle\right]=\frac{1}{\sqrt{2}}\left[\gamma(|0000\rangle+|1111\rangle)+\delta(|1100\rangle-|0011\rangle)\right]$ $|\delta|\ll|\gamma|$

Controllo blocco per blocco, procedimento di prima

1° BLOCCO: $Z_1 \otimes Z_2$	2° BLOCCO: $Z_4 \otimes Z_5$	3° BLOCCO: $Z_7 \otimes Z_8$
$\rightarrow \lambda = 1$ OK	OK	OK
$\rightarrow \lambda = -1$ • correggo BIT FLIP $Z_1 \otimes Z_2$ & $Z_1 \otimes Z_3$	• correggo BIT-FLIP $Z_4 \otimes Z_5$ & $Z_4 \otimes Z_6$	• correggo BIT-FLIP $Z_7 \otimes Z_8$ & $Z_7 \otimes Z_9$
• correggo PHASE-FLIP $Z_1(\otimes Z_2 \otimes Z_3)$	• correggo PHASE-FLIP $Z_4(\otimes Z_5 \otimes Z_6)$	• correggo PHASE-FLIP $Z_7(\otimes Z_8 \otimes Z_9)$

16