

NUMERI COMPLESSI

$x \rightarrow$ PARTE REALE

$$z = x + iy$$

$iy \rightarrow$ PARTE IMMAGINARIA

$$\mathbb{C} = \mathbb{R} \times \mathbb{R}$$

VIENE INTRODOTTA L'UNITÀ IMMAGINARIA COL SIMBOLO i PER POTER ESTENDERE L'INSIEME DEI NUMERI \mathbb{R} .

$$i = \sqrt{-1} \quad i^2 = -1$$

ADDITIONE E SOTTRAZIONE

$$z = a + ib, z' = a' + ib' \Rightarrow z + z' = (a + a') + (b + b')i$$

MOLTIPLICAZIONE (NON È COMMUTATIVA COME OPERAZIONE)

$$z \cdot z' = (a + ib)(a' + ib') = (aa' + i^2 bb') + (ab' + a'b)i = (aa' - bb') + (ab' + a'b)i$$

CONIUGAZIONE

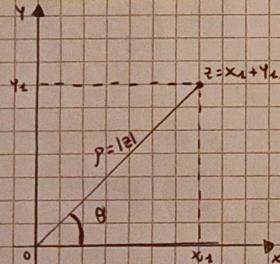
$$z = a + ib \quad z^* = a - ib$$

DIVISIONE

$$z = a + ib \quad z' = a' + ib'$$

$$\frac{z}{z'} = \frac{z}{z'} \cdot \frac{z'^*}{z'^*} = \frac{(a+ib)}{(a'+ib')} \cdot \frac{(a'-ib')}{(a'^2+b'^2)} = \frac{aa' + ibb'}{a'^2+b'^2} + i \frac{ba' - ab'}{a'^2+b'^2}$$

RAPPRESENTAZIONE GEOMETRICA



$$z = p(\cos \theta + i \sin \theta), z' = p'(\cos \theta' + i \sin \theta')$$

$$z \cdot z' = pp' [\cos(\theta + \theta') + i \sin(\theta + \theta')]$$

①

FORMULA DI TAYLOR

TALE FORMULA PERMETTE DI CALCOLARE APPROSSIMATIVAMENTE $f(a+x)$ CONOSCENDO $f(a)$ E LE PRIME n DERIVATE DI $f(x)$ VALUTATE IN a , CHE SI INDICANO $f^{(n)}(a)$

$$f(a+x) = f(a) + xf'(a) + \frac{f''(a)x^2}{2!} + \dots + \frac{f^{(n)}(a)x^n}{n!}$$

ESEMPI CON $a=0$

$$\begin{aligned} \sin(x) &= \sin(0) + \cos(0)x + \left(-\sin(0)\frac{x^2}{2!}\right) + \left(-\cos(0)\frac{x^3}{3!}\right) + \sin(0)\frac{x^4}{4!} + \dots = \\ &= 0 + 1 \cdot x + 0 \cdot \frac{x^2}{2!} + \left(-1 \cdot \frac{x^3}{3!}\right) + 0 \cdot \frac{x^4}{4!} + \dots = x - \frac{x^3}{3!} + \dots \end{aligned}$$

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots$$

$$\cos(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \frac{x^8}{8!} - \dots$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \dots$$

SE PER x SCEGLIAMO UN VALORE IMMAGINARIO $x = i\theta$ LA FORMULA DI TAYLOR DIVENTA

$$e^{i\theta} = 1 + i\theta + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} \quad \text{SCEGLIENDO } \theta = \gamma$$

$e^{i\gamma} + 1 = 0$ TALE FORMULA PERMETTE DI SCRIVERE LA RAPPRESENTAZIONE TRIGONOMETRICA DI UN NUMERO COMPLESSO DI MODULO p E ARGOMENTO θ

$$z = p e^{i\theta}$$

TEOREMA FONDAMENTALE DELL'ALGEBRA

$$a z^2 + bz + c = 0 \quad \text{CON } a, b, c \in \mathbb{R} \quad z = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

CON $b^2 - 4ac \geq 0$ ALTRIMENTI ABBIAMO SOLUZIONI COMPLESSE

$$z = \frac{-b \pm i\sqrt{4ac - b^2}}{2a}$$

MATICI

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \end{pmatrix} \quad A_{m \times n} \quad A \in \mathbb{R}^{2 \times 3}$$

m RIGHE
n COLONNE

$$B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \quad \text{SI COME } n=m \\ \text{TALE MATRICE} \\ \text{E QUADRATA}$$

ADDITIONE

$$\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} + \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} A_{11} + B_{11} & A_{12} + B_{12} \\ A_{21} + B_{21} & A_{22} + B_{22} \end{pmatrix}$$

PRODOTTO SI FA IL PRODOTTO RIGHE PER COLONNE, NOTA MA NON È COMMUTATIVO

$$\begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \end{pmatrix} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \\ B_{31} & B_{32} \end{pmatrix} = \begin{pmatrix} A_{11}B_{11} + A_{12}B_{21} + A_{13}B_{31} & A_{11}B_{12} + A_{12}B_{22} + A_{13}B_{32} \\ A_{21}B_{11} + A_{22}B_{21} + A_{23}B_{31} & A_{21}B_{12} + A_{22}B_{22} + A_{23}B_{32} \end{pmatrix}$$

$$(AB)_{ij} = \sum_k A_{ik} B_{kj}$$

$$\lambda A = \begin{pmatrix} \lambda A_{11} & \lambda A_{12} \\ \lambda A_{21} & \lambda A_{22} \end{pmatrix}$$

TRASPOSIZIONE

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \end{pmatrix} \quad A^T = \begin{pmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \\ A_{13} & A_{23} \end{pmatrix} \quad \text{UNA MATRICE QUADRATA} \\ \text{TALE CHE } A^T = A \text{ SI} \\ \text{DICE SIMMETRICA}$$

INVERSA

PER UNA MATRICE QUADRATA A, L'INVERSA A^{-1} È DEFINITA $A \cdot A^{-1} = I$

PER OTTENERE LA MATRICE INVERSA SI FA

$$A^{-1} = \frac{1}{(ad-bc)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \quad \text{con } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

L'INVERSA DI A ESISTE $\Leftrightarrow ad-bc \neq 0$

③

SPAZI VETTORIALI COMPLESSI

TAI VETTORI SONO DENOTATI COL SIMBOLICO |> NOTAZIONE DI DIRAC
(VETTORE KET)

I VETTORI $\{v_i \in \mathbb{R}^2 \mid i = 1, 2, \dots, k\}$ SONO LINEARMENTE INDEPENDENTI SE

$$a_1 v_1 + a_2 v_2 + \dots + a_k v_k = 0 \quad \text{con } a_i \in \mathbb{R} \quad \text{con } a_i = 0 \quad \forall i \in \mathbb{N}$$

ALTRIMENTI SONO

LINEARMENTE DIPENDENTI

COME CALCOLARE LA NORMA DI UN VETTORE W (LUNGHEZZA VETTORE = NORMA)

$$w = \begin{pmatrix} a \\ b \end{pmatrix} \quad \text{LA NORMA È } \|w\| = \sqrt{|a|^2 + |b|^2}$$

CON $a, b \in \mathbb{C}$

IL CONIUGATO COMPLESSO DI w È IL VETTORE RIGA $w^* = (a^*, b^*)$

PRODOTTO SCALARE DI DUE VETTORI (PRODOTTO SCALARE $\langle w_1 | w_2 \rangle \simeq (w_1, w_2)$)

$$w_1 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \quad w_2 = \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}$$

$$\langle w_1, w_2 \rangle = w_1^* w_2 = (a_1^* \quad b_1^*) \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = a_1^* a_2 + b_1^* b_2$$

PRODOTTO SCALARE

SE $\langle w_1, w_2 \rangle = 0$ ALLORA I 2 VETTORI SONO DETTI ORTOPRONALI (QUANDO SE IL PRODOTTO SCALARE 2 ENTI FORMANO UN ANGOLI RETTO)

NOTA $\langle w_1 | w_2 \rangle = 1$

SE 2 VETTORI v_1 E v_2 SONO LINEARMENTE INDEPENDENTI ALLORA FORMANO UNA BASE ORTONORMALE

SONO ORTONORMALI QUANDO: SONO ORTOPRONALI OSSIA IL PRODOTTO SCALARE È PARI A 1

E LE LORO NORMA È PARI A 1

④

OPERATORE LINEARE

È UN OPERATORE LINEARE APPLICATO AD UN VETTORE TRASFORMA UN VETTORE IN UN ALTRO VETTORE.

$$A|v\rangle = |w\rangle, \quad A(\alpha|v\rangle + \beta|w\rangle) = \alpha A|v\rangle + \beta A|w\rangle$$

RAPPRESENTAZIONE MATRICIALE DI UN OPERATORE LINEARE

$$A|u_1\rangle = |u_2\rangle + 2|u_3\rangle$$

$$\begin{pmatrix} 1 & 4 & 1+2i \\ 0 & 3i & 7 \\ 2 & -5 & 0 \end{pmatrix}$$

$$A|u_2\rangle = 4|u_1\rangle + 3i|u_2\rangle - 5|u_3\rangle$$

$$A|u_3\rangle = (-1+2i)|u_1\rangle + 7|u_2\rangle$$

SOMMA E PRODOTTO DI OPERATORI

$$(A+B)|v\rangle = A|v\rangle + B|v\rangle \quad \text{con } A, B \text{ OPERATORI}$$

$$L'OPERATORE NUOLO |0\rangle \text{ È TALE CHE } |0\rangle = 0 \forall |v\rangle$$

$$AB|v\rangle = A(B|v\rangle)$$

OPERATORE IDENTITÀ

È UN OPERATORE LINEARE CHE PRESERVA I VETTORI SU CUI AGISCE OVVERO:

$$I|v\rangle = |v\rangle \quad \forall |v\rangle$$

$$AI = IA = A$$

OPERATORE INVERSO

È UN OPERATORE CHE QUANDO È APPLICATO ALL'OUTPUT PRODOTTO DELL'OPERATORE ORIGINALE, RIPORTA IL VETTORE ALLO STATO DI PARTENZA.

$$A^{-1} \text{ INVERSO DI } A$$

$$A^{-1}(A(|v\rangle)) = |v\rangle$$

(5)

OPERATORE UNITARIO

È UN TIPO PARTICOLARE DI OPERATORE LINEARE CHE PRESERVA LA NORMA DEI VETTORI SU CUI AGISCE.

1) CONSERVA LA NORMA

2) PRESERVA L'ORTOGONALITÀ OVVERO SE U È UN OPERATORE UNITARIO E $|v\rangle$ E $|w\rangle$ SONO 2 VETTORI ORTOGONALI ALLORA ANCHE I VETTORI $U|v\rangle$ E $U|w\rangle$ SONO ORTOGONALI

3) UN OPERATORE UNITARIO HA UN OPERATORE INVERSO CHE È ANCH'ESSO UNITARIO.

4) PER LE RETELE \rightarrow 2) ALLORA SE DUE VETTORI $|v\rangle$ E $|w\rangle$ SONO ORTOGONALI ALLORA ANCHE $U|v\rangle$ E $U|w\rangle$ SONO ORTOGONALI TRA DI LORO.

5) CONSERVAZIONE DELL'ANGOLI: SE U È UN OPERATORE UNITARIO, ALLORA L'ANGOLI TRA DUE VETTORI $|v\rangle$ E $|w\rangle$ È UGUALE ALL'ANGOLI TRA IL LORO COPII STORNATI $U|v\rangle$ E $U|w\rangle$.

OPERATORE AGGIUNTO

DATO UN'OPERATORE A SI DEFINISCE AGGIUNTO A^+ UN OPERATORE CONIUGATO TRASTONICO. SI DEFINISCE COME segue:

$$(|\psi\rangle, A|\phi\rangle) \equiv (A^+|\psi\rangle, |\phi\rangle) \quad \forall |\psi\rangle, |\phi\rangle$$

(6)

QUBIT → È L'UNITÀ DI INFORMAZIONE DI BASE NELLA COMPUTAZIONE QUANTISTICA

PUÒ RAPPRESENTARE LO STATO DI UN qubit MEDIANTE UN VETTORE UNITARIO IN UNO SPAZIO VETTORIALE COMPLESSO A 2 DIMENSIONI.

I VETTORI $|0\rangle$ e $|1\rangle$ FORMANO UNA BASE ORTHONORMALE

IL VETTORE $|0\rangle$ VIENE RAPPRESENTATO COSÌ $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

IL VETTORE $|1\rangle$ VIENE RAPPRESENTATO COSÌ $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

LA DIFFERENZA TRA bit E qubit STA NEL FATTO CHE UN qubit SI PUÒ TROVARE ANCHE IN ALTRI STATI DIVERSI DA $|0\rangle$ E $|1\rangle$. INFATTI, OGNI COMBINAZIONE LINEARE

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \text{ DOVE } \alpha, \beta \in \mathbb{C} \text{ TAL CHE } |\alpha|^2 + |\beta|^2 = 1$$

È UN POSSIBILE STATO PER UN qubit. IL VETTORE $|\Psi\rangle$ SI PUÒ RAPPRESENTARE COSÌ:

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \text{ TAL STATI SONO SPesso CHIAMATI SOVRAPPZIONI.}$$

PRINCIPIO DI MISURAZIONE

LA MECCANICA QUANTISTICA CI DICE CHE QUANDO MISURIAMO UN qubit POSSIAMO OBTENERE SOLO LO STATO $|0\rangle$ CON UNA PROBABILITÀ PARI A $|\alpha|^2$ OPPURE LO STATO $|1\rangle$ CON UNA PROBABILITÀ PARI A $|\beta|^2$.

$|\alpha|^2 + |\beta|^2 = 1$ GEOMETRICAMENTE SIGNIFICA CHE GLI STATI DI UN qubit SONO VETTORI NORMALIZZATI (DI LUNGHEZZA 1).

UN qubit SI PUÒ TROVARE IN UN NUMERO DI STATI CHE È INFINTAMENTE MAGGIORE DI QUELLO DEI POSSIBILI STATI DI UN bit CLASSICO.
FISICAMENTE PERò, NON È POSSIBILE OSSERVARE DIRETTAMENTE QUESTI STATI DEL qubit POICHÉ LA MISURAZIONE DI UN qubit DÀ SEMPRE COME RISULTATO O LO STATO $|0\rangle$ O LO STATO $|1\rangle$.

Così, un qubit SI PUÒ TROVARE NELLO STATO $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ FINO AL MOMENTO IN CUI

SI È OSSERVATO, NEI MOMENTI IN CUI LO MISURIAMO IL RISULTATO SARÀ $|0\rangle$ NEL 50% DEI CASI E $|1\rangle$ NEL RIMANENTE 50% DEI CASI.

REGOLA DI BORN

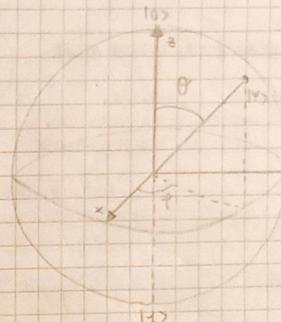
$$|\alpha|^2 + |\beta|^2 = 1$$

$$P(|0\rangle) = |\alpha|^2 \quad P(|1\rangle) = |\beta|^2$$

VETTORE UNITARIO
È UN VETTORE DI LUNGHEZZA 1
CHE CONSERVA LA DIREZIONE DI UN VETTORE PIÙ LUNGO, ONDRA,
È UN VETTORE NORMALIZZATO CHE PUNTA NELLA STESSA DIREZIONE DEL VETTORE ORIGINALE MA DI NORMA PARI A 1

INTERPRETAZIONE GEOMETRICA DEL QUBIT

LA SFERA DI BLOCH È UNA FIGURA GEOMETRICA CHE ASSOCIA GLI STATI DI UN qubit AI PUNTI SULLA SUPERFICIE DI UNA SFERA DI RAGGIO UNITARIO. IL POLO SUD DELLA SFERA CORRISPONDE A $|1\rangle$ MENTRE IL POLO NORD A $|0\rangle$, INGLE LE ALTRE LOCAZIONI SONO LE SOVRAPPZIONI QUANTISTICHE DI 0 E 1.



ESISTE UNA CORRISPONDENZA BIUNIVOCAMENTE TRA UN GENERICO STATO DI UN qubit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$

E UN PUNTO SULLA SFERA UNITARIA IN \mathbb{R}^3 RAPPRESENTATO COME

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right)|1\rangle, \text{ DOVE } \theta, \phi \in \mathbb{R}$$

MANCANO I PASSAGGI PER ARRIVARE A QUESTA FORMULA

INTERPRETAZIONE FISICA DI UN QUBIT

[POLARIZZAZIONE SI RIFERISCE ALLO DIREZIONE
O ALL'ORIENTAMENTO DI UN'ENTITÀ FISICA]

⑨

UN QUBIT HA UN CORRISPONDENTE NEL MONDO REALE, IN PARTICOLARE
UN QUALSIASI SISTEMA FISICO CON ALMENO DUE LIVELLI DI ENERGIA DISCRETI
E SUFFICIENTEMENTE SEPARATI E' UN POSSIBILE QUBIT.
PER RENDERE PIEMONTE UN QUBIT GLI APPROCCI PIÙ COMUNI SONO:

- LE DUE DIVERSE POLARIZZAZIONE DI UN FOTONE
- DUE LIVELLI DI ENERGIA DI UN ELETTRONE CHE CIRCA IN UN SINGOLO ATOMO.

FOTONE → È UNA PARTICELLA ELEMENTARE CHE COSTITUISCE L'UNICO SONORIENTE DELLA LUCE E IN PIRETTO FORTE DI RADIAZIONE ELETROMAGNETICO. È UNA PARTICELLA SENZA MASSA E SENZA CARICA ELETTRICA CHE SI PROPAGA NEL VUOTO CON VELOCITÀ DELLA LUCE.

IN SINTESI, I FOTONI SONO PARTICELLE NEUTRE CHE NON PORTANO CARICA ELETTRICA, MA INTERAGISCONO CON LE PARTICELLE CARICATE E CON I CAMPI ELETROMAGNETICI ATTRaverso LE FORZE ELETROMAGNETICHE.

IN QUANTISTICA SI CONSIDERANO DUE POLARIZZAZIONI DI UN FOTONE.

LA POLARIZZAZIONE DI UN FOTONE NELL'QUANTISTICA SI RIFERISCE ALLE 2 POSSIBILI DIREZIONI DI OSCILLAZIONE DEL CAMPO ELETTRICO ASSOCIAUTO AL FOTONE DURANTE LA SUA PROPAGAZIONE.

QUESTE 2 POLARIZZAZIONI SONO Dette:

- ① POLARIZZAZIONE ORIZZONTALE
- ② POLARIZZAZIONE VERTICALE

- ① IL PRIMO HA IL CAMPO ELETTRICO CHE OSCILLA ALONG UN PIANO ORIZZONTALE
- ② IL SECONDO HA IL CAMPO ELETTRICO CHE OSCILLA ALONG UN PIANO VERTICALE

QUESTE DUE POLARIZZAZIONI SONO PERPENDICOLARI TRA LORO.

NOTA CHE IN UN DATO STATO DI POLARIZZAZIONE, UN SINGOLO FOTONE PUÒ ESSERE OSSERVATO SOLO IN UNA DUE DUE POLARIZZAZIONI. TUTTOVA, È POSSIBILE OTTERE STATI DI POLARIZZAZIONE CHE SONO UNA COMBINAZIONE LINEARE DI QUESTE 2 POLARIZZAZIONI DI BASE. AD ESEMPIO, UN FOTONE PUÒ ESSERE POLARIZZATO LINEARMENTE AD UN ANGOLO INCLINATO RISpetto AL PIANO VERTICALE O ORIZZONTALE.

ATOMO → FORMATO DA 3 COMPONENTI: PROTONI (PARTICELLE SUBATOMICHE POSITIVE), NEUTRONI (PARTICELLE SUBATOMICHE CON CARICA NEUTRA) E ELETTRONI (PARTICELLE SUBATOMICHE NEGATIVE).

I PROTONI E I NEUTRONI SI TROVANO DENTRO IL NUCLEO DI UN ATOMO E HANNO UNA MASSA SIMILE MENTRE GLI ELETTRONI CIRCOLANO ATRAMO AL NUCLEO ATOMICO IN SPECIFICHE ROTAZIONI CHIAMATE ORBITALI O LIVELLI ENERGETICI.

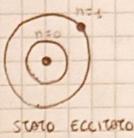
GLI ELETTRONI HANNO UNA MASSA MOLTO INFERIORE RISPETTO AI PROTONI E AI NEUTRONI. IL NUMERO DI ELETTRONI IN UN ATOMO DETERMINA IL SUO NUMERO ATOMICO.

GL ATOMI SONO MOLTO PIÙ GRANDI DEI FOTONI.

CONSIDERA IL SISTEMA COSTITUITO DALL'ATOMO DI IDROGENO
(IN GENERE SONO USATI NEI LABORATORI GLI ATOMI DI RUBIDIUM E BERILLIO)

⑩

LO STATO $|10\rangle$ DEL QUBIT PUÒ ESSERE RAPPRESENTATO DAL PRIMO LIVELLO DI ENERGIA ($n=0$) E CORRISPONDE ALLO STATO BASE DELL'ELETTRONE MENTRE LO STATO $|11\rangle$ DEL SECONDO LIVELLO DI ENERGIA ($n=1$) CORRISPONDE ALLO STATO ECCITATO DELL'ELETTRONE.



IL PASSAGGIO DELL'ELETTRONE DA UNO STATO ALL'ALTRO PUÒ ESSERE RAPPRESENTATO SOTTOPOENDO L'ELETTRONE AD UN IMPULSO LASER DI AMPLITUDINE "INTENSITÀ", DURATA E LUNGHEZZA D'ONDA.

REGISTRI QUANTISTICI

QUANTI STATI SI POSSONO OTTENERE CON n qubit?

LO SPAZIO DEGLI STATI GENERATO DA UN SISTEMA DI n qubit HA DIMENSIONE 2^n . OGNI VETTORE NORMALIZZATO IN QUESTO SPAZIO RAPPRESENTA UN POSSIBILE STATO COMPUTAZIONALE, CHE SI CHIAMA REGISTRO QUANTISTICO A n qubit.

$$\text{IL CASO DI 1 qubit} \quad |0\rangle \quad |1\rangle \quad \text{REGISTRO A 1qubit}$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad |1\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\text{IL CASO DI 2 qubit} \quad |00\rangle \quad |01\rangle \quad |10\rangle \quad |11\rangle \quad \text{REGISTRO A 2qubit}$$

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad |1\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$\text{IL CASO DI 3 qubit} \quad |000\rangle \quad |001\rangle \quad |010\rangle \quad |011\rangle \quad |100\rangle \quad |101\rangle \quad |110\rangle \quad |111\rangle \quad \text{REGISTRO A 3qubit}$$

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|\Psi\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle$$

*) SI COSTRUISCE LA BASE COMPUTAZIONALE DELLO SPAZIO DEGLI STATI COME FORMATO DEI VETTORI SOPRA (NEL CASO DI 1 qubit, 2 qubit, 3 qubit ecc.)

$|x\rangle|\gamma\rangle$ È PARI A $|x\rangle \otimes |\gamma\rangle$ IL PRODOTTO TENSORE DI $x \times y$.

PRODOTTO TENSORE \rightarrow OPERAZIONE CHE COMBINA SPAZI VETTORIALI PER FORMARE SPAZI VETTORIALI PIÙ GRANDI

(1)

$$M = \begin{bmatrix} 1 & 3 \\ 0 & 1 \\ 0 & -1 \end{bmatrix} \quad N = \begin{bmatrix} 0 & 1 & 0 & 3 \\ -1 & 2 & -3 & 6 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & -1 & 2 \end{bmatrix} \quad M \otimes N = \begin{bmatrix} 0 & 1 & 0 & 3 \\ -1 & 2 & -3 & 6 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & -1 & 2 \end{bmatrix}$$

MATRICE $A_{m \times n}$ $B_{p \times q}$ $A \otimes B = C_{(m+p) \times (n+q)}$

STATI ENTANGLED

UNA PROPRIETÀ IMPORTANTE DEI REGISTRI QUANTISTICI A n qubit È CHE NON È SEMPRE POSSIBILE DECOMPORLI NEI STATI DEI QUBIT COMPONENTI. GLI STATI DI QUESTO TIPO SONO DETTI ENTANGLED E GODONO DI PROPRIETÀ CHE NON SI POSSANO RITROVARE IN NESSUN OGGETTO DELLA FISICA CLASSICA.
I MEMBRI DI UNA COLLEZIONE ENTANGLED NON HANNO UN PROPRIO STATO INDIVIDUALE, SOLO L'INTERA COLLEZIONE CORRISPONE A UNO STATO BEN DEFINITO. TUTTI STATI SI COMPORTANO COME SE FOSSENNO STRETTAMENTE CONNESSI L'UNO ALL'ALTRO INDEPENDENTEMENTE DALLA DISTANZA CHE LI SEPARA.
AD ESEMPIO, UNA MISURAZIONE DI UNO DEI 2 STATI DI UNA COPPIA ENTANGLED FORNISCE SIMULTANEAEMENTE INFORMAZIONI RIGUARDO L'ALTRO STATO.

LO STATO $|100\rangle + |111\rangle$ NON PUÒ ESSERE FATTORIZZATO NEL PRODOTTO TENSORE DI 2 qubit INDEPENDENTI, CIOÈ NON ESISTONO a_1, a_2, b_1, b_2 TALI CHE

$$|100\rangle + |111\rangle = (a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle)$$

QUESTA UGUALDADÈ NON SI PUÒ MAI VERIFICARE

DA COMPRENDERE COSA VOLGONO DIRE FATTORIZZARE IN QUESTO CASO?

$$|a\rangle \otimes |b\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|0\rangle + \delta|1\rangle$$

CONFRONTA QUESTA ESPRESSIONE CON $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
SI PUÒ OSSERVARE CHE

$$\alpha = \frac{1}{\sqrt{2}}, \quad \beta = 0, \quad \gamma = 0, \quad \delta = \frac{1}{\sqrt{2}}$$

SE $\alpha = 0$ ALLORA $\beta = 0 \vee \delta = 0$ PERÒ SE $\alpha = 0$ ALLORA $\beta = 0 \neq \frac{1}{\sqrt{2}}$

OPPURE SE $\beta = 0$ $\alpha = \frac{1}{\sqrt{2}}$ ALLORA $\gamma = 0 \neq \frac{1}{\sqrt{2}}$

QUINDI NON ESISTONO $\alpha, \beta, \gamma, \delta$ TALI CHE $|a\rangle \otimes |b\rangle$ SIA UGUALE A $|\Phi^+\rangle$ DI CONSEQUENZA QUESTO STATO NON PUÒ ESSERE FATTORIZZATO NEL PRODOTTO TENSORE DI DUE qubit INDEPENDENTI E QUINDI È UNO STATO ENTANGLED

$$|10\rangle + |11\rangle + |01\rangle + |00\rangle$$

$$= |10\rangle (|11\rangle + |01\rangle)$$

$$|10\rangle + |11\rangle = (a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle)$$

$$= 2\sqrt{|00\rangle} + 2\sqrt{|11\rangle} + 2\sqrt{|10\rangle} + 2\sqrt{|01\rangle}$$

$$\alpha = \frac{1}{\sqrt{2}}, \quad \beta = \frac{1}{\sqrt{2}}, \quad \gamma = 0, \quad \delta = 0$$

$$|10\rangle + |11\rangle =$$

$$\alpha = \frac{1}{\sqrt{2}}, \quad \beta = \frac{1}{\sqrt{2}}, \quad \gamma = 0, \quad \delta = 0$$

$$|11\rangle (|10\rangle + |01\rangle)$$

$$|10\rangle \cdot |11\rangle + |11\rangle \cdot |10\rangle$$

$$|10\rangle \cdot |10\rangle + |11\rangle \cdot |11\rangle$$

→ $\frac{1}{\sqrt{2}}(|100\rangle + |111\rangle)$ { SE ALICE FA UNA MISURA SUL SUO qubit EPR PUÒ OTTENERE α OPPURE β CON VULGARE PROBABILITÀ E ANCHE BOB NELLA SUA MISURA OTTERRA' CERTAMENTE α MA DI QUALE DEI DUE STATI? LE 2 STATISTICHE NON SONO CORRELATE TRA LORO E L'ORDINE DELLE MISURAZIONI (OPERA I RISULTATI OBTENUTI DA ALICE E DA BOB) NON CAMBIA A SECONDA DI CHI LE FA PRIMA.

→ $\frac{1}{\sqrt{2}}(|100\rangle + |111\rangle)$ { SE ALICE OBTIENE α L'INTERO SISTEMA COLLASCA NELLO STATO $|100\rangle$ IN QUESTO CASO LE MISURAZIONI DI ALICE E DI BOB SONO CORRELATE

PORTE LOGICHE QUANTISTICHE

UN COMPUTER QUANTISTICO È FORMATO DA CIRCUITI QUANTISTICI COSTITUITI DA PORTE LOGICHE QUANTISTICHE ELEMENTARI

PER DEFINIRE UN'OPERAZIONE SU UN QUBIT, NON BASTA STABILIRE LA SUA AZIONE SULLI STATI DI BASE $|0\rangle$ E $|1\rangle$, BENJI SI DEVE SPECIFICARE ANCHE COME DOVE ESSERE TRASFORMATO UN QUBIT CHE SI TROVA IN UNA SOVRAPPOSIZIONE DEGLI STATI $|0\rangle$ E $|1\rangle$.

MATRICI UNITARIE

DATA UNA MATRICE $n \times n$ A, LA TRASPPOSTA A^T È DEFINITA DA $(A^T)_{ij} = (A)_{ji}$

LA CONIGUATA A^* DI A È LA MATRICE $(A^*)_{ij} = (A^T)_{ji}$. LA MATERIALE ASSOCIA

A^+ DI A È LA MATRICE $A^+ = (A^T)^*$

UNA MATRICE A È DETTA UNITARIA SE $A^+ = A^{-1}$, DOVE A^{-1} È L'INVERSA DI A

CIOÈ $A A^{-1} = I$ ($I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ MATERIALE IDENTITÀ)

MATRICI DI PAULI

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

$$X^{-1} = \frac{1}{(ad-bc)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{0+1} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -1 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$X X^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$Y^{-1} = \frac{1}{(ad-bc)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{0+i^2} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = -i \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Y Y^{-1} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -i^2 & 0 \\ 0 & -i^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$Z^{-1} = \frac{1}{(ad)-(bc)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{-1-0} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = -1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$Z Z^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

(12)

PORTE LOGICHE QUANTISTICHE A UN qubit

MATRICE CORRISPONDENTE AL NOT QUANTISTICO

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

(cioè PRE FA IL VETTORE INVERTITO)

NOTA UNA FUNZIONE LINEARE TRASFORMA UN qubit IN UN qubit SE E SOLO SE E' UNITARIA.

LA PORTA Z: APPLICA SOLO UNA COMPONENTE \rightarrow SCOMBINARE IL SEGNO

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

LA PORTA DI HADAMARD: IL SUO EFFETTO È QUELLO DI TRASFORMARE UNO STATO BASE IN UNA SOVRAPPOSIZIONE CHE RISULTA, DOPO UNA MISURAZIONE NELLA BASE COMPUTAZIONALE, ESSERE 0 O 1 CON UGUALE PROBABILITÀ.

TUTTI PORTA LOGICHE SONO COST RAPPRESENTATE:

$$\text{CON } |Y\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|Y\rangle \xrightarrow{X} \beta|0\rangle + \alpha|1\rangle$$

$$|Y\rangle \xrightarrow{Z} \bar{\alpha}|0\rangle - \bar{\beta}|1\rangle$$

$$|Y\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

RICORDA LE MATERIE X, Z CON LA MATERIA Y

$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ SONO LE MATERIE DI PAULI
E RAPPRESENTANO LE COMPONENTI X, Y, Z DELLO SPIN DI UN ELETTRONE.

NOTA GATE S DETTO GATE DI FASE

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

PORTE LOGICHE QUANTISTICHE A PIÙ QUBIT

(4)

LE OPERAZIONI SU REGISTRI QUANTISTICI DI DUE O PIÙ QUBIT SONO NECESSARIE PER DESCRIVERE LE TRASFORMAZIONI DI STATI COMPOSTI E IN PARTICOLARE NEGLI STATI ENTANGLED.

Abbiamo visto che non sempre un registro di 2 qubit può essere decomposto nel prodotto tensoriale dei singoli qubit componenti, di conseguenza non possiamo in questi casi simulare un'operazione sui due qubit mediante operazioni su ciascun qubit componente.

PORTA CNOT (CONTROLLED-NOT) È L'ANALOGO QUANTISTICO DI XOR.

OPERA SU DUE QUBIT: IL PRIMO È IL QUBIT DI CONTROLLO E IL SECONDO qubit è il target.

SE IL CONTROLLO È ZERO IL TARGET È LASCIATO INVARIATO, SE IL CONTROLLO È UNO, ALLORA IL TARGET VIENE NEGATO.

$$\begin{array}{l} |1A\rangle \xrightarrow{\text{CNOT}} |1A\rangle \\ |1B\rangle \xrightarrow{\text{CNOT}} |1A\oplus B\rangle \end{array} \quad \begin{array}{l} |AB\rangle \xrightarrow{\text{CNOT}} |AB\rangle \\ |00\rangle \xrightarrow{\text{CNOT}} |00\rangle \\ |01\rangle \xrightarrow{\text{CNOT}} |01\rangle \\ |10\rangle \xrightarrow{\text{CNOT}} |11\rangle \\ |11\rangle \xrightarrow{\text{CNOT}} |10\rangle \end{array}$$

A è il qubit di controllo
B è il qubit target

RAPPRESENTAZIONE MATETRICIALE DELLA CNOT È:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

VERIANTE DELLA CNOT

$$\begin{array}{l} |1A\rangle \xrightarrow{\text{CNOT}} |1A\rangle \\ |1B\rangle \xrightarrow{\text{CNOT}} |1A\oplus B\rangle \end{array}$$

IL TARGET È NEGATO SE IL QUBIT DI CONTROLLO È ZERO ANZICHÉ UNO.

$$\begin{array}{ll} AB & A B \\ |00\rangle \mapsto |01\rangle & |01\rangle \\ |01\rangle \mapsto |00\rangle & |10\rangle \\ |11\rangle \mapsto |10\rangle & |00\rangle \\ |10\rangle \mapsto |11\rangle & |01\rangle \\ |11\rangle \mapsto |11\rangle & |00\rangle \end{array}$$

NOTA CHE IL CNOT, COME TUTTE LE TRANSFORMAZIONI UNITARIE, È INVERTIBILE OSSIA DALL'OUTPUT SI PUÒ SEMPRE OTTENERE L'INPUT. CIÒ NON È VERO PER LE PORTE CLASSICHE COME XOR E NAND.

In GENERALE LE OPERAZIONI CLASSICHE SONO IRREVERSIBILI.

LA PORTA CNOT E LE PORTE A UN qubit RAPPRESENTANO I PROTOTIPI DI TUTTE LE PORTE LOGICHE QUANTISTICHE.

CIRCUITI QUANTISTICI EXCHANGER

(5)

IL CIRCUITO REALIZZA LO SCAMBIO DEGLI STATI DI 2 qubit.

IN INPUT ABBIAMO IL REGISTRO DI 2 qubit $|a, b\rangle$ E VIENE EFFETTUATO UN CNOT CON IL PRIMO qubit DI CONTROLLO A.

$$|1A\rangle = |10\rangle + \beta |11\rangle$$

$$|1B\rangle = \alpha |10\rangle + \beta |11\rangle$$

$$|1Y_0\rangle = |1Y_1\rangle = |1Y_2\rangle = |1Y_3\rangle$$

$$|1Y_3\rangle = |1P\rangle \cdot |1A\rangle = (\alpha |10\rangle + \beta |11\rangle) (|10\rangle + \beta |11\rangle) = \alpha^2 |100\rangle + \alpha \beta |101\rangle + \alpha \beta |110\rangle + \beta^2 |111\rangle$$

QUESTO È CIÒ CHE CI DÀE DANE $|1Y_3\rangle$ AFFINCHÉ LO SCAMBIO È ANDATO A BUON FINE.

$$|1Y_0\rangle = |1Y_1\rangle \cdot |1P\rangle = (\alpha |10\rangle + \beta |11\rangle) (\alpha |10\rangle + \beta |11\rangle) = \alpha^2 |100\rangle + 2\alpha \beta |101\rangle + \beta^2 |110\rangle + \beta^2 |111\rangle$$

A Σ_0 APPLICO LA CNOT CON qubit di controllo A

$$\text{CNOT } |\Sigma_0\rangle = |\Sigma_1\rangle = \alpha |100\rangle + \alpha |101\rangle + \beta |110\rangle + \beta |111\rangle$$

A Σ_1 APPLICO CNOT CON qubit di controllo B

$$\text{CNOT } |\Sigma_1\rangle = |\Sigma_2\rangle = \alpha |100\rangle + \alpha |111\rangle + \beta |101\rangle + \beta |110\rangle$$

A Σ_2 APPLICO CNOT CON qubit di controllo A

$$\text{CNOT } |\Sigma_2\rangle = |\Sigma_3\rangle = \alpha |100\rangle + \alpha |101\rangle + \beta |110\rangle + \beta |111\rangle$$

SIMBOLO CIRUITALE PER LA MISURAZIONE DI UN q-bit

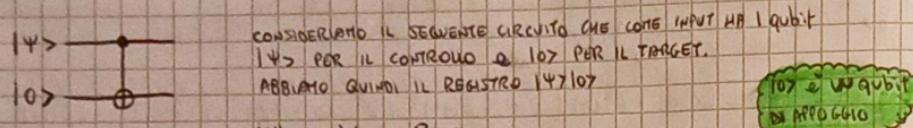
IL RISULTATO DELLA MISURAZIONE È UN bit CLASSICO M CHE SARÀ 0 oppure 1 CON LA STESSA PROBABILITÀ.

NO-CLONING

UNA PROPRIETÀ DEI SISTEMI QUANTISTICI È IL TEOREMA DEL NO-CLONING.

NON ESISTE UNA TRANSFORMAZIONE UNITARIA M TALE CHE $M|\Psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle$
PER OGNI STATO $|\Psi\rangle$

DIMOSTRAZIONE PER ASSURDO PER DIMOSTRARE IL TEOREMA NO-CLONING.



$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

NOI IN USCITA VOGLIAMO OBTENERE $|\Psi\rangle|\Psi\rangle = (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) =$

$$= \alpha^2|00\rangle + 2\alpha\beta|01\rangle + \beta^2|11\rangle.$$

IN INGRESSO POSSIAMO

$$|\Psi\rangle|0\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|0\rangle$$

APPLICO CHI T → OTTENGO $\alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle$

OSSERVIAMO CHE QUESTO STATO È IN GENERALE DIVERSO DAL RISULTATO $|\Psi\rangle|\Psi\rangle$
A MENO CHE $\alpha = \beta = 0$

MA SICCOME $|\alpha|^2 + |\beta|^2 = 1$ DIMOSTRA CHE QUESTO CIRCUITO NON E' EFFETTIVO.
LA COPIA DI UN qubit.

PERCHÉ SI USA LA PORTA CNOT?

(16)

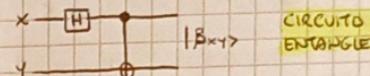
STATI DI BELL

ABBIAMO VISTO CHE LA PORTA CNOT PUÒ ESSERE USATA PER CREARE STATI CHE SONO ENTANGLED.

IL CIRCUITO QUI SOTTO GENERA PER OGNI STATO COMBINAZIONALE $|00\rangle, |10\rangle, |11\rangle, |01\rangle$ UN PARTICOLARE STATO ENTANGLED.

QUESTI STATI CHE INDICHIAMO CON $B_{00}, B_{01}, B_{10}, B_{11}$ SONO CHIAMATI STATI DI BELL
O BPR (EINSTEIN, PODOLSKY, ROSEN)

L'INTERAZIONE TRA QUESTE COPPIE DI STATI QUANTISTICI DA LUCIO A UN FENOMENO CHE VIOLAVA I PRINCIPI FONDAMENTALI DELLA TEORIA DELLA RELATIVITÀ.



$$|00\rangle \text{ APPLICO } H \quad \frac{|0\rangle + |1\rangle}{\sqrt{2}} \cdot |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \text{ STATO ENTANGLED PER } |00\rangle \quad B_{00}$$

$$|01\rangle \text{ APPLICO } H \quad \frac{|0\rangle + |1\rangle}{\sqrt{2}} \cdot |1\rangle = \frac{|01\rangle + |11\rangle}{\sqrt{2}} = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \text{ STATO ENTANGLED PER } |01\rangle \quad B_{01}$$

$$|10\rangle \text{ APPLICO } H \quad \frac{|0\rangle - |1\rangle}{\sqrt{2}} \cdot |0\rangle = \frac{|00\rangle - |10\rangle}{\sqrt{2}} = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \text{ STATO ENTANGLED PER } |10\rangle \quad B_{10}$$

$$|11\rangle \text{ APPLICO } H \quad \frac{|0\rangle - |1\rangle}{\sqrt{2}} \cdot |1\rangle = \frac{|01\rangle - |11\rangle}{\sqrt{2}} = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \text{ STATO ENTANGLED PER } |11\rangle \quad B_{11}$$

GLI STATI DI BELL SONO ??
ORTONORMALI TRA LORO

(17)

$$\text{esercizio} \quad |++\rangle + |--\rangle = |00\rangle + |11\rangle$$

$$|00\rangle + |11\rangle$$

$$\left| +\rangle = \frac{1}{\sqrt{2}} (\lvert 0\rangle + \lvert 1\rangle) \right. \\ \left. -\rangle = \frac{1}{\sqrt{2}} (\lvert 0\rangle - \lvert 1\rangle) \right.$$

SONO ALTRI POSSIBILI
STATI DI qubit

(18)

$$|+\rangle |+\rangle = |+\rangle = \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} (\lvert 0\rangle + \lvert 1\rangle) (\lvert 0\rangle + \lvert 1\rangle) = \frac{1}{2} (\lvert 00\rangle + \lvert 01\rangle + \lvert 10\rangle + \lvert 11\rangle)$$

$$|- \rangle |- \rangle = | - \rangle = \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} (\lvert 0\rangle - \lvert 1\rangle) (\lvert 0\rangle - \lvert 1\rangle) = \frac{1}{2} (\lvert 00\rangle - \lvert 01\rangle - \lvert 10\rangle + \lvert 11\rangle)$$

$$|++\rangle + |--\rangle = \left[\frac{1}{2} (\lvert 00\rangle + \lvert 01\rangle + \lvert 10\rangle + \lvert 11\rangle) + \frac{1}{2} (\lvert 00\rangle - \lvert 01\rangle - \lvert 10\rangle + \lvert 11\rangle) \right] = |00\rangle + |11\rangle$$

$$\text{esercizio}$$

$$- (|+-\rangle - |-+\rangle) = |0+\rangle - |1-\rangle$$

$$|+-\rangle = \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} (\lvert 0\rangle + \lvert 1\rangle) (\lvert 0\rangle - \lvert 1\rangle) = \frac{1}{2} (\lvert 00\rangle - \lvert 01\rangle + \lvert 10\rangle - \lvert 11\rangle)$$

$$|+-\rangle = \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} (\lvert 0\rangle - \lvert 1\rangle) (\lvert 0\rangle + \lvert 1\rangle) = \frac{1}{2} (\lvert 00\rangle - \lvert 01\rangle + \lvert 10\rangle - \lvert 11\rangle)$$

$$- (|+-\rangle - |-+\rangle) = - \left(\frac{1}{2} (\lvert 00\rangle - \lvert 01\rangle + \lvert 10\rangle - \lvert 11\rangle) - \frac{1}{2} (\lvert 00\rangle - \lvert 01\rangle + \lvert 01\rangle - \lvert 11\rangle) \right) =$$

$$= - (- \lvert 0+\rangle + \lvert 1-\rangle) = \lvert 0+\rangle - \lvert 1-\rangle$$

TELETRASPORTO QUANTISTICO (1993)

IL TELETRASPORTO QUANTISTICO È UNA TECNICA USATA PER TRASPORTARE STATI QUANTISTICI DA UN POSTO AD UN ALTRO SFRUTTANDO SOLO LA TRANSMISSIONE DI BIT CLASSICI.

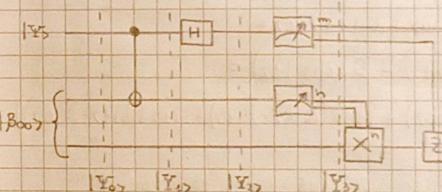
(IL 13 SETTEMBRE 2012) IN UN ARTICOLO VIENE RIPORTATO CHE UN ESTERIMENTO CHE HA PERMESSO AD UN TEAM DI TELETRASPORTARE FOTONI AD UNA DISTANZA DI CIRCA 143 KM TRA DUE ISOLE DELLE CANARIE (TRA LA PAULO E TENERIFE).

SCENARIO → IMMAGINIAMO UNA SITUAZIONE IN CUI ALICE (A) DEVE FAR CONOSCERE LO STATO DI UN qubit A BOB (B).
 A NON CONOSCE LO STATO DEL qubit E PER IL TEOREMA DEL NO-CLONING STABBIANO CHE NON SI PUÒ FARE UNA COPIA DI QUESTO qubit. INOLTRÒ A PUÒ SOLO MANDARE A B INFORMAZIONE CLASSICA, CIOÈ I VALORI 0 E 1 DI UN BIT CLASSICO.

VEDIAMO COME CIÒ È POSSIBILE GRAZIE ALLE PROPRIETÀ DEGLI STATI ENTANGLED.

POTESTI FONDAMENTALE È CHE BOB E ALICE POSSESSANO CIASCUNO UN qubit DI UNA COPPIA EPR GENERATA PRECEDENTEMENTE. ALICE PUÒ OPERARE SUL SUO qubit E BOB PUÒ FARLO ALTRETTANNO SULLA SUA PARTE DELLA COPPIA EPR.

IL CIRCUITO ILLUSTRA COME AVVIENE LA TRANSMISSIONE DI UN qubit $|Y\rangle = \alpha|0\rangle + \beta|1\rangle$ DI CUI SI IGNORANO LE AMPIZZE DI α E β , LA PARTE DI ALICE E BOB, LO STATO DI INIZIO DEL CIRCUITO È $|Y_0\rangle = |Y\rangle \otimes |B_{00}\rangle$



$$\begin{aligned} &\text{COME È DIVISO IL CIRCUITO} \\ &\text{PER ALICE E BOB} \\ &|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &\text{COME È COMBINATO IL CIRCUITO} \\ &\text{EPR} \end{aligned}$$

ALICE COMBINA $|Y\rangle$ CON LA SUA META' DELLA COPPIA EPR E MISURA I SUOI DUE qubit DOPO aver APPLICATO LE PORTE CNOT E H. I 2 bit CHE OTTIENE DOPO LA MISURAZIONE VENGONO MANDATI ATTRAVERSO UN CANALE DI COMUNICAZIONE CLASSICO A BOB, IL QUALE SAPO' IN GRADO DI RICOSTRUIRE LO STATO $|Y\rangle$ SFRUTTANDO L'INFORMAZIONE CLASSICA RICEVUTA DA ALICE E LA SUA META' DELLA COPPIA EPR.

LE PRIME DUE LINEE CORRISPONDONO AI qubit USCATI DA ALICE, MENTRE L'ULTIMA LINEA CORRISPONDE AL qubit POSSESSATO DA BOB.

$$|\Psi\rangle = |\alpha\rangle + \beta|\gamma\rangle \quad \text{QUBIT DA TELETRASPORTARE}$$

$$|\beta_{00}\rangle = \frac{|\alpha\rangle + \beta|\gamma\rangle}{\sqrt{2}}$$

(20)

$$|\Psi_0\rangle = |\Psi\rangle |\beta_{00}\rangle = (|\alpha\rangle + \beta|\gamma\rangle) \frac{|\alpha\rangle + \beta|\gamma\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} (|\alpha\rangle (|\alpha\rangle + \beta|\gamma\rangle) + \beta|\gamma\rangle (|\alpha\rangle + \beta|\gamma\rangle))$$

Dopo la CNOT

$|\Psi_1\rangle$ = NOT IL CONTROLLO è $|\Psi\rangle$ QUINDI $|\alpha\rangle$ DIVENTA $\beta|\gamma\rangle$
MENTRE IL TARGET È IL PRIMO QUBIT DI $|\beta_{00}\rangle$ DIVENTO $(|\alpha\rangle + \beta|\gamma\rangle)$

$$|\Psi_1\rangle = \text{CNOT } |\Psi_0\rangle = \frac{1}{\sqrt{2}} (|\alpha\rangle (|\alpha\rangle + \beta|\gamma\rangle) + \beta|\gamma\rangle (|\alpha\rangle + \beta|\gamma\rangle))$$

Dopo la H

NOTA LA PORTA DI HADAMARD VENNE
APPLICATA AL 1° qubit QUINDI A $|\Psi\rangle$

$$\begin{aligned} |\Psi_2\rangle &= H |\Psi_1\rangle = \frac{1}{\sqrt{2}} \left(\left(\alpha \frac{|\alpha\rangle + \beta|\gamma\rangle}{\sqrt{2}} \right) (|\alpha\rangle + \beta|\gamma\rangle) + \left(\beta \frac{|\alpha\rangle - |\gamma\rangle}{\sqrt{2}} \right) (|\alpha\rangle + \beta|\gamma\rangle) \right) = \\ &= \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \left(\alpha (|\alpha\rangle + \beta|\gamma\rangle) (|\alpha\rangle + \beta|\gamma\rangle) + \beta (|\alpha\rangle - |\gamma\rangle) (|\alpha\rangle + \beta|\gamma\rangle) \right) = \\ &= \frac{1}{2} \left(2|\alpha\rangle|\alpha\rangle + \alpha|\alpha\rangle|\gamma\rangle + \alpha|\gamma\rangle|\alpha\rangle + 2|\alpha\rangle|\gamma\rangle + \beta|\alpha\rangle|\alpha\rangle + \beta|\alpha\rangle|\gamma\rangle - \beta|\gamma\rangle|\alpha\rangle - \beta|\gamma\rangle|\gamma\rangle \right) = \\ &= \frac{1}{2} (|\alpha\rangle (\alpha|\alpha\rangle + \beta|\gamma\rangle) + |\gamma\rangle (\alpha|\alpha\rangle + \beta|\gamma\rangle) + |\alpha\rangle (\beta|\alpha\rangle - \beta|\gamma\rangle) + |\gamma\rangle (\beta|\alpha\rangle - \beta|\gamma\rangle)). \end{aligned}$$

A QUESTO PUNTO ALICE MISURA I 2 qubit OTTENENDO UNA DELLE QUATTRO COPIE di bit

$$\{00, 01, 10, 11\} \quad |\Psi_3\rangle$$

PER EFFETTO DELLA MISURAZIONE ANCHE IL QUBIT DI BOB COLLEGHERÀ NUOVO STATO CORRISPONDENTE AL RISULTATO DELLA MISURAZIONE, CIOÈ:

$$\begin{aligned} 00 &\rightarrow \alpha|\alpha\rangle + \beta|\gamma\rangle \\ 01 &\rightarrow \alpha|\alpha\rangle + \beta|\alpha\rangle \\ 10 &\rightarrow \alpha|\gamma\rangle + \beta|\alpha\rangle \\ 11 &\rightarrow \alpha|\gamma\rangle + \beta|\gamma\rangle \end{aligned}$$

ALICE COMMUNICA I DUE bit MESSI OTTENUTI A BOB MEDIANTE UN CANALE CLASSICO.
BOB È OBLIGATO A SPEDIRE IL QUBIT $|\Psi_3\rangle$ APPLICANDO AL SUO QUBIT IL CIRCUITO

$$X^h \quad Z^m$$

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

POSTULATI DELLA MECCANICA QUANTISTICA

(21)

(1) OGNI SISTEMA FISICO ISOLATO HA ASSOCIAZIONE UNO SPAZIO DI HILBERT COMPLESSO, DETTO SPAZIO DEGLI STATI DEL SISTEMA. IL SISTEMA È COMPLETAMENTE DESCRITTO DAL SUO VETTORE DI STATO CHE È UN VETTORE UNITARIO NELLO SPAZIO DEGLI STATI.

NELLO SPAZIO DI HILBERT I VETTORI RAPPRESENTANO LE POSSIBILI CONFIGURAZIONI DELLO STATO DI UN SISTEMA FISICO.

IL SISTEMA FISICO SOLATO PIÙ SEMPLICE È IL QUBIT IN CUI LO SPAZIO DI HILBERT ASSOCIAZIONE È \mathbb{C}^2 .

LA BASE COMPUTAZIONALE È FORMATA DA $|0\rangle$ E $|1\rangle$ È UNA BASE ORTHONORMALE E LA CONDIZIONE CHE OGNI VETTORE $|\Psi\rangle = a|0\rangle + b|1\rangle$ CON $a, b \in \mathbb{C}$ SIA UN VETTORE UNITARIO È ESPRESSA DA $|a|^2 + |b|^2 = 1$ O DA $\langle\Psi|\Psi\rangle = 1$

RICORDO a E b SONO LE AMPLITUDE RISPECTIVAMENTE DEL VETTORE $|0\rangle$ E DEL VETTORE $|1\rangle$

CODIFICA SUPERDENSA → TALE PROTOCOLLO PERMETTE DI COMPARTIRE INFORMATIIONI CLASSICHE IN QUBIT UTILIZZANDO UNO QUBIT DEL BIT NECESSARI PER IL MESSAGGIO CLASSICO.
SARÒ NOMINATO CHE ALICE DEVE COMMUNICARE A BOB D'INFORMAZIONE CONTENUTA IN 2 bit CLASSICI QUINDI UN NUMERO TRA 0, 1, 2, 3 E DOVE FARLO TRASMETTERE UN SOLO qubit.

QUESTO PROBLEMA PUÒ ESSERE RISOLTO ATTRAVERSO L'USO DI UNA COPPIA EPR.

SUPPONIAMO AL PRIORIO ALICE E BOB SIANO IN POSSESSO RISPECTIVAMENTE DEL PRIMO E DEL SECONDO qubit DELLA COPPIA ENTANGLED

$$|\Psi\rangle = \frac{|\alpha\rangle + |\beta\rangle}{\sqrt{2}}$$

ALICE APPLICA AL SUO qubit UNA DELLE TRANSFORMAZIONI I, X, Y, Z A SECONDA DEL NUMERO CHE VOLUO TRASMETTERE. QUESTI SONO I VARI CASI:

$$\text{INVIO 0: } |\Psi\rangle \rightarrow (I \otimes I) |\Psi\rangle = \frac{|\alpha\rangle + |\beta\rangle}{\sqrt{2}}$$

$$\text{INVIO 1: } |\Psi\rangle \rightarrow (X \otimes I) |\Psi\rangle = \frac{|\alpha\rangle + i|\beta\rangle}{\sqrt{2}}$$

$$\text{INVIO 2: } |\Psi\rangle \rightarrow (Y \otimes I) |\Psi\rangle = \frac{|\alpha\rangle - i|\beta\rangle}{\sqrt{2}}$$

$$\text{INVIO 3: } |\Psi\rangle \rightarrow (Z \otimes I) |\Psi\rangle = \frac{|\alpha\rangle - |\beta\rangle}{\sqrt{2}}$$

I QUATTRO STATI RISULTANTI FORMANO UNA BASE ORTHONORMALE NOTA COME BASE DI BELL.
AURO ALICE NON PUÒ FAR ALTRO CHE INVIERE IL SUO qubit A BOB, IL QUBIT DI BOB DETERMINA I 2 bit CHE ALICE VOLVVA TRASMETTERE, ATTRAVERSO UNA MISURA NELLA BASE DI BELL.

PiÙ PRECISAMENTE ANDIAMO A INDICARE CON $|\beta_0\rangle, |\beta_1\rangle, |\beta_2\rangle, |\beta_3\rangle$ I 4 STATI DI BELL PER RICEVERE D'INFORMAZIONE BOB DÀDE MISURE UN OSSERVABILE DEL TIPO

$$M \equiv \sum_{i=0}^3 i |\beta_i\rangle \langle \beta_i| \quad \text{NUOVO STATO DEL 2 qubit IN SUO POSSESSO.}$$

RICHIAMI DI ALGEBRA LINEARE

DATO UNO SPAZIO VETTORIALE V ,

UNA FUNZIONE $(\cdot, \cdot) : V \times V \rightarrow \mathbb{C}$ È UN PRODOTTO SCALARE SE
SODDISFA I SEGUENTI REQUISITI:

$$-(1v, 1v) \geq 0$$

$$-(1v, 1v) = 0 \Leftrightarrow v = 0$$

$$-(1v, 1w) = (1w, 1v)^*$$

$$-(1v, \sum_i a_i (1w_i)) = \sum_i a_i (1v, 1w_i)$$

IN NOTAZIONE DI DIRAC, IL PRODOTTO SCALARE DEL VETTORE $|1v\rangle$

CON IL VETTORE $|1w\rangle$ È DENOTATO DA $\langle v | w \rangle$

MEDIANTE IL PRODOTTO SCALARE SI PUÒ DEFINIRE LA NORMA DI UN VETTORE

$$\text{COME } \|v\| = \sqrt{v \cdot v}$$

BASES ORTHONORMALI

UN VETTORE $|1v\rangle$ IN UNO SPAZIO VETTORIALE V SI DICE VETTORE UNITARIO

SE LA SUA NORMA È 1, CIOÈ $\|v\| = 1$

I VETTORI $|1v\rangle$ E $|1w\rangle$ SI DICONO ORTOPRONOMALI SE IL LORO PRODOTTO SCALARE È ZERO

$$\text{cioè } \langle v | w \rangle = 0 \quad \langle v, w \rangle = \sum_{i=1}^n v_i w_i \quad \text{CON } v_i \text{ E } w_i \text{ CHE SONO LE COMPONENTI DI } |v\rangle \text{ E } |w\rangle$$

ESEMPIO: PRODOTTO SCALARE

$$v = [1, 2, 3] \quad w = [4, 5, 6] \quad \langle v, w \rangle = (1 \cdot 4) + (2 \cdot 5) + (3 \cdot 6) = 32$$

UN INSIEME DI VETTORI $\{|1i\rangle\}$ CON IMPILE i SI DICE ORTHONORMALE SE PER OGNI i

$\{|1i\rangle\}$ È UN VETTORE UNITARIO E VETTORI DISTINTI SONO A DUE A DUE ORTOPRONOMALI

$$\text{cioè } \langle i | j \rangle = \delta_{ij} = \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases}$$

22

OPERATORI LINEARI E PRODOTTO ESTERNO

UNA RAPPRESENTAZIONE UTILE UN OPERATORE LINEARE È QUELLA MEDIANTE
PRODOTTO ESTERNO. DATI $|1v\rangle \in V$ E $|1w\rangle \in W$

$$|1v\rangle = [1, 2, 3] \quad \langle 1w | = [4, 5, 6]$$

$$|1v\rangle \times |1w\rangle = [(2 \cdot 6) - (3 \cdot 5), (3 \cdot 4) - (1 \cdot 6), (1 \cdot 5) - (2 \cdot 4)] = [-3, 6, -3]$$

NOTA: IL PRODOTTO ESTERNO DA SOLO NON RAPPRESENTA UN OPERATORE LINEARE COMPLETO.

AUTOVETTORE

UN AUTOVETTORE DI UN OPERATORE LINEARE L SU UNO SPAZIO VETTORIALE V È UN VETTORE NON NULLO $|1v\rangle \in V$ TALE CHE $L|1v\rangle = \lambda|1v\rangle$, DOVE λ È UN NUMERO COMPLESSO DETTO AUTOVALORE DI L CORRISPONDENTE A $|1v\rangle$.

AUTOVETTORE \Rightarrow È UN VETTORE NON NULLO CHE QUANDO È SOTTOPONTO AD UNA TRASFORMAZIONE LINEARE VIENE MOLTIPLICATO PER UNO SCALARE CHIAMATO AUTOVALORE CORRISPONDENTE.

UN AUTOVETTORE È UN VETTORE CHE RIMANE NELLA STESSA DIREZIONE (O IN DIREZIONE OPPOSTA) DOPO ESSERE STATO TRASFORMATO DA UNA CERTA OPERAZIONE LINEARE.

A MATRICE QUADRATA A VETTORE NON NULLO

SE ESISTE UNO SCALARE λ TALE CHE $A^* v = \lambda^* v$ ALLORA v È UN AUTOVETTORE DI A E λ È L'AUTOVALORE CORRISPONDENTE

OPERATORI AGGIUNTIVI E HERMITIANI

DATO UN OPERATORE LINEARE L SU UNO SPAZIO DI HILBERT V ESISTE UN UNICO OPERATORE LINEARE L^+ TALE CHE PER TUTTI I VETTORI $|1v\rangle, |1w\rangle \in V$

$$(|1v\rangle, L|1w\rangle) = (|1v\rangle, L^+|1w\rangle)$$

L^+ È L'OPERATORE AGGIUNTIVO CHE IN CORRISPONDENZA MATEMATICA CORRISPONE ALLA MATRICE TRASPOSTA COMPIAGNATA DI L

$$L^+ = (L^*)^T$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}^T = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix}$$

UN OPERATORE HERMITIANO È UN OPERATORE L TALE CHE $L^+ = L$

$$\text{PROPRIETÀ: } 1) (L^*)^+ = L, \quad 2) (\sum_i a_i |1i\rangle L |1i\rangle)^+ = \sum_i a_i^* |1i\rangle L^+ |1i\rangle$$

OPERATORE UNITARIO \Rightarrow OPERATORE CHE GODE DELLE SEGUENTI PROPRIETÀ

$$1) U^+ U = I$$

2) PRESERVANO I PRODOTTI SCALARI, INFATTI SE U È UNITARIO DATI 2 VETTORI $|1v\rangle$ E $|1w\rangle$

$$(U|1v\rangle, U|1w\rangle) = \langle v, w \rangle$$

23

PRODOTTO SCALARE TRA DUE qubit

$|1\bar{0}\rangle$ e $|1\bar{1}\rangle$ SONO I 2 LIVELLI ENERGETICI DEL 1° qubit

$|W\rangle$ e $|X\rangle$ SONO I 2 LIVELLI ENERGETICI DEL 2° qubit

$$(|1\bar{0}\rangle|W\rangle, |1\bar{2}\rangle|X\rangle) = \langle 1\bar{1}1\bar{2}| \cdot \langle W|X\rangle$$

INTRODUZIONE AGLI ALGORITMI QUANTISTICI

UNA DIFFERENZA FONDAMENTALE TRA PORTE LOGICHE CLASSICHE E PORTE LOGICHE QUANTISTICHE È CHE LE PRIME SONO IRREVERSIBILI MENTRE LE SECONDE SONO SEMPRE UNITARIE E QUINDI REVERSIBILI.

IL PRIMO OBIETTIVO È QUELLO DI RAPPRESENTARE LE COMPUTAZIONI CLASSICHE COME TRASFORMAZIONI UNITARIE, CIOÈ COMPUTAZIONI QUANTISTICHE.

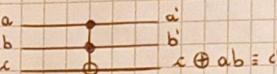
PONCHE' LE TRASFORMAZIONI UNITARIE SONO INVERTIBILI (CIOÈ REVERSIBILI), IL PRIMO PASSO DA FARÈ È QUELLO DI TRASFORMARE OGNI COMPUTAZIONE CLASSICA IRREVERSIBILE IN UNA REVERSIBILE.

UNA QUALSIASI COMPUTAZIONE CLASSICA IRREVERSIBILE SI PUÒ TRASFORMARE IN UNA COMPUTAZIONE EQUIVALENTE MA REVERSIBILE USANDO LA PORTA DI TOFFOLI.

QUESTA È UNA OPERAZIONE CLASSICA REVERSIBILE, RAPPRESENTATA NEL CIRCUITO SOTTO CHE OPERA SU 3 bit IN INPUT.

2 bit sono in controllo e il terzo bit è il bit target che viene scambiato se i bit di controllo sono entrambi 1.

TAVOLA DI VERITÀ



a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	1	1	1

LA REVERSIBILITÀ DI QUESTA OPERAZIONE SI VERIFICA FACILMENTE OSSERVANDO CHE APPLICANDO PER DUE VOLTE CONSECUTIVE LA PORTA DI TOFFOLI SI OTTIENE LO STESSO (RISULTATO DI PERTINENZA).

(a, b, c) $\xrightarrow{\text{APPLICO TOFFOLI}}$ ($a, b, c \oplus ab$)

$\xrightarrow{\text{APPLICO TOFFOLI}}$ (a, b, c)

RISULTATO: L'OPERAZIONE STESSA
GUINDATE CON LA SUA INVERSIONE.

LA PORTA DI TOFFOLI È UNIVERSALE PER LE COMPUTAZIONI CLASSICHE REVERSIBILI, CIOÈ OGNI COMPUTAZIONE CLASSICA SI PUÒ COSTRUIRE IN MODO REVERSIBILE MEDIANTE LA PORTA DI TOFFOLI.

FAN OUT REALIZZATO MEDIANTE LA PORTA DI TOFFOLI

IL FAN OUT È
L'OPERAZIONE DI COPIA
DI UN BIT CLASSICO



RICORDA CHE L'OPERAZIONE DI COPIA NON È POSSIBILE PER UN qubit

NAND REALIZZATA MEDIANTE PORTA DI TOFFOLI



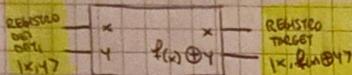
PARALLELOSMO QUANTISTICO

SU UN COMPUTER QUANTISTICO SI PUÒ VARIARE UNA FUNZIONE $f(x)$ SU VALORI DIFFERENTI DI x CONTEMPORANEAMENTE E CIÒ È NOTO COME PARALLELOSMO QUANTISTICO, ED È UNA CARATTERISTICA FONDAMENTALE DEI CIRCUITI QUANTISTICI.

CONSIDERI UNA FUNZIONE BOOLEANA DELLA FORMA: $f(x) : \{0,1\} \mapsto \{0,1\}$

PER CALCOLARE $f(x)$ MEDIANTE UNA COMPUTAZIONE QUANTISTICA SI DEVE DEFINIRE LA TRASFORMAZIONE $f(x)$ COME UNA OPERAZIONE UNITARIA U_f .

CIÒ SI PUÒ FARLE APPLICANDO SULLO STATO DI INPUT $|x, y\rangle$ DETTO REGISTRO DEI DATI UN'APPROPRIATA SEQUENZA DI PORTE LOGICHE QUANTISTICHE (CHE SI INDICA CON UNA SOTTOVOLTA CHIAMATA U_f^{\otimes}) CHE TRASFORMA $|x, y\rangle$ NELLO STATO $|x, y \oplus f(x)\rangle$, DETTO REGISTRO TARGET.



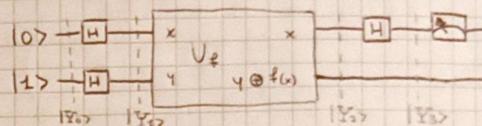
CON UN qubit POSSIAMO AVERE $|0\rangle$ o $|1\rangle$
QUINDI POSSIAMO AVERE $2^2 = 4$ FUNZIONI CHE SONO:

FUNZIONE 0	$\begin{bmatrix} 0 \\ 0 \end{bmatrix}$	FUNZIONE X	$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$	FUNZIONE INVERTITO	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	FUNZIONE NOT	$\begin{bmatrix} 1 \\ 1 \end{bmatrix}$
U_f È FATTA		U_f È FATTA		U_f È FATTA		U_f È FATTA	
\downarrow							
	$\begin{array}{c} \text{---} \\ \text{---} \end{array}$						

(25)

ALGORITMO DI DEUTSCH

TALE ALGORITMO MOSTRA COME ATTIVARSO LA VARIAZIONE PARALLELA DI UNA FUNZIONE SU TUTTI I SUOI INPUTS SI POSSANO DETERMINARE PROPRIETÀ GLOBALI DELLA FUNZIONE COME, PER ESEMPIO, QUELLA DI ESSERE UNA FUNZIONE COSTANTE O BILANCIATA.



FUNZIONE BILANCIATA VEDRA' SEMPRE
VALORE 0 SU ESITAZIONE METà DEI INPUTS
E VALORE 1 SUA RESTANTE METà

$$|Y_0\rangle = |0\rangle|1\rangle \quad // \text{ è lo stato prodotto dei 2 qubit}$$

$$\begin{aligned} |Y_1\rangle &= \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \text{DOPO AVER APPLICATO } H \text{ SU A } |0\rangle \text{ STA A } |1\rangle \\ &= \frac{|00\rangle+|01\rangle+|10\rangle-|11\rangle}{2} \end{aligned}$$

DOPODICHE' APPLICO U_f^{\otimes}

$$|Y_2\rangle = \frac{1}{2} (|00\rangle|0\rangle + f(0)|0\rangle - |00\rangle|1\rangle + f(0)|1\rangle + |10\rangle|0\rangle + f(1)|0\rangle - |10\rangle|1\rangle + f(1)|1\rangle)$$

IN PIÙ APPLICO H A x

$$|Y_3\rangle = \frac{1}{2} \cdot \frac{1}{\sqrt{2}} ((|00\rangle+|11\rangle)|f(0)\rangle - (|00\rangle+|11\rangle)|1\oplus f(0)\rangle + (|00\rangle-|11\rangle)|0+f(1)\rangle - (|00\rangle-|11\rangle)|1+f(1)\rangle)$$

VARIARE f STA IN 0 STA IN 1 (ESISTONO 2 CASI $f(0) = f(1)$ oppure f NON È COSTANTE)

CASO $f(0) = f(1)$

$$|Y_3\rangle = \frac{1}{2\sqrt{2}} ((|00\rangle+|11\rangle)|f(0)\rangle - (|00\rangle+|11\rangle)|1\oplus f(0)\rangle + (|00\rangle-|11\rangle)|f(0)\rangle - (|00\rangle-|11\rangle)|1\oplus f(0)\rangle).$$

OBTURE RE

DA SEMPLIFICARE

CASO f NON È COSTANTE

$$|Y_3\rangle = \frac{1}{2\sqrt{2}} ((|00\rangle+|11\rangle)|f(0)\rangle - (|00\rangle+|11\rangle)|1\oplus f(0)\rangle + (|00\rangle-|11\rangle)|f(0)\rangle - (|00\rangle-|11\rangle)|1\oplus f(1)\rangle).$$

DA SEMPLIFICARE

ATTRAVERSO UNA MISURAZIONE DEL 1° qubit POSSIAMO QUINDI DETERMINARE CON CERTEZZA IL VALORE DI $f(0) \oplus f(1)$ E QUINDI SE LA FUNZIONE f È COSTANTE OPPURE BILANCIATA. PER FAR CIÒ APPLICATO DAVANTI VARIARE UNA SOLO VOLTA f .

(26)

ALGORITMO DI DEUTSCH - JOSZA

(27)

L'ALGORITMO PRECEDENTE SI PUÒ ESTENDERE A FUNZIONI BOOLEANE SU n bit.

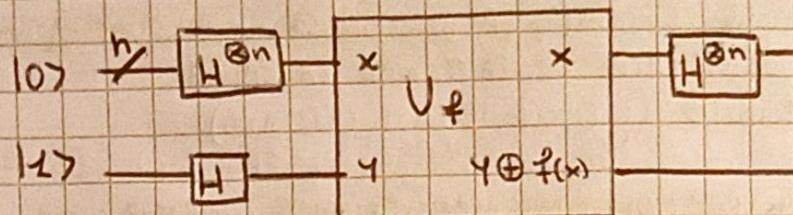
CONSIDERA UNA FUNZIONE $f: \{0,1\}^n \mapsto \{0,1\}$ E SUPPONIAMO DI SAPERE CHE f PUÒ ESSERE O COSTANTE OPPURE BILANCIATA.

L'ALGORITMO QUANTISTICO DI DEUTSCH - JOSZA CI PERMETTE DI STABILIRLO IN UN SOLO PASSO.

L'INPUT x DELLA FUNZIONE È DATO DA n qubit PREPARATI NELLO STATO $|0\rangle$

DETTO REGISTRO DEI DATI.

IL QUBIT TARGET È DESTINATO A CONTENERE IL RISULTATO DI $f(x)$ È INVECE NELLO STATO $|1\rangle$.



Lo stato iniziale $|\Psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$, dove $|0\rangle^{\otimes n}$ indica il prodotto tensoriale di n qubit $|0\rangle$.

Al registro dei dati $|0\rangle^{\otimes n}$ viene applicata la trasformazione di WALS - HADAMARD $H^{\otimes n}$ per produrre una sovrapposizione equiprobabile di tutti i 2^n stati della base computazionale.

QUANTUM MONEY

L'INTRODUZIONE DEL DENARO QUANTICO PUÒ DIVENTARE UNA RISORSA
A RISOLVERE (ALMENO IN LUNGA DI PRINCIPIO) IL PROBLEMA DELLA STAMPATURA DI BANCONOTE FALSE.

PER FAR CIO' E' SUFFICIENTE "STAMPARE" SU OGNI BANCONOTA UNA STRANIA DI
STATI QUANTISTICI.

$$|0\rangle, \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \left(\text{OSSERVA 2 STATI QUANTISTICI ORTOGONALI COSÌ}$$

(FACENDO, UNA MISURA NELLA BASE CHE INCLIDE QUESTI)

STATI LI DISTINGUERA'.

OGNI BANCONOTA HA UNA STRANIA DIVERSA, ASSOCIATA AD UN NUMERO SERIALE
CHE COMPRESE SUO BANCONOTA.

POICHÉ GLI STATI NON ORTOGONALI NON POSSONO ESSERE CLONATI, LA BANCONOTA NON PUÒ ESSERE
DIFUGGIBILE E LA SUA AUTENTICITÀ PUÒ ESSERE VERIFICATA CONTATTANDO LA BANCA.
NONC'E' ELENCO DELLE CORRISPONDENZE E CUSTODITO. (RICORDA IL NOT CLONING).

LA BANCA DIRETTA QUINDI UNA SEQUENZA DI MISURAZIONI NELL'APPOSITA BASE COMPUTAZIONALE
ASSOCIATA ALLA SEQUENZA DI STATI, IN MODO CHE TUTTE LE MISURAZIONI DEBBANO
AVERE ESITO $|0\rangle$ O + SOLO SE LA BANCONOTA È QUELLA ORIGINALE.

IL MANCATO OTTENIMENTO DEI RISULTATI CORRETTI, AL DI SOPRA DI UNA SORSA DI NOVITA'
DI ERROI Sperimentali, Segnala CHE LA BANCONOTA È FALESIA.

$(\text{RICORDA 2 STATI QUANTISTICI SONO}) \quad \text{IN ALTRE PAROLE 2 STATI QUANTISTICI ORTOGONALI SONO}$
 $\text{ORTOGONALI QUANDO IL LORO PRODOTTO} \Rightarrow \text{COMPLETAMENTE DISTINTI E NON HANNO SOVRAPPOSIZIONE}$
 SCALARIA E' ZERO.

$$|00\rangle = |0\rangle \otimes |0\rangle$$

$$|11\rangle = |1\rangle \otimes |1\rangle$$

$$\langle 00|11\rangle = \langle 0| \otimes \langle 0| \cdot |1\rangle \otimes |1\rangle$$

$$\langle 00|11\rangle = \langle 0|1\rangle \otimes \langle 0|1\rangle = 0 \otimes 0 = 0$$

$$\langle 01|1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1 \cdot 0 + 0 \cdot 1 = 0 \quad \text{ORTOGONALI}$$

$$|00\rangle = |0\rangle \otimes |0\rangle$$

$$|01\rangle = |0\rangle \otimes |1\rangle$$

$$\langle 00|01\rangle = \langle 0|0\rangle \otimes \langle 0|1\rangle$$

$$\langle 01|0\rangle = 1$$

$$\langle 01|1\rangle = 0$$

22

CRITTOGRAFIA SIMMETRICA \rightarrow C'E' UNA CHIAVE COMUNE SIA PER IL MITENTE
PER LA CIFRATURA SIA PER IL DESTINATARIO PER LA DECIFRATURA.

23

CRITTOGRAFIA ASIMMETRICA \rightarrow USANO UNA COPPIA DI CHIAVI PUBBLICA E CHIAVE PRIVATA.
LA CIFRATURA PUÒ ESSERE FATTA CON DUE TIPI DI CHIAVI, SE FATTA CON CHIAVE PRIVATA SI GARantisce
L'AUTENTICITÀ POICHE' SOLO QUELL'UTENTE POTREBBE AVER CIFRATO IL MESSAGGIO CON QUELLA CHIAVE
MENTRE SE CIFRATO CON CHIAVE PUBBLICA SI GARantisce CONFIDENZIALITÀ POICHE' IL MESSAGGIO È PUBBLICO
E PUÒ ESSERE CIFRATO DA CHI DOVESSE AVERE LA CHIAVE PRIVATA.

ARITMETICA MODULARE

NOTAZIONE $a \equiv b \pmod{n}$

SIGNIFICA CHE I RELATIVI INTERI a E b DIFFERISCONO
PER I MULTIPLI INTERI DI n CIOÈ: $a = b + nk$ con k numero
RELATIVO.

PER ESEMPIO:

$$2 \equiv 38 \pmod{12} \quad \text{E ANCHE} \quad 38 \equiv 2 \pmod{12}$$

ALGORITMO RSA (CRIPTOGRAFIA A CHIAVE PUBBLICA [CHIAVE ASIMMETRICA])

(30)

L'ALGORITMO DI RIVEST, SHAMIR E ADLEHAN (RSA) SI BASA SU UNA CHIAVE ASIMMETRICA. SI USA UNA CHIAVE PUBBLICA PER CODIFICARE MENTRE PER DECODIFICARE SI USA UNA CHIAVE PRIVATA.

- ① BOB VUOLE INVIARE UN MESSAGGIO M AD ALICE. AD ESEMPIO ALICE È UNA BANCA E BOB È UN CLIENTE CHE DESIDERÀ INVIARE ALLA BANCA IL NUMERO DELLA SUA CARTA DI CREDITO M . ($M=88$) IL PROTOCOLO FUNZIONA COSÌ:

ALICE: MANDA LA CHIAVE PUBBLICA

- ② SCEGLIE 2 NUMERI PRIMI MOLTO GRANDI, p E q , E NE FA IL PRODOTTO $N = pq$

SUPPONIAMO CHE $p=17$ E $q=11$ $N=187$

- ③ SCEGLIE UN ALTRO NUMERO e CHE DEVE ESSERE COPRIMO CON $(p-1)(q-1)$

$(p-1)(q-1)=160$ ALICE SCEGLIE $e=7$

- ④ ALICE MANDA IN RETE I NUMERI e ED N . TUTTI I NUMERI COSTITUISCONO LA CHIAVE PUBBLICA.

BOB

- ① CRIPTOGRAFA IL NUMERO DELLA SUA CARTA DI CREDITO M IN UN MESSAGGIO IN CODICE C CON LA FORMULA

$$C = M^e \pmod{N} \text{ USANDO LA CHIAVE PUBBLICA } (N, e)$$

esempio se $M=88$

$$C = 88^7 \pmod{187} = 11 \text{ ED È IL MESSAGGIO IN CODICE.}$$

- ② INVIA C AD ALICE.

UN INTERCETTORE (DETTO Eve) NON SARÀ IN GRADO DI DECODIFICARE IL MESSAGGIO SE p E q SONO NUMERI PRIMI MOLTO GRANDI. INFATTI PER DECIFRARE C È NECESSARIO CONOSCERE p E q .

EVE PUÒ PROVARE A DEDURRE p E q FATTORIZZANDO IL NUMERO N , PERÒ TALE COMITO È ARDUTO CON I COMPUTER TRADIZIONALI.

ALICE

- ① CALCOLA LA CHIAVE DI DECRITTAZIONE d CHE È COSÌ DEFINITA:

$$ed = 1 \pmod{(p-1)(q-1)}$$

NELL'ESEMPIO $e=7$ $7d = 1 \pmod{160}$ PUÒ ESSERE RISOLTO USANDO L'ALGORITMO ESTESO DI EUCLIDE PER TROVARE $d=23$.

- ② USANDO QUESTA CHIAVE (CHE RICHIENDE LA CONOSCENZA DELLA COPPIA SEGRETA (p, q)) SI PUÒ DECRIFRARE IL MESSAGGIO IN CODICE C .

$$M = C^d \pmod{N} = 11^{23} \pmod{187} = 88$$

COMPLESSITÀ

LE PRINCIPALI CLASSI DI COMPLESSITÀ SONO:

- 1) P → PROBLEMI RISOLVIBILI IN TEMPO POLINOMIALE
- 2) NP → PROBLEMI IN CUI SOLUZIONE PUÒ ESSERE VERIFICATA IN TEMPO POLINOMIALE
- 3) NP-COMPLETO → SONO I PIÙ DIFFICILI PROBLEMI DELLA CLASSE NP.

SE SI TROVASSSE UN ALGORITMO IN GRADO DI RISOLVERE IN TEMPO POLINOMIALE UN QUALSIASI PROBLEMA NP-COMPLETO, ALLORA SI POTREBBE USARLO PER RISOLVERE IN TEMPO POLINOMIALE OGNI PROBLEMA NP.

→ SPOILER NON È STATO TROVATO!!!

$NP \subseteq P$ ED INOLTRE NON ESISTE ALCUNA PROVA MO SI RITIENE CHE $NP \neq P$.

SE FOSSE TROVATO TALE ALGORITMO ALLORA $NP = P$.

- 3) D → PROBLEMI DI DECISIONE OVVERO PROBLEMI CHE RICHIEDONO DI VERIFICARE UNA CERTA PROPRIETÀ SUL INPUT E COME OUTPUT DANNÒ TRUE o FALSE.
- ESSEMPIO → NELLO UN GRAFO G DIRE SE È CONNESSO.

ESEMPIO

USIAMO I GRAFI PER QUESTO ESEMPIO.

RICORDA UN CICLO È UN PERCORSO CHIUSO NEL GRAFO.

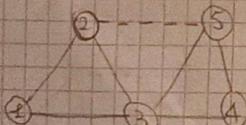
DATO UN GRAFO, NON È NOTO ALCUN ALGORITMO POLINOMIALE PER DECIDERE SE AMMETTE UN CICLO HAMILTONIANO. INOLTRE SI PUÒ DEMONSTRARE CHE IL PROBLEMA DEL CICLO HAMILTONIANO È NP-COMPLETO.

- CICLO HAMILTONIANO: CICLO IN CUI TUTTI I VERTICI DI UN GRAFO COMPARIONO UNA SOLA VOLTA
- CICLO EULERIANO: CICLO IN CUI OGNI ARCO DEL GRAFO VIENE ATTRAVERSATO UNA SOLA VOLTA.

IL PROBLEMA DEL CICLO EULERIANO È RISOLVIBILE IN TEMPO POLINOMIALE OVVERO È DI CLASSE P.

- UN GRAFO AMMETTE UN CICLO EULERIANO SE È CONNESSO E SOLO SE OGNI VERTICE HA UN NUMERO PARI DI ARCHI USCITI.

GRAFO ESEMPIO



SE CONSIDERO L'ARCO TRATTEGGIATO NON ESISTE IL CICLO EULERIANO MA ESISTE QUELLO HAMILTONIANO
PER ESEMPI:
SE NO, LO HAMMER L'ARCO TRATTEGGIATO NON ESISTE IL CICLO HAMILTONIANO MA ESISTE QUELLO EULERIANO.

LA TRANSFORMAZIONE DI FOURIER QUANTISTICA RAPPRESENTA FINO AD OGGI
DUMICO STRUMENTO IL CUI USO PERMETTE DI COSTRUIRE ALGORITMI QUANTISTICI
CHE SONO ESponentIALMENTE PIÙ EFFICIENTI DEI CORRISPONDENTI CLASSICI.

(33)

ALGORITMO DI RICERCA QUANTISTICA (GROVER)

PROBLEMI DI RICERCA

ESISTONO I PROBLEMI DI RICERCA NON STRUTTURATI DOVE NON SI CONOSCE LA STRUTTURA NELLO SPAZIO DELLE SOLUZIONI E I PROBLEMI DI RICERCA STRUTTURATI DOVE LE INFORMAZIONI SONO UTILIZZATE PER COSTRUIRE STRUTTURE CHE PERMETTONO DI COSTRUIRE ALGORITMI EFFICIENTI (E ALBERO BINARIO).

NEL CASO GENERALE DI UN PROBLEMA DI RICERCA NON STRUTTURATO, IL MIGLIOR ALGORITMO CLASSICO CHE SI PUÒ APPLICARE È QUELLO CHE CONTROLLA LA CONDIZIONE $P(x)$ SU CIASCUÑ NEGLI ELEMENTI X SCELTI CASUALMENTE NELL'INSIEME DELLE POSSIBILI SOLUZIONI.

SE QUEST'ULTIMO HA DIMENSIONE N, ALLORA L'ALGORITMO RICHIENDE $O(n)$ VALUTAZIONI DI P.
SU UN COMPUTER QUANTISTICO, QUESTI PROBLEMI SI POSSANO RISOLVERE CON UNA PROBABILITÀ DI ERRORE LIMITATA, CON $O(\sqrt{N})$ VALUTAZIONI DI P, USANDO IL METODO DI GROVER.

PROBLEMA DI GROVER → L'OPERATORE DI SERCA È UN ALGORITMO QUANTISTICO VERSO PER LA RICERCA DI ELEMENTI IN UN INSIEME NON STRUTTURATO.

IL PROBLEMA È TROVARE, IN UN INSIEME DI $N=2^n$ ELEMENTI, UN SOTTOINSIEME DI M ELEMENTI CHE SODDISFANO DETERMINATE CONDIZIONI. DICHIARO ALLORA CHE IL PROBLEMA DI RICERCA HA M SOLUZIONI. ASSUMIAMO L'ESISTENZA DI UNA FUNZIONE $f(x)$ DA n bits A 1 bit, CHE ASSUME IL VALORE DI $f(x)=1$ SE X È UNA SOLUZIONE E DI $f(x)=0$ SE X NON È UNA SOLUZIONE.

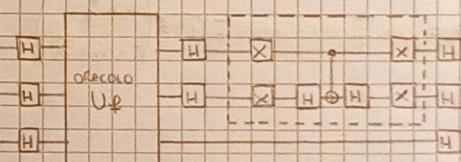
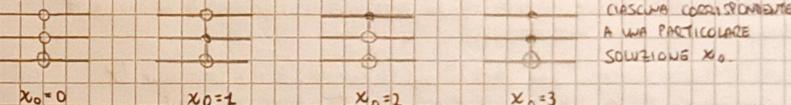
INOLTRE, ASSUMIAMO ANCHE L'ESISTENZA DI UNA SCATOLA NERA (ORACOLO) UÈ IN GRADO DI ESEGUIRE L'OPERAZIONE SU $n+1$ qubit $|x\rangle|0\rangle$, DOVE

$|x\rangle$ È UN STATO A n qubit MEME $|0\rangle$ È UN STATO AD UN qubit.

$$U_f |x\rangle|0\rangle = |x\rangle|f(x)\rangle \quad \text{in particolare se } f=0 \quad U_f |0\rangle|0\rangle = |0\rangle|f(0)\rangle$$

ESEMPIO A DUE BIT

IN QUESTO ESEMPIO CON $n=2$ $N=2^2=4$, E L'ORACOLO CHE METTE ALLA PROVA X È UNA DELLE SEGUENTI 4 PORTE:



I PRIMI DUE qubit (i qubit query) CODIFIANO X, L'ULTIMO qubit È LA RISPOSTA DELL'ORACOLO.

All'INIZIO, I DUE qubit DI QUERY SONO NELLO STATO $|00\rangle$ MENTRE L'ULTIMO qubit È NELLO STATO $|0\rangle$. È NECESSARIA UNA SOLA ITERAZIONE PER OTTENERE ESATTAMENTE x_0 E CIÒ SI PUÒ VERIFICARE USANDO IL CIRCUITO, CHE LA MISURA DEI PRIMI 2 qubit DA x_0 DOPO aver USATO L'ORACOLO SOLO UNA VOLTA.

AL CONTRARIO, UN COMPUTER CLASSICO CHE CERCA DI TROVARE x_0 ESTIMENDO TUTTI I DUE bit X RICHIEDEREbbe IN MEDIA 2,25 CERCATE.

(34)

OPERATORI DI ROTAZIONE

TALI OPERATORI, IN QUANTISTICA, SONO RAPPRESENTATI DAGLI ESPONENZIALI DELLE MATRICI DI PAULI.

Gli operatori di rotazione sono operatori unitari che agiscono su stati di 1 qubit. Sono chiamati operatori di rotazione perché ruotano i qubit sulla sfera di Bloch, di un angolo θ , rispettivamente attorno all'asse x , y e z .

$$R_x(\theta) = e^{-\frac{i\theta \hat{x}}{2}} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) \hat{x} = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -i \sin\left(\frac{\theta}{2}\right) \\ -i \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

$$R_y(\theta) = e^{-\frac{i\theta \hat{y}}{2}} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) \hat{y} = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

$$R_z(\theta) = e^{-\frac{i\theta \hat{z}}{2}} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) \hat{z} = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix}$$

Considera il qubit $|10\rangle$ corrispondente al polo nord sulla sfera di Bloch. Le sue componenti nello spazio vettoriale bidimensionale degli stati fisici del qubit sono date da $(1, 0)$. Se agiamo su questo vettore con l'operatore di rotazione $R_x(\theta)$ si trova:

$$R_x(\theta)|10\rangle = \begin{pmatrix} \cos\frac{\theta}{2} & -i \sin\frac{\theta}{2} \\ -i \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot \cos\frac{\theta}{2} + 0 \cdot (-i \sin\frac{\theta}{2}) \\ 1 \cdot (-i \sin\frac{\theta}{2}) + 0 \cdot \cos\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} \\ -i \sin\frac{\theta}{2} \end{pmatrix}$$

Il vettore risultante corrisponde ad una rotazione del polo nord di un angolo θ attorno all'asse x in senso antiorario.

Inoltre il punto ruotato sulla sfera di Bloch corrisponde allo longitudinale θ e longitudinale $\phi = \frac{\pi}{2}$ perciò corrisponde allo stato fisico del qubit

$$|\Psi\rangle = \cos\frac{\theta}{2}|10\rangle + e^{i\phi} \sin\frac{\theta}{2}|11\rangle = \cos\frac{\theta}{2}|10\rangle - i \sin\frac{\theta}{2}|11\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ -i \sin\frac{\theta}{2} \end{pmatrix}$$



$$S = \begin{pmatrix} 0 & 0 \\ 0 & i \end{pmatrix}$$

$$|Y_0\rangle = |10\rangle |10\rangle |14\rangle$$

$$|Y_1\rangle = \frac{1}{2} (|10\rangle + |11\rangle) (|10\rangle + |11\rangle) |14\rangle = \frac{1}{2} (|100\rangle |12\rangle + |101\rangle |12\rangle + |100\rangle |13\rangle + |101\rangle |13\rangle)$$

$$\begin{aligned} |Y_2\rangle &= \frac{1}{2} (|100\rangle |14\rangle + |101\rangle |14\rangle + |102\rangle |14\rangle + |103\rangle |14\rangle) = \\ &= \frac{1}{2} ((|100\rangle + |101\rangle + |102\rangle) |14\rangle + |103\rangle \times |14\rangle) \end{aligned}$$

$$|Y_3\rangle = \frac{1}{2} ((|100\rangle + |101\rangle + |102\rangle) S |14\rangle + |103\rangle S \times |14\rangle)$$

$$|Y_4\rangle = \frac{1}{2} ((|100\rangle + |101\rangle + |102\rangle) S |14\rangle + |103\rangle \times S \times |14\rangle)$$

$$\begin{aligned} |Y_5\rangle &= \frac{1}{2} \cdot \frac{1}{2} \left((|10\rangle + |11\rangle) (|10\rangle + |11\rangle) + \right. \\ &\quad (|10\rangle - |11\rangle) (|10\rangle - |11\rangle) + \\ &\quad (|10\rangle - |11\rangle) (|10\rangle + |11\rangle) S |14\rangle + |10\rangle \times S \times |14\rangle = \\ &= \frac{1}{4} \left[(|100\rangle + |101\rangle + |102\rangle + |103\rangle + |110\rangle - |111\rangle - |100\rangle - |101\rangle - |102\rangle - |103\rangle) S |14\rangle + \right. \\ &\quad \left. |11\rangle \times S \times |14\rangle \right] = \end{aligned}$$

$$= \frac{1}{4} \left[(3|100\rangle + |101\rangle + |102\rangle - |103\rangle) S |14\rangle + |11\rangle \times S \times |14\rangle \right]$$

In cosa consiste il protocollo BB84 Bennet e Bressard (crittografia quantistica)?

Il protocollo BB84, sviluppato da Charles H. Bennett e Gilles Brassard, è un protocollo di crittografia quantistica che permette di scambiare messaggi crittografati in modo sicuro tra due parti che condividono una chiave crittografica quantistica. Questo protocollo sfrutta le proprietà della meccanica quantistica per garantire la sicurezza della comunicazione.

Il protocollo BB84 coinvolge due parti: il mittente (Alice) e il ricevente (Bob). La comunicazione tra Alice e Bob si basa su particelle quantistiche, solitamente fotoni, che vengono inviati attraverso un canale di comunicazione. Ecco come funziona il protocollo BB84:

1. Preparazione delle particelle: Alice genera una sequenza di particelle quantistiche, ad esempio fotoni, e le prepara in uno stato quantistico specifico, scelto casualmente tra quattro possibili stati: due basi ortogonali (di solito le basi di polarizzazione) e due stati quantistici possibili per ciascuna base. Ad esempio, Alice può preparare i fotoni nello stato $|0\rangle$, $|1\rangle$, $|+\rangle$ o $|-\rangle$, dove $|0\rangle$ e $|1\rangle$ sono le basi di polarizzazione orizzontale e verticale, mentre $|+\rangle$ e $|-\rangle$ sono le basi di polarizzazione diagonale. La scelta degli stati è casuale.
2. Trasmissione delle particelle: Alice invia le particelle quantistiche attraverso il canale di comunicazione verso Bob, che le riceve.
3. Misura delle particelle: Bob, una volta ricevute le particelle, decide casualmente su quale base effettuare le misurazioni, utilizzando una base di polarizzazione casuale. Ad esempio, Bob può decidere di misurare nella base orizzontale o diagonale.
4. Comunicazione delle basi: Successivamente, Alice comunica a Bob, tramite un canale pubblico e non crittografato, le basi che ha utilizzato per preparare le particelle, ma non i valori specifici degli stati quantistici inviati. Bob registra queste informazioni.
5. Sincronizzazione delle basi: Bob confronta le basi che ha utilizzato per le misurazioni con le basi comunicate da Alice. Solo quando Bob ha utilizzato la stessa base di polarizzazione di Alice, si può stabilire che la misura sia stata effettuata correttamente.
6. Scambio delle informazioni: Alice e Bob selezionano casualmente una sotto-sequenza delle particelle quantistiche misurate in cui le basi erano corrispondenti. Queste particelle costituiscono una chiave crittografica quantistica condivisa tra Alice e Bob.
7. Verifica dell'integrità: Alice e Bob eseguono una verifica dell'integrità della chiave crittografica quantistica condivisa. Attraverso un processo noto come "verifica dell'error rate", confrontano una porzione della chiave per rilevare eventuali errori o interferenze. Se la verifica ha successo, possono procedere con la comunicazione.

Il protocollo BB84 fornisce un metodo per rilevare eventuali tentativi di intercettazione o hacking durante la trasmissione delle particelle quantistiche.

A vuole inviare un messaggio a B in una forma di una stringa di bits.

Per far ciò A invia una sequenza di questi bits con polarizzazioni corrispondenti agli stati 107 e 117.

B ha un polarizzatore verticale e può quindi distinguere i 2 stati di polarizzazione ortogonale e riconstruire il messaggio di A.

Tuttavia i fotoni possono essere intercettati da Eve che può misurarne la polarizzazione usando un polarizzatore verticale e quindi, può leggere il messaggio e inviare la stessa sequenza a B, che non sospetterà l'intercettazione di Eve.

Per ovviare a ciò A invia una stringa di fotoni per controllare la sicurezza del canale diciamo 200 fotoni.

Questi fotoni li invia in due basi diverse 107 e 117 corrispondenti alle polarizzazioni orizzontali e verticali e la base 117 e 1-7 corrispondente alle polarizzazioni 45° e 135°. Alice sceglie le basi a caso e Bob quando misura i fotoni inviati da Alice usa i polarizzatori verticali o 45°.

bit 0 è pari a 107 e 1+7, bit 1 è pari a 117 e 1-7

→ A invia i fotoni, quando B misura i fotoni ci sono due casi:

→ la base scelta da B è la stessa scelta da A

→ se A e B usano basi diverse B ha probabilità $\frac{1}{2}$ di concordare con il bit inviato da A (ad es un fotone inviato da Alice nello stato 1-7 (bit 1) ha probabilità $\frac{1}{2}$ di passare (bit 1) il polarizzatore verticale di B).

→ dopo aver effettuato tutte le misurazioni A chiama B per telefono in un canale pubblico e confronta con B le basi usate per ogni fotone.

→ A e B si scrivono l'elenco dei fotoni che sono stati inviati e misurati nella stessa base (circa la metà in teoria) mentre i risultati sugli altri fotoni vengono scartati.

→ A e B controllano se sono d'accordo sui bit codificati nelle polarizzazioni.

→ se i disaccordi sono al di sopra di una certa soglia A e B devono concludere che Eve ha cercato di intercettare. (la soglia dipende dal rumore della fibra ottica usata).

→ infatti se Eve sta intercettando, misura i fotoni inviati da A con 2 polarizzatori ma non può sapere quale delle due basi è stata usata da A. Eve ha quindi probabilità 50% di indovinare la base corretta e usare il polarizzatore corretto per misurare i fotoni senza disturbarli.

Se azzecca il polarizzatore corretto il bit inviato da A coincide con il bit ricevuto da B.

Tuttavia nell'altro 50% dei casi Eve non azzecca il polarizzatore scelto da Alice e in questo caso il fotone che Eve trasmette a B ha una probabilità del 50% di fornire il bit corretto (cioè lo stesso bit inviato da A) quando viene misurato da B.

Quindi Eve sommando queste probabilità $\left[\frac{1}{2} + \left(\frac{1}{2} \cdot \frac{1}{2}\right)\right] = \frac{3}{4} = 75\%$ di probabilità di farla franca per 1 fotone

per N fotoni? $\frac{3^N}{4^N}$ con $N=100$ $\left(\frac{3}{4}\right)^{100} = 3,21 \times 10^{-13}$ probabilità di farla franca molto molto molto bassa.

Dopo questo controllo di sicurezza A e B possono usare lo stesso canale se sicuro per inviare messaggi o una chiave segreta per codificare messaggi futuri.